Theoretical Computer Science 523 (2014) 1–36

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

Verification of gap-order constraint abstractions of counter systems ☆

Laura Bozzelli [a,*], Sophie Pinchinat [b]

[a] Technical University of Madrid (UPM), 28660 Boadilla del Monte, Madrid, Spain
[b] IRISA, Campus de Beaulieu, 35042 Rennes Cedex, France

ARTICLE INFO

Article history:
Received 7 November 2012
Received in revised form 20 November 2013
Accepted 2 December 2013
Communicated by P. Aziz Abdulla

Keywords:
Abstractions of counter systems
Temporal logics with Presburger constraints
Model checking
Verification of infinite-state systems
Complexity and decidability issues

ABSTRACT

We investigate verification problems for *gap-order constraint systems* (GCS), an (infinitely-branching) abstract model of counter machines, in which constraints (over $\mathbb{Z}$) between the variables of the source state and the target state of a transition are *gap-order constraints* (GC) [32]. GCS extend monotonicity constraint systems [7], integral relation automata [16], and constraint automata in [19]. First, we address termination and fairness analysis of GCS. Since GCS are infinitely-branching, termination does not imply *strong termination*, i.e. the existence of an upper bound on the lengths of the runs from a given state. We show that the termination problem, the strong termination problem, and the fairness problem for GCS (the latter consisting in checking the existence of infinite runs in GCS satisfying acceptance conditions à la Büchi) are decidable and PSPACE-complete. Moreover, for each control location of the given GCS, one can build a GC representation of the set of counter variable valuations from which termination (resp., strong termination, resp., fairness) does *not* hold (resp., does *not* hold, resp., does hold).

Next, we consider a constrained branching-time logic, GCCTL*, obtained by enriching CTL* with GC, thus enabling expressive properties and subsuming the setting of [16]. We establish that, while model-checking GCS against the universal fragment of GCCTL* is undecidable, model-checking against the existential fragment, and satisfiability of both the universal and existential fragments are instead decidable and PSPACE-complete (note that the two fragments are not dual since GC are not closed under negation). Moreover, our results imply PSPACE-completeness of known verification problems that were shown to be decidable in [16] with no elementary upper bounds.

1. Introduction

Abstractions of counter systems. One standard approach in formal analysis is the abstraction-based one: the analysis is performed on an *abstraction* of the given system, specified in some weak computational formalism for which checking the properties of interest is decidable. The relation between the abstraction and the concrete system is usually specified as a semantic over-approximation. This ensures that the approach is conservative, by giving a decision procedure that (for correct systems) is sound but in general incomplete. Such a methodology has been applied in particular to the verification of counter systems which represent a widely investigated complete computational model, used for instance to model broadcast

☆ This paper is an extended version of the results published in the proceedings of the following two conferences: (1) 13th International Conference on Verification, Model Checking, and Abstract Interpretation (VMCAI'12), Lect. Notes Comput. Sci., vol. 7148, Springer, 2012, pp. 88–103; and (2) 6th International Conference on Language and Automata Theory and Applications (LATA'12), Lect. Notes Comput. Sci., vol. 7183, Springer, 2012, pp. 155–168.

* Corresponding author.
E-mail addresses: laura.bozzelli@fi.upm.es (L. Bozzelli), Sophie.Pinchinat@irisa.fr (S. Pinchinat).

0304-3975/$ – see front matter
http://dx.doi.org/10.1016/j.tcs.2013.12.002

protocols [23] and programs with pointer variables [11]. Counter systems extend finite-state systems by allowing a finite set of counter variables, with each counter taking values from the infinite domain of integers. Moreover, constraints on the transitions specify the relation between the variables of the target state and the variables of the source state. Though simple problems like reachability are already undecidable for 2-counter Minsky machines [28], interesting abstractions of counter systems have been studied, for which expressive classes of verification problems have been shown to be decidable. Many of these abstractions are in fact restrictions: examples include Petri nets [29], reversal-bounded counter machines [25], and flat counter systems [10,17]. Genuine abstractions are obtained by approximating counting operations by non-functional fragments of Presburger constraints between the variables of the target state and the variables of the source state. Examples include the class of Monotonicity Constraint Systems (MCS) [7] and its variants, like constraint automata in [19], and integral relation automata (IRA) [16], for which the (monotonicity) constraints (MC) are boolean combinations of inequalities of the form $u < v$ or $u \leqslant v$, where u and v range over variables or integer constants. MCS and their subclasses (namely, *size-change systems*) have found important applications for automated termination proofs of functional programs (see e.g. [7,8]). Richer classes of non-functional fragments of Presburger constraints have been investigated, e.g. difference bound constraints [18], and their extension, namely octagon relations [13], where it is shown that the transitive closure of a single constraint is Presburger definable (these results are useful for the verification of safety properties for flat counter systems). Note that difference bound constraints over (real-valued or integer-valued) variables (clocks) are also used as guards of transitions in timed automata [4]. Size-change systems extended with difference bound constraints over the natural number domain have been investigated in [6]: there, the atomic difference constraints are of the form $x - y' \geqslant c$, where c is an integer constant, and y' (resp., x) range over the variables of the target (resp., source) state. Termination for this class of systems is shown to be undecidable. To regain decidability, the authors consider a restriction, where at most one bound per target variable in each transition is allowed.

Temporal logics with Presburger constraints. An important classification of temporal logics is based on the underlying nature of time. In the *linear-time* setting, formulas are interpreted over linear sequences (corresponding to single computations of the system), and temporal operators are provided for describing the ordering of events along a single computation path. In the *branching-time* setting, formulas are instead interpreted over computation trees, which describe all the possible computations of the system from a designated initial state. Branching-time temporal logics are in general more expressive than linear-time temporal logics since they provide both temporal operators for describing properties of a path in the computation tree, and path quantifiers for describing the branching structure in computation trees.

In order to specify behavioral properties of counter systems, standard propositional linear-time temporal logics (like LTL [30]) and propositional branching-time temporal logics (like CTL* [22]) can be extended by replacing atomic propositions with Presburger constraints, which usually refer to the values of the (counter) variables at two consecutive states along a computation path (run). These enriched temporal logics allow to specify properties of counter systems that go beyond simple reachability. Hence, basic decision problems are generally undecidable. However, decidability has been established for various interesting fragments. We focus on fragments where the constraint language includes MC. For the *linear-time setting*, many decidable fragments of full Presburger LTL have been obtained either by restricting the underlying constraint language, see e.g. [19,21], or by restricting the logical language, see e.g. [12,17]. In particular, satisfiability and model checking (w.r.t. constraint automata) of standard LTL extended with MC are decidable and PSPACE-complete [19] (which matches the complexity of LTL). For the *branching-time setting*, to the best of our knowledge, very few decidability results are known. The extension of standard CTL* with MC, here denoted by MCCTL*, has been introduced in [16], where it is shown that model checking IRA against its existential and universal fragments is decidable (by contrast, model checking for the full logic MCCTL* is undecidable, even for its CTL-like fragment[1]). As done in [21], adding periodicity constraints and the ability for a fixed $k \geqslant 1$, to compare the variable values at states of a run at distance at most k, decidability of the above problems is preserved [14]. However, no elementary upper bounds for these problems are known [16,14]. Moreover, it is shown in [20] that model checking a subclass of *finitely-branching flat* counter machines w.r.t. full Presburger CTL* is decidable. In this subclass of systems, counting acceleration over every cycle in the control graph is Presburger definable. Thus, since the relation between the variables at the current and next state is functional and the control graph is flat (i.e., it contains only simple cycles), Presburger definability can be extended in a natural way to the set of states satisfying a given formula.

Our contribution. We investigate verification problems for an (infinitely-branching) abstract model of counter machines, we call *gap-order constraint systems* (GCS), in which constraints (over $\mathbb{Z}$) between the variables of the source state and the target state of a transition are (transitional) *gap-order constraints* (GC) [32]. These constraints are positive boolean combinations of inequalities of the form $u - v \geqslant k$, where u, v range over variables and integer constants, and k is a natural number. Thus, GC can express simple relations on variables such as lower and upper bounds on the values of individual variables, and equality, and gaps (minimal differences) between values of pairs of variables. GC have been introduced in the field of constraint query languages (constraint Datalog) for deductive databases [32], and also have found applications in the analysis of safety properties for parameterized systems [1,2], and for determining state invariants in counter systems [24]. As pointed

[1] Quantification over variables can be simulated by the path quantifiers of the logic.

out in [2], using GC for expressing the enabling conditions of transitions allow to handle a large class of protocols, where the behavior depends on the relative ordering of values among variables, rather than the actual values of these variables.

GCS strictly extend IRA (and its variants, namely, MCS and the constraint automata in [19]). This because GC extend MC and, differently from MC, are closed under existential quantification (but not under negation). Moreover, the parameterized systems investigated in [1,2] correspond to the parameterized version of GCS, where a system consists of an arbitrary number of processes which are instances of the same GCS (additionally, transitions of a process can specify global conditions which check the current local states and variables of all, or some of, other active processes). This framework is useful to verify correctness regardless of the number of processes. However, basic decision problems like reachability for the parameterized version of GCS are undecidable [1,2]. Decidability of reachability can be regained for a restricted class of parameterized systems in which processes have at most one integer local variable [1,2].

Note that if we extend the constraint language of GCS by allowing either negation, or, equivalently, constraints of the form $u - v \geqslant -k$, with $k \in \mathbb{N}$, then the resulting class of systems can trivially emulate Minsky counter machines, leading to undecidable basic decision problems. Moreover, note that GC extended with constraints of the form $u - v \geqslant -k$, with $k \in \mathbb{N}$, correspond to standard diagonal bound constraints [4,18]. As mentioned above, these constraints are used as guards in timed automata [4], where (integer-valued or real-valued) variables (clocks) record the elapsed time among events. However, guards in timed automata express constraints only over the clocks of the source state, and clocks are synchronized, i.e., they always advance at same speed. Hence, timed automata with integer-valued clocks and GCS are incomparable formalisms.

In this paper, first we address termination analysis of GCS. Since GCS are infinitely-branching, termination (i.e., the non-existence of states from which there is an infinite run) does not imply the existence of an upper bound on the lengths of the runs from a given state.[2] The fulfillment of this last condition, we call *strong termination*, can be a necessary requirement in some contexts, such as running-time analysis [3] for infinitely-branching formalisms. Strong termination has been addressed in [9]. There, it is shown that for the subclass of MCS where integer constants are disallowed except for 0, checking strong termination is PSPACE-complete. For termination and strong termination of GCS, we establish the following results.

1. For each control location of the given GCS, the set of variable valuations from which strong termination (resp., termination) does *not* hold is *effectively* GC representable;
2. Checking strong termination (resp., termination) and strong termination (resp., termination) from a designated state in GCS are decidable and PSPACE-complete.

The proposed approach is as follows. First, we consider a subclass of GCS, called *simple* GCS: we establish our first result for simple GCS, and provide two polynomial-time checkable conditions for verifying strong termination and termination in simple GCS. Second, for a given unrestricted GCS $\mathcal{S}$, we show that one can construct a finite family $\mathcal{F}$ of *simple* GCS such that the union of the sets of strongly-terminating (resp., terminating) states of the single components in $\mathcal{F}$ correspond to the set of strongly-terminating (resp., terminating) states of $\mathcal{S}$. Then, we show that it is possible to compute separately and in exponential time suitable abstractions of the simple GCS in $\mathcal{F}$ (we are not able to give an upper bound on the size of $\mathcal{F}$), which preserve the fulfillment of the above polynomial-time checkable conditions for simple GCS. This leads to exponential-time procedures for solving strong termination (resp., termination) and strong termination (resp., termination) from a designated state in GCS. Finally, we show that in fact, the considered problems are PSPACE-complete. A potential application of our results on strong termination of GCS is to use them as a basic tool in running-time analysis (based on GCS abstraction) of infinitely-branching computational systems. Note that concurrent open systems are usually infinitely-branching because of the ongoing interaction with an unpredictable environment, and GCS can be used to abstractly model such an interaction. Moreover, note that our results extend the known results about termination and strong termination of MCS [9,8] in two directions: (i) we consider a strict extension of MCS, namely GCS, and (ii) our symbolic algorithm builds a GC representation of the set of non-strongly-terminating states (resp., non-terminating states), a very substantial information compared to the algorithm in [9,8]. For example, by using such a decidable finite representation, one can check whether two GCS have the same set of strongly-terminating (resp., terminating) states.

We also investigate the *fairness problem* for GCS (which is crucial for the verification of liveness properties), that is checking the existence of infinite runs satisfying acceptance conditions à la Büchi over the set of control locations. We show that this problem is decidable and PSPACE-complete; moreover, for the given GCS, one can compute a GC representation of the set of states from which there is a 'fair' infinite run. The proposed approach is a generalization of that used for solving non-termination of GCS.

Finally, we address verification problems of GCS against a *strict* extension, denoted by GCCTL*, of the logic MCCTL* (given in *complete* positive normal form) [16] obtained by adding transitional GC. Note that while MCCTL* is closed under negation, its strict extension GCCTL* is not (if we allow negation, the resulting logic would be undecidable also for small fragments). We show that while model-checking GCS against the *universal fragment* of GCCTL* is undecidable, model checking GCS against the *existential fragment* of GCCTL*, and satisfiability of both the existential and universal fragments of GCCTL* are instead decidable and PSPACE-complete (which matches the complexity of finite-state model checking and

[2] A state is an instantaneous description of the system specifying both a control location and a valuation of the counter variables.

satisfiability for the existential and universal fragments of standard CTL* [27]). Note that the existential and universal fragments of GCCTL* are not dual. Moreover, for a given GCS $\mathcal{S}$ and *existential* GCCTL* formula φ, the set of states in $\mathcal{S}$ satisfying φ is *effectively* GC representable. Since the existential fragment of GCCTL* subsumes the existential fragment of MCCTL*, and the existential and universal fragments of MCCTL* are dual, our results imply PSPACE-completeness for model-checking (w.r.t. IRA or GCS) of both the existential and universal fragments of MCCTL*. Hence, in particular, we solve complexity issues left open in [16] (see also [14]).

The rest of this paper is organized as follows. In Section 2, we introduce the framework of GCS. In Section 3, we recall some basic polynomial-time computable operations on GC. Moreover, we introduce a sound and complete (w.r.t. satisfiability) approximation scheme of GC, and give constructive results on the reachability relation in GCS. In Section 4, we address termination, strong termination, and fairness for the class of *simple* GCS. Then, in Section 5, we extend the results of Section 4 to the general framework of GCS. Next, in Section 6, we introduce the logic GCCTL* and investigate decidability and complexity issues for satisfiability and model checking (w.r.t. GCS) of GCCTL* and its existential and universal fragments. Finally, in Section 7, we give some concluding remarks.

2. Gap-order constraint systems

Let $\mathbb{Z}$ be the set of integers and $\mathbb{N}$ be the set of natural numbers. Throughout this paper, we fix a finite set $Var = \{x_1, \ldots, x_r\}$ of variables, a finite set of integer constants $Const \subseteq \mathbb{Z}$ such that $0 \in Const$, and a primed copy of Var, $Var' = \{x'_1, \ldots, x'_r\}$. For an arbitrary finite set of variables V, an (integer) *valuation* over V is a mapping of the form $\nu : V \to \mathbb{Z}$, assigning to each variable in V an integer value. For $V' \subseteq V$, $\nu_{V'}$ denotes the restriction of ν to V'. For two valuations ν and ν' over Var, the *composition* of ν and ν', written $\nu \oplus \nu'$, is the valuation over $Var \cup Var'$ which behaves like ν over Var and like ν' over Var'. Formally, $(\nu \oplus \nu')(x_i) = \nu(x_i)$ and $(\nu \oplus \nu')(x'_i) = \nu'(x_i)$ for all $1 \leqslant i \leqslant r$.

Notation. In the following, for a valuation $\nu : V \to \mathbb{Z}$, we also consider the extension of ν over the domain $V \cup \mathbb{Z}$ which behaves like ν over V and it is the identity mapping over $\mathbb{Z}$. With a little abuse of notation, this extension of ν is denoted still by ν (in particular, $\nu(c) = c$ for all $c \in \mathbb{Z}$).

Definition 1. (See [32].) For a finite set V of variables, a (conjunctive) *gap-order constraint* (GC for short) over V (and $Const$) is a finite conjunction ξ of inequalities of the form $u - v \geqslant k$, where $u, v \in V \cup Const$ and $k \in \mathbb{N}$. W.l.o.g. we assume that for all $u, v \in V \cup Const$, there is at most one conjunct in ξ of the form $u - v \geqslant k$ for some k. A valuation $\nu : V \to \mathbb{Z}$ *satisfies* ξ if for each conjunct $u - v \geqslant k$ of ξ, $\nu(u) - \nu(v) \geqslant k$. We denote by $Sat(\xi)$ the set of such valuations. A *transitional* GC is a GC over $Var \cup Var'$.

We use graph representations to manipulate GC in terms of (*gap-order*) *Monotonicity Graphs* (MG for short) [16].[3] A different graph representation of GC can be found in [32].

Definition 2. (See [16].) For a finite set V of variables, a (*gap-order*) *monotonicity graph* (MG for short) over V (and $Const$) is a directed weighted graph G with set of vertices $V \cup Const$ and edges $u \xrightarrow{k} v$ labeled by natural numbers k, and such that for all vertices u and v, there is at most one edge from u to v. The set $Sat(G)$ of *solutions* of G is the set of valuations ν over V such that for each edge $u \xrightarrow{k} v$ in G, it holds that $\nu(u) - \nu(v) \geqslant k$. A *transitional* MG is an MG over $Var \cup Var'$. GC and MG are equivalent formalisms since there is a trivial linear-time computable bijection assigning to each GC ξ an MG $G(\xi)$ such that $Sat(G(\xi)) = Sat(\xi)$.

Definition 3. A *gap-order constraint system* (GCS) (over Var and $Const$) is a finite directed labeled graph $\mathcal{S}$ such that each edge is labeled by a *transitional* GC. $Q(\mathcal{S})$ denotes the set of vertices in $\mathcal{S}$, called *control points*, and $E(\mathcal{S})$ the set of edges.

For a finite path $\wp$ of a GCS $\mathcal{S}$, $s(\wp)$ and $t(\wp)$ denote the source and target control points of $\wp$. For a finite path $\wp$ and a path $\wp'$ such that $t(\wp) = s(\wp')$, the composition of $\wp$ and $\wp'$, written $\wp\wp'$, is defined as usual.

The semantics of a GCS $\mathcal{S}$ is given by an infinite directed graph $[\![\mathcal{S}]\!]$ defined as follows:

- the vertices of $[\![\mathcal{S}]\!]$, called *states* of $\mathcal{S}$, are the pairs of the form (q, ν), where q is a control point of $\mathcal{S}$ and $\nu : Var \to \mathbb{Z}$ is a valuation over Var;
- there is an edge in $[\![\mathcal{S}]\!]$ from (q, ν) to (q', ν') iff there is a (labeled) edge in $\mathcal{S}$ of the form $q \xrightarrow{\xi} q'$ such that $\nu \oplus \nu' \in Sat(\xi)$. We say that the edge of $[\![\mathcal{S}]\!]$ from (q, ν) to (q', ν') is an *instance* of the edge $q \xrightarrow{\xi} q'$ of $\mathcal{S}$.

A path of $[\![\mathcal{S}]\!]$ is called a *run* of $\mathcal{S}$. The length $|\wp|$ (resp., $|\pi|$) of a path $\wp$ (resp., run π) of $\mathcal{S}$ is defined in the standard way. A *non-null* path (resp., *non-null* run) of $\mathcal{S}$ is a path (resp., run) of $\mathcal{S}$ of non-null length. Let $\wp = q_0 \xrightarrow{\xi_0} q_1 \xrightarrow{\xi_1} q_2, \ldots$

[3] MG are called Positive Graphose Inequality Systems in [16].

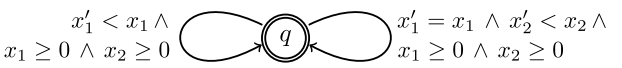

Fig. 1. A GCS.

be a path of $\mathcal{S}$. A run π of $\mathcal{S}$ is an *instance* of $\wp$ if π is of the form $\pi = (q_0, \nu_0) \to (q_1, \nu_1) \to (q_2, \nu_2), \ldots$ and for each i, $(q_i, \nu_i) \to (q_{i+1}, \nu_{i+1})$ is an instance of $q_i \xrightarrow{\xi_i} q_{i+1}$. Given $F \subseteq Q(\mathcal{S})$, an infinite run $(q_0, \nu_0) \to (q_1, \nu_1) \to \ldots$ of $\mathcal{S}$ is *fair w.r.t.* F if for infinitely many $i \geqslant 0$, $q_i \in F$. A state s of $\mathcal{S}$ is *terminating* if there is *no* infinite run of $\mathcal{S}$ starting from s. A state s of $\mathcal{S}$ is *unbounded* if the set of lengths of the *finite* runs of $\mathcal{S}$ starting from s is unbounded (equivalently, infinite). A state s of $\mathcal{S}$ is *strongly terminating* if it is *not* unbounded. Since $[\![\mathcal{S}]\!]$ may be infinitely-branching, termination and strong termination are distinct concepts. In particular, strong termination implies termination, but the vice-versa in general does not hold. This is illustrated by the following example.

Example 1. Fig. 1 depicts a GCS $\mathcal{S}$ consisting of a unique control point q and two self-loops. We deduce that each state s of $\mathcal{S}$ is terminating. For this, we assume the contrary and derive a contradiction. Hence, there is an infinite run $\pi = (q, \nu_0) \to (q, \nu_1) \to \ldots$ of $\mathcal{S}$. By construction, for all $i \geqslant 0$, the following hold: $(\nu(x_1), \nu(x_2)) \in \mathbb{N} \times \mathbb{N}$, and *either* $\nu_{i+1}(x_1) < \nu_i(x_1)$, *or* $\nu_{i+1}(x_1) = \nu_i(x_1)$ and $\nu_{i+1}(x_2) < \nu_i(x_2)$. Hence, along the run π, the pair (x_1, x_2) decreases strictly w.r.t. the lexicographic order over $\mathbb{N} \times \mathbb{N}$. Since the latter is a well-founded order, π cannot be infinite. Thus, each state of $\mathcal{S}$ is terminating. On the other hand, one can easily check that each state $s = (q, \nu)$ with $\nu(x_1) > 0$ and $\nu(x_2) \geqslant 0$ is unbounded. Indeed, for each $k \geqslant 2$, a run from s of length k can be obtained as follows: for the first step of the run, we use the left edge in Fig. 1, obtaining a state $s' = (q, \nu')$, where $\nu'(x_1) = \nu(x_1) - 1$ and $\nu'(x_2) > k$. Then, the successive $k - 1$ steps of the run are obtained as instances of the right edge in Fig. 1.

Investigated problems. Let $\mathcal{S}$ be a GCS. We denote by $Inf_{\mathcal{S}}$ the set of non-terminating states of $\mathcal{S}$ and by $Unb_{\mathcal{S}}$ the set of unbounded states of $\mathcal{S}$. Note that $Inf_{\mathcal{S}} \subseteq Unb_{\mathcal{S}}$. Moreover, for a set F of control points of $\mathcal{S}$, we denote by $Inf_{\mathcal{S},F}$ the set of states of $\mathcal{S}$ from which there is an infinite run that is fair w.r.t. F. Note that $Inf_{\mathcal{S}} = Inf_{\mathcal{S},Q(\mathcal{S})}$.

Definition 4 *(*MG*-representability of sets of states).* A set U of states of a GCS $\mathcal{S}$ is MG *representable* if there is a family $\{\mathcal{G}_q\}_{q \in Q(\mathcal{S})}$ of finite sets of MG over *Var* such that $\bigcup_{G \in \mathcal{G}_q} Sat(G) = \{\nu \mid (q, \nu) \in U\}$ for each $q \in Q(\mathcal{S})$.

In other terms, a set U of states of a GCS $\mathcal{S}$ is MG representable if for each control point $q \in Q(\mathcal{S})$, the set of valuations ν over *Var* such that $(q, \nu) \in U$ corresponds to the set of valuations satisfying some finite disjunction of GC over *Var*. In this paper, we study some verification questions for GCS. In particular, we consider the following decision problems:

- *Termination Problem:* given a GCS $\mathcal{S}$, is the set $Inf_{\mathcal{S}}$ empty?
- *Strong Termination Problem:* given a GCS $\mathcal{S}$, is the set $Unb_{\mathcal{S}}$ empty?
- *Fairness Problem:* given a GCS $\mathcal{S}$ and $F \subseteq Q(\mathcal{S})$, is the set $Inf_{\mathcal{S},F}$ non-empty?

We will show that the problems above are all PSPACE-complete and the sets $Unb_{\mathcal{S}}$ and $Inf_{\mathcal{S},F}$ for a given GCS $\mathcal{S}$ and $F \subseteq Q(\mathcal{S})$, are effectively MG representable. Moreover, for each of the mentioned problems $\mathfrak{P}$, we also investigate the version of $\mathfrak{P}$ w.r.t. a designated state and the version of $\mathfrak{P}$ w.r.t. a designated control point, which are defined in the obvious way. For example, the strong termination problem w.r.t. a designated state (resp., a control point) is checking, for a given GCS $\mathcal{S}$ and state s of $\mathcal{S}$ (resp., control point $q \in Q(\mathcal{S})$), whether $s \notin Unb_{\mathcal{S}}$ (resp., $(q, \nu) \notin Unb_{\mathcal{S}}$ for every valuation ν over *Var*). We conclude this section by observing two facts.

Proposition 1. *Let $\mathfrak{P}$ be the termination (resp., strong termination, resp., fairness) problem. Then, the version of $\mathfrak{P}$ w.r.t. a designated state can be reduced in linear-time to the version of $\mathfrak{P}$ w.r.t. a control point.*

Proof. Fix a GCS $\mathcal{S}$, a state (q_0, ν_0) of $\mathcal{S}$, and $F \subseteq Q(\mathcal{S})$. W.l.o.g. we can assume that $\nu_0(x) \in Const$ for each $x \in Var$ (otherwise, we extend *Const* by including the integers $\nu_0(x)$ with $x \in Var$). Let $\xi_=$ be the GC given by $\bigwedge_{x \in Var} x = \nu_0(x)$, and $q_0' \notin Q(\mathcal{S})$ be a fresh control point. We construct a new GCS $\mathcal{S}_0$ as follows: $\mathcal{S}_0$ is obtained from $\mathcal{S}$ by adding for each edge of $\mathcal{S}$ of the form $q_0 \xrightarrow{\xi} q$, the edge $q_0' \xrightarrow{\xi \wedge \xi_=} q$. By construction, it easily follows that: (i) $(q_0, \nu_0) \notin Inf_{\mathcal{S}}$ iff $(q_0', \nu) \notin Inf_{\mathcal{S}_0}$ for each valuation ν over *Var*, (ii) $(q_0, \nu_0) \notin Unb_{\mathcal{S}}$ iff $(q_0', \nu) \notin Unb_{\mathcal{S}_0}$ for each valuation ν over *Var*, and (iii) $(q_0, \nu_0) \in Inf_{\mathcal{S},F}$ iff $(q_0', \nu) \in Inf_{\mathcal{S}_0,F}$ for some valuation ν over *Var*. Hence, the result follows. □

Proposition 2. *The termination problem, the strong termination problem, the fairness problem, and their versions w.r.t. a designated state and w.r.t. a control point are all* PSPACE*-hard.*

Proof. It is known that for Boolean Programs [26], termination and termination w.r.t. a designated state are PSPACE-complete [26]. Since GCS subsume Boolean Programs and Boolean Programs are finitely-branching (hence, for these systems, strong

termination corresponds to termination), by Proposition 1, it follows that the termination problem and the strong termination problem for GCS, and their versions w.r.t. a designated state and w.r.t. a control point are PSPACE-hard. For the fairness problem and its versions w.r.t. a designated state and w.r.t. a control point, it suffices to observe that the fairness problem subsumes the dual of the termination problem and PSPACE = coPSPACE. □

Remark 1. For the ease of presentation, we do not allow disjunction in the gap-order constraints labeling the edges of a GCS. Note that disjunctions of (conjunctive) GC can be emulated by multiple edges from a given source control point to a given target control point. Even if the disjunctive normal form of an arbitrary gap-order constraint ξ may be of size singly exponential in the size of ξ, our main results (see Theorems 8, 9, and 13 in the rest of the paper) can be trivially generalized to GCS whose edges are labeled by arbitrary gap-order constraints.

Convention. We will use MG representations to manipulate (conjunctive) GC; therefore, we assume that the edge-labels in GCS are transitional MG.

3. Preliminary results

This section is organized as follows. First, in Section 3.1, we recall some basic operations on MG [16] which can be computed in polynomial time. Then, in Section 3.2, we define a sound and complete (w.r.t. satisfiability) approximation scheme of MG and show that the basic operations on MG preserve soundness and completeness of this approximation. Finally, in Section 3.3, we give constructive results on the reachability relation in GCS.

3.1. Known properties of monotonicity graphs

Let G be an MG over V. We say that G is *satisfiable* if $Sat(G) \neq \emptyset$. For $V' \subseteq V$, *the restriction of G to V'*, written $G_{V'}$, is the MG over V' given by the subgraph of G whose set of vertices is $V' \cup Const$. For all vertices u, v of G, we denote by $p_G(u, v)$ the least upper bound (possibly ∞) of the weight sums on all paths in G from u to v (we set $p_G(u, v) = -\infty$ if there is no such a path). The MG G is *normalized* if the following hold:

- for all vertices u, v of G, if $p_G(u, v) > -\infty$, then $p_G(u, v) \neq \infty$ and $u \xrightarrow{p_G(u,v)} v$ is an edge of G;
- for all constants $c_1, c_2 \in Const$, $p_G(c_1, c_2) \leqslant c_1 - c_2$.

The following two propositions (Propositions 3 and 4) summarize some known basic properties of MG [16] (in particular, checking satisfiability of MG or, equivalently, GC can be done in polynomial time).

Proposition 3. *(See [16].) An* MG *G is satisfiable $\Leftrightarrow$ G contains no loop with positive weight sum and for all $c_1, c_2 \in Const$, $p_G(c_1, c_2) \leqslant c_1 - c_2$ (this can be checked in polynomial time).*

Definition 5 *(Closure of* MG*).* (See [16].) For a *satisfiable* MG G over V, the *closure* of G, denoted by $\overline{G}$, is the MG over V defined as follows: for all vertices $u, v \in V \cup Const$, there is an edge $u \xrightarrow{k} v$ in $\overline{G}$ *iff* $p_G(u, v) > -\infty$ and $k = p_G(u, v)$ (note that since G is satisfiable, by Proposition 3, $p_G(u, v) \neq \infty$). Moreover, for all unsatisfiable MG G over V, we use a unique closure corresponding to some MG G_{nil} over V such that $(G_{nil})_\emptyset$ is unsatisfiable (recall that $(G_{nil})_\emptyset$ denotes the MG given by the subgraph of G_{nil} whose set of vertices is $Const$). As for satisfiable MG, the closure of an unsatisfiable MG G is denoted by $\overline{G}$.

Proposition 4. *(See [16].) Let G be an* MG *over V. Then*:

1. *If G is* normalized *and $V' \subseteq V$, then G is satisfiable and every solution of $G_{V'}$ can be extended to a whole solution of G.*
2. *If G is satisfiable, then its closure $\overline{G}$ can be computed in polynomial time. Moreover, $\overline{G}$ is normalized and $Sat(\overline{G}) = Sat(G)$.*

We conclude this subsection by recalling some effective operations on MG which can be computed in polynomial time. Let $Var'' = \{x''_1, \ldots, x''_r\}$ be an additional copy of $Var = \{x_1 \ldots, x_r\}$.

Definition 6. (See [16].) Let G be an MG over V and G' be an MG over V'.

1. **Projection:** if $V' \subseteq V$, the *projection of G over V'* is the MG given by $(\overline{G})_{V'}$.
2. **Intersection:** the *intersection $G \sqcap G'$ of G and G'* is the MG over $V \cup V'$ defined as follows: $u \xrightarrow{k} v$ is an edge of $G \sqcap G'$ iff *either* (1) $u \xrightarrow{k} v$ is an edge of G (resp., G') and there is no edge from u to v in G' (resp., G), *or* (2) $k = \max(\{k', k''\})$, $u \xrightarrow{k'} v$ is an edge of G and $u \xrightarrow{k''} v$ is an edge of G'.

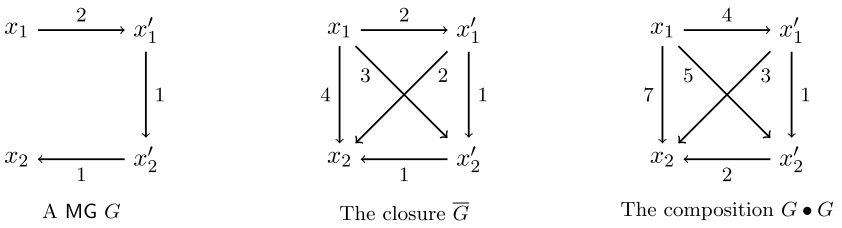

Fig. 2. A transitional MG G, its closure $\overline{G}$, and the composition $G \bullet G$.

3. **Composition:** assume that G and G' are two transitional MG. Let G'' be obtained from G' by renaming any variable x'_i into x''_i and x_i into x'_i. The *composition* $G \bullet G'$ of G and G' is the transitional MG obtained from the *projection* of $G \sqcap G''$ over $Var \cup Var''$ by renaming any variable x''_i into x'_i.

Fig. 2 depicts a satisfiable transitional MG, its closure $\overline{G}$, and the composition $G \bullet G$. As we will see in Section 3.3, the composition operator allows to capture the binary reachability relation in a GCS for a fixed non-null finite path in the control graph. By Definition 6 and Proposition 4, we easily obtain the following known result [16], which essentially asserts that MG (or, equivalently, GC) are closed under intersection and existential variable quantification.

Proposition 5. *(See [16].) Let G be an* MG *over V and G' be an* MG *over V'.*

1. **Projection:** *if G' is the projection of G over V', then for $\nu' : V' \to \mathbb{Z}$, $\nu' \in Sat(G')$ if and only if $\nu' = \nu|_{V'}$ for some $\nu \in Sat(G)$.*
2. **Intersection:** *for $\nu : V \cup V' \to \mathbb{Z}$, $\nu \in Sat(G \sqcap G')$ if and only if $\nu|_V \in Sat(G)$ and $\nu|_{V'} \in Sat(G')$. Hence, for $V = V'$, $Sat(G \sqcap G') = Sat(G) \cap Sat(G')$.*
3. **Composition:** *assume that G and G' are transitional* MG*. Then, for all $\nu, \nu' : Var \to \mathbb{Z}$. $\nu \oplus \nu' \in Sat(G \bullet G')$ if and only if $\nu \oplus \nu'' \in Sat(G)$ and $\nu'' \oplus \nu' \in Sat(G')$ for some $\nu'' : Var \to \mathbb{Z}$. Moreover, the composition operator $\bullet$ is associative.*

3.2. Approximation scheme of monotonicity graphs

Note that for the fixed sets *Var* and *Const* of variables and constants, the class of transitional MG is infinite (since the edge-weights are arbitrary natural numbers). In this subsection, we introduce a sound and complete (w.r.t. satisfiability) finite over-approximation scheme of (transitional) MG. The latter is based on the use of a cut-off value K for finitely abstracting the edge-weights (gaps) in MG.

In the rest of this paper, we denote by K the positive natural number given by

$$K \stackrel{\text{def}}{=} \max\big(\{|c_1 - c_2| + 1 \mid c_1, c_2 \in Const\}\big)$$

that is the maximum distance between the constants in *Const* plus one. For each $h \in \mathbb{N}$, we denote by $\lfloor h \rfloor_K$ the minimum between h and K.

Definition 7 *(K-bounded approximation).* An MG G is *K-bounded* if the weights of the edges of G are bounded by K. For an MG G over V, its *K-bounded approximation*, denoted by $\lfloor G \rfloor_K$, is the K-bounded MG over V obtained from G by replacing each edge-weight h of G with $\lfloor h \rfloor_K$. For a set $\mathcal{G}$ of MG, $\lfloor \mathcal{G} \rfloor_K$ denotes the set of K-bounded MG given by $\{\lfloor G \rfloor_K \mid G \in \mathcal{G}\}$. We extend the previous set operation to families of sets of MG in the obvious way. For a GCS $\mathcal{S}$, its *K-bounded approximation* $\lfloor \mathcal{S} \rfloor_K$ is the GCS obtained by replacing each MG of $\mathcal{S}$ with its K-bounded approximation. For a set $\mathcal{F}$ of GCS, $\lfloor \mathcal{F} \rfloor_K$ denotes the set $\{\lfloor \mathcal{S} \rfloor_K \mid \mathcal{S} \in \mathcal{F}\}$.

Note that each K-bounded transitional MG has at most $2|Var| + |Const|$ vertices and for all vertices u and v, there is at most one edge from u to v, and this edge has the form $u \xrightarrow{h} v$, where $h = 0, 1, \ldots, K$. Hence, we obtain the following upper bound on the cardinality of the finite set of K-bounded transitional MG.

Remark 2. The number of K-bounded transitional MG is bounded by $(K+2)^{(2|Var|+|Const|)^2}$, that is singly exponential in the number of variables and constants and in the size of the binary encoding of the constants.

Now, we show that the K-bounded approximation scheme is sound and complete w.r.t. satisfiability, and basic operations on MG preserve soundness and completeness of this approximation. These results (Propositions 6 and 7) are crucial since they represent the basis for solving in an asymptotical optimal way the considered verification questions on GCS.

Proposition 6. *For an* MG *G, G is satisfiable* iff *$\lfloor G \rfloor_K$ is satisfiable. Moreover, $\lfloor \overline{G} \rfloor_K = \lfloor \overline{\lfloor G \rfloor_K} \rfloor_K$.*

Proof. By Proposition 3 and definition of K-bounded MG, it easily follows that G is satisfiable iff $\lfloor G \rfloor_K$ is satisfiable. It remains to show that $\lfloor \overline{G} \rfloor_K = \lfloor \overline{\lfloor G \rfloor_K} \rfloor_K$. If G is unsatisfiable, then $\lfloor G \rfloor_K$ is unsatisfiable as well. Hence, G and $\lfloor G \rfloor_K$ have the same closure, and the result holds in this case. Now, assume that G is satisfiable. From the first part of the proposition and Proposition 4(2), $\lfloor \overline{G} \rfloor_K$ and $\lfloor \overline{\lfloor G \rfloor_K} \rfloor_K$ are both satisfiable. Thus, by definition of K-bounded MG it suffices to show the following:

Property 1: for each edge $u \xrightarrow{k} v$ of $\overline{G}$, there is an edge $u \xrightarrow{k'} v$ of $\overline{\lfloor G \rfloor_K}$ such that $\lfloor k \rfloor_K = \lfloor k' \rfloor_K$;
Property 2: for each edge $u \xrightarrow{k} v$ of $\overline{\lfloor G \rfloor_K}$, there is an edge $u \xrightarrow{k'} v$ of $\overline{G}$ such that $\lfloor k \rfloor_K = \lfloor k' \rfloor_K$.

Proof of Property 1. Let $u \xrightarrow{k} v$ be an edge in $\overline{G}$. Then, $k = p_G(u, v)$. Thus, there is a path p of G from u to v whose weight sum is k. We distinguish two cases:

- p contains an edge of weight greater than or equal to K. Hence, $k \geqslant K$. By definition of $\lfloor G \rfloor_K$, there is a path of $\lfloor G \rfloor_K$ from u to v of weight sum greater than or equal to K. It follows that there is an edge $u \xrightarrow{k'} v$ of $\overline{\lfloor G \rfloor_K}$ such that $k' \geqslant K$. Since $\lfloor k \rfloor_K = \lfloor k' \rfloor_K = K$, in this case Property 1 holds.
- p contains only edges of weight smaller than K. By definition of $\lfloor G \rfloor_K$, p is also a path of $\lfloor G \rfloor_K$. Since $p_{\lfloor G \rfloor_K}(u, v) \leqslant p_G(u, v) = k$ and the weight sum of p is k, $u \xrightarrow{k} v$ must be also an edge of $\overline{\lfloor G \rfloor_K}$, and Property 1 holds in this case as well. □

Proof of Property 2. Let $u \xrightarrow{k} v$ be an edge in $\overline{\lfloor G \rfloor_K}$. By definitions of K-bounded MG and closure of a satisfiable MG, it follows that $u \xrightarrow{k'} v$ is an edge of $\overline{G}$ for some k'. Recall that for an MG and vertices u and v, there is at most one edge from u to v. Thus, by Property 1, we obtain that $\lfloor k \rfloor_K = \lfloor k' \rfloor_K = K$, and Property 2 follows. This concludes the proof of Proposition 6. □

Proposition 7. *For* MG G *and* G', $\lfloor G \sqcap G' \rfloor_K = \lfloor G \rfloor_K \sqcap \lfloor G' \rfloor_K$. *Moreover, if* G *and* G' *are transitional, then* $\lfloor G \bullet G' \rfloor_K = \lfloor \lfloor G \rfloor_K \bullet \lfloor G' \rfloor_K \rfloor_K$.

Proof. First, we prove that $\lfloor G \sqcap G' \rfloor_K = \lfloor G \rfloor_K \sqcap \lfloor G' \rfloor_K$. It suffices to show the following:

Property 1: for each edge $u \xrightarrow{k} v$ of $G \sqcap G'$, there is an edge $u \xrightarrow{k'} v$ of $\lfloor G \rfloor_K \sqcap \lfloor G' \rfloor_K$ such that $\lfloor k \rfloor_K = k'$;
Property 2: for each edge $u \xrightarrow{k} v$ of $\lfloor G \rfloor_K \sqcap \lfloor G' \rfloor_K$, there is an edge $u \xrightarrow{k'} v$ of $G \sqcap G'$ such that $k = \lfloor k' \rfloor_K$.

Proof of Property 1. Let $u \xrightarrow{k} v$ be an edge in $G \sqcap G'$. By Definition 6, there are three cases:

- $u \xrightarrow{k} v$ is an edge of G and there is no edge from u to v in G'. It follows that $u \xrightarrow{\lfloor k \rfloor_K} v$ is an edge of $\lfloor G \rfloor_K$ and there is no edge from u to v in $\lfloor G' \rfloor_K$. Hence, $u \xrightarrow{\lfloor k \rfloor_K} v$ is an edge of $\lfloor G \rfloor_K \sqcap \lfloor G' \rfloor_K$. Thus, in this case Property 1 holds.
- $u \xrightarrow{k} v$ is an edge of G' and there is no edge from u to v in G. This case is similar to the previous one.
- G has an edge $u \xrightarrow{h} v$, G' has an edge $u \xrightarrow{h'} v$, and $k = \max(\{h, h'\})$. It follows that there is an edge $u \xrightarrow{k'} v$ of $\lfloor G \rfloor_K \sqcap \lfloor G' \rfloor_K$ with $k' = \max(\{\lfloor h \rfloor_K, \lfloor h' \rfloor_K\})$. Since $\lfloor \max(\{h, h'\}) \rfloor_K = \max(\{\lfloor h \rfloor_K, \lfloor h' \rfloor_K\})$, Property 1 holds in this case as well. □

Proof of Property 2. Let $u \xrightarrow{k} v$ be an edge in $\lfloor G \rfloor_K \sqcap \lfloor G' \rfloor_K$. Then, there must be an edge of $G \sqcap G'$ of the form $u \xrightarrow{k'} v$ for some k'. Recall that for an MG and vertices u and v, there is at most one edge from u to v. Thus, by Property 1, we obtain that $k = \lfloor k' \rfloor_K = K$, and Property 2 follows. □

In order to conclude the proof of Proposition 7, it remains to show that for transitional MG G and G', $\lfloor G \bullet G' \rfloor_K = \lfloor \lfloor G \rfloor_K \bullet \lfloor G' \rfloor_K \rfloor_K$. Let G'' be obtained from G' by renaming any variable x'_i into x''_i and x_i into x'_i. By Definition 6 and definition of K-bounded MG, it suffices to prove that $\lfloor \overline{G \sqcap G''} \rfloor_K = \lfloor \overline{\lfloor G \rfloor_K \sqcap \lfloor G'' \rfloor_K} \rfloor_K$. By Proposition 6 and the first part of Proposition 7, it holds that $\lfloor \overline{G \sqcap G''} \rfloor_K = \lfloor \overline{\lfloor G \sqcap G'' \rfloor_K} \rfloor_K$ and $\lfloor G \sqcap G'' \rfloor_K = \lfloor G \rfloor_K \sqcap \lfloor G'' \rfloor_K$. Hence, $\lfloor \overline{G \sqcap G''} \rfloor_K = \lfloor \lfloor G \rfloor_K \sqcap \lfloor G'' \rfloor_K \rfloor_K$, which concludes the proof of Proposition 7. □

3.3. Results on the reachability relation in GCS

In this subsection, we give constructive results on the reachability relation in GCS.

Definition 8 *(Reachability relation for a finite path).* Let $\mathcal{S}$ be a GCS. For a finite path $\wp$ of $\mathcal{S}$, the *reachability relation w.r.t.* $\wp$, denoted by $\rightsquigarrow_\wp$, is the binary relation on the set of valuations over *Var* defined as follows: for all $\nu, \nu' : Var \to \mathbb{Z}$, $\nu \rightsquigarrow_\wp \nu'$ *iff*

there is a run of $\mathcal{S}$ from $(s(\wp), \nu)$ to $(t(\wp), \nu')$ which is an instance of the path $\wp$. For a transitional MG G, G *characterizes the reachability relation* $\rightsquigarrow_\wp$ *iff* $Sat(G) = \{\nu \oplus \nu' \mid \nu \rightsquigarrow_\wp \nu'\}$. A finite path $\wp$ of $\mathcal{S}$ is *satisfiable* if there is a run which is an instance of $\wp$ (i.e., there are valuations ν and ν' such that $\nu \rightsquigarrow_\wp \nu'$).

Fix a GCS $\mathcal{S}$. We associate to each non-null finite path $\wp$ of $\mathcal{S}$ a transitional MG $G_\wp$ and a transitional K-bounded MG $G^{bd}_\wp$, defined by induction on $\wp$ as follows:

- $\wp = q \xrightarrow{G} q'$: $G_\wp \stackrel{\text{def}}{=} G$ and $G^{bd}_\wp \stackrel{\text{def}}{=} \lfloor G \rfloor_K$;
- $\wp = \wp'\wp''$, $|\wp'| > 0$, and $\wp'' = q \xrightarrow{G} q'$: $G_\wp \stackrel{\text{def}}{=} G_{\wp'} \bullet G$ and $G^{bd}_\wp \stackrel{\text{def}}{=} \lfloor G^{bd}_{\wp'} \bullet \lfloor G \rfloor_K \rfloor_K$.

Note that $G_\wp$ is the composition of the transitional MG along the edges of $\wp$. By a straightforward induction on the length of the path $\wp$ and by using Propositions 5 and 7, we obtain the following result.

Proposition 8. *For a non-null finite path $\wp$ of $\mathcal{S}$, $G^{bd}_\wp = \lfloor G_\wp \rfloor_K$ and $G_\wp$ characterizes the reachability relation $\rightsquigarrow_\wp$.*

For the given GCS $\mathcal{S}$, define $\mathcal{G}^K_\mathcal{S}$ as

$$\mathcal{G}^K_\mathcal{S} \stackrel{\text{def}}{=} \left\{ \left(\lfloor G_\wp \rfloor_K, s(\wp), t(\wp) \right) \;\middle|\; \wp \text{ is a satisfiable non-null finite path of } \mathcal{S} \right\}.$$

Thus, $\mathcal{G}^K_\mathcal{S}$ keeps tracks of the K-bounded approximations of the transitional MG associated with the satisfiable non-null finite paths $\wp$ of $\mathcal{S}$ together with the source and target control points of $\wp$. Note that $\mathcal{G}^K_\mathcal{S}$ is finite since the set of transitional K-bounded MG is finite. In particular, by Remark 2, the cardinality of $\mathcal{G}^K_\mathcal{S}$ is bounded by $|Q(\mathcal{S})|^2 \cdot (K+2)^{(2|Var|+|Const|)^2}$. Moreover, by Proposition 8, $\mathcal{G}^K_\mathcal{S}$ is exactly the set $\{(G^{bd}_\wp, s(\wp), t(\wp)) \mid \wp \text{ is a non-null finite path and } G^{bd}_\wp \text{ is satisfiable}\}$. It follows that we can compute the set $\mathcal{G}^K_\mathcal{S}$ by the following transitive closure procedure: initialize a set B to $\{(\lfloor G \rfloor_K, q, q') \mid q \xrightarrow{G} q' \text{ is an edge of } \mathcal{S} \text{ and } \lfloor G \rfloor_K \text{ is satisfiable}\}$ and repeat the following step until no more elements can be added to B (at this point $B = \mathcal{G}^K_\mathcal{S}$): for each $(G^{bd}, q, q') \in B$ and edge $q' \xrightarrow{G} q''$ of $\mathcal{S}$ include in B also $(\lfloor G^{bd} \bullet \lfloor G \rfloor_K \rfloor_K, q, q'')$, unless $\lfloor G^{bd} \bullet \lfloor G \rfloor_K \rfloor_K$ is unsatisfiable. Thus, we obtain the following result.

Theorem 1. *For a GCS $\mathcal{S}$, the size of $\mathcal{G}^K_\mathcal{S}$ is bounded by $O(|Q(\mathcal{S})|^2 \cdot (K+2)^{(2|Var|+|Const|)^2})$ and $\mathcal{G}^K_\mathcal{S}$ can be computed in time $O(|E(\mathcal{S})| \cdot |Q(\mathcal{S})|^2 \cdot (K+2)^{(2|Var|+|Const|)^2})$.*

By [16] (see also [14]), for a GCS $\mathcal{S}$, the reflexive transitive closure of the transition relation of $[\![\mathcal{S}]\!]$ is effectively GC definable (a similar result can be found in [32], where it is shown that for Datalog queries with GC, there is a closed form evaluation). The GC representation can be computed by a fixpoint iteration whose termination is guaranteed by a suitable decidable well-quasi-ordering defined over the set of transitional MG. By an insight in the proof given in [16] (see also [14]), and applying the K-bounded approximation scheme, we easily obtain the following result. For completeness, we give a proof of Theorem 2 in Appendix A.1. Note that we are not able to give an upper bound on the cardinality of the set $\mathcal{P}_\mathcal{S}$.

Theorem 2. *Given a GCS $\mathcal{S}$, one can compute a finite set $\mathcal{P}_\mathcal{S}$ of non-null finite paths of $\mathcal{S}$ such that for each non-null finite path $\wp'$ of $\mathcal{S}$, there is a path $\wp \in \mathcal{P}_\mathcal{S}$ so that $s(\wp) = s(\wp')$, $t(\wp) = t(\wp')$, $\lfloor G_\wp \rfloor_K = \lfloor G_{\wp'} \rfloor_K$, and $\rightsquigarrow_{\wp'}$ implies $\rightsquigarrow_\wp$ (hence, $Sat(G_{\wp'}) \subseteq Sat(G_\wp)$).*

By Theorem 2, one can compute a GC representation of the binary reachability relation (for arbitrary finite paths) in a GCS $\mathcal{S}$. Although we are not able to provide an upper bound on the size of this GC representation, it is important to highlight, as we show below, that the reachability problem in GCS between two given states can be solved in singly exponential time. This problem is closely related to the recognition problem investigated in [32], which asks for a given Datalog query with gap-order constraints (consisting of a program P and a generalized relational database) and a given ground relational tuple $A(t)$, whether $A(t)$ is in the full-model of the query (corresponding to the bottom-up evaluation of the query). Revesz in [32] provided an exponential-time algorithm to solve this problem (which is polynomial-time bounded for a fixed program P). We use an approach similar to the one in [32] to show that the reachability problem in GCS can be solved in singly exponential time.[4] First, we observe that the K-bounded approximation scheme is sound and complete w.r.t. the valuations ν assigning to each variable an integer in *Const*.

Claim. *Let G be an MG over V (and Const) and $\nu : V \to \mathbb{Z}$ such that $\nu(x) \in Const$ for all $x \in V$. Then, $\nu \in Sat(G)$ iff $\nu \in Sat(\lfloor G \rfloor_K)$.*

[4] The main difference with respect to the result in [32] is that we use a different graph representation of GC and a more general approximation scheme than the one exploited in [32].

Proof of the claim. If $\nu \in Sat(G)$, the $\nu \in Sat(\lfloor G \rfloor_K)$ (since $Sat(G) \subseteq Sat(\lfloor G \rfloor_K)$). For the proof of the converse implication, we assume that $\nu \in Sat(\lfloor G \rfloor_K)$ and $\nu \notin Sat(G)$, and derive a contradiction. Hence, by construction, there must be an edge $u \xrightarrow{h} v$ of G and an edge $u \xrightarrow{\lfloor h \rfloor_K} v$ of $\lfloor G \rfloor_K$ such that $\nu(u) - \nu(v) < h$ and $\nu(u) - \nu(v) \geqslant \lfloor h \rfloor_K$. By hypothesis, $\nu(u) - \nu(v) \leqslant \max\{|c_1 - c_2| \mid c_1, c_2 \in Const\} < K$. It follows that $\lfloor h \rfloor_K < K$, hence, $\lfloor h \rfloor_K = h$, which is a contradiction, and we are done. □

For a given GCS $\mathcal{S}$ and given states (q_0, ν_0) and (q_1, ν_1) of $\mathcal{S}$, in order to check if (q_1, ν_1) is reachable from (q_0, ν_0), we proceed as follows. Fist, we extend *Const* by including all the integers $\nu_0(x)$ and $\nu_1(x)$ with $x \in Var$. If $(q_1, \nu_1) = (q_0, \nu_0)$, then the check is positive. Now, assume that $(q_1, \nu_1) \neq (q_0, \nu_0)$. Then, (q_1, ν_1) is reachable from (q_0, ν_0) iff there is a satisfiable non-null finite path $\wp$ of $\mathcal{S}$ such that $s(\wp) = q_0$, $t(\wp) = q_1$, and $\nu_0 \oplus \nu_1 \in Sat(G_\wp)$. By Theorem 1, one can compute in singly exponential time the following set

$$\mathcal{G}_{\mathcal{S}}^{K} \stackrel{\text{def}}{=} \big\{ \big(\lfloor G_\wp \rfloor_K, s(\wp), t(\wp) \big) \;\big|\; \wp \text{ is a satisfiable non-null finite path of } \mathcal{S} \big\}.$$

Thus, by the claim above (and since *Const* includes all the integers $\nu_0(x)$ and $\nu_1(x)$ with $x \in Var$), we obtain that (q_1, ν_1) is reachable from (q_0, ν_0) iff there is a triple $(G, q_0, q_1) \in \mathcal{G}_{\mathcal{S}}^{K}$ such that $\nu_0 \oplus \nu_1 \in Sat(G)$. Hence, the reachability problem between two given states of a given GCS can be solved in singly exponential time.

3.4. Outline of the main results

In this subsection, we outline the approach proposed for solving the considered verification questions for GCS. The approach consists of two main steps.

Step 1. First, in Section 4, we address termination and strong termination for a subclass of GCS, we call *simple* GCS. The control graph of these GCS consists just of a self-loop and an additional edge which connects the initial control point with the control point of the self-loop. We define two polynomial-time checkable conditions on simple GCS, namely the *termination condition* and the *unboundedness condition*. Then, we show that the first condition characterizes the simple GCS $\mathcal{S}$ whose set $Inf_{\mathcal{S}}$ of non-terminating states is empty (Proposition 11 and Theorem 4), while the second one characterizes the simple GCS whose set of unbounded states with initial control point is non-empty (Proposition 12 and Theorem 6). Additionally, and importantly, the K-bounded approximation scheme is sound and complete w.r.t. these two conditions (Proposition 11 and Proposition 12). Then, by using these two conditions and the results of the previous subsections, we establish the main results for simple GCS (Theorem 3 and Theorem 5):

- **Main results of Section 4.** For a simple GCS $\mathcal{S}$, one can compute MG representations of the sets $Inf_{\mathcal{S}}$ and $Unb_{\mathcal{S}}$, and K-bounded approximations of these representations can be computed in polynomial time. Moreover, the latter coincide with the K-bounded approximations of the MG representations associated with the sets $Inf_{\lfloor \mathcal{S} \rfloor_K}$ and $Unb_{\lfloor \mathcal{S} \rfloor_K}$.

Step 2. In Section 5, we address fairness and (strong) termination for the whole class of GCS. For a GCS $\mathcal{S}$ and a set $F \subseteq Q(\mathcal{S})$ of accepting control points, by using Theorem 1, the computable finite set of sample finite paths of Theorem 2, and Ramsey's theorem in its infinitary version [31], we show (Theorem 7 and Lemmata 16 and 17) that it is possible to construct two finite families $\mathcal{F}(\mathcal{S}, F)$ and $\mathcal{U}(\mathcal{S})$ of simple GCS such that the following hold:

- $Inf_{\mathcal{S},F}$ corresponds to the set of non-terminating states with initial control point of the single components in $\mathcal{F}(\mathcal{S}, F)$,
- $Unb_{\mathcal{S}}$ corresponds the set of unbounded states with initial control point of the single components in $\mathcal{U}(\mathcal{S})$, and
- the K-bounded approximations of $\mathcal{F}(\mathcal{S}, F)$ and $\mathcal{U}(\mathcal{S})$ can be computed in singly exponential time.

Then, by using the main results of Section 4, we obtain the main results of Section 5 (Theorems 8 and 9).

- **Main results of Section 5.** For a GCS $\mathcal{S}$ and a set $F \subseteq Q(\mathcal{S})$ of accepting control points, one can compute MG representations of the sets $Inf_{\mathcal{S},F}$ and $Unb_{\mathcal{S}}$, and the K-bounded approximations of these representation can be computed in polynomial time. Moreover, the latter coincide with the K-bounded approximations of the MG representations associated with the sets $Inf_{\lfloor \mathcal{S} \rfloor_K, F}$ and $Unb_{\lfloor \mathcal{S} \rfloor_K}$. Note that this last result is crucial to solve in an optimal way the model checking problem of GCS against the existential fragment of the logic GCCTL* (see Section 6).

These results lead to singly exponential time algorithms to solve termination, strong termination, and fairness for the whole class of GCS. In fact, we also show that these algorithms need only polynomial space.

4. Fairness and (strong) termination for simple GCS

In this section, we address fairness and (strong) termination for a subclass of GCS, we call *simple* GCS. Before defining this subclass, we need additional definitions and notation.

For an MG G and vertices u and v, the notation $G \models u < v$ means that there is path in G from v to u with weight sum $k > 0$. Moreover, $G \models u \leqslant v$ means that there is a path of G from v to u, and $G \models u = v$ means $G \models u \leqslant v$ and $G \models v \leqslant u$. Also, we write $G \models u_1 \lhd_1 \cdots \lhd_{n-1} u_n$ to mean that $G \models u_i \lhd_i u_{i+1}$ for each $1 \leqslant i < n$, where $\lhd_i \in \{<, \leqslant, =\}$.

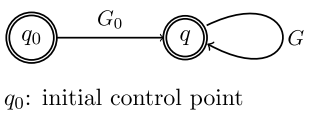

Fig. 3. The control graph of a simple GCS.

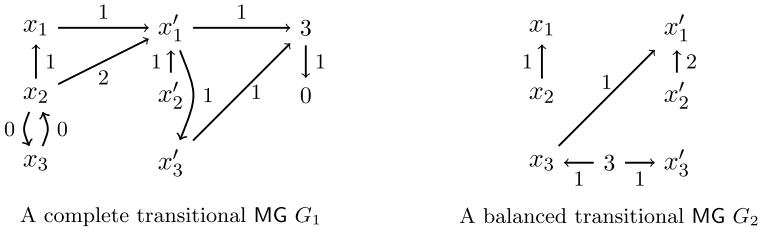

Fig. 4. A complete transitional MG and a balanced transitional MG.

Definition 9 *(Complete transitional* MG*).* A transitional MG G is *complete* if the following hold:

- for all vertices u and v, $G \models u \leqslant v$ implies $G \models u \lhd v$ for some $\lhd \in \{<, =\}$;
- for all $u, v \in Var \cup Const$, either $G \models u \leqslant v$ or $G \models v \leqslant u$;
- for all $u, v \in Var' \cup Const$, either $G \models u \leqslant v$ or $G \models v \leqslant u$.

A GCS $\mathcal{S}$ is *complete* if each MG in $\mathcal{S}$ is complete.

Intuitively, complete transitional MG induce a total ordering on the set of vertices in $Var \cup Const$ and a total ordering on the set of vertices in $Var' \cup Const$.

Remark 3. For a transitional MG G, G is complete *iff* $\lfloor G \rfloor_K$ is complete.

Definition 10. A transitional MG G is (*weakly*) *idempotent* if $\lfloor G \bullet G \rfloor_K = \lfloor G \rfloor_K$.

Definition 11 *(Simple* GCS*).* A simple GCS is a *complete* GCS $\mathcal{S}$ consisting of just two edges of the form $q_0 \xrightarrow{G_0} q$ and $q \xrightarrow{G} q$ such that $q_0 \neq q$, $G_0 \bullet G$ is satisfiable, and G is idempotent. We say that q_0 is the *initial* control point of $\mathcal{S}$. (See Fig. 3.)

Evidently, for a simple GCS, the fairness problem can be trivially reduced in linear time to the dual of the termination problem. Thus, in the following we focus on termination and strong termination of simple GCS. The rest of this section is organized as follows. In Section 4.1, we establish some basic properties of simple GCS. Then, in Sections 4.2 and 4.3, we address termination of simple GCS and strong termination of simple GCS, respectively.

4.1. Basic properties of simple GCS

We need two additional definitions.

Definition 12 *(Balanced transitional* MG*).* A transitional MG G is *balanced* if for all $u, v \in Var \cup Const$ and $\lhd \in \{<, =\}$, $G \models u \lhd v$ if and only if $G \models u' \lhd v'$ (where for $u \in Var \cup Const$, we write u' to denote the corresponding variable in Var' if $u \in Var$, and u itself otherwise).

Intuitively, for a balanced transitional MG, the partial orderings induced by G on the set of vertices $Var \cup Const$ and on the set of vertices $Var' \cup Const$ coincide.

Example 2. Let $Var = \{x_1, x_2, x_3\}$ and $Const = \{0, 3\}$. Fig. 4 depicts two transitional MG G_1 and G_2. Note that G_1 is complete but non-balanced, while G_2 is balanced but non-complete.

Definition 13 *(Lower, upper, and bounded variables).* We denote by MAX (resp., MIN) the maximum (resp., minimum) of $Const$. For a transitional MG G and $y \in Var \cup Var'$, y is a *lower* (resp., *upper*) *variable* of G if $G \models y < MIN$ (resp., $G \models MAX < y$). Moreover, y is a *bounded variable* of G if $G \models MIN \leqslant y$ and $G \models y \leqslant MAX$.

The following two propositions summarize some basic properties of simple GCS.

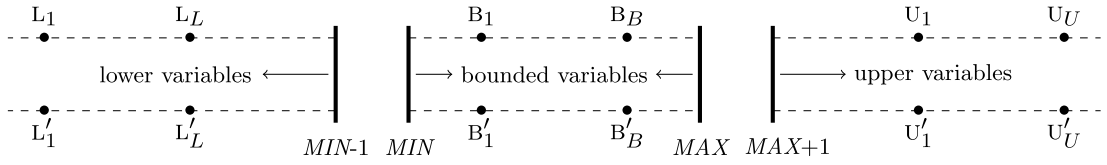

Fig. 5. Partial ordering of the variables in the transitional MG G.

Proposition 9. *For a* GCS $\mathcal{S}$, $\mathcal{S}$ *is simple* iff *if* $\lfloor \mathcal{S} \rfloor_K$ *is simple.*

Proof. The result directly follows from Remark 3 and Propositions 6 and 7. □

For a transitional MG G and $k \geqslant 1$, define $G^k \stackrel{\text{def}}{=} \underbrace{G \bullet \cdots \bullet G}_{k \text{ times}}$.

Proposition 10. *For a simple* GCS $\mathcal{S}$ *with edges* $q_0 \xrightarrow{G_0} q$ *and* $q \xrightarrow{G} q$, *the following hold*:

1. G_0 *is satisfiable and for all* $k \geqslant 1$, $G_0 \bullet G^k$ *and* G^k *are satisfiable as well*;
2. G *is balanced*;
3. *Let* $\mathcal{L}$ (*resp.*, $\mathcal{U}$, *resp.*, $\mathcal{B}$) *be the set of lower* (*resp., upper, resp., bounded*) *variables of* G *in Var. Then,* $\mathcal{L}$, $\mathcal{U}$, *and* $\mathcal{B}$ *represent a partition of Var.*

Proof. Since $G_0 \bullet G$ is satisfiable ($\mathcal{S}$ is a simple GCS), by definition of the composition operator, it follows that G_0 and G are satisfiable as well. Since the composition operator is associative and G is idempotent, by using Proposition 7, we obtain that $\lfloor G_0 \bullet G^k \rfloor_K = \lfloor G_0 \bullet G \rfloor_K$ and $\lfloor G^k \rfloor_K = \lfloor G \rfloor_K$. Thus, since the K-bounded approximation preserves satisfiability of MG (Proposition 6), Property 1 follows. Property 2 directly follows from Property 1 (in particular, $G \bullet G$ is satisfiable), the definition of the composition operator, and the fact that G is complete ($\mathcal{S}$ is a simple GCS). Finally, Property 3 directly follows from the facts that G is satisfiable and complete. □

In the rest of Section 4, we fix a simple GCS $\mathcal{S}$ with edges $q_0 \xrightarrow{G_0} q$ and $q \xrightarrow{G} q$. We denote by $\mathrm{L}_1, \ldots, \mathrm{L}_L$ (resp., $\mathrm{U}_1, \ldots, \mathrm{U}_U$) the lower (resp., the upper) variables of G in *Var*, and by $\mathrm{B}_1, \ldots, \mathrm{B}_B$ the bounded variables of G in *Var*. (See Fig. 5.) By Proposition 10(3), $Var = \{\mathrm{L}_1, \ldots, \mathrm{L}_L, \mathrm{U}_1, \ldots, \mathrm{U}_U, \mathrm{B}_1, \ldots, \mathrm{B}_B\}$ and we can assume that

$$G \models \mathrm{L}_1 \lhd_2 \cdots \lhd_L \mathrm{L}_L < MIN \leqslant \mathrm{B}_1 \lhd'_2 \cdots \lhd'_B \mathrm{B}_B \leqslant MAX < \mathrm{U}_1 \lhd''_2 \cdots \lhd''_U \mathrm{U}_U$$

where $\lhd_2 \cdots \lhd_L, \lhd'_2 \cdots \lhd'_B, \lhd''_2 \cdots \lhd''_U \in \{<, =\}$. Since G is balanced (Proposition 10(3)), it follows that the lower variables (resp., upper variables) of G in Var' are $\mathrm{L}'_1, \ldots, \mathrm{L}'_L$ (resp., $\mathrm{U}'_1, \ldots, \mathrm{U}'_U$), and the bounded variables of G in Var' are $\mathrm{B}'_1, \ldots, \mathrm{B}'_B$. Moreover,

$$G \models \mathrm{L}'_1 \lhd_2 \cdots \lhd_L \mathrm{L}'_L < MIN \leqslant \mathrm{B}'_1 \lhd'_2 \cdots \lhd'_B \mathrm{B}'_B \leqslant MAX < \mathrm{U}'_1 \lhd''_2 \cdots \lhd''_U \mathrm{U}'_U.$$

Notation. Define $\mathrm{L}_{L+1} \stackrel{\text{def}}{=} MIN$, $\mathrm{L}'_{L+1} \stackrel{\text{def}}{=} MIN$, $\mathrm{U}_0 \stackrel{\text{def}}{=} MAX$, and $\mathrm{U}'_0 \stackrel{\text{def}}{=} MAX$.

We conclude this subsection by giving three technical preliminary lemmata, which are fundamental to understand the "interaction" between the variables in *Var* and those in Var' for the *idempotent* transitional MG G associated with the self-loop of the fixed simple GCS $\mathcal{S}$. The first two lemmata (Lemmata 1 and 2) are a consequence of the idempotence of G.

Lemma 1 *(Lower variables). For all* $1 \leqslant i < j \leqslant L$, *the following hold*:

1. $G \models \mathrm{L}_i \leqslant \mathrm{L}'_j \Rightarrow$ *either* $G \models \mathrm{L}_j \leqslant \mathrm{L}'_j$ *or* $G \models \mathrm{L}_i \leqslant \mathrm{L}'_{j-1}$.
2. $G \models \mathrm{L}'_i \leqslant \mathrm{L}_j \Rightarrow$ *either* $G \models \mathrm{L}'_j \leqslant \mathrm{L}_j$ *or* $G \models \mathrm{L}'_i \leqslant \mathrm{L}_{j-1}$.

Proof. We prove Property 1 (Property 2 is similar). Assume that $G \models \mathrm{L}_i \leqslant \mathrm{L}'_j$ where $1 \leqslant i < j \leqslant L$. Then, since G is idempotent, it easily follows that $G \bullet G \models \mathrm{L}_i \leqslant \mathrm{L}'_j$. Hence, by definition of the composition operator, there is $u \in Var \cup Const$ such that $G \models \mathrm{L}_i \leqslant u'$ and $G \models u \leqslant \mathrm{L}'_j$.[5] Since $G \models u \leqslant \mathrm{L}'_j$, we deduce that u is a lower variable of G in *Var*, hence $u = \mathrm{L}_h$ for some $1 \leqslant h \leqslant L$, and we obtain

[5] Where u' denotes the corresponding variable in Var' if $u \in Var$, and u itself otherwise.

$$G \models \mathrm{L}_i \leqslant \mathrm{L}'_h \quad \text{and} \quad G \models \mathrm{L}_h \leqslant \mathrm{L}'_j.$$

We distinguish two cases:

- $h \geqslant j$: hence, $G \models \mathrm{L}_j \leqslant \mathrm{L}_h$. Since $G \models \mathrm{L}_h \leqslant \mathrm{L}'_j$, we obtain that $G \models \mathrm{L}_j \leqslant \mathrm{L}'_j$. Thus, in this case, the result holds.
- $h < j$: hence, $G \models \mathrm{L}'_h \leqslant \mathrm{L}'_{j-1}$. Since $G \models \mathrm{L}_i \leqslant \mathrm{L}'_h$, we obtain that $G \models \mathrm{L}_i \leqslant \mathrm{L}'_{j-1}$. Thus, the result holds in this case as well. □

Lemma 2 *(Upper variables). For all $1 \leqslant i < j \leqslant U$, the following hold*:

1. $G \models \mathrm{U}'_i \leqslant \mathrm{U}_j \Rightarrow$ *either* $G \models \mathrm{U}'_j \leqslant \mathrm{U}_j$ *or* $G \models \mathrm{U}'_i \leqslant \mathrm{U}_{j-1}$.
2. $G \models \mathrm{U}_i \leqslant \mathrm{U}'_j \Rightarrow$ *either* $G \models \mathrm{U}_j \leqslant \mathrm{U}'_j$ *or* $G \models \mathrm{U}_i \leqslant \mathrm{U}'_{j-1}$.

Proof. We prove Property 1 (Property 2 is similar). Assume that $G \models \mathrm{U}'_i \leqslant \mathrm{U}_j$ where $1 \leqslant i < j \leqslant U$. Then, since G is idempotent, it easily follows that $G \bullet G \models \mathrm{U}'_i \leqslant \mathrm{U}_j$. Hence, by definition of the composition operator, there is $u \in \mathit{Var} \cup \mathit{Const}$ such that $G \models u' \leqslant \mathrm{U}_j$ and $G \models \mathrm{U}'_i \leqslant u$. Since $G \models \mathrm{U}'_i \leqslant u$, we deduce that u is an upper variable of G in Var, hence $u = \mathrm{U}_h$ for some $1 \leqslant h \leqslant U$, and we obtain

$$G \models \mathrm{U}'_h \leqslant \mathrm{U}_j \quad \text{and} \quad G \models \mathrm{U}'_i \leqslant \mathrm{U}_h.$$

We distinguish two cases:

- $h \geqslant j$: hence, $G \models \mathrm{U}'_j \leqslant \mathrm{U}'_h$. Since $G \models \mathrm{U}'_h \leqslant \mathrm{U}_j$, we obtain that $G \models \mathrm{U}'_j \leqslant \mathrm{U}_j$. Thus, in this case, the result holds.
- $h < j$: hence, $G \models \mathrm{U}_h \leqslant \mathrm{U}_{j-1}$. Since $G \models \mathrm{U}'_i \leqslant \mathrm{U}_h$, we obtain that $G \models \mathrm{U}'_i \leqslant \mathrm{U}_{j-1}$. Thus, the result holds in this case as well. □

In Sections 4.2 and 4.3, for each of the two considered problems (termination and strong termination), we define a subset of the upper and lower variables of G, called the set of *unconstrained variables*, which depends on the specific problem. Here, we capture by Definition 14 and Lemma 3 some common properties of these sets. Thus, Lemma 3 can be seen as a template which will be instantiated in Sections 4.2 and 4.3 with the specific set of unconstrained variables.

Definition 14. Let $L_c, U_c \in \mathbb{N}$. We say that the pair (L_c, U_c) is *well-formed* w.r.t. G if the following conditions are satisfied:

- $1 \leqslant L_c \leqslant L + 1$ and $G \models \mathrm{L}_{L_c} = \mathrm{L}'_{L_c}$;
- $0 \leqslant U_c \leqslant U$ and $G \models \mathrm{U}_{U_c} = \mathrm{U}'_{U_c}$;
- for each $L_c \leqslant i \leqslant L$, $G \not\models \mathrm{L}'_i < \mathrm{L}_i$ and $G \not\models \mathrm{L}_i < \mathrm{L}'_i$;
- for each $1 \leqslant i \leqslant U_c$, $G \not\models \mathrm{U}'_i < \mathrm{U}_i$ and $G \not\models \mathrm{U}_i < \mathrm{U}'_i$.

The set of *unconstrained variables in Var w.r.t.* (L_c, U_c) is given by $\{\mathrm{L}_1, \ldots, \mathrm{L}_{L_c-1}, \mathrm{U}_{U_c+1}, \ldots, \mathrm{U}_U\}$.

Lemma 3 *(Separation lemma). Let (L_c, U_c) be well-formed w.r.t. G. Then*:

Lower variables: *for all $L_c \leqslant i \leqslant L$, $\sim \in \{<, =, >\}$, and $x \in \mathit{Var}$,*

$$\left(G \models \mathrm{L}'_i \sim x \text{ or } G \models \mathrm{L}_i \sim x'\right) \quad \Rightarrow \quad G \models \mathrm{L}_i \sim x.$$

Upper variables: *for all $1 \leqslant i \leqslant U_c$, $\sim \in \{<, =, >\}$, and $x \in \mathit{Var}$,*

$$\left(G \models \mathrm{U}'_i \sim x \text{ or } G \models \mathrm{U}_i \sim x'\right) \quad \Rightarrow \quad G \models \mathrm{U}_i \sim x.$$

Proof. *Lower variables.* Let $L_c \leqslant i \leqslant L$, $\sim \in \{<, =, >\}$, and $x \in \mathit{Var}$ such that either $G \models \mathrm{L}'_i \sim x$ or $G \models \mathrm{L}_i \sim x'$. Assume that $G \models \mathrm{L}'_i \sim x$ (the other case is similar). We distinguish three cases:

- $\sim$ *is* $<$: hence, $G \models \mathrm{L}'_i < x$. We need to prove that $G \models \mathrm{L}_i < x$. Assume that x is a lower variable (otherwise, the result is obvious). Then, $x = \mathrm{L}_j$ for some $1 \leqslant j \leqslant L$. First, we prove that $i < j$. We assume the contrary and derive a contradiction. Then, $G \models \mathrm{L}_j \leqslant \mathrm{L}_i$. Since $G \models \mathrm{L}'_i < \mathrm{L}_j$, we obtain that $G \models \mathrm{L}'_i < \mathrm{L}_i$, which is a contradiction because $L_c \leqslant i \leqslant L$ and (L_c, U_c) is well-formed w.r.t. G. Thus, $i < j$. Hence, $G \models \mathrm{L}_i \leqslant \mathrm{L}_j$. Since G is complete, either $G \models \mathrm{L}_i < \mathrm{L}_j$ or $G \models \mathrm{L}_i = \mathrm{L}_j$. Since $G \models \mathrm{L}'_i < \mathrm{L}_j$, the second condition would imply $G \models \mathrm{L}'_i < \mathrm{L}_i$, which leads to a contradiction. Thus, $G \models \mathrm{L}_i < \mathrm{L}_j$ and the result follows.
- $\sim$ *is* $>$: this case is similar to the previous one.

- $\sim$ *is* $=$: hence, $G \models \mathrm{L}'_i = x$. We need to prove that $G \models \mathrm{L}_i = x$. Evidently, x is a lower variable. Hence, $x = \mathrm{L}_j$ for some $1 \leqslant j \leqslant L$. Assume that $j < i$ (the other case being similar). We claim that there is $j \leqslant h \leqslant i$ such that $G \models \mathrm{L}_h = \mathrm{L}'_h$. If $j < L_c$, then since (L_c, U_c) is well-formed w.r.t. G and $L_c \leqslant i \leqslant L$, the claim holds. Now, assume that $L_c \leqslant j \leqslant L$. Since $G \models \mathrm{L}'_i = \mathrm{L}_j$ and $j < i$, by applying repeatedly Lemma 1(1), it follows that there is $j \leqslant h \leqslant i$ so that $G \models \mathrm{L}_h \leqslant \mathrm{L}'_h$. Since G is complete, either $G \models \mathrm{L}_h = \mathrm{L}'_h$ or $G \models \mathrm{L}_h < \mathrm{L}'_h$. The second condition cannot hold since $L_c \leqslant h \leqslant L$ and (L_c, U_c) is well-formed w.r.t. G. Thus, $G \models \mathrm{L}'_h = \mathrm{L}_h$. Hence, the claim holds. Since $j \leqslant h \leqslant i$ and G is balanced, we have that $G \models \mathrm{L}_j \lhd \mathrm{L}_h \lhd' \mathrm{L}_i$ and $G \models \mathrm{L}'_j \lhd \mathrm{L}'_h \lhd' \mathrm{L}'_i$ for some $\lhd, \lhd' \in \{<, =\}$. Since $G \models \mathrm{L}'_h = \mathrm{L}_h$ and $G \models \mathrm{L}'_i = \mathrm{L}_j$, it follows that $G \models \mathrm{L}_j \lhd \mathrm{L}_h = \mathrm{L}'_h \lhd' \mathrm{L}'_i = \mathrm{L}_j$. Thus, since G is satisfiable, $\lhd, \lhd' \in \{=\}$, hence, $G \models \mathrm{L}_i = \mathrm{L}_j$, and we are done.

Upper variables. This case is analogous to the previous case with the unique difference that now we use Lemma 2. Thus, we omit the details here. □

Notation. For a valuation ν over *Var*, $\nu[Var' \leftarrow Var]$ denotes the valuation over Var' defined as $\nu[Var' \leftarrow Var](x') = \nu(x)$ for each $x \in Var$.

4.2. Termination of simple GCS

First, we outline the proposed approach to solve termination for simple GCS. We define a polynomial-time checkable condition on simple GCS, called *termination condition*, such that the K-bounded approximation scheme is sound and complete w.r.t. this condition. We show that this condition characterizes the simple GCS $\mathcal{S}$ whose set $Inf_{\mathcal{S}}$ of non-terminating states is empty. Moreover, we show that $Inf_{\mathcal{S}}$ is effectively MG representable and one can compute separately and in polynomial-time the K-bounded approximation of the computable MG representation $\sigma(\mathcal{S})$ of $Inf_{\mathcal{S}}$ (we are not able to give an upper bound on the size of $\sigma(\mathcal{S})$). These results lead to polynomial-time algorithms to solve termination and termination w.r.t. a designated control point of simple GCS.

The rest of this subsection is organized as follows. After having formally defined the termination condition (Definition 15), we show by Proposition 11 that it represents a sufficient condition for emptiness of $Inf_{\mathcal{S}}$ (for the fixed simple GCS $\mathcal{S}$), and, additionally, the K-bounded approximation scheme is sound and complete w.r.t. this condition. Next, we provide by Lemma 9, a characterization of the set of non-terminating states of $\mathcal{S}$ under the assumption that $\mathcal{S}$ does not satisfy the termination condition. The characterization is given in terms of a subset of the lower and upper variables of G, called the set of *unconstrained variables for non-termination* (Definition 16). The characterization lemma is then used in the proof of the main result of this subsection (Theorem 3) to show that one can construct an MG representation of $Inf_{\mathcal{S}}$ whose K-bounded approximation can be computed in polynomial time. Finally, by using Lemma 9 and Lemma 3 in Section 4.1, we show (Theorem 4) that the termination condition is also a necessary condition for the emptiness of $Inf_{\mathcal{S}}$.

Termination condition

Definition 15 *(Termination condition).* We say that the fixed simple GCS $\mathcal{S}$ satisfies the termination condition if one of the following holds:

Lower variables: either $G \models \mathrm{L}_i < \mathrm{L}'_i$ for some $1 \leqslant i \leqslant L$,
or $G \models \mathrm{L}_i = \mathrm{L}'_i$ and $G \models \mathrm{L}'_j < \mathrm{L}_j$ for some $1 \leqslant i < j \leqslant L$.

Upper variables: either $G \models \mathrm{U}'_i < \mathrm{U}_i$ for some $1 \leqslant i \leqslant U$,
or $G \models \mathrm{U}_j = \mathrm{U}'_j$ and $G \models \mathrm{U}_i < \mathrm{U}'_i$ for some $1 \leqslant i < j \leqslant U$.

Intuitively, the above condition asserts that either there is a lower (resp., upper) variable of G in *Var* whose value strictly increases (resp., decreases) along each run of $\mathcal{S}$ from control point q, or there are two lower (resp., upper) variables of G in *Var* such that their distance strictly decreases along each run of $\mathcal{S}$ from q. Let $\mathcal{TC}$ be the class of simple GCS satisfying the termination condition. By Definition 15, we easily obtain the following result (by Proposition 9, $\lfloor \mathcal{S} \rfloor_K$ is a simple GCS).

Proposition 11. *$\mathcal{S} \in \mathcal{TC}$ if and only if $\lfloor \mathcal{S} \rfloor_K \in \mathcal{TC}$. Moreover, if $\mathcal{S} \in \mathcal{TC}$, then $Inf_{\mathcal{S}} = \emptyset$ and $Unb_{\mathcal{S}}$ does* not *contain states from control point q (i.e., each state from q is strongly terminating).*

Characterization of the set of non-terminating states. It remains to consider the case when $\mathcal{S} \notin \mathcal{TC}$. We first provide (under the assumption that $\mathcal{S} \notin \mathcal{TC}$), a characterization of the set of non-terminating states of $\mathcal{S}$ (Lemma 9). For this, we need additional definitions and preliminary results.

Definition 16 *(Unconstrained variables for non-termination).* We define two integers L_c and U_c as follows: L_c is the smallest $1 \leqslant i \leqslant L + 1$ such that $G \models \mathrm{L}_i = \mathrm{L}'_i$. Finally, U_c is the greatest $0 \leqslant i \leqslant U_c$ such that $G \models \mathrm{U}_i = \mathrm{U}'_i$. Note that $1 \leqslant L_c \leqslant L + 1$

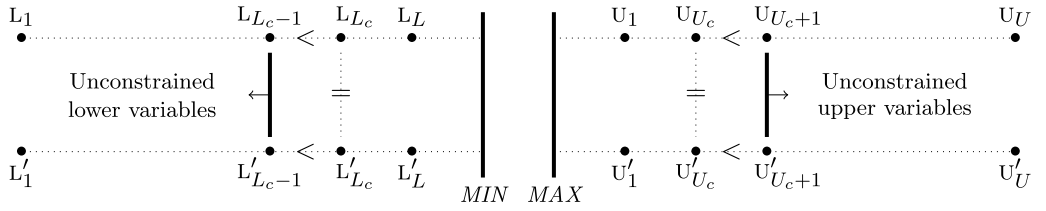

Fig. 6. Unconstrained variables for non-termination in the transitional MG G.

and $0 \leqslant U_c \leqslant U$. The set of *unconstrained variables in Var for non-termination*, written *Unc*, consists of the lower variables $\mathrm{L}_1 \ldots \mathrm{L}_{L_c-1}$ and the upper variables $\mathrm{U}_{U_c+1}, \ldots \mathrm{U}_U$. Let *Unc*′ be the corresponding subset in *Var*′. (See Fig. 6.)

By Definitions 15 and 16, evidently, the following holds.

Lemma 4. *For a valuation $\nu_0 : Var \to \mathbb{Z}$, the set of valuations $\{\nu_{(Var \setminus Unc)} \mid (q, \nu)$ is reachable from (q, ν_0) in $[\![\mathcal{S}]\!]\}$ is finite. Moreover, if $\mathcal{S} \notin \mathcal{TC}$, then the pair (L_c, U_c) is well-formed w.r.t. G.*

Moreover, we make the following observation.

Lemma 5. *Assume that $\mathcal{S} \notin \mathcal{TC}$. Then, the following hold*:

Lower variables: *for all* $1 \leqslant i < L_c$, $G \models \mathrm{L}_i < \mathrm{L}_{L_c}$.
Upper variables: *for all* $U_c < i \leqslant U$, $G \models \mathrm{U}_{U_c} < \mathrm{U}_i$.

Proof. We consider the case of the lower variables (the other case being similar). Let $1 \leqslant i < L_c$. We need to show that $G \models \mathrm{L}_i < \mathrm{L}_{L_c}$. We assume the contrary and derive a contradiction. Then, since G is complete and $G \models \mathrm{L}_i \leqslant \mathrm{L}_{L_c}$, it follows that $G \models \mathrm{L}_i = \mathrm{L}_{L_c}$. Since G is balanced, $G \models \mathrm{L}'_i = \mathrm{L}'_{L_c}$ holds as well. Thus, since, $G \models \mathrm{L}_{L_c} = \mathrm{L}'_{L_c}$, we obtain that $G \models \mathrm{L}_i = \mathrm{L}'_i$ with $i < L_c$, which contradicts the definition of L_c. Hence, the result follows. □

The intuitive meaning of the unconstrained lower (resp., upper) variables is that under the assumption that $\mathcal{S} \notin \mathcal{TC}$, they can increase (resp., decrease) arbitrarily along a run of $\mathcal{S}$ from control point q. This does not mean that the unconstrained variables can get arbitrary values, but that the distances (gaps) between primed variables x' and y' in *Unc*′ such that $G \models x' \neq y'$ are *not* constrained by the values of the variables in *Var* and the constants in *Const*, i.e. they are unbounded. In other terms, the unique ordering constraint imposed by G on the variables in $Unc' = \{\mathrm{L}'_1 \ldots \mathrm{L}'_{L_c-1}, \mathrm{U}'_{U_c+1}, \ldots, \mathrm{U}'_U\}$ is the following one

$$G \models \mathrm{L}'_1 \leqslant \cdots \leqslant \mathrm{L}'_{L_c-1} < \mathrm{L}'_{L_c} \leqslant MIN \leqslant MAX \leqslant \mathrm{U}'_{U_c} < \mathrm{U}'_{U_c+1} \leqslant \cdots \leqslant \mathrm{U}'_U.$$

This is formalized by the following lemma.

Lemma 6. *Assume that $\mathcal{S} \notin \mathcal{TC}$. Then, the following hold*:

Lower variables: *for all* $1 \leqslant i \leqslant L$ *and* $1 \leqslant j < L_c$, $G \not\models \mathrm{L}_i \leqslant \mathrm{L}'_j$.
Upper variables: *for all* $U_c < i \leqslant U$ *and* $1 \leqslant j \leqslant U$, $G \not\models \mathrm{U}'_i \leqslant \mathrm{U}_j$.

Proof. *Lower variables*. Let $1 \leqslant i \leqslant L$ and $1 \leqslant j < L_c$. We need to show that $G \not\models \mathrm{L}_i \leqslant \mathrm{L}'_j$. We assume the contrary and derive a contradiction. Hence, $G \models \mathrm{L}_i \leqslant \mathrm{L}'_j$. We distinguish two cases:

- $j \leqslant i$: hence, $G \models \mathrm{L}_j \leqslant \mathrm{L}_i$. Since $G \models \mathrm{L}_i \leqslant \mathrm{L}'_j$, it follows that $G \models \mathrm{L}_j \leqslant \mathrm{L}'_j$.
- $j > i$: since $G \models \mathrm{L}_i \leqslant \mathrm{L}'_j$, by applying repeatedly Lemma 1(1), it follows that there is $i \leqslant h \leqslant j$ such that $G \models \mathrm{L}_h \leqslant \mathrm{L}'_h$.

Thus, in both cases we obtain that $G \models \mathrm{L}_k \leqslant \mathrm{L}'_k$ for some $1 \leqslant k < L_c$. Since G is complete, it follows that $G \models \mathrm{L}_k \lhd \mathrm{L}'_k$ for some $\lhd \in \{=, <\}$, which is a contradiction by definition of L_c (Definition 16) and the hypothesis that $\mathcal{S} \notin \mathcal{TC}$. Hence, the result follows.

Upper variables. This case is analogous to the previous one with the difference that now we use Lemma 2(1). Thus, we omit the details here. □

Now, in order to provide a characterization of the set of non-terminating states of $\mathcal{S}$, we give two preliminary technical lemmata (Lemmata 7 and 8 below).

Let $\succeq_G$ be the partial order (depending on the MG G) on the set of valuations over Var defined as follows: $\nu' \succeq_G \nu$ iff the following properties are satisfied:

- for each bounded variable $\mathtt{B}_i$ of G in Var, $\nu'(\mathtt{B}_i) = \nu(\mathtt{B}_i)$;
- for all $u, v \in Var \cup Const$ and $\lhd \in \{<, =\}$, $\nu(u) \lhd \nu(v)$ iff $\nu'(u) \lhd \nu'(v)$;
- for all $u, v \in Var \cup Const$, if $\nu(u) - \nu(v) \geqslant 0$, then $\nu'(u) - \nu'(v) \geqslant \nu(u) - \nu(v)$.

Lemma 7 *(Simulation lemma). Let $\nu_1 \oplus \nu_2 \in Sat(G)$ and $\nu_1' \succeq_G \nu_1$. Then, $\nu_1' \oplus \nu_2' \in Sat(G)$ for some valuation ν_2' over Var such that $\nu_2' \succeq_G \nu_2$.*

Proof. By definition of $\succeq_G$, ν_1' and ν_1 agree on the set of bounded variables of G in Var. Moreover, since $\nu_1 \oplus \nu_2 \in Sat(G)$, $\nu_1 \oplus \nu_2$ induces an ordering of the upper and lower variables of G which is consistent with the constraints of G. Also, by definition of $\succeq_G$, ν_1' induce the same ordering of the upper and lower variables in Var as ν_1, with the following additional constraint: the distance between the values of two consecutive (upper and lower) variables u, v in Var such that $G \not\models u = v$ or the distance between a lower (resp., upper) variable and MIN (resp., MAX) is greater than that associated with ν_1. Hence, the existence of a valuation ν_2' such that $\nu_1' \oplus \nu_2' \in Sat(G)$ and satisfying the additional requirement $\nu_2' \succeq_G \nu_2$ easily follows. □

The simulation lemma ensures that the existence of a non-null finite run π of $\mathcal{S}$ from a state (q, ν) to a state (q, ν') such that $\nu' \succeq_G \nu$ implies, in turn, the existence of a non-null run of $\mathcal{S}$ from state (q, ν') to a state of the form (q, ν'') satisfying $\nu'' \succeq_G \nu'$ (hence, by iterating the reasoning, it follows that there exists also an infinite run of $\mathcal{S}$ from state (q, ν)).

Under the assumption that $\mathcal{S} \notin \mathcal{TC}$, the following technical lemma (whose proof is based on Lemma 6) provides for a given state of $\mathcal{S}$ of the form (q, ν), a sufficient condition for the existence of a non-null finite run π from (q, ν) to a state (q, ν') satisfying $\nu' \succeq_G \nu$ (the finite run π can be then "pumped" arbitrarily many times by repeatedly applying the simulation lemma).

Lemma 8 *(Pumping lemma for non-termination). Assume that $\mathcal{S} \notin \mathcal{TC}$. Let (q, ν) be a state of $\mathcal{S}$ and π be a non-null finite run of $\mathcal{S}$ from (q, ν) leading to a state (q, ν') such that ν and ν' agree on the variables in $Var \setminus Unc$. Then, there exists a non-null finite run π' of $\mathcal{S}$ from (q, ν) leading to a state (q, ν'') such that $\nu'' \succeq_G \nu$.*

Proof. Let π be as in the statement of the lemma. Hence, π can be written in the form

$$(q, \nu) \to \cdots \to (q, \nu_0) \to \left(q, \nu'\right)$$

such that ν and ν' agree on the variables in $Var \setminus Unc$. Note that $\nu_0 \oplus \nu' \in Sat(G)$. We prove that there is a valuation ν'' over Var such that $\nu_0 \oplus \nu'' \in Sat(G)$ and $\nu'' \succeq_G \nu$. Hence, the lemma follows. Let Δ be the maximum over the edge weights of G. First, we show the following.

Claim. *There is a valuation ν'' over Var satisfying the following properties*:

1. *ν'' and ν agree on $Var \setminus Unc$*;
2. *$\nu'' \succeq_G \nu$*;
3. *$\nu''[Var' \leftarrow Var]$ is a solution of the restriction of G to Var'*;
4. *for each upper variable $\mathtt{U}_i \in Unc$ (hence, $U_c < i \leqslant U$), $\nu''(\mathtt{U}_i) - \nu_0(\mathtt{U}_U) > \Delta$*;
5. *for each lower variable $\mathtt{L}_i \in Unc$ (hence, $1 \leqslant i < L_c$), $\nu_0(\mathtt{L}_1) - \nu''(\mathtt{L}_i) > \Delta$.*

Proof of the claim. Recall that $Unc = \{\mathtt{L}_1, \ldots, \mathtt{L}_{L_c-1}, \mathtt{U}_{U_c+1}, \ldots, \mathtt{U}_U\}$ and for each $x \in Var \setminus Unc$, $G \models \mathtt{L}_{L_c} \leqslant x \leqslant \mathtt{U}_{U_c}$. Moreover, by Lemma 5, for all $\mathtt{L}_i, \mathtt{U}_j \in Unc$, $G \models \mathtt{L}_i < \mathtt{L}_{L_c} \leqslant \mathtt{U}_{U_c} < \mathtt{U}_j$. By hypothesis, $\nu \in Sat(G_{Var})$. Thus, since $Var \setminus Unc$ contains the set of bounded variables of G in Var, we easily deduce the existence of a valuation $\nu'' \in Sat(G_{Var})$ satisfying Properties 1, 2, 4, and 5 of the claim. Now, by hypothesis, $\nu_0 \oplus \nu' \in Sat(G)$ and ν and ν' agree on $Var \setminus Unc$. Hence, the restriction of $\nu[Var' \leftarrow Var]$ to $Var' \setminus Unc'$ is a solution of $G_{Var' \setminus Unc'}$. Since G is balanced, it follows that ν'' can be chosen in such a way that Property 3 in the claim holds as well. □

Let ν'' be a valuation over Var satisfying the claim above. We prove that $\nu_0 \oplus \nu'' \in Sat(G)$. Thus, since $\nu'' \succeq_G \nu$ (Property 2 of the claim), the lemma follows. By hypothesis $\nu_0 \oplus \nu' \in Sat(G)$ and ν and ν' agree on the variables in $Var \setminus Unc$. Thus, by Property 1 of the claim, the restriction of $\nu_0 \oplus \nu''$ to $Var \cup (Var' \setminus Unc')$ is a solution of the restriction of G to $Var \cup (Var' \setminus Unc')$. Thus, by Property 3 in the claim, in order to prove that $\nu_0 \oplus \nu'' \in Sat(G)$, it remains to show that for each edge $e = x \xrightarrow{k} y'$ (resp., $e = y' \xrightarrow{k} x$) of G such that $x \in Var$ and $y' \in Unc'$, it holds that $\nu_0(x) - \nu''(y) \geqslant k$ (resp., $\nu''(y) - \nu_0(x) \geqslant k$).

Case $e = x \xrightarrow{k} y'$ **with** $x \in Var$ **and** $y \in Unc$**:** first, we show that y is not an upper variable. We assume the contrary and derive a contradiction. Hence, $y = \mathrm{U}_i$ for some $U_c < i \leqslant U$. Then, x must be an upper variable U_j for some $1 \leqslant j \leqslant U$. Since $\mathcal{S} \notin \mathcal{TC}$, by Lemma 6, $G \not\models \mathrm{U}'_i \leqslant \mathrm{U}_j$, which is a contradiction. Thus, $y = \mathrm{L}_i \in Unc$ for some $1 \leqslant i < L_c$. Since $\nu_0 \in Sat(G_{Var})$, it holds that $\nu_0(x) \geqslant \nu_0(\mathrm{L}_1)$. Hence, by Property 5 of the claim above, we obtain $\nu_0(x) - \nu''(y) \geqslant \nu_0(\mathrm{L}_1) - \nu''(y) > \Delta \geqslant k$, and the result follows.

Case $e = y' \xrightarrow{k} x$ **with** $x \in Var$ **and** $y \in Unc$**:** first, we show that y is not a lower variable. We assume the contrary and derive a contradiction. Hence, $y = \mathrm{L}_j$ for some $1 \leqslant j < L_c$. Then, x must be a lower variable L_i for some $1 \leqslant i \leqslant L$. Since $\mathcal{S} \notin \mathcal{TC}$, by Lemma 6, $G \not\models \mathrm{L}_i \leqslant \mathrm{L}'_j$, which is a contradiction. Thus, $y = \mathrm{U}_i \in Unc$ for some $U_c < i \leqslant U$. Since $\nu_0 \in Sat(G_{Var})$, it holds that $\nu_0(x) \leqslant \nu_0(\mathrm{U}_U)$. Hence, by Property 4 of the claim above, we obtain $\nu''(y) - \nu_0(x) \geqslant \nu''(y) - \nu_0(\mathrm{U}_U) > \Delta \geqslant k$, and the result follows.

This concludes the proof of the pumping lemma. □

By Lemmata 4, 7 and 8, we obtain the following characterization of the set of states in $Inf_{\mathcal{S}}$ (under the assumption that $\mathcal{S} \notin \mathcal{TC}$).

Lemma 9 *(Characterization lemma for non-termination). Let $\mathcal{S} \notin \mathcal{TC}$ and s be a state of $\mathcal{S}$. Then, $s \in Inf_{\mathcal{S}}$ iff there are a state (q, ν) reachable from s in $[\![\mathcal{S}]\!]$ and a non-null run of $\mathcal{S}$ from (q, ν) to a state (q, ν') such that ν and ν' agree in $Var \setminus Unc$.*

Proof. Let $\mathcal{S} \notin \mathcal{TC}$ and s be a state of $\mathcal{S}$. For the right implication $\Rightarrow$, assume that $s \in Inf_{\mathcal{S}}$. Hence, there is an infinite run from s in $\mathcal{S}$. Then, by Lemma 4, the result follows.

For the left implication $\Leftarrow$, assume that there is a state (q, ν) reachable from s in $[\![\mathcal{S}]\!]$ and a non-null run π of $\mathcal{S}$ from (q, ν) to a state (q, ν') such that ν and ν' agree in $Var \setminus Unc$. By applying the pumping lemma (Lemma 8) to the non-null run π, it follows that there is a non-null finite run π' in $\mathcal{S}$ from state (q, ν) to a state (q, ν'') such that $\nu'' \succeq_G \nu$. Thus, by applying repeatedly Lemma 7, we deduce that there is an infinite run of $\mathcal{S}$ from (q, ν). Since (q, ν) is reachable from s in $[\![\mathcal{S}]\!]$, we obtain that $s \in Inf_{\mathcal{S}}$, which concludes. □

Construction of an MG *representation of $Inf_{\mathcal{S}}$.* By using the characterization lemma for non-termination (Lemma 9), we can prove the main result of this subsection.

Theorem 3. *The set $Inf_{\mathcal{S}}$ is* MG *representable and one can construct an* MG *representation of $Inf_{\mathcal{S}}$, written $\sigma(\mathcal{S})$, satisfying the following*:

1. $\lfloor \sigma(\mathcal{S}) \rfloor_K$ *can be computed in polynomial time*;
2. $\lfloor \sigma(\mathcal{S}) \rfloor_K = \lfloor \sigma(\lfloor \mathcal{S} \rfloor_K) \rfloor_K$ ($\lfloor \mathcal{S} \rfloor_K$ *is a simple* GCS).

Proof. First, assume that $\mathcal{S} \in \mathcal{TC}$. Then, by Proposition 11, $Inf_{\mathcal{S}} = Inf_{\lfloor \mathcal{S} \rfloor_K} = \emptyset$, hence the result trivially holds. Now, assume that $\mathcal{S} \notin \mathcal{TC}$. By Theorem 2, one can compute a *finite* set $\mathcal{P}_{\mathcal{S}}$ of non-null finite paths of $\mathcal{S}$ from q to q such that for each non-null finite path $\wp'$ of $\mathcal{S}$ from q to q, there is a path $\wp \in \mathcal{P}$ so that $\rightsquigarrow_{\wp'}$ implies $\rightsquigarrow_{\wp}$. Let $G_{=,\mathcal{S}}$ be the transitional MG (depending on $\mathcal{S}$) corresponding to the GC given by $\bigwedge_{x \in Var \setminus Unc} x' = x$ and $\mathcal{G}_{\mathcal{S}}$ be the set of transitional MG given by

$$\mathcal{G}_{\mathcal{S}} = \left\{ G_{\wp} \bullet (G_{\wp'} \sqcap G_{=,\mathcal{S}}) \;\middle|\; \wp, \wp' \in \mathcal{P}_{\mathcal{S}} \right\} \cup \{ G_{\wp} \sqcap G_{=,\mathcal{S}} \mid \wp \in \mathcal{P}_{\mathcal{S}} \}$$

where for each $\wp \in \mathcal{P}_{\mathcal{S}}$, $G_{\wp}$ is the transitional MG associated with the path $\wp$, which characterizes the reachability relation $\rightsquigarrow_{\wp}$. Then, $\sigma(\mathcal{S}) = \{\sigma(\mathcal{S})_{q_0}, \sigma(\mathcal{S})_q\}$ where

$$\sigma(\mathcal{S})_q = \left\{ G' \;\middle|\; G' \text{ is the projection of } G'' \text{ over } Var \text{ for some } G'' \in \mathcal{G}_{\mathcal{S}} \right\},$$
$$\sigma(\mathcal{S})_{q_0} = \left\{ G' \;\middle|\; G' \text{ is the projection of } G_0 \bullet G'' \text{ over } Var \text{ for some } G'' \in \mathcal{G}_{\mathcal{S}} \right\}.$$

Correctness of the construction easily follows from Lemma 9 and Theorem 2. It remains to prove Properties 1 and 2.

Proof of Property 1. By Definition 6, for all transitional MG G' and G'', $G' \bullet G'' = \overline{\overline{G'} \bullet \overline{G''}}$. Thus, $\sigma(\mathcal{S})_q$ and $\sigma(\mathcal{S})_{q_0}$ can be rewritten as:

$$\sigma(\mathcal{S})_q = \left\{ \left(\overline{G'}\right)_{Var} \;\middle|\; G' \in \mathcal{G}_{\mathcal{S}} \right\} \quad \text{and} \quad \sigma(\mathcal{S})_{q_0} = \left\{ \left(G_0 \bullet G'\right)_{Var} \;\middle|\; G' \in \mathcal{G}_{\mathcal{S}} \right\}.$$

Thus, by Propositions 6 and 7, we obtain

$$\left\lfloor \sigma(\mathcal{S})_q \right\rfloor_K = \left\{ \left(\left\lfloor \overline{G'} \right\rfloor_K \right)_{Var} \;\middle|\; G' \in \lfloor \mathcal{G}_{\mathcal{S}} \rfloor_K \right\}, \tag{1}$$
$$\left\lfloor \sigma(\mathcal{S})_q \right\rfloor_K = \left\{ \left(\left\lfloor \lfloor G_0 \rfloor_K \bullet G' \right\rfloor_K \right)_{Var} \;\middle|\; G' \in \lfloor \mathcal{G}_{\mathcal{S}} \rfloor_K \right\}. \tag{2}$$

Now, let us consider the set $\lfloor \mathcal{G}_{\mathcal{S}} \rfloor_K$. Note that for each non-null finite path $\wp$ from q, $G_\wp$ is given by G^k for some $k \geqslant 1$. Since G is idempotent, by Proposition 7, we obtain that for each $\wp \in \mathcal{P}_{\mathcal{S}}$, $\lfloor G_\wp \rfloor_K = \lfloor G \rfloor_K$. Since $G_{=,\mathcal{S}}$ is K-bounded, applying again Proposition 7, we obtain

$$\lfloor \mathcal{G}_{\mathcal{S}} \rfloor_K = \left\{ \left\lfloor \lfloor G \rfloor_K \bullet \left(\lfloor G \rfloor_K \sqcap G_{=,\mathcal{S}} \right) \right\rfloor_K, \lfloor G \rfloor_K \sqcap G_{=,\mathcal{S}} \right\}. \tag{3}$$

By equalities (1)–(3), Property 1 follows. □

Proof of Property 2. By Proposition 11, $\lfloor \mathcal{S} \rfloor_K$ is a simple GCS such that $\lfloor \mathcal{S} \rfloor_K \notin \mathcal{TC}$. Moreover, the sets of unconstrained variables of $\mathcal{S}$ and $\lfloor \mathcal{S} \rfloor_K$ coincide. Hence, $G_{=,\lfloor \mathcal{S} \rfloor_K} = G_{=,\mathcal{S}}$. By equality (3), it follows that $\lfloor \mathcal{G}_{\lfloor \mathcal{S} \rfloor_K} \rfloor_K = \lfloor \mathcal{G}_{\mathcal{S}} \rfloor_K$. Thus, by equalities (1)–(2), $\lfloor \sigma(\mathcal{S}) \rfloor_K = \lfloor \sigma(\lfloor \mathcal{S} \rfloor_K) \rfloor_K$, and we are done. This concludes the proof of Theorem 3. □

Additional results on the termination condition. By using the characterization lemma for non-termination (Lemma 9) and Lemma 3 in Section 4.1, we show that the termination condition is also a necessary condition for emptiness of $Inf_{\mathcal{S}}$.

Theorem 4. *If $\mathcal{S} \notin \mathcal{TC}$, then the set of states s with control point q_0 (resp., q) such that $s \in Inf_{\mathcal{S}}$ is non-empty.*

Proof. Let $\mathcal{S} \notin \mathcal{TC}$. Evidently, it suffices to prove that the set of states s with control point q_0 such that $s \in Inf_{\mathcal{S}}$ is non-empty. Then, by the characterization lemma (Lemma 9), it suffices to show that there are $k \geqslant 1$, $n \geqslant 1$, and valuations ν_0, ν, and ν' over Var such that $(\nu_0 \oplus \nu) \in Sat(G_0 \bullet G^k)$, $(\nu \oplus \nu') \in Sat(G^n)$, and ν and ν' agree on $Var \setminus Unc$. Recall that for all $k \geqslant 1$ and $n \geqslant 1$, $G_0 \bullet G^k$ and G^n are satisfiable (Proposition 10). Thus, by definition of the composition operator and Proposition 4(2), $G_0 \bullet G^k$ and G^n are normalized if $n > 1$. Therefore, by Proposition 4(1), the result directly follows from the following claim, whose proof is given below.

Claim. *There are $k \geqslant 1$, $n > 1$, and a valuation ν over Var satisfying the following*:

1. *$(\nu \oplus \nu)_{Var \cup (Var' \setminus Unc')}$ is a solution of the restriction of G^n to $Var \cup (Var' \setminus Unc')$;*
2. *$\nu[Var' \leftarrow Var]$ is a solution of the restriction of $G_0 \bullet G^k$ to Var'.*

Proof of the claim. Recall that for each bounded variable $\mathrm{B}_i \in \mathcal{B}$, $G \models MIN \leqslant \mathrm{B}_i \leqslant MAX$. Thus, since $G_0 \bullet G^h$ is satisfiable for all $h \geqslant 1$, it follows that there are $k \geqslant 1$, $n > 1$, and a valuation ν_0 over Var such that

- $(\nu_0 \oplus \nu_0)_{\mathcal{B} \cup \mathcal{B}'}$ is a solution of the restriction of G^n to $\mathcal{B} \cup \mathcal{B}'$;
- $\nu_0[Var' \leftarrow Var]$ is a solution of the restriction of $G_0 \bullet G^k$ to Var'.

Thus, if $Var = \mathcal{B}$, then the result follows. Now, assume that $Var \setminus \mathcal{B} \neq \emptyset$. For a valuation ν over Var, let $N(\nu)$ be the natural number defined as

$$N(\nu) \stackrel{\text{def}}{=} \min\left(\left\{ \left| \nu(u) - \nu(v) \right| \;\middle|\; u \in Var \cup Const, v \in Var \setminus \mathcal{B} \text{ and } G \not\models v = u \right\} \right).$$

Since G is idempotent and for each variable $x \in Var \setminus \mathcal{B}$, either $G \models x < MIN$ or $G \models MAX < x$, it follows that for all $H \geqslant 1$, there is a valuation ν over Var such that $N(\nu) \geqslant H$, ν is a solution of the restriction of G^n to Var, and ν and ν_0 agree on $\mathcal{B}$. We choose ν in such a way that $N(\nu) \geqslant \max(\{\Delta_n, \Delta_{0,k}\})$, where Δ_n (resp., $\Delta_{0,k}$) is the maximum over the edge weights of G^k (resp., $G_0 \bullet G^k$). Now, we show that ν satisfies Properties 1 and 2 of the claim.

- *Property* 1. Since G is idempotent and balanced, by construction and definition of $N(\nu)$, we easily deduce the following:
  - $\nu[Var' \leftarrow Var]$ is a solution of the restriction of G^n to Var';
  - $(\nu \oplus \nu)_{Var \cup \mathcal{B}'}$ is a solution of the restriction of G^n to $Var \cup \mathcal{B}'$.

  Thus, since $(Var' \setminus Unc') \setminus \mathcal{B}' = \{\mathrm{L}'_{L_c}, \ldots, \mathrm{L}'_L, \mathrm{U}'_1, \ldots, \mathrm{U}'_{U_c}\}$, it remains to show that for all $x \in Var$ and $y \in \{\mathrm{L}_{L_c}, \ldots, \mathrm{L}_L, \mathrm{U}_1, \ldots, \mathrm{U}_{U_c}\}$, whenever $x \xrightarrow{k} y'$ (resp., $y' \xrightarrow{k} x$) is an edge of G^n, then $\nu(x) - \nu(y) \geqslant k$ (resp., $\nu(y) - \nu(x) \geqslant k$). We consider the edges of the form $x \xrightarrow{k} y'$ (for the other edges, the proof is similar). Thus, let $x \xrightarrow{k} y'$ be an edge of G^n such that $x \in Var$ and $y \in \{\mathrm{L}_{L_c}, \ldots, \mathrm{L}_L, \mathrm{U}_1, \ldots, \mathrm{U}_{U_c}\}$. We need to show that $\nu(x) - \nu(y) \geqslant k$. Since G is idempotent and complete, either $G \models y' < x$, or $G \models y' = x$ and $k = 0$. Since $\mathcal{S} \notin \mathcal{TC}$, by Lemma 4, the pair (L_c, U_c) is well-formed w.r.t. G. Hence, we can apply Lemma 3, obtaining that *either* $G \models y < x$ and $G^n \models y < x$, *or* $G \models y = x$, $G^n \models y = x$, and $k = 0$. Since ν is a solution of the restriction of G^n to Var, by definition of $N(\nu)$, we obtain that *either* $\nu(x) - \nu(y) \geqslant N(\nu)$, *or* $\nu(x) - \nu(y) = 0$ and $k = 0$. Thus, since $N(\nu) \geqslant \Delta_n \geqslant k$, the result follows.
- *Property* 2. Since G is complete, by the definition of the composition operator, G and $G_0 \bullet G^k$ induce the same total ordering on $Var' \cup Const$. Thus, since G is balanced, $N(\nu) \geqslant \Delta_{0,k}$, ν and ν_0 agree on $\mathcal{B}$, and $\nu_0[Var' \leftarrow Var]$ is a solution of the restriction of $G_0 \bullet G^k$ to Var', it follows that ν satisfies Property 2 in the claim, which concludes. □

By Proposition 11 and Theorem 4, it follows that the termination condition represents a criterion for checking termination and termination w.r.t. a designated control point of simple GCS. Hence, we obtain the following result.

Corollary 1. *The termination problem and the termination problem w.r.t. a designated control point of simple* GCS *can be solved in polynomial time.*

Note that Corollary 1 can also be directly deduced from Property 1 of Theorem 3. We conclude this subsection by making the following observation, which will be used in Section 4.3.

Corollary 2. *For each state s of $\mathcal{S}$ with control point q, $s \in Unb_{\mathcal{S}}$* iff *$s \in Inf_{\mathcal{S}}$.*

Proof. The result easily follows from Proposition 11, Lemma 4, and Lemma 9. □

4.3. Strong termination for simple GCS

First, we outline the proposed approach to solve strong termination for simple GCS. We define a polynomial-time checkable condition on simple GCS, called *unboundedness condition*, such that the K-bounded approximation scheme is sound and complete w.r.t. this condition. We show that this condition characterizes the simple GCS whose set of unbounded states with initial control point is non-empty. By Proposition 11, Theorem 4, and Corollary 2, the termination condition characterizes the simple GCS such that the set of unbounded states whose control point is the one associated with the self-loop is empty. Thus, we obtain polynomial-time algorithms to solve strong termination and strong termination w.r.t. a designated control point of simple GCS. Moreover, we show that $Unb_{\mathcal{S}}$ is effectively MG representable and one can compute separately and in polynomial time the K-bounded approximation of the computable MG representation $\sigma(\mathcal{S})$ of $Unb_{\mathcal{S}}$ (we are not able to give an upper bound on the size of $\sigma(\mathcal{S})$).

The rest of this subsection is organized as follows. After having formally defined the unboundedness condition (Definition 18), we show by Proposition 12 that it represents a necessary condition for the existence of unbounded states with initial control point, and, additionally, the K-bounded approximation scheme is sound and complete w.r.t. the unboundedness condition. Next, we provide by Lemma 15, a characterization of the set of unbounded states of $\mathcal{S}$ with initial control point under the assumption that $\mathcal{S}$ satisfies the unbounded condition. Similarly to the characterization lemma for non-termination, the unboundedness characterization is given in terms of a subset of the lower and upper variables of G, called the set of *unconstrained variables for unboundedness* (Definition 19) (however, here, the proof of the characterization lemma is more involved). The characterization lemma is then used in the main result of this subsection (Theorem 5) to show that one can construct an MG representation of $Unb_{\mathcal{S}}$ whose K-bounded approximation can be computed in polynomial time. Finally, by using Lemma 15 and Lemma 3 in Section 4.1, we show (Theorem 6) that the unboundedness condition is also a sufficient condition for the existence of unbounded states with initial control point.

Unboundedness condition. In order to define the unboundedness condition, we need the following preliminary definition.

Definition 17. The transitional MG G_0 (associated with the edge from the initial control point of the fixed simple GCS $\mathcal{S}$) is *bounded* if the following hold:

- for all $1 \leqslant i \leqslant L$, $G_0 \models \mathrm{L} \leqslant \mathrm{L}'_i$ for some lower variable L of G_0 in Var;
- for all $1 \leqslant i \leqslant U$, $G_0 \models \mathrm{U}'_i \leqslant \mathrm{U}$ for some upper variable U of G_0 in Var.

Thus, G_0 is bounded if each lower (resp., upper) variable of G in Var' is lower (resp., upper) bounded in G_0 by a lower (resp., upper) variable of G_0 in Var. Recall that

$$G \models \mathrm{L}_1 \lhd_2 \cdots \lhd_L \mathrm{L}_L < MIN \leqslant \mathrm{B}_1 \lhd'_2 \cdots \lhd'_B \mathrm{B}_B \leqslant MAX < \mathrm{U}_1 \lhd''_2 \cdots \lhd''_U \mathrm{U}_U$$

where $\lhd_2 \cdots \lhd_L, \lhd'_2 \cdots \lhd'_B, \lhd''_2 \cdots \lhd''_U \in \{<, =\}$. Since $G_0 \bullet G$ is satisfiable and G and G_0 are complete, it follows that

$$G_0 \models \mathrm{L}'_1 \lhd_2 \cdots \lhd_L \mathrm{L}'_L < MIN \leqslant \mathrm{B}'_1 \lhd'_2 \cdots \lhd'_B \mathrm{B}'_B \leqslant MAX < \mathrm{U}'_1 \lhd''_2 \cdots \lhd''_U \mathrm{U}'_U.$$

Hence, the total ordering induced by the complete MG G_0 over $Var' \cup Const$ corresponds to the total ordering induced by G on $Var \cup Const$. As a consequence, boundedness of G_0 ensures that for each state s_0 with control point q_0, the set of states reachable in $[\![\mathcal{S}]\!]$ from s_0 in a single step is finite.

Definition 18 *(Unboundedness condition).* We say that the fixed simple GCS $\mathcal{S}$ *satisfies the unboundedness condition* if one of the following holds:

- *either* G_0 is bounded and $\mathcal{S} \notin \mathcal{TC}$,
- *or* G_0 is *not* bounded and **none** of the following properties holds:
  lower variables: there is a lower variable $\mathtt{l}$ of G_0 in *Var* such that
  – *either* $G_0 \models \mathtt{l} \leqslant \mathtt{l}'_i$ and $G \models \mathtt{l}_i < \mathtt{l}'_i$ for some $1 \leqslant i \leqslant L$,
  – *or* $G_0 \models \mathtt{l} \leqslant \mathtt{l}'_i$, $G \models \mathtt{l}_i = \mathtt{l}'_i$, and $G \models \mathtt{l}'_j < \mathtt{l}_j$ for some $1 \leqslant i < j \leqslant L$.
  upper variables: there is an upper variable $\mathtt{u}$ of G_0 in *Var* such that
  – *either* $G_0 \models \mathtt{u}'_i \leqslant \mathtt{u}$ and $G \models \mathtt{u}'_i < \mathtt{u}_i$ for some $1 \leqslant i \leqslant U$,
  – *or* $G_0 \models \mathtt{u}'_i \leqslant \mathtt{u}$, $G \models \mathtt{u}_i = \mathtt{u}'_i$, and $G \models \mathtt{u}'_j > \mathtt{u}_j$ for some $1 \leqslant j < i \leqslant U$.

Intuitively, the unboundedness condition requires that $\mathcal{S}$ does not satisfy the termination condition if G_0 is bounded, and the following hold otherwise: (i) there is no lower (resp., upper) variable of G in Var' – or equivalently of G in *Var* – whose value strictly increases (resp., decreases) along each run of $\mathcal{S}$ and at the same time is lower (resp., upper) bounded in G_0 by a lower (resp., upper) variable of G_0 in *Var*, and (ii) there is no pair of lower (resp., upper) variables of G in Var' whose distance strictly decreases along each run of $\mathcal{S}$, and at the same time is lower (resp., upper) bounded in G_0 by a lower (resp., upper) variable of G_0 in *Var*. Let $\mathcal{UC}$ be the class of simple GCS satisfying the unboundedness condition. We make the following observation.

Proposition 12. *$\mathcal{S} \in \mathcal{UC}$ if and only if $\lfloor \mathcal{S} \rfloor_K \in \mathcal{UC}$. Moreover, if $\mathcal{S} \notin \mathcal{UC}$, then all the states with initial control point q_0 are strongly terminating.*

Proof. The first part of the proposition easily follows from Definitions 15, 17, and 18. For the second part of the proposition, assume that $\mathcal{S} \notin \mathcal{UC}$, and let s_0 be a state with control point q_0. We need to show that s_0 is strongly terminating. We distinguish two cases:

- G_0 is bounded: hence, the set of states reachable from s_0 in a single step is finite (note that these states have control point q). Thus, it suffices to show that each state from control point q is strongly terminating. Since $\mathcal{S} \notin \mathcal{UC}$, by Definition 18, $\mathcal{S} \in \mathcal{TC}$. Thus, by Proposition 11, the result follows in this case.
- G_0 is not bounded: since $\mathcal{S} \notin \mathcal{UC}$, by Definition 18, either the condition for the lower variables or the condition for the upper variable in Definition 18 is satisfied. Hence, the result easily follows. □

Characterization of the set of unbounded states with initial control point. It remains to consider the case when $\mathcal{S} \in \mathcal{UC}$. We first provide (under the assumption that $\mathcal{S} \in \mathcal{UC}$), a characterization of the set of unbounded states of $\mathcal{S}$ with control point q_0. This characterization is similar to the characterization lemma for non-termination given in Section 4.2 (Lemma 9), but the set *Unc* of unconstrained variables is defined differently.

Definition 19 *(Unconstrained variables for unboundedness).* We define four integers L_0, U_0, L_c, and U_c as follows: L_0 is the smallest $1 \leqslant i \leqslant L$ such that $G_0 \models \mathtt{l} \leqslant \mathtt{l}'_i$ for some lower variable $\mathtt{l}$ of G_0 in *Var* (if such an i does not exist, we set $L_0 = L+1$), while U_0 is the greatest $1 \leqslant i \leqslant U$ such that $G_0 \models \mathtt{u}'_i \leqslant \mathtt{u}$ for some upper variable $\mathtt{u}$ of G_0 in *Var* (if such an i does not exist, we set $U_0 = 0$). Moreover, L_c and U_c are defined as in Definition 16 if G_0 is bounded, and as follows otherwise: L_c is the smallest $L_0 \leqslant i \leqslant L+1$ such that $G \models \mathtt{l}_i = \mathtt{l}'_i$, while U_c is the greatest $0 \leqslant i \leqslant U_0$ such that $G \models \mathtt{u}'_i = \mathtt{u}_i$. Note that if G_0 is *not* bounded, $1 \leqslant L_0 \leqslant L_c \leqslant L+1$ and $0 \leqslant U_c \leqslant U_0 \leqslant U$. The set of *unconstrained variables w.r.t. G_0 in Var*, written Unc_0, consists of the lower variables $\mathtt{l}_1 \ldots \mathtt{l}_{L_0-1}$ and the upper variables $\mathtt{u}_{U_0+1}, \ldots, \mathtt{u}_U$. We denote by $Unc_0{}'$ the corresponding set in Var'. Moreover, the set of *unconstrained variables for unboundedness in Var*, written *Unc*, consists of the lower variables $\mathtt{l}_1 \ldots \mathtt{l}_{L_c-1}$ and the upper variables $\mathtt{u}_{U_c+1}, \ldots, \mathtt{u}_U$. We denote by Unc' the corresponding set in Var'. Note that if G_0 is *not* bounded, then $Unc_0 \subseteq Unc$. (See Fig. 7.)

Here, the term "unconstrained" used to denote the variables in $Unc \cup Unc'$ has a weaker meaning than the one in Section 4.2. Indeed, here the distances (gaps) between the primed unconstrained variables x' and y' in Unc' such that $G \models x' \neq y'$ are not in general unbounded, since they may be constrained by the values of the variables in Unc_0 (see Lemma 11). However, if G_0 is not bounded and $\mathcal{S} \in \mathcal{UC}$, then we will show that Unc_0 is non-empty and for a given initial state (q_0, ν_0), the set of the values assumed by the variables in Unc_0 in the states (q, ν) reachable from (q_0, ν_0) is unbounded. This will allow us to provide (under the assumption that $\mathcal{S} \in \mathcal{UC}$) a characterization of the set of unbounded states of $\mathcal{S}$ with control point q_0 similar to the characterization lemma for non-termination given in Section 4.2. Now, we proceed with the technical details.

We make the following observations (in particular, if G_0 is not bounded, then the sets of unconstrained variables Unc_0 and *Unc* are non-empty). Recall that $\mathtt{l}_{L+1}, \mathtt{l}'_{L+1} \stackrel{\text{def}}{=} MIN$ and $\mathtt{u}_0, \mathtt{u}'_0 \stackrel{\text{def}}{=} MAX$.

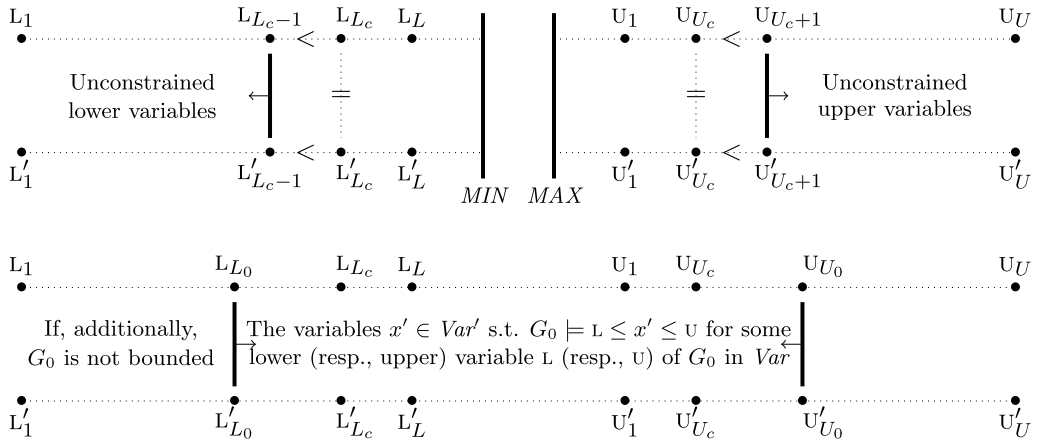

Fig. 7. Unconstrained variables for unboundedness in the transitional MG G.

Lemma 10. *The following hold*:

1. *An upper (resp., lower) variable x' of G in Var' is upper (resp., lower) bounded in G_0 by some upper (resp., lower) variable of G_0 in Var* iff $x' \notin Unc_0{}'$.
2. *For all lower variables $\mathrm{L}_i \in Unc_0$, $G_0 \models \mathrm{L}'_i < \mathrm{L}'_{L_0}$ and $G \models \mathrm{L}_i < \mathrm{L}_{L_0}$.*
3. *For all upper variables $\mathrm{U}_i \in Unc_0$, $G_0 \models \mathrm{U}'_{U_0} < \mathrm{U}'_i$ and $G \models \mathrm{U}_{U_0} < \mathrm{U}_i$.*
4. *For all lower variables $\mathrm{L}_i \in Unc$, $G_0 \models \mathrm{L}'_i < \mathrm{L}'_{L_c}$ and $G \models \mathrm{L}_i < \mathrm{L}_{L_c}$.*
5. *For all upper variables $\mathrm{U}_i \in Unc$, $G_0 \models \mathrm{U}'_{U_c} < \mathrm{U}'_i$ and $G \models \mathrm{U}_{U_c} < \mathrm{U}_i$.*
6. *For each valuation ν_0 over Var, the set of valuations $\{\nu_{(Var \setminus Unc)} \mid (q, \nu)$ is reachable from (q_0, ν_0) in $[\![\mathcal{S}]\!]\}$ is finite.*
7. *If G_0 is* not *bounded, then Unc_0 and Unc are non-empty.*

Proof. Properties 1–5 easily follow from Definitions 17 and 19, and the observation that the total ordering on $Var' \cup Const$ induced by the complete transitional MG G_0 corresponds to the total ordering induced by G on $Var \cup Const$. For Property 6, fix a valuation ν_0 over Var. Let L be a lower variable of G_0 in Var such that $G_0 \models \mathrm{L} \leqslant \mathrm{L}'_{L_c}$ if $L_c \neq L+1$, and $\mathrm{L} = MIN$ otherwise. Moreover, let U be an upper variable of G_0 in Var such that $G_0 \models \mathrm{U}'_{U_c} \leqslant \mathrm{U}$ if $U_c \neq 0$, and $\mathrm{U} = MAX$ otherwise. Note that by Definitions 17 and 19, L and U are well-defined. Moreover, for each state (q, ν) reachable from (q_0, ν_0) in $[\![\mathcal{S}]\!]$, it holds that $\nu_0(\mathrm{L}) \leqslant \nu(x) \leqslant \nu_0(\mathrm{U})$ for all $x \in Var \setminus Unc$. Hence, Property 6 follows. It remains to prove Property 7. Let G_0 be non-bounded. By Definition 17, either there is a lower variable L_i such that L'_i is not lower bounded in G_0 by any lower variable of G_0 in Var, or there is an upper variable U_i such that U'_i is not upper bounded in G_0 by any upper variable of G_0 in Var. Thus, by Property 1, it follows that $Unc_0 \neq \emptyset$. Thus, since $Unc_0 \subseteq Unc$, the result follows. □

Now, we show that if $\mathcal{S}$ satisfies the unboundedness condition and G_0 is not bounded, then no primed lower (resp., upper) unconstrained variable is lower (resp., upper) bounded in G by a lower (resp., upper) variable in $Unc \setminus Unc_0$.

Lemma 11. *Assume that $\mathcal{S} \in \mathcal{UC}$ and G_0 is not bounded. Then, the following hold*:

Lower variables: *for all $\mathrm{L}_i \in Unc \setminus Unc_0$ and $\mathrm{L}_j \in Unc$, $G \not\models \mathrm{L}_i \leqslant \mathrm{L}'_j$.*
Upper variables: *for all $\mathrm{U}_i \in Unc$ and $\mathrm{U}_j \in Unc \setminus Unc_0$, $G \not\models \mathrm{U}'_i \leqslant \mathrm{U}_j$.*

Proof. *Lower variables*. We assume that the result does not hold and derive a contradiction. Hence, there are $\mathrm{L}_i \in Unc \setminus Unc_0$ and $\mathrm{L}_j \in Unc$ such that $G \models \mathrm{L}_i \leqslant \mathrm{L}'_j$. Since $\mathrm{L}_i \notin Unc_0$, by Lemma 10(1), there is a lower variable L of G_0 in Var such that $G_0 \models \mathrm{L} \leqslant \mathrm{L}'_i$. Moreover, since G_0 is not bounded, by Definition 19, $L_0 \leqslant i < L_c$ and $1 \leqslant j < L_c$. We distinguish two cases:

- $j \leqslant i$: hence, $G \models \mathrm{L}'_j \leqslant \mathrm{L}'_i$. Since $G \models \mathrm{L}_i \leqslant \mathrm{L}'_j$, it follows that $G \models \mathrm{L}_i \leqslant \mathrm{L}'_i$.
- $j > i$: since $G \models \mathrm{L}_i \leqslant \mathrm{L}'_j$, by applying repeatedly Lemma 1(1) in Section 4.1, it follows that there is $i \leqslant h \leqslant j$ so that $G \models \mathrm{L}_h \leqslant \mathrm{L}'_h$. Note that $L_0 \leqslant h < L_c$. Moreover, since $G \models \mathrm{L}_i \leqslant \mathrm{L}_h$, it hold that $G_0 \models \mathrm{L}'_i \leqslant \mathrm{L}'_h$.[6] Thus, since $G_0 \models \mathrm{L} \leqslant \mathrm{L}'_i$, it follows that $G_0 \models \mathrm{L} \leqslant \mathrm{L}'_h$.

[6] Recall that the total ordering induced by G_0 on $Var' \cup Const$ corresponds to the total ordering induced by G on $Var \cup Const$.

Thus, in both cases we obtain that $G \models \mathrm{L}_k \leqslant \mathrm{L}'_k$ and $G_0 \models \mathrm{L} \leqslant \mathrm{L}'_k$ for some $L_0 \leqslant k < L_c$ and lower variable L of G_0 in Var. Since G is complete, $G \models \mathrm{L}_k \lhd \mathrm{L}'_k$ for some $\lhd \in \{<, =\}$, which is a contradiction by definition of L_c (Definition 19) and the fact that $\mathcal{S} \in \mathcal{UC}$ and G_0 is not bounded. Hence, the result follows.

Upper variables. This case is analogous to the previous case with the unique difference that now we use Lemma 2(1) in Section 4.1. Thus, we omit the details here. □

For a valuation ν over Var, let $N_0(\nu)$ and $N_c(\nu)$ be the natural numbers defined as follows:

$$N_0(\nu) \stackrel{\text{def}}{=} \min\big\{\big|\nu(x) - \nu(y)\big| \;\big|\; x, y \in Unc_0 \cup \{\mathrm{L}_{L_0}, \mathrm{U}_{U_0}\},\ \text{and either } G \models x < y \text{ or } G \models y < x\big\},$$

$$N_c(\nu) \stackrel{\text{def}}{=} \min\big\{\big|\nu(x) - \nu(y)\big| \;\big|\; x, y \in Unc \cup \{\mathrm{L}_{L_c}, \mathrm{U}_{U_c}\},\ \text{and either } G \models x < y \text{ or } G \models y < x\big\}$$

where the minimum of the empty set is 0. Thus, for a valuation ν over Var, $N_0(\nu)$ (resp., $N_c(\nu)$) represents the minimum over the distances between the values of variables x and y in $Unc_0 \cup \{\mathrm{L}_{L_0}, \mathrm{U}_{U_0}\}$ (resp., $x, y \in Unc \cup \{\mathrm{L}_L, \mathrm{U}_U\}$) such that $G \not\models x = y$. Note that if G_0 is not bounded, then, since $Unc_0 \subseteq Unc$, it holds that $N_c(\nu) \leqslant N_0(\nu)$.

Now, in order to provide a characterization of the set of unbounded states of $\mathcal{S}$ with initial control point, we give three technical lemmata (Lemmata 12–14 below). The first lemma holds under the assumption that G_0 is not bounded, and ensures the following property. Let s_0 be a state of $\mathcal{S}$ with initial control point q_0 and (q, ν) be a state satisfying the following requirement: (q, ν) is reachable from s_0 in $[\![\mathcal{S}]\!]$ in a single step and ν is a solution of G_{Var} (the restriction of G to Var). Then, the set of states (q, ν') satisfying the same requirement as (q, ν) and such that ν and ν' agree on $Var \setminus Unc_0$ is infinite, and the associated set of natural numbers $N_0(\nu')$ is infinite as well.

Lemma 12. *Assume that G_0 is not bounded. Let $\nu_0 \oplus \nu \in Sat(G_0)$ and $\nu \in Sat(G_{Var})$. Then, the following set of natural numbers is* infinite

$$\big\{N_0(\nu') \;\big|\; \nu_0 \oplus \nu' \in Sat(G_0), \nu' \in Sat(G_{Var}),\ \textit{and } \nu \textit{ and } \nu' \textit{ agree on } Var \setminus Unc_0\big\}.$$

Proof. By Lemma 10(1), no upper (resp., lower) variable in $Unc_0{}'$ can be upper (resp., lower) bounded in G_0 by a variable in $(Var \cup Var') \setminus Unc_0{}'$. Moreover, by Lemma 10(7), if G_0 is not bounded, then $Unc_0{}'$ is non-empty. Thus, since the total ordering on $Var' \cup Const$ induced by G_0 corresponds to the total ordering induced by G on $Var \cup Const$, by Lemma 10(2–3) and definition of $N_0(\nu)$, the result easily follows. □

Let $\Delta \in \mathbb{N}$ be the maximum over the edge weights of G. The second technical lemma ensures the following crucial property. Let $\pi = (q, \nu_0) \ldots (q, \nu_n)$ be a non-null run of $\mathcal{S}$ such that ν_0 and ν_n agree on $Var \setminus Unc$. Then, for all $k \geqslant 1$ and valuations $\nu \in Sat(G_{Var})$ such that ν and ν_0 agree on $Var \setminus Unc$, if $N_c(\nu)$ *is sufficiently large*, then there is also a run of length greater than k from (q, ν) (intuitively, obtained by pumping the pseudo-cycle π).

Lemma 13 *(Pumping lemma for unboundedness). Let $\nu_0 \oplus \nu'_0 \in Sat(G)$ and $\nu \in Sat(G_{Var})$ such that ν_0 and ν agree on $Var \setminus Unc$, $(\nu'_0)_{Var \setminus Unc} \in Sat(G_{Var \setminus Unc})$, and $\lceil \frac{N_c(\nu)}{|Var|+1} \rceil > \Delta$. Then, there exists a valuation $\nu' \in Sat(G_{Var})$ such that $\nu \oplus \nu' \in Sat(G)$, ν'_0 and ν' agree on $Var \setminus Unc$, and $N_c(\nu') \geqslant \lceil \frac{N_c(\nu)}{|Var|+1} \rceil$.*

Proof. Let ν_0, ν'_0, and ν as in the statement of the lemma. First, we observe the following.

Claim. *The restriction of $\nu \oplus \nu'_0$ to $Var \cup (Var' \setminus Unc')$ is a solution of the restriction of G to $Var \cup (Var' \setminus Unc')$.*

Proof of the claim. By hypothesis, $\nu \in Sat(G_{Var})$, $N_c(\nu) > \Delta$, and the restriction of $\nu \oplus \nu'_0$ to $(Var \setminus Unc) \cup (Var' \setminus Unc')$ is a solution of the restriction of G to $(Var \setminus Unc) \cup (Var' \setminus Unc')$. Moreover, by Lemma 10(4–5), the following hold: (i) for all $\mathrm{L}_i \in Unc$, $G \models \mathrm{L}_i < \mathrm{L}_{L_c} = \mathrm{L}'_{L_c}$, (ii) for all $\mathrm{U}_i \in Unc$, $G \models \mathrm{U}'_{U_c} = \mathrm{U}_{U_c} < \mathrm{U}_i$, and (iii) for all $x' \in Var' \setminus Unc'$, $G \models \mathrm{L}'_{L_c} \leqslant x' \leqslant \mathrm{U}'_{U_c}$. Thus, by definition of $N_c(\nu)$, the result easily follows. □

Now, we prove Lemma 13. Since G is satisfiable, there exists a linear ordering of the set of vertices $Unc \cup Unc' \cup \{\mathrm{U}_{U_c}, \mathrm{L}_{L_c}\}$ which is consistent with the constraints of G (in particular, for all $\mathrm{L}_i \in Unc$, $G \models \mathrm{L}_i < \mathrm{L}_{L_c}$ and $G \models \mathrm{L}'_i < \mathrm{L}_{L_c}$, and for all $\mathrm{U}_i \in Unc$, $G \models \mathrm{U}_{U_c} < \mathrm{U}_i$ and $G \models \mathrm{U}_{U_c} < \mathrm{U}'_i$). Moreover, for two consecutive vertices $u, v \in \{\mathrm{U}_{U_c}, \ldots, \mathrm{U}_U\}$ (resp., $u, v \in \{\mathrm{L}_1, \ldots, \mathrm{L}_{L_c}\}$), with $G \not\models u = v$, the maximum number of variables in Unc' which lie (according to the above linear ordering) between u and v is at most $|Var|$, and $|\nu(u) - \nu(v)| \geqslant N_c(\nu)$. By hypothesis, $\lceil \frac{N_c(\nu)}{|Var|+1} \rceil > \Delta$ and $(\nu'_0)_{Var \setminus Unc} \in Sat(G_{Var \setminus Unc})$. Thus, since G is balanced, by the claim above, it follows that we can assign to the variables in Unc' integers values in such a way that the corresponding extension ν' of $(\nu'_0)_{Var \setminus Unc}$ satisfies the statement of the lemma. □

The third technical lemma, which is a consequence of Lemma 11, is a variant of the pumping lemma above and holds under the assumption that $\mathcal{S} \in \mathcal{UC}$ and G_0 is not bounded.

Lemma 14. *Assume that $\mathcal{S} \in \mathcal{UC}$ and G_0 is not bounded. Let $\nu_0 \oplus \nu'_0 \in Sat(G)$ and $\nu \in Sat(G_{Var})$ such that ν_0 and ν agree on $Var \setminus Unc_0$, $\nu'_0 \in Sat(G_{Var})$, and $\lceil \frac{N_0(\nu)}{|Var|+1} \rceil > \Delta$. Then, there exists a valuation $\nu' \in Sat(G_{Var})$ such that $\nu \oplus \nu' \in Sat(G)$, ν'_0 and ν' agree on $Var \setminus Unc$, and $N_c(\nu') \geqslant \lceil \frac{N_0(\nu)}{|Var|+1} \rceil$.*

Proof. Let ν_0, ν'_0, and ν be as in the statement of the lemma. First, we observe the following.

Claim. *The restriction of $\nu \oplus \nu'_0$ to $Var \cup (Var' \setminus Unc')$ is a solution of the restriction of G to $Var \cup (Var' \setminus Unc')$.*

Proof of the claim. By hypothesis, $\nu \in Sat(G_{Var})$, $N_0(\nu) > \Delta$, and the restriction of $\nu \oplus \nu'_0$ to $(Var \setminus Unc_0) \cup (Var' \setminus Unc')$ is a solution of the restriction of G to $(Var \setminus Unc_0) \cup (Var' \setminus Unc')$. Moreover, by Lemma 10(2–3), the following hold: (i) for all $\mathrm{L}_i \in Unc_0$, $G \models \mathrm{L}_i < \mathrm{L}_{L_0} \leqslant \mathrm{L}_{L_c} = \mathrm{L}'_{L_c}$, (ii) for all $\mathrm{U}_i \in Unc_0$, $G \models \mathrm{U}'_{U_c} = \mathrm{U}_{U_c} \leqslant \mathrm{U}_{U_0} < \mathrm{U}_i$, and (iii) for all $x' \in Var' \setminus Unc'$, $G \models \mathrm{L}'_{L_c} \leqslant x' \leqslant \mathrm{U}'_{U_c}$. Thus, by definition of $N_0(\nu)$, the result easily follows. □

Now, we prove Lemma 14. By Lemma 11, the upper variables in Unc' are not upper-bounded by the upper variables in $Unc \setminus Unc_0$, and the lower variables in Unc' are not lower-bounded by the lower variables in $Unc \setminus Unc_0$. Hence, since G is satisfiable, there exists a linear ordering of the set of vertices $Unc \cup Unc' \cup \{\mathrm{U}_{U_c}, \mathrm{L}_{L_c}\}$ which is consistent with the constraints

$$\mathrm{U}_{U_0} < \mathrm{U}'_{U_c+1} \leqslant \cdots \leqslant \mathrm{U}'_U \wedge \mathrm{L}'_1 \leqslant \cdots \leqslant \mathrm{L}'_{L_c-1} < \mathrm{L}_{L_0}$$

and with the constraints of G (in particular, $G \models \mathrm{U}_{U_0} < \mathrm{U}_{U_0+1} \leqslant \cdots \leqslant \mathrm{U}_U$ and $G \models \mathrm{L}_1 \leqslant \cdots \leqslant \mathrm{L}_{L_0-1} < \mathrm{L}_{L_0}$). Moreover, for two consecutive vertices $u, v \in \{\mathrm{U}_{U_0}, \mathrm{U}_{U_0+1}, \ldots, \mathrm{U}_U\}$ (resp., $u, v \in \{\mathrm{L}_1, \ldots, \mathrm{L}_{L_0-1}, \mathrm{L}_{L_0}\}$), with $G \not\models u = v$, the maximum number of variables in Unc' which lie (according to the above linear ordering) between u and v is at most $|Var|$, and $|\nu(u) - \nu(v)| \geqslant N_0(\nu)$. By hypothesis, $\lceil \frac{N_0(\nu)}{|Var|+1} \rceil > \Delta$ and $\nu'_0 \in Sat(G_{Var})$. Thus, since G is balanced, by the claim above, it follows that we can assign to the variables in Unc' integers values in such a way that the corresponding extension ν' of $(\nu'_0)_{Var \setminus Unc}$ satisfies the statement of the lemma. □

By Lemmata 12–14, we obtain the following characterization of the set of states in $Unb_{\mathcal{S}}$ with control point q_0 (under the assumption that $\mathcal{S} \in \mathcal{UC}$).

Lemma 15 *(Characterization lemma for unboundedness). Let $\mathcal{S} \in \mathcal{UC}$ and s_0 be a state of $\mathcal{S}$ with control point q_0. Then, $s_0 \in Unb_{\mathcal{S}}$* iff *there is a state (q, ν) reachable from s_0 in $[\![\mathcal{S}]\!]$ by a run of length at least 2, and there is a non-null run of $\mathcal{S}$ from (q, ν) to a state (q, ν') such that ν and ν' agree in $Var \setminus Unc$.*

Proof. Let $\mathcal{S} \in \mathcal{UC}$ and $s_0 = (q_0, \nu_0)$ be a state of $\mathcal{S}$ with control point q_0. For the right implication $\Rightarrow$, assume that $(q_0, \nu_0) \in Unb_{\mathcal{S}}$. Hence, the set of lengths of the finite runs from (q_0, ν_0) is infinite. Then, by Lemma 10(6), the result follows.

For the left implication $\Leftarrow$, assume that there are a run of $\mathcal{S}$ of length at least 2 from (q_0, ν_0) to a state (q, ν) and a non-null run of $\mathcal{S}$ from (q, ν) to a state (q, ν') such that ν and ν' agree in $Var \setminus Unc$. First, assume that G_0 is bounded. Then, since $\mathcal{S} \in \mathcal{UC}$, by Definition 18, $\mathcal{S} \notin \mathcal{TC}$. Since G_0 is bounded, the set Unc is defined as in Definition 16. Thus, by the characterization lemma for non-termination (Lemma 9), it follows that $(q_0, \nu_0) \in Inf_{\mathcal{S}} \subseteq Unb_{\mathcal{S}}$, and the result follows. Now, assume that G_0 is not bounded. By hypothesis there is a run π from (q_0, ν_0) of the form $\pi = (q_0, \nu_0) \to (q, \nu_1) \to (q, \nu_2) \to \cdots \to (q, \nu) \to \cdots \to (q, \nu')$ such that ν and ν' agree in $Var \setminus Unc$ and the subrun $(q, \nu) \to \cdots \to (q, \nu')$ has non-null length. Let us consider the prefix of π of length 2 given by $(q_0, \nu_0) \to (q, \nu_1) \to (q, \nu_2)$, and let $S(\nu_2)$ be the set of valuations over Var given by

$$S(\nu_2) \stackrel{\text{def}}{=} \left\{ \nu'_2 \;\middle|\; \nu_0 \oplus \nu'_2 \in Sat(G_0 \bullet G),\ \nu'_2 \in Sat(G_{Var}),\ \text{and } \nu_2 \text{ and } \nu'_2 \text{ agree on } Var \setminus Unc \right\}.$$

Since $\nu_0 \oplus \nu_1 \in Sat(G_0)$, $\nu_1 \oplus \nu_2 \in Sat(G)$, and $\nu_2 \in Sat(G_{Var})$, by Lemmata 12 and 14, it follows that the set $S(\nu_2)$ is infinite, and the set $\{N_c(\nu'_2) \mid \nu'_2 \in S(\nu_2)\}$ is infinite as well. Let us consider the suffix π' of π, $(q, \nu_2) \to \cdots \to (q, \nu) \to \cdots \to (q, \nu')$. Let $h \geqslant 1$. Since ν and ν' agree in $Var \setminus Unc$ and for each $\nu'_2 \in S(\nu_2)$, $\nu'_2 \in Sat(G_{Var})$ and ν_2 and ν'_2 agree in $Var \setminus Unc$, Lemma 13 (applied repetitively to the single steps of the suffix π') ensures the following property: there is $n_h \in \mathbb{N}$ such that for all $\nu'_2 \in S(\nu_2)$ with $N_c(\nu'_2) \geqslant n_h$, there is a finite run from (q, ν'_2) of length at least h. Since the set $\{N_c(\nu'_2) \mid \nu'_2 \in S(\nu_2)\}$ is infinite and there is a finite run from (q_0, ν_0) to (q, ν'_2) for all $\nu'_2 \in S(\nu_2)$, we deduce that there is a finite run from (q_0, ν_0) of length at least h. Since h is arbitrary, we obtain that (q_0, ν_0) is unbounded. Hence, the result follows. This concludes the proof of the lemma. □

Construction of an MG *representation of $Unb_{\mathcal{S}}$.* By using the characterization lemma for unboundedness (Lemma 15), we can prove the main result of this subsection.

Theorem 5. *The set $Unb_{\mathcal{S}}$ is* MG *representable and one can construct an* MG *representation of $Unb_{\mathcal{S}}$, written $\sigma(\mathcal{S})$, satisfying the following*:

1. $\lfloor \sigma(\mathcal{S}) \rfloor_K$ *can be computed in polynomial time*;
2. $\lfloor \sigma(\mathcal{S}) \rfloor_K = \lfloor \sigma(\lfloor \mathcal{S} \rfloor_K) \rfloor_K$ ($\lfloor \mathcal{S} \rfloor_K$ *is a simple* GCS).

Proof. By Corollary 2, for each state s of $\mathcal{S}$ with control point q, $s \in Inf_{\mathcal{S}}$ iff $s \in Unb_{\mathcal{S}}$. Thus, by Theorem 3, it suffices to prove the version of the theorem obtained by replacing $Unb_{\mathcal{S}}$ with $Unb^{q_0}_{\mathcal{S}}$, where $Unb^{q_0}_{\mathcal{S}}$ denotes the set of states in $Unb_{\mathcal{S}}$ having control point q_0. We distinguish two cases:

- $\mathcal{S} \notin \mathcal{UC}$: by Proposition 12, $Unb^{q_0}_{\mathcal{S}} = Unb^{q_0}_{\lfloor \mathcal{S} \rfloor_K} = \emptyset$, hence, in this case, the result trivially holds.
- $\mathcal{S} \in \mathcal{UC}$: for this case, the proof of the result is similar to the proof of Theorem 3 for the case $\mathcal{S} \notin \mathcal{TC}$. The difference is that now we use the characterization lemma for unboundedness (Lemma 15) instead of the characterization lemma for non-termination (Lemma 9). Thus, we omit the details here. □

Additional results on the unboundedness condition. By using the characterization lemma for unboundedness (Lemma 15) and Lemma 3 in Section 4.1, we show that the unboundedness condition is also a sufficient condition for the existence of unbounded states with initial control point q_0.

Theorem 6. *If $\mathcal{S} \in \mathcal{UC}$, then the set of states s with control point q_0 such that $s \in Unb_{\mathcal{S}}$ is non-empty.*

Proof. Let $\mathcal{S} \in \mathcal{UC}$. First, we show that the pair of integers (L_c, U_c) of Definition 19 is well-formed w.r.t. G. If G_0 is bounded, then $\mathcal{S} \notin \mathcal{TC}$ and L_c and U_c are as defined in Definition 16. Hence, by Lemma 4, the result follows. Now, let G_0 be non-bounded. By Lemma 10(1), for all $L_c \leqslant i \leqslant L$ (resp., $1 \leqslant i \leqslant U_c$), L_i (resp., U_i) is lower (resp., upper) bounded in G_0 by a lower (resp., upper) variable of G_0 in Var. Thus, by Definitions 18 and 19, the result follows.

Now, we prove the theorem. By the characterization lemma for unboundedness (Lemma 15), it suffices to show that there are $k \geqslant 1$, $n \geqslant 1$, and valuations ν_0, ν, and ν' over Var such that $(\nu_0 \oplus \nu) \in Sat(G_0 \bullet G^k)$, $(\nu \oplus \nu') \in Sat(G^n)$, and ν and ν' agree on $Var \setminus Unc$. Since the pair (L_c, U_c) is well-formed w.r.t. G, this can be proved as in the second part of the proof of Theorem 4 (which is based on the application of Lemma 3 in Section 4.1), and we omit the details here. □

By Proposition 12 and Theorem 6, it follows that the negation of the unboundedness condition represents a criterion for checking strong termination w.r.t. the initial control point of simple GCS. Moreover, by Proposition 11, Theorem 4, and Corollary 2, the termination condition represents a criterion for checking strong termination w.r.t. the control point associated with the self-loop of simple GCS. Hence, we obtain the following result.

Corollary 3. *The strong termination problem and the strong termination problem w.r.t. a designated control point of simple* GCS *can be solved in polynomial time.*

Note that Corollary 3 can also be directly deduced from Property 1 of Theorem 5.

5. Fairness and (strong) termination for unrestricted GCS

In this section, we address fairness and (strong) termination for the whole class of GCS. The proposed approach consists of two main steps. For a GCS $\mathcal{S}$ and a set $F \subseteq Q(\mathcal{S})$ of accepting control points, first we show (Theorem 7 and Lemmata 16 and 17) that it is possible to construct two finite families $\mathcal{F}(\mathcal{S}, F)$ and $\mathcal{U}(\mathcal{S})$ of simple GCS such that the following hold:

- $Inf_{\mathcal{S},F}$ corresponds to the set of non-terminating states with initial control point of the simple GCS in $\mathcal{F}(\mathcal{S}, F)$, and
- $Unb_{\mathcal{S}}$ corresponds to the set of unbounded states with initial control point of the simple GCS in $\mathcal{U}(\mathcal{S})$.

Then, we show (Theorems 8 and 9) that it is possible to compute separately and in exponential time the K-bounded abstractions of the simple GCS in $\mathcal{F}(\mathcal{S}, F)$ and $\mathcal{U}(\mathcal{S})$ (we are not able to give upper bounds on the sizes of $\mathcal{F}(\mathcal{S}, F)$ and $\mathcal{U}(\mathcal{S})$), which are sound and complete w.r.t. the existence of non-terminating states and unbounded states, respectively. Now, we proceed with the technical details.

Let $\mathcal{S}$ be a GCS. For a non-null finite path $\wp$ of $\mathcal{S}$ such that $s(\wp) = t(\wp)$ (i.e., $\wp$ is cyclic), $(\wp)^\omega$ denotes the infinite path $\wp\wp\ldots$. An infinite path $\wp$ of $\mathcal{S}$ of the form $\wp = \wp'(\wp'')^\omega$ is said to be *ultimately periodic*. A state s of $\mathcal{S}$ is *neatly unbounded* w.r.t. an infinite path $\wp$ of $\mathcal{S}$, if there is a sequence of finite runs $(\pi_n)_{n\in\mathbb{N}}$ of $\mathcal{S}$ starting from s such that $\{|\pi_n| \mid n \in \mathbb{N}\}$ is infinite and for each $n \in \mathbb{N}$, π_n is an instance of the prefix of $\wp$ of length $|\pi_n|$. We make the following observation.

Proposition 13. *Let $\mathcal{S}$ be a* GCS, *s_0 be an $\mathcal{S}$-state such that $s_0 \in Unb_{\mathcal{S}}$. Then, s_0 is neatly unbounded w.r.t. some infinite path of $\mathcal{S}$.*

Proof. By hypothesis, there is a sequence of finite runs $(\pi_n)_{n\in\mathbb{N}}$ of $\mathcal{S}$ starting from s_0 such that $|\pi_n| = n$ for each $n \in \mathbb{N}$. Since the set of $\mathcal{S}$-edges is finite, it easily follows that for all $h \in \mathbb{N}$, there is a subsequence $(\pi_n^h)_{n\in\mathbb{N}}$ of $(\pi_n)_{n\in\mathbb{N}}$ and a finite path $\wp_h$ of $\mathcal{S}$ of length h such that the following hold:

- for each $n \in \mathbb{N}$, $|\pi_n^h| \geqslant h$ and the prefix of π_n^h of length h is an instance of $\wp_h$;
- $(\pi_n^{h+1})_{n\in\mathbb{N}}$ is a subsequence of $(\pi_n^h)_{n\in\mathbb{N}}$;
- $\wp_h$ is a prefix of $\wp_{h+1}$.

Hence, the sequence $(\wp_h)_{h\geqslant 1}$ corresponds to an infinite path $\wp$ of $\mathcal{S}$, where $\wp_h$ is its prefix of length h. Moreover, it follows that there is a subsequence $(\pi'_n)_{n\in\mathbb{N}}$ of $(\pi_n)_{n\in\mathbb{N}}$ such that for each $n \geqslant 1$, $|\pi'_n| \geqslant n$ and the prefix of π'_n of length n is an instance of $\wp_n$. Hence, state s_0 is neatly unbounded w.r.t. the infinite path $\wp$, and the result follows. □

The key result which allows us to reduce fairness and strong termination for unrestricted GCS to non-termination and strong termination for simple GCS, respectively, is represented by the following theorem which is proved by using Ramsey's theorem in its infinite version [31].

Theorem 7 *(Characterization theorem). Let $\mathcal{S}$ be a* GCS*, s_0 be an $\mathcal{S}$ state, $F \subseteq Q(\mathcal{S})$ and $\mathcal{P}_\mathcal{S}$ be the finite set of sample paths of $\mathcal{S}$ satisfying Theorem 2. Then, the following hold*:

1. *$s_0 \in Inf_{\mathcal{S},F}$* iff *there is an infinite run of $\mathcal{S}$ starting from s_0 which is an instance of an* ultimately periodic *path $\wp_0 \cdot (\wp)^\omega$ such that $\wp_0, \wp \in \mathcal{P}_\mathcal{S}$, $s(\wp) \in F$, $G_{\wp_0} \bullet G_\wp$ is satisfiable, and $G_\wp$ is idempotent*;
2. *$s_0 \in Unb_\mathcal{S}$* iff *s_0 is neatly unbounded w.r.t. an* ultimately periodic *path $\wp_0 \cdot (\wp)^\omega$ such that $\wp_0, \wp \in \mathcal{P}_\mathcal{S}$, $G_{\wp_0} \bullet G_\wp$ is satisfiable, and $G_\wp$ is idempotent.*

Proof. Let $\mathcal{S}$ be a GCS, s_0 be an $\mathcal{S}$ state, $F \subseteq Q(\mathcal{S})$ and $\mathcal{P}_\mathcal{S}$ be the finite set of sample paths of $\mathcal{S}$ satisfying Theorem 2. We prove Property 2 (Property 1 is similar). The left implication $\Leftarrow$ of Property 2 is obvious. For the right implication $\Rightarrow$, assume that $s_0 \in Unb_\mathcal{S}$. Then, by Proposition 13, there is an infinite path $\wp_\infty$ of $\mathcal{S}$ such that s_0 is neatly unbounded w.r.t. $\wp_\infty$.

For each $\wp \in \mathcal{P}_\mathcal{S}$, we denote by $[\wp]$ the set of non-null finite paths $\wp'$ of $\mathcal{S}$ such that $s(\wp') = s(\wp)$, $t(\wp') = t(\wp)$, $\rightsquigarrow_{\wp'}$ implies $\rightsquigarrow_\wp$, and $\lfloor G_{\wp'} \rfloor_K = \lfloor G_\wp \rfloor_K$. Let H be the *finite* set given by $H = \{[\wp] \mid \wp \in \mathcal{P}_\mathcal{S}\}$. For each non-null finite path $\wp'$ of $\mathcal{S}$, we associate to $\wp'$ a *color* given by some element $[\wp] \in H$ such that $\wp' \in [\wp]$ (note that by Theorem 2 such an element of H must exist). Let us consider the infinite path $\wp_\infty$. Then, there is a control point q such that $\wp_\infty$ is of the form $\wp_\infty = \wp_0\wp_1\wp_2\ldots$, where for each $i \geqslant 1$, $\wp_i$ is a non-null (cyclic) path from q to q. Let us consider the set of positive natural numbers, and label each pair (i, j) of its elements with $i < j$ with the color of the subpath $\wp_i \ldots \wp_j$ of $\wp_\infty$. By Ramsey's theorem (in its infinite version) [31], there is an infinite set I of positive natural numbers such that all the pairs (i, j) with $i, j \in I$ (and $i < j$) carry the same label in H, say $[\wp]$. It follows that $\wp_\infty$ can be written in the form $\wp_\infty = \wp'_0\wp'_1\wp'_2\ldots$ such that $|\wp'_0| > 0$ and for all $i \geqslant 1$, $\wp'_i \in [\wp]$ and $\wp'_i\wp'_{i+1} \in [\wp]$. Hence, in particular, $\lfloor G_{\wp'_i} \rfloor_K = \lfloor G_\wp \rfloor_K$ and $\lfloor G_{\wp'_i\wp'_{i+1}} \rfloor_K = \lfloor G_\wp \rfloor_K$. By Proposition 7 and associativity of $\bullet$, we obtain that $\lfloor G_\wp \rfloor_K = \lfloor G_\wp \bullet G_\wp \rfloor_K$. Hence, for the cyclic path $\wp \in \mathcal{P}_\mathcal{S}$, $G_\wp$ is idempotent.

Since s_0 is neatly unbounded w.r.t. $\wp_\infty$, there is a sequence of finite runs $(\pi_n)_{n\geqslant 0}$ from s_0 such that π_n is an instance of the prefix $\wp'_0\wp'_1\ldots\wp'_n$ of $\wp_\infty$. Let $\wp''_0 \in \mathcal{P}_\mathcal{S}$ such that $\wp'_0 \in [\wp''_0]$. Since $\wp'_i \in [\wp]$ for each $i \geqslant 1$ (hence, $\rightsquigarrow_{\wp'_i}$ implies $\rightsquigarrow_\wp$), it follows that for each $n \in \mathbb{N}$, there is a finite run π'_n starting from s_0 which is an instance of the finite path $\wp''_0 \underbrace{\wp \cdots \wp}_{n \text{ times}}$. Hence, s_0 is neatly unbounded w.r.t. the *ultimately periodic* path $\wp''_0(\wp)^\omega$. Moreover, $\wp''_0, \wp \in \mathcal{P}_\mathcal{S}$, $G_{\wp''_0} \bullet G_\wp$ is satisfiable, and $G_\wp$ is idempotent. Hence, the result follows. □

Let $\mathcal{S}$ be a GCS, $F \subseteq Q(\mathcal{S})$, and $\mathcal{P}_\mathcal{S}$ be the computable finite set of sample paths of $\mathcal{S}$ satisfying Theorem 2. According to Theorem 7, we define two computable finite families $\mathcal{F}(\mathcal{S}, F)$ and $\mathcal{U}(\mathcal{S})$ of GCS as follows:

- for a GCS $\mathcal{S}_0$, $\mathcal{S}_0 \in \mathcal{F}(\mathcal{S}, F)$ *iff* $\mathcal{S}_0$ consists of the edges

$$\big(\natural, s(\wp_0)\big) \xrightarrow{G_{\wp_0}} t(\wp_0) \quad \text{and} \quad s(\wp) \xrightarrow{G_\wp} t(\wp)$$

  for some sample paths $\wp_0, \wp \in \mathcal{P}_\mathcal{S}$ such that $t(\wp_0) = s(\wp) = t(\wp)$, $s(\wp) \in F$, $G_{\wp_0} \bullet G_\wp$ is satisfiable, and $G_\wp$ is idempotent;
- for a GCS $\mathcal{S}_0$, $\mathcal{S}_0 \in \mathcal{U}(\mathcal{S})$ *iff* $\mathcal{S}_0$ consists of the edges

$$\big(\natural, s(\wp_0)\big) \xrightarrow{G_{\wp_0}} t(\wp_0) \quad \text{and} \quad s(\wp) \xrightarrow{G_\wp} t(\wp)$$

  for some sample paths $\wp_0, \wp \in \mathcal{P}_\mathcal{S}$ such that $t(\wp_0) = s(\wp) = t(\wp)$, $G_{\wp_0} \bullet G_\wp$ is satisfiable, and $G_\wp$ is idempotent.

Note that the special symbol $\natural$ is used just to ensure that the control points $(\natural, s(\wp_0))$ and $t(\wp_0)$ of the GCS $\mathcal{S}_0$ are distinct. Moreover, if $\mathcal{S}$ is complete, then since the composition operator $\bullet$ preserves completeness of transitional MG, by construction, it follows that the families $\mathcal{F}(\mathcal{S}, F)$ and $\mathcal{U}(\mathcal{S})$ consist of *simple* GCS. In particular, by Theorem 7, we easily obtain the following results (recall that for a family $\mathcal{F}$ of GCS, $\lfloor \mathcal{F} \rfloor_K$ denotes the set of K-bounded approximations of the GCS in $\mathcal{F}$).

Lemma 16 *(Reduction lemma for fairness). Let $\mathcal{S}$ be a* complete GCS *and $F \subseteq Q(\mathcal{S})$. Then*:

1. *$\mathcal{F}(\mathcal{S}, F)$ and $\lfloor \mathcal{F}(\mathcal{S}, F) \rfloor_K$ consist of simple* GCS;
2. *for a state (q_0, ν_0) of $\mathcal{S}$, $(q_0, \nu_0) \in Inf_{\mathcal{S},F}$ iff there is $\mathcal{S}_0 \in \mathcal{F}(\mathcal{S}, F)$ such that $\mathcal{S}_0$ has initial control point $(\natural, q_0)$ and $((\natural, q_0), \nu_0) \in Inf_{\mathcal{S}_0}$;*
3. *for a* GCS *$\mathcal{S}_0$, $\mathcal{S}_0 \in \lfloor \mathcal{F}(\mathcal{S}, F) \rfloor_K$ iff $\mathcal{S}_0$ consists of the edges*

$$\big(\natural, s(\wp_0)\big) \xrightarrow{\lfloor G_{\wp_0} \rfloor_K} t(\wp_0) \quad \text{and} \quad s(\wp) \xrightarrow{\lfloor G_{\wp} \rfloor_K} t(\wp)$$

   for some non-null finite and satisfiable paths $\wp_0$ and $\wp$ of $\mathcal{S}$ such that $t(\wp_0) = s(\wp) = t(\wp)$, $s(\wp) \in F$, $\lfloor G_{\wp_0} \rfloor_K \bullet \lfloor G_{\wp} \rfloor_K$ is satisfiable, and $\lfloor G_{\wp} \rfloor_K$ is idempotent;
4. *$\lfloor \mathcal{F}(\mathcal{S}, F) \rfloor_K$ can be computed in time $O(|E(\mathcal{S})| \cdot |Q(\mathcal{S})|^2 \cdot (K+2)^{(2|Var|+|Const|)^2})$;*
5. *$\lfloor \mathcal{F}(\mathcal{S}, F) \rfloor_K = \lfloor \mathcal{F}(\lfloor \mathcal{S} \rfloor_K, F) \rfloor_K$.*

Proof. Since the K-bounded approximation of a simple GCS is a simple GCS too (Proposition 9), Property 1 holds. Property 2 directly follows from Theorem 7 and definition of $\mathcal{F}(\mathcal{S}, F)$. Property 3 easily follows from definition of $\mathcal{F}(\mathcal{S}, F)$, Theorem 2, Propositions 6 and 7, and the fact that for a transitional MG G, G is idempotent iff $\lfloor G \rfloor_K$ is idempotent. Property 4 directly follows from Property 3 and Theorem 1. It remains to prove Property 5. By Proposition 7, the following holds: for each non-null finite path $\wp$ of $\mathcal{S}$ (resp., $\lfloor \mathcal{S} \rfloor_K$), there is a non-null finite path $\wp'$ of $\lfloor \mathcal{S} \rfloor_K$ (resp., $\mathcal{S}$) such that $s(\wp) = s(\wp')$, $t(\wp) = t(\wp')$, and $\lfloor G_{\wp} \rfloor_K = \lfloor G_{\wp'} \rfloor_K$. Thus, by Property 3, Property 5 follows, which concludes the proof of the lemma. □

Lemma 17 *(Reduction lemma for unboundedness). Let $\mathcal{S}$ be a* complete GCS. *Then*:

1. *$\mathcal{U}(\mathcal{S})$ and $\lfloor \mathcal{U}(\mathcal{S}) \rfloor_K$ consist of simple* GCS;
2. *for a state (q_0, ν_0) of $\mathcal{S}$, $(q_0, \nu_0) \in Unb_{\mathcal{S}}$ iff there is $\mathcal{S}_0 \in \mathcal{U}(\mathcal{S})$ such that $\mathcal{S}_0$ has initial control point $(\natural, q_0)$ and $((\natural, q_0), \nu_0) \in Unb_{\mathcal{S}_0}$;*
3. *for a* GCS *$\mathcal{S}_0$, $\mathcal{S}_0 \in \lfloor \mathcal{U}(\mathcal{S}) \rfloor_K$ iff $\mathcal{S}_0$ consists of the edges*

$$\big(\natural, s(\wp_0)\big) \xrightarrow{\lfloor G_{\wp_0} \rfloor_K} t(\wp_0) \quad \text{and} \quad s(\wp) \xrightarrow{\lfloor G_{\wp} \rfloor_K} t(\wp)$$

   for some non-null finite and satisfiable paths $\wp_0$ and $\wp$ of $\mathcal{S}$ such that $t(\wp_0) = s(\wp) = t(\wp)$, $\lfloor G_{\wp_0} \rfloor_K \bullet \lfloor G_{\wp} \rfloor_K$ is satisfiable, and $\lfloor G_{\wp} \rfloor_K$ is idempotent;
4. *$\lfloor \mathcal{U}(\mathcal{S}) \rfloor_K$ can be computed in time $O(|E(\mathcal{S})| \cdot |Q(\mathcal{S})|^2 \cdot (K+2)^{(2|Var|+|Const|)^2})$;*
5. *$\lfloor \mathcal{U}(\mathcal{S}) \rfloor_K = \lfloor \mathcal{U}(\lfloor \mathcal{S} \rfloor_K) \rfloor_K$.*

Proof. The proof is similar to the proof of Lemma 16. Thus, we omit the details here. □

For unrestricted GCS, we observe the following.

Proposition 14. *Let $\mathcal{S}$ be a* GCS. *Then, one can compute a* complete GCS, *written $\mathcal{C}(\mathcal{S})$, such that $[\![\mathcal{C}(\mathcal{S})]\!] = [\![\mathcal{S}]\!]$ and the following hold*:

1. *$Q(\mathcal{C}(\mathcal{S})) = Q(\mathcal{S})$ and $|E(\mathcal{C}(\mathcal{S}))| = O(|E(\mathcal{S})| \cdot 2^{(2|Var|+|Const|)^2})$; moreover, $\mathcal{C}(\mathcal{S})$ has the same sets of variables and constants as $\mathcal{S}$;*
2. *$\lfloor \mathcal{C}(\lfloor \mathcal{S} \rfloor_K) \rfloor_K = \lfloor \mathcal{C}(\mathcal{S}) \rfloor_K$.*

Proof. We need an additional definition. A *basic complete transitional* MG G is a transitional MG such that

- the weight of each edge is in $\{0, 1\}$;
- for all vertices u and v, either $G \models u \lhd v$ or $G \models v \lhd u$ for some $\lhd \in \{<, =\}$.

Let $\mathcal{G}_b$ be the set of basic complete transitional MG. Evidently, $\mathcal{G}_b$ is finite and its cardinality is bounded by $O(2^{(2|Var|+|Const|)^2})$. Moreover, note that for each transitional MG G and $G' \in \mathcal{G}_b$, $G \sqcap G'$ is complete. Furthermore,

$Sat(G) = \bigcup_{G' \in \mathcal{G}_b} Sat(G \sqcap G')$. Then, $\mathcal{C}(\mathcal{S})$ is obtained from $\mathcal{S}$ by replacing each edge $q \xrightarrow{G} q'$ with the edges $q \xrightarrow{G \sqcap G'} q'$, where $G' \in \mathcal{G}_b$. Evidently, $[\![\mathcal{C}(\mathcal{S})]\!] = [\![\mathcal{S}]\!]$ and Property 1 holds. Note that each $G' \in \mathcal{G}_b$ is K-bounded. Thus, by Proposition 7, we obtain that for all transitional MG G and $G' \in \mathcal{G}_b$, $\lfloor G \sqcap G' \rfloor_K = \lfloor G \rfloor_K \sqcap G'$. Hence, Property 2 holds as well, which concludes. □

Now, we can prove the main results of this section.

Theorem 8 *(Fairness for unrestricted* GCS*). Let $\mathcal{S}$ be a* GCS *and $F \subseteq Q(\mathcal{S})$. Then, $Inf_{\mathcal{S},F}$ is* MG *representable and one can build an* MG *representation $\sigma(\mathcal{S}, F)$ of $Inf_{\mathcal{S},F}$ such that*:

1. *$\lfloor \sigma(\mathcal{S}, F) \rfloor_K$ can be computed in time $O(|E(\mathcal{S})| \cdot |Q(\mathcal{S})|^2 \cdot (K+2)^{(2|Var|+|Const|)^2})$;*
2. *$\lfloor \sigma(\mathcal{S}, F) \rfloor_K = \lfloor \sigma(\lfloor \mathcal{S} \rfloor_K, F) \rfloor_K$;*
3. *given $q_0 \in Q(\mathcal{S})$ and a K-bounded* MG *G over Var, checking whether G is in the q_0-component of $\lfloor \sigma(\mathcal{S}, F) \rfloor_K$ can be done in polynomial space.*

Proof. We distinguish two cases:

- **$\mathcal{S}$ is complete:** hence, the computable family $\mathcal{F}(\mathcal{S}, F)$ of GCS consists of simple GCS. By Theorem 3, given a simple GCS $\mathcal{S}_0$ with initial control point q_0, one can compute a finite set $\mathcal{G}(\mathcal{S}_0)$ of MG over Var such for each valuation ν over Var, $(q_0, \nu) \in Inf_{\mathcal{S}_0}$ iff $\nu \in Sat(G)$ for some $G \in \mathcal{G}(\mathcal{S}_0)$. Moreover, $\lfloor \mathcal{G}(\mathcal{S}_0) \rfloor_K$ can be computed in time polynomial in the size of $\mathcal{S}_0$ and $\lfloor \mathcal{G}(\mathcal{S}_0) \rfloor_K = \lfloor \mathcal{G}(\lfloor \mathcal{S}_0 \rfloor_K) \rfloor_K$. Then, $\sigma(\mathcal{S}, F)$ is defined as

$$\sigma(\mathcal{S}, F) \stackrel{\text{def}}{=} \left\{ \bigcup_{\{\mathcal{S}_0 \in \mathcal{F}(\mathcal{S},F) \mid \mathcal{S}_0 \text{ has initial control point } (\natural, q)\}} \mathcal{G}(\mathcal{S}_0) \right\}_{q \in Q(\mathcal{S})}. \tag{1}$$

  Note that $\sigma(\mathcal{S}, F)$ is effectively computable. Moreover, by Lemma 16(2), it follows that $\sigma(\mathcal{S}, F)$ is an MG representation of $Inf_{\mathcal{S},F}$. Thus, the first part of the theorem holds. Now, let us consider Properties 1–3.

  Proof of Property 1. Since for all simple GCS $\mathcal{S}_0$, $\lfloor \mathcal{G}(\mathcal{S}_0) \rfloor_K = \lfloor \mathcal{G}(\lfloor \mathcal{S}_0 \rfloor_K) \rfloor_K$, we obtain

$$\lfloor \sigma(\mathcal{S}, F) \rfloor_K = \left\{ \bigcup_{\{\mathcal{S}_0 \in \lfloor \mathcal{F}(\mathcal{S},F) \rfloor_K \mid \mathcal{S}_0 \text{ has initial control point } (\natural, q)\}} \lfloor \mathcal{G}(\mathcal{S}_0) \rfloor_K \right\}_{q \in Q(\mathcal{S})}. \tag{2}$$

  By Lemma 16(4), the family $\lfloor \mathcal{F}(\mathcal{S}, F) \rfloor_K$ of simple GCS can be computed in time $O(|E(\mathcal{S})| \cdot |Q(\mathcal{S})|^2 \cdot (K+2)^{(2|Var|+|Const|)^2})$. Thus, since for all simple GCS $\mathcal{S}_0$, $\lfloor \mathcal{G}(\mathcal{S}_0) \rfloor_K$ can be computed in time polynomial in the size of $\mathcal{S}_0$, by Eq. (2), Property 1 follows. □

  Proof of Property 2. By Lemma 16(5), $\lfloor \mathcal{F}(\mathcal{S}, F) \rfloor_K = \lfloor \mathcal{F}(\lfloor \mathcal{S} \rfloor_K, F) \rfloor_K$. Thus, by Eq. (2), Property 2 follows. □

  Proof of Property 3. We outline an NPSPACE algorithm to check whether for a given $q_0 \in Q(\mathcal{S})$ and a K-bounded MG G over Var, G is in the q_0-component of $\lfloor \sigma(\mathcal{S}, F) \rfloor_K$. Since NPSPACE = PSPACE (by Savitch's theorem), the result follows. Initially, a control point $q \in F$ is guessed. Then, at each step, the nondeterministic algorithm guesses two non-null finite paths $\wp_0$ and $\wp$ of $\mathcal{S}$ such that $s(\wp_0) = q_0$ and $s(\wp) = q$, and it computes the GCS $\mathcal{S}_0$ having the edges $(\natural, s(\wp_0)) \xrightarrow{\lfloor G_{\wp_0} \rfloor_K} t(\wp_0)$ and $s(\wp) \xrightarrow{\lfloor G_{\wp} \rfloor_K} t(\wp)$. The algorithm keeps in memory only the MG $\lfloor G_{\wp_0} \rfloor_K$ and $\lfloor G_{\wp} \rfloor_K$ associated with the paths $\wp_0$ and $\wp$ generated so far, together with their source and target control points. If the current GCS $\mathcal{S}_0$ corresponds to a simple GCS such that $t(\wp_0) = s(\wp) = t(\wp) = q$ and $G \in \lfloor \mathcal{G}(\mathcal{S}_0) \rfloor_K$ (since $\lfloor \mathcal{G}(\mathcal{S}_0) \rfloor_K$ can be computed in polynomial time in the size of $\mathcal{S}_0$, this check can be done in polynomial time in the size of $\mathcal{S}_0$), then the algorithm terminates with success. Otherwise, the algorithm chooses two edges of $\mathcal{S}$ from control points $t(\wp_0)$ and $t(\wp)$, say $t(\wp_0) \xrightarrow{G_0} q'$ and $t(\wp) \xrightarrow{G'} q''$, computes the MG $\lfloor \lfloor G_{\wp_0} \rfloor_K \bullet \lfloor G_0 \rfloor_K \rfloor_K$ and $\lfloor \lfloor G_{\wp} \rfloor_K \bullet \lfloor G' \rfloor_K \rfloor_K$ associated with the currently guessed paths, and re-writes the memory by replacing $\lfloor G_{\wp_0} \rfloor_K$ and $\lfloor G_{\wp} \rfloor_K$ with $\lfloor \lfloor G_{\wp_0} \rfloor_K \bullet \lfloor G_0 \rfloor_K \rfloor_K$ and $\lfloor \lfloor G_{\wp} \rfloor_K \bullet \lfloor G' \rfloor_K \rfloor_K$, and $t(\wp_0)$ and $t(\wp)$ with q' and q'', respectively, and the procedure is repeated. Correctness of the procedure easily follows from Lemma 16(3), Eq. (2), and Proposition 7. □

- **$\mathcal{S}$ is not complete:** we can assume that the theorem holds for complete GCS. By Proposition 14, one can compute a complete GCS $\mathcal{C}(\mathcal{S})$ such that $[\![\mathcal{C}(\mathcal{S})]\!] = [\![\mathcal{S}]\!]$. Thus, we set $\sigma(\mathcal{S}, F) \stackrel{\text{def}}{=} \sigma(\mathcal{C}(\mathcal{S}), F)$, and the first part of the theorem holds.

  Proof of Property 1. Since Property 1 holds for complete GCS, $\lfloor \sigma(\mathcal{C}(\mathcal{S}), F) \rfloor_K$ can be computed in time $O(|E(\mathcal{C}(\mathcal{S}))| \cdot |Q(\mathcal{C}(\mathcal{S}))|^2 \cdot (K+2)^{(2|Var|+|Const|)^2})$. Thus, by Proposition 14, we obtain that $\lfloor \sigma(\mathcal{S}, F) \rfloor_K$ can be computed in time $O(|E(\mathcal{S})| \cdot |Q(\mathcal{S})|^2 \cdot (K+2)^{(2|Var|+|Const|)^2})$, and Property 1 follows. □

Proof of Property 2. Note that $\lfloor \mathcal{S} \rfloor_K$ is not complete. Then,

$$\begin{aligned}
\lfloor \sigma(\mathcal{S}, F) \rfloor_K &= \lfloor \sigma(\mathcal{C}(\mathcal{S}), F) \rfloor_K \\
&= \lfloor \sigma(\lfloor \mathcal{C}(\mathcal{S}) \rfloor_K, F) \rfloor_K && \text{Property 2 holds for complete GCS} \\
&= \lfloor \sigma(\lfloor \mathcal{C}(\lfloor \mathcal{S} \rfloor_K) \rfloor_K, F) \rfloor_K && \text{by Proposition 14} \\
&= \lfloor \sigma(\mathcal{C}(\lfloor \mathcal{S} \rfloor_K), F) \rfloor_K && \text{Property 2 holds for complete GCS} \\
&= \lfloor \sigma(\lfloor \mathcal{S} \rfloor_K, F) \rfloor_K .
\end{aligned}$$

Thus, Property 2 holds. □

Proof of Property 3. Note that by the proof of Proposition 14, an edge of $\mathcal{C}(\mathcal{S})$ is of the form $q \xrightarrow{G \sqcap G'} q'$, where $q \xrightarrow{G} q'$ is an edge of $\mathcal{S}$, and G' is an arbitrary basic complete transitional MG. Thus, by the proof of Property 3 when $\mathcal{S}$ is complete, the result easily follows. □

This concludes the proof of the theorem. □

A similar result holds for unboundedness.

Theorem 9 *(Unboundedness for unrestricted* GCS*). Let $\mathcal{S}$ be a* GCS*. Then, $Unb_{\mathcal{S}}$ is* MG *representable and one can construct an* MG *representation $\sigma(\mathcal{S})$ of $Unb_{\mathcal{S}}$ such that*:

1. *$\lfloor \sigma(\mathcal{S}) \rfloor_K$ can be computed in time $O(|E(\mathcal{S})| \cdot |Q(\mathcal{S})|^2 \cdot (K+2)^{(2|Var|+|Const|)^2})$;*
2. *$\lfloor \sigma(\mathcal{S}) \rfloor_K = \lfloor \sigma(\lfloor \mathcal{S} \rfloor_K) \rfloor_K$;*
3. *given $q_0 \in Q(\mathcal{S})$ and a K-bounded* MG *G over Var, checking whether G is in the q_0-component of $\lfloor \sigma(\mathcal{S}) \rfloor_K$ can be done in polynomial space.*

Proof. The proof is similar to the proof of Theorem 8. The difference is that we use Lemma 17 instead of Lemma 16, and Theorem 5 instead of Theorem 3. Thus, we omit the details here. □

By Theorem 8(3), Theorem 9(3), and Propositions 1 and 2, we obtain the following result.

Corollary 4. *The termination problem, the strong termination problem, and the fairness problem of* GCS*, and their versions w.r.t. a designated state and w.r.t. a control point are all* PSPACE*-complete.*

6. The constrained branching-time temporal logic GCCTL*

In this section, we introduce the constrained branching-time temporal logic GCCTL* and investigate the related satisfiability and model checking problems.

6.1. Syntax and semantics of GCCTL*

The logic GCCTL* is an extension of standard logic CTL* [22], where atomic propositions are replaced with transitional GC. As for standard CTL*, there are two types of formulas in GCCTL*: *state formulas* φ, whose satisfaction is related to a specific state, and *path formulas* ψ, whose satisfaction is related to a specific path. Formally, for the fixed set of variables *Var* and the fixed set of integer constants *Const*, the *state formulas* φ and *path formulas* ψ of GCCTL* are inductively defined as follows:

$$\varphi := \top \mid \varphi \vee \varphi \mid \varphi \wedge \varphi \mid \mathsf{A}\psi \mid \mathsf{E}\psi,$$
$$\psi := \varphi \mid \xi \mid \psi \vee \psi \mid \psi \wedge \psi \mid \bigcirc\psi \mid \Box\psi \mid \psi \,\mathsf{U}\, \psi$$

where $\top$ denotes "*true*", E ("for some path") and A ("for all paths") are *path quantifiers*, ξ is a *transitional* GC, and $\bigcirc$ ("next"), U ("until"), and $\Box$ ("always") are the usual linear temporal operators. We also use the following classical shortcut: $\Diamond\psi \stackrel{\text{def}}{=} \top \,\mathsf{U}\, \psi$ ("eventually"). Since GC constraints are not closed under negation, the logic is not closed under negation as well.[7] The set of state formulas φ forms the language GCCTL*. We also consider the existential and universal fragments E–GCCTL* and A–GCCTL* of GCCTL*, obtained by disallowing the universal and existential path quantifiers, respectively. For a *path* GCCTL* formula ψ, a *maximal* subformula of ψ is a subformula ϑ of ψ such that there is an occurrence of ϑ in ψ which is not in the scope of a path quantifier.

[7] If we allow negation, then the successor relation is definable and by [21], basic decision problems become undecidable.

GCCTL* formulas are interpreted over (possibly infinite) directed graphs $\mathcal{G} = \langle S, \rightarrow, \mu \rangle$ augmented with a mapping μ assigning to each vertex (or state) a valuation over *Var*. For an infinite path $\pi = s_0 \rightarrow s_1 \rightarrow \ldots$ of $\mathcal{G}$, we denote the suffix $s_i \rightarrow s_{i+1} \rightarrow \ldots$ of π by π^i, and the i-th state of π by $\pi(i)$. Let $s \in S$ and π be an infinite path of $\mathcal{G}$. For a state formula φ and a path formula ψ, the satisfaction relations $(\mathcal{G}, s) \models \varphi$ and $(\mathcal{G}, \pi) \models \psi$, meaning that φ holds at state s and ψ holds along π in $\mathcal{G}$, are inductively defined as follows (we omit the clauses for conjunction and disjunction which are standard):

$$
\begin{array}{lcl}
(\mathcal{G}, s) \models \mathsf{A}\psi & \stackrel{\text{def}}{\Leftrightarrow} & \text{for each infinite path } \pi \text{ of } \mathcal{G} \text{ from } s,\ (\mathcal{G}, \pi) \models \psi, \\
(\mathcal{G}, s) \models \mathsf{E}\psi & \stackrel{\text{def}}{\Leftrightarrow} & \text{there is an infinite path } \pi \text{ of } \mathcal{G} \text{ from } s \text{ such that } (\mathcal{G}, \pi) \models \psi, \\
(\mathcal{G}, \pi) \models \varphi & \stackrel{\text{def}}{\Leftrightarrow} & (\mathcal{G}, \pi(0)) \models \varphi, \\
(\mathcal{G}, \pi) \models \xi & \stackrel{\text{def}}{\Leftrightarrow} & \mu(\pi(0)) \oplus \mu(\pi(1)) \models \xi, \\
(\mathcal{G}, \pi) \models \bigcirc\psi & \stackrel{\text{def}}{\Leftrightarrow} & (\mathcal{G}, \pi^1) \models \psi, \\
(\mathcal{G}, \pi) \models \Box\psi & \stackrel{\text{def}}{\Leftrightarrow} & \text{for all } i \geqslant 0, (\mathcal{G}, \pi^i) \models \psi, \\
(\mathcal{G}, \pi) \models \psi_1 \,\mathsf{U}\, \psi_2 & \stackrel{\text{def}}{\Leftrightarrow} & \text{there is } i \geqslant 0 \text{ such that } (\mathcal{G}, \pi^i) \models \psi_2 \text{ and for all } j < i,\ (\mathcal{G}, \pi^j) \models \psi_1.
\end{array}
$$

Note that the *dual* until operator $\widetilde{\mathsf{U}}$ can be expressed in the logic since: $\psi_1 \,\widetilde{\mathsf{U}}\, \psi_2 \equiv \Box\psi_2 \vee (\psi_2 \,\mathsf{U}\, (\psi_1 \wedge \psi_2))$. A GCCTL* formula φ is *satisfiable* iff $(\mathcal{G}, s) \models \varphi$ for some labeled graph $\mathcal{G}$ and state s of $\mathcal{G}$. The *model checking problem of* GCS *against* GCCTL* is checking for a given GCS $\mathcal{S}$, state s of $\mathcal{S}$, and GCCTL* formula φ, whether $(\mathcal{G}(\mathcal{S}), s) \models \varphi$, where $\mathcal{G}(\mathcal{S})$ is obtained from $[\![\mathcal{S}]\!]$ by adding the mapping which assigns to each state of $\mathcal{S}$ the associated valuation over *Var*. We denote by $[\![\varphi]\!]_{\mathcal{S}}$ the set of states s of $\mathcal{S}$ such that $(\mathcal{G}(\mathcal{S}), s) \models \varphi$.

Example 3. Let us consider the requirement: "there is an infinite run from the given state such that variables x and y behave like clocks with rates at least k and k', respectively". This can be expressed by the E–GCCTL* formula

$$\mathsf{E}\Box\big[\big((x' = 0) \vee (x' - x) \geqslant k\big) \wedge \big((y' = 0) \vee (y' - y) \geqslant k'\big)\big].$$

We can also use our framework to solve verification of non-local constraints (between variables at states arbitrarily far away from each other), which are not directly expressible in GCCTL*. As a relevant example, we consider *unboundedness requirements* on the values of a given variable along an infinite run.[8] For each $x \in Var$, let us denote by ξ_x a special atomic formula (*unboundedness constraint*) that holds along an infinite run π iff the set of x-values along π is unbounded. Formally,

$$(\mathcal{G}, \pi) \models \xi_x \quad \stackrel{\text{def}}{\Leftrightarrow} \quad \big\{\big[\mu\big(\pi(i)\big)\big](x) \;\big|\; i \geqslant 0\big\} \text{ is infinite}$$

where $\mathcal{G} = \langle S, \rightarrow, \mu \rangle$. Let E–GCCTL$^*_{ub}$ be the extension of E–GCCTL* with these constraints. We show the following result.

Theorem 10. *Model checking* GCS *against* E–GCCTL$^*_{ub}$ *can be reduced in polynomial time to model checking* GCS *against* E–GCCTL*.

6.1.1. Proof of Theorem 10

Fix a GCS $\mathcal{S}$ over *Var* and an E–GCCTL$^*_{ub}$ formula φ over *Var*. We construct in polynomial-time an extension Var_{ext} of *Var*, a GCS $\mathcal{S}_{ext}$ over Var_{ext}, and an E–GCCTL* formula $f(\varphi)$ over Var_{ext} as follows. For each $x \in Var$, let x_r and x_{prop} be fresh copies of x. Intuitively, x_r is used as register to keep track of the current value of variable x, and x_{prop} is used as atomic proposition. Then, Var_{ext} is the extension of *Var* with these new variables. Moreover, $\mathcal{S}_{ext}$ is defined as follows:

- for each $y \in Var$ and $q \in Q(\mathcal{S})$, let q_y be a fresh copy of q. Then,

$$Q(\mathcal{S}_{ext}) \stackrel{\text{def}}{=} Q(\mathcal{S}) \cup \bigcup_{q \in Q(\mathcal{S})} \bigcup_{y \in Var} \{q_y\}.$$

- $E(\mathcal{S}_{ext})$ is obtained from $E(\mathcal{S})$ by replacing each edge $q \xrightarrow{\xi} p$ in $E(\mathcal{S})$ with the following edges, where y and z range over *Var*:
  - the edges $q \xrightarrow{\xi \wedge \xi'} p$ and $q \xrightarrow{\xi \wedge \xi'} p_y$, where

$$\xi' = \bigwedge_{x \in Var} (x'_r = x_r) \wedge (x_{prop} > 0);$$

[8] Such properties are very useful when checking e.g. the risk of having an unbounded number of duplications of a critical data in a security system which significantly impacts the control enforcement cost for this data.

– the edges $q_z \xrightarrow{\xi \wedge \xi''} p$ and $q_z \xrightarrow{\xi \wedge \xi''} p_y$, where

$$\xi'' = \big(z'_r = z\big) \wedge (z_{prop} = 0) \wedge \bigwedge_{x \in Var \setminus \{z\}} \big(x'_r = x_r\big) \wedge (x_{prop} > 0).$$

Intuitively, the proposition "$x_{prop} = 0$" is used to mark states in which the current value of variable x is stored in the corresponding register x_r. Moreover, whenever "$x_{prop} > 0$" holds, then the value of register x_r is not modified. Finally, the E–GCCTL* formula $f(\varphi)$ is obtained from φ by replacing each occurrence of an unboundedness constraint ξ_x with the E–GCCTL* path formula $f(\xi_x) = f_<(\xi_x) \vee f_>(\xi_x)$, where for each $\sim \in \{<, >\}$, $f_\sim(\xi_x)$ is defined as follows:

$$\big(\Box\Diamond(x_{prop} = 0)\big) \wedge \bigcirc\Box\big((x_{prop} = 0) \rightarrow \bigcirc\big[(x_{prop} > 0)\, \mathsf{U}\, \big((x_{prop} = 0) \wedge (x \sim x_r)\big)\big]\big).$$

Intuitively, by requiring that the proposition "$x_{prop} = 0$" holds infinitely often, we require that the value of register x_r of x is changed infinitely often. Furthermore, every time the register x_r is modified, the old value must be $>$ than the current value (or symmetrically $<$). Thus, along an infinite run we have an infinite number of updates of x with larger and larger values (symmetrically, with smaller and smaller values). Theorem 10 directly follows from the following result.

Theorem 11. *For each state s of $\mathcal{S}$, one can compute in linear-time a state s_{ext} of $\mathcal{S}_{ext}$ so that $(\mathcal{G}(\mathcal{S}), s) \models \varphi$ iff $(\mathcal{G}(\mathcal{S}_{ext}), s_{ext}) \models f(\varphi)$.*

In order to prove Theorem 11, we need additional definitions and preliminary results. A *well-formed mapping* is a function $\Upsilon : N \rightarrow Var$ such that: $N \subseteq \mathbb{N}$ and for each $x \in Var$, $\Upsilon^{-1}(x)$ is infinite. Evidently, the following holds.

Lemma 18. *Let $\xi_{x_1}, \ldots, \xi_{x_n}$ be unboundedness constraints over Var and π be an infinite run of $\mathcal{S}$ of the form $\pi = (q_0, \nu_0) \rightarrow (q_1, \nu_1) \ldots$. Then, $\xi_{x_1} \wedge \cdots \wedge \xi_{x_n}$ holds along π iff there is a well-formed mapping $\Upsilon : N \rightarrow Var$ such that for each $1 \leqslant i \leqslant n$,*

1. *there is $\sim_i \in \{<, >\}$ so that for each $h \in \Upsilon^{-1}(x_i)$, $\nu_{next(h)}(x_i) \sim_i \nu_h(x_i)$, where $next(h)$ is the smaller $k > h$ such that $\Upsilon(k) = x_i$ (note that such a $next(h)$ exists).*

For a state (q, ν) of $\mathcal{S}$, an *extension* of (q, ν) is a state of $\mathcal{S}_{ext}$ of the form (q', ν') such that ν' is an extension of ν, and the following hold: either $q' = q$ and $\nu'(x_{prop}) > 0$ for each $x \in Var$, or for some $y \in Var$, $q' = q_y$, $\nu'(y_{prop}) = 0$ and $\nu'(x_{prop}) > 0$ for each $x \in Var \setminus \{y\}$. An *extension* of an infinite run π of $\mathcal{S}$ is an infinite run π' of $\mathcal{S}_{ext}$ such that for each $i \geqslant 0$, state $\pi'(i)$ is an extension of $\pi(i)$. Now, we prove the following result.

Lemma 19. *Let $\xi_{x_1}, \ldots, \xi_{x_n}$ be unboundedness constraints over Var, π be an infinite run of $\mathcal{S}$ starting from (q, ν), and (q', ν') be an extension of (q, ν). Then, $\xi_{x_1} \wedge \cdots \wedge \xi_{x_n}$ holds along π iff there is an extension π' of π starting from (q', ν') such that $(\mathcal{G}(\mathcal{S}_{ext}), \pi') \models f(\xi_{x_1}) \wedge \cdots \wedge f(\xi_{x_n})$.*

Proof. ($\Rightarrow$) Assume that $\xi_{x_1} \wedge \cdots \wedge \xi_{x_n}$ holds along $\pi = (q_0, \nu_0) \rightarrow (q_1, \nu_1) \ldots$, where $(q_0, \nu_0) = (q, \nu)$. By Lemma 18, there is a well-formed mapping $\Upsilon : N \rightarrow Var$ such that for each $1 \leqslant i \leqslant n$, Property 1 in Lemma 18 holds. Let $\pi' = (q'_0, \nu'_0), (q'_1, \nu'_1), \ldots$ be the infinite sequence of states of $\mathcal{S}_{ext}$ defined as follows: $(q'_0, \nu'_0) = (q', \nu')$ and for all $i > 0$,

- $q'_i = q_i$ if $i \notin N$, and $q'_i = (q_i)_{\Upsilon(i)}$ otherwise;
- $(\nu'_i)_{Var} = \nu_i$ and for each $x \in Var$, $\nu'_i(x_r) = \nu'_{i-1}(x)$ if $i - 1 \in \Upsilon^{-1}(x)$, and $\nu'_i(x_r) = \nu'_{i-1}(x_r)$ otherwise;
- for each $x \in Var$, $\nu'_i(x_{prop}) = 0$ if $i \in \Upsilon^{-1}(x)$, and $\nu'_i(x_{prop}) = 1$ otherwise.

By definition of $\mathcal{S}_{ext}$, it follows that π' is an infinite run of $\mathcal{S}_{ext}$ starting from (q', ν') which is an extension of π. Moreover, since Υ satisfies Property 1 in Lemma 18, by construction it easily follows that $(\mathcal{G}(\mathcal{S}_{ext}), \pi') \models f(\xi_{x_1}) \wedge \cdots \wedge f(\xi_{x_n})$.

($\Leftarrow$) Assume that π' is an extension of $\pi = (q_0, \nu_0) \rightarrow (q_1, \nu_1) \ldots$ starting from (q', ν') such that $(\mathcal{G}(\mathcal{S}_{ext}), \pi') \models f(\xi_{x_1}) \wedge \cdots \wedge f(\xi_{x_n})$. Then, by construction, there is a well-formed mapping $\Upsilon : N \rightarrow Var$ such that for each $1 \leqslant i \leqslant n$, Property 1 in Lemma 18 holds. Thus, by Lemma 18, the result follows. □

Theorem 11 directly follows from the following result, which is proved by using Lemma 19 (since φ is an existential formula, we can assume that $\varphi = \mathsf{E}\psi$ for some path formula ψ).

Lemma 20. *Let $\mathsf{E}\psi$ be a subformula of φ. Then, for each state s of $\mathcal{S}$ and extension s_{ext} of s, $(\mathcal{G}(\mathcal{S}), s) \models \mathsf{E}\psi$ iff $(\mathcal{G}(\mathcal{S}_{\text{ext}}), s_{\text{ext}}) \models f(\mathsf{E}\psi)$.*

Proof. The proof is by structural induction on $\mathsf{E}\psi$. By induction hypothesis, we can assume that the result holds for each state subformula of ψ of the form $\mathsf{E}\psi'$.

($\Rightarrow$) Assume that $(\mathcal{G}(\mathcal{S}), s) \models \mathsf{E}\psi$. Then, there is an infinite run π of $\mathcal{S}$ starting from s such that $(\mathcal{G}(\mathcal{S}), \pi) \models \psi$. Let $\xi_{x_1}, \ldots, \xi_{x_n}$ be all and only the unboundedness constraints over Var that hold along π. By Lemma 19, there is an extension π' of π starting from s_{ext} such that $(\mathcal{G}(\mathcal{S}_{ext}), \pi') \models f(\xi_{x_1}) \wedge \cdots \wedge f(\xi_{x_n})$. Since for each suffix $(\pi')^i$ of π', $(\mathcal{G}(\mathcal{S}_{ext}), (\pi')^i) \models f(\xi_{x_1}) \wedge \cdots \wedge f(\xi_{x_n})$ holds as well, and ψ is in positive normal form (and negation is never used), by a nested structural induction, it easily follows that for each *maximal* subformula ψ' of ψ and $i \geqslant 0$, $(\mathcal{G}(\mathcal{S}), \pi^i) \models \psi'$ implies $(\mathcal{G}(\mathcal{S}_{ext}), (\pi')^i) \models f(\psi')$. Hence, the result follows.

($\Leftarrow$) Assume that $(\mathcal{G}(\mathcal{S}_{ext}), s_{ext}) \models f(\mathsf{E}\psi)$. Then, there is an infinite run π' of $\mathcal{S}_{ext}$ starting from s_{ext} such that $(\mathcal{G}(\mathcal{S}_{ext}), \pi') \models f(\psi)$. By definition of $\mathcal{S}_{ext}$, it easily follow that π' is an extension of some infinite run π of $\mathcal{S}$ starting from s. Let $\xi_{x_1}, \ldots, \xi_{x_n}$ be all and only the unboundedness constraints over Var such that $(\mathcal{G}(\mathcal{S}_{ext}), \pi') \models f(\xi_{x_1}) \wedge \cdots \wedge f(\xi_{x_n})$. By Lemma 19, $\xi_{x_1}, \ldots, \xi_{x_n}$ hold along π. Since for each suffix $(\pi')^i$ of π', $(\mathcal{G}(\mathcal{S}_{ext}), (\pi')^i) \models f(\xi_{x_1}) \wedge \cdots \wedge f(\xi_{x_n})$ holds as well, and ψ is in positive normal form (and negation is never used), by a nested structural induction, it follows that for each maximal subformula ψ' of ψ and $i \geqslant 0$, $(\mathcal{G}(\mathcal{S}_{ext}), (\pi')^i) \models f(\psi')$ implies $(\mathcal{G}(\mathcal{S}), \pi^i) \models \psi'$. Hence, the result follows. □

6.2. Decision procedures

In this subsection, we investigate decidability and complexity issues for satisfiability and model checking of GCCTL* and its fragments E–GCCTL* and A–GCCTL*. By [16], model checking GCS against GCCTL* is undecidable. It is straightforward to extend this negative result to model checking GCS against A–GCCTL*.

Theorem 12. *Model checking* GCS *against* A–GCCTL* *is undecidable.*

Proof. We say that a GCS $\mathcal{S}$ is *total* if for each control point q, the disjunction of all transitional GC labeling the edges with source q is a valid formula, i.e. every valuation over $Var \cup Var'$ satisfies the formula (note that we can effectively check this condition). Note that in a total GCS $\mathcal{S}$, each state has at least a successor. Let NE–GCCTL* be the logic defined exactly as E–GCCTL* with the unique difference that an atomic formula is the negation of a transitional GC. Now, we observe that positive boolean combinations of negations of transitional GC allow to express increment and decrement of a counter variable, and test for zero. For example, $x' = x + 1$ is equivalent to $\neg(x' - x \geqslant 2) \wedge \neg(x - x' \geqslant 0)$, and $x = 0$ is equivalent to $\neg(x \geqslant 1) \wedge \neg(-x \geqslant 1)$. It follows that one can easily encode in NE–GCCTL* the evolution of a Minsky counter machine. Hence, undecidability of its satisfiability and model checking (w.r.t. the class of total GCS) problems easily follows. Now, we observe that over total GCS, NE–GCCTL* is the dual of A–GCCTL*. Hence, undecidability of model checking GCS against A–GCCTL* follows. □

In the following we show that model checking GCS against E–GCCTL* and satisfiability for E–GCCTL* and A–GCCTL* are instead decidable and PSPACE-complete. The decidability status for satisfiability of full GCCTL* remains open.

First, we consider model checking GCS against E–GCCTL*. The proposed approach is a generalization of the standard automata-theoretic approach for model checking finite-state systems against standard linear temporal logic LTL [33]. Recall that for a finite alphabet Σ, a Büchi (nondeterministic finite-state word) automaton over Σ is a tuple $\mathcal{A} = \langle P, p_0, \Delta, F \rangle$, where P is the finite set of states, $p_0 \in P$ is the initial state, Δ is the finite set of transitions of the form $p \xrightarrow{\sigma} p'$, where $p, p' \in P$ and $\sigma \in \Sigma$, and $F \subseteq P$ is the set of accepting states. An infinite run of $\mathcal{A}$ is an infinite sequence π (from the initial state p_0) of the form $\pi = p_0 \xrightarrow{\sigma_0} p_1 \xrightarrow{\sigma_1} p_2 \ldots$ such that $p_i \xrightarrow{\sigma_i} p_{i+1} \in \Delta$ for all $i \geqslant 0$. The run π is *accepting* if for infinitely many $i \geqslant 0$, $p_i \in F$. The ω-language $\mathcal{L}(\mathcal{A})$ of $\mathcal{A}$ is the set of infinite words $w = w(0)w(1)\ldots$ over Σ such that there is an accepting infinite run of the form $\pi = p_0 \xrightarrow{w(0)} p_1 \xrightarrow{w(1)} p_2 \ldots$. The following is a well-known result [33].

Proposition 15. *(See [33].) Given an* LTL *formula ϕ over a finite set Prop of atomic propositions, one can construct in singly exponential time a Büchi automaton $\mathcal{A}_\phi$ over 2^{Prop} of size $2^{O(|\phi|)}$ such that $\mathcal{L}(\mathcal{A}_\phi)$ is the set of infinite words over 2^{Prop} satisfying ϕ.*

Let ψ be a path E–GCCTL* formula. Let $At(\psi)$ be the set of atomic formulas (i.e., transitional GC) which are *maximal* subformulas of ψ and $St(\psi)$ be the set of existential state formulas $\mathsf{E}\psi'$ which are *maximal* subformulas of ψ. A *ψ-valuation* is an infinite word over the finite alphabet $2^{At(\psi) \cup St(\psi)}$. Note that ψ can be seen as an LTL formula, written LTL(ψ), over the set of atomic propositions given by $At(\psi) \cup St(\psi)$. In accordance with this, we denote by $\mathcal{A}_\psi$ the Büchi automaton over the alphabet $2^{At(\psi) \cup St(\psi)}$ associated with LTL(ψ) and satisfying Proposition 15. By the semantics of E–GCCTL* and Proposition 15, we easily obtain the following result.

Lemma 21. *Let $\mathcal{S}$ be a* GCS*, s be an $\mathcal{S}$-state, and* Eψ *be* E–GCCTL* *formula. Then,* $(\mathcal{G}(\mathcal{S}), s) \models \mathsf{E}\psi$ iff *there are an infinite run $\pi = (q_0, \nu_0) \to (q_1, \nu_1) \ldots$ of $\mathcal{S}$ with $(q_0, \nu_0) = s$ and a ψ-valuation $X = X(0)X(1)\ldots$ such that $X \in \mathcal{L}(\mathcal{A}_\psi)$ and for all $i \geqslant 0$,*

- *for all $\xi \in X(i)$, $\nu_i \oplus \nu_{i+1} \in Sat(\xi)$;*
- *for all $\mathsf{E}\psi' \in X(i)$, $(\mathcal{G}(\mathcal{S}), (q_i, \nu_i)) \models \mathsf{E}\psi'$.*

Now, we can prove the main result of this subsection.

Theorem 13. *Given a* GCS $\mathcal{S}$ *and an* E–GCCTL* *formula* φ, $[\![\varphi]\!]_{\mathcal{S}}$ *is* MG *representable and one can construct an* MG *representation of* $[\![\varphi]\!]_{\mathcal{S}}$, *written* $\pi(\mathcal{S},\varphi)$, *satisfying the following*:

1. $\lfloor \pi(\mathcal{S},\varphi)\rfloor_K$ *can be built in time* $O(|E(\mathcal{S})|\cdot|Q(\mathcal{S})|^2\cdot 2^{O(|\varphi|)}\cdot(K+2)^{O((2|Var|+|Const|)^2)})$;
2. *for a* K*-bounded* MG G *on* Var *and* $q\in Q(\mathcal{S})$, *checking whether* G *is in the* q*-component of* $\lfloor \pi(\mathcal{S},\varphi)\rfloor_K$ *can be done in polynomial space.*

Proof. Fix a GCS $\mathcal{S}$. For an E–GCCTL* formula φ, we construct $\pi(\mathcal{S},\varphi)$ and prove Properties 1 and 2 by induction on the structure of φ. If φ is either $\top$ or a conjunction or a disjunction of E–GCCTL* formulas, then the result easily follows from the induction hypothesis, Proposition 5, and Proposition 7. The remaining case is when $\varphi=\mathsf{E}\psi$ for some path E–GCCTL* formula ψ. We prove the result by a reduction to the fairness problem of GCS. By the induction hypothesis, we can assume that the theorem holds for each state formula θ such that $\theta\in St(\psi)$. Let $\mathcal{A}_\psi=\langle P,p_0,\Delta,F\rangle$ be the Büchi finite state automaton over $2^{At(\psi)\cup St(\psi)}$ associated with LTL(ψ). We construct two GCS $\mathcal{S}_\varphi$ and $\mathcal{S}^{bd}_\varphi$ as follows:

- $Q(\mathcal{S}_\varphi)\stackrel{\text{def}}{=}Q(\mathcal{S})\times P$ and $Q(\mathcal{S}^{bd}_\varphi)\stackrel{\text{def}}{=}Q(\mathcal{S})\times P$. Thus, $Q(\mathcal{S}_\varphi)=Q(\mathcal{S}^{bd}_\varphi)$ and a control point of $Q(\mathcal{S}_\varphi)$ consists of a pair (q,p), where q is a control point of $\mathcal{S}$ and p is a state of $\mathcal{A}_\psi$.
- $(q,p)\xrightarrow{G}(q',p')$ is an edge of $\mathcal{S}_\varphi$ iff there are an edge of $\mathcal{S}$ of the form $q\xrightarrow{G_0}q'$ and a transition $p\xrightarrow{X}p'$ of $\mathcal{A}_\psi$ with $X\cap St(\psi)=\{\theta_1,\ldots,\theta_k\}$ and $X\cap At(\psi)=\{\xi_1,\ldots,\xi_h\}$ such that
$$G=G_0\sqcap G_1\sqcap\cdots\sqcap G_k\sqcap G(\xi_1)\sqcap\cdots\sqcap G(\xi_h)$$
where for all $1\leqslant j\leqslant k$, the MG G_j belongs to the q-component of the computable MG-representation $\pi(\mathcal{S},\theta_j)$ of $[\![\theta_j]\!]_{\mathcal{S}}$.
- $(q,p)\xrightarrow{G}(q',p')$ is an edge of $\mathcal{S}^{bd}_\varphi$ iff there are an edge of $\mathcal{S}$ of the form $q\xrightarrow{G_0}q'$ and a transition $p\xrightarrow{X}p'$ of $\mathcal{A}_\psi$ with $X\cap St(\psi)=\{\theta_1,\ldots,\theta_k\}$ and $X\cap At(\psi)=\{\xi_1,\ldots,\xi_h\}$ such that
$$G=\lfloor G_0\rfloor_K\sqcap G_1\sqcap\cdots\sqcap G_k\sqcap\left\lfloor G(\xi_1)\right\rfloor_K\sqcap\cdots\sqcap\left\lfloor G(\xi_h)\right\rfloor_K$$
where for all $1\leqslant j\leqslant k$, the MG G_j belongs to the q-component of $\lfloor\pi(\mathcal{S},\theta_j)\rfloor_K$.

Note that by construction $((q,p_0),\nu)\in Inf_{\mathcal{S}_\varphi,Q(\mathcal{S})\times F}$ *iff* there are an infinite run $\pi=(q_0,\nu_0)\to(q_1,\nu_1)\ldots$ of $\mathcal{S}$ with $(q_0,\nu_0)=(q,\nu)$ and a ψ-valuation $X=X(0)X(1)\ldots$ such that $X\in\mathcal{L}(\mathcal{A}_\psi)$ and for all $i\geqslant 0$, the following hold:

- for all $\xi\in X(i)$, $\nu_i\oplus\nu_{i+1}\in Sat(\xi)$;
- for all $\mathsf{E}\psi'\in X(i)$, $\nu_i\in Sat(G)$ for some MG G belonging to the q_i-component of $\pi(\mathcal{S},\mathsf{E}\psi')$. Hence, for all $\mathsf{E}\psi'\in X(i)$, $(\mathcal{G}(\mathcal{S}),(q_i,\nu_i))\models\mathsf{E}\psi'$.

Thus, by Lemma 21, the following claim follows.

Claim 1. $(q,\nu)\in[\![\varphi]\!]_{\mathcal{S}}$ *if and only if there is an infinite run of* $\mathcal{S}_\varphi$ *from* $((q,p_0),\nu)$ *which is fair w.r.t.* $Q(\mathcal{S})\times F$ (*i.e.,* $((q,p_0),\nu)\in Inf_{\mathcal{S}_\varphi,Q(\mathcal{S})\times F}$).

Moreover, by construction, the induction hypothesis, and Propositions 7 and 15, we easily obtain the following.

Claim 2. $\mathcal{S}^{bd}_\varphi$ *can be built in time* $O(|E(\mathcal{S})|\cdot|Q(\mathcal{S})|^2\cdot 2^{O(|\varphi|)}\cdot(K+2)^{O((2|Var|+|Const|)^2)})$ *starting from* $\mathcal{S}$ *and* $\{\lfloor\pi(\mathcal{S},\theta)\rfloor_K\mid\theta\in X\}$. *Moreover,* $\mathcal{S}^{bd}_\varphi=\lfloor\mathcal{S}_\varphi\rfloor_K$.

Now, by using Claims 1 and 2, we construct an MG representation $\pi(\mathcal{S},\varphi)$ of $[\![\varphi]\!]_{\mathcal{S}}$ and show that it satisfies Properties 1 and 2 of the theorem. Let $\sigma_F(\mathcal{S}_\varphi)$ be the *computable* MG representation of $Inf_{\mathcal{S}_\varphi,Q(\mathcal{S})\times F}$ satisfying the statement of Theorem 8. Then, for each $q\in Q(\mathcal{S})$, the q-component of $\pi(\mathcal{S},\varphi)$ is the (q,p_0)-component of $\sigma_F(\mathcal{S}_\varphi)$. By Claim 1, it follows that $\pi(\mathcal{S},\varphi)$ is a *computable* MG representation of $[\![\varphi]\!]_{\mathcal{S}}$. By Claim 2, $\mathcal{S}^{bd}_\varphi=\lfloor\mathcal{S}_\varphi\rfloor_K$, hence, by Property 2 of Theorem 8, $\lfloor\sigma_F(\mathcal{S}_\varphi)\rfloor_K=\lfloor\sigma_F(\mathcal{S}^{bd}_\varphi)\rfloor_K$. Thus, since $Q(\mathcal{S}^{bd}_\varphi)$ has cardinality bounded by $|Q(\mathcal{S})|\cdot 2^{O(|\varphi|)}$ and $E(\mathcal{S}^{bd}_\varphi)$ has cardinality bounded by $|E(\mathcal{S})|\cdot 2^{O(|\varphi|)}\cdot(K+2)^{(2|Var|+|Const|)^2}$ (the MG of $\mathcal{S}^{bd}_\varphi$ are K-bounded), by Property 1 of Theorem 8 and Claim 2, Property 1 in the theorem follows. Now, let us consider Property 2. By the induction hypothesis, we can assume that Property 2 holds for each formula in $St(\psi)$. Moreover, by the above considerations, it suffices to show that given a K-bounded MG G over Var and $(q,p)\in Q(\mathcal{S}^{bd}_\varphi)$, checking whether G is in the (q,p)-component of $\lfloor\sigma_F(\mathcal{S}^{bd}_\varphi)\rfloor_K$ can be done in space polynomial in the sizes of $\mathcal{S}$ and φ. By Property 3 of Theorem 8, this check can be done in space polynomial in the size of $\mathcal{S}^{bd}_\varphi$. However, we can do better as follows. In fact, as illustrated in the proof of Theorem 8, the nondeterministic algorithm that checks whether G is in the (q,p)-component of $\lfloor\sigma_F(\mathcal{S}^{bd}_\varphi)\rfloor_K$ keeps in memory only the K-bounded MG $\lfloor G_{\wp_0}\rfloor_K$ and

$\lfloor G_{\wp} \rfloor_K$ associated with the guessed two non-null finite paths $\wp_0$ and $\wp$ generated so far, together with their source and target control points. If the successful termination condition is not satisfied, then:

(a) the algorithm chooses two edges e_0 and e of $\mathcal{S}^{bd}_{\varphi}$ from control points $t(\wp_0)$ and $t(\wp)$, and
(b) computes the K-bounded transitional MG associated with the new guessed paths $\wp_0 \cdot e_0$ and $\wp \cdot e$.

Now, by definition of $\mathcal{S}^{bd}_{\varphi}$, the K-bounded transitional MG labeling the edge e_0 (resp., e) depend on the MG belonging to the components of $\lfloor \pi(\mathcal{S}, \theta) \rfloor_K$, where $\theta \in St(\psi)$. Then, we modify part (a) of the algorithm as follows:

(a′) the algorithm guesses two edges e_0 and e from control points $t(\wp_0)$ and $t(\wp)$ whose labels are K-bounded transitional MG, and checks that e_0 and e are indeed edges of $\mathcal{S}^{bd}_{\varphi}$. If the check is negative, then the algorithm terminates unsuccessfully. Otherwise, the algorithm performs part (b).

Recall that the finite-state automaton $\mathcal{A}_{\psi}$ can be constructed on-the-fly [33]. Then, the crucial observation is that by the induction hypothesis, the check in (a′) can be done in space polynomial in the sizes of $\mathcal{S}$ and the state subformulas $\theta \in St(\psi)$. Hence, the nondeterministic algorithm runs in space polynomial in the sizes of $\mathcal{S}$ and φ. Since NPSPACE = PSPACE, Property 2 in the theorem follows, which concludes. □

Theorem 14. *Model checking* GCS *against* E–GCCTL* *and satisfiability of* E–GCCTL* *and* A–GCCTL* *are* PSPACE*-complete.*

Proof. The lower bounds directly follow from PSPACE-hardness of model checking and satisfiability for the existential and universal fragments of standard CTL* (see, e.g., [27]). Now, let us consider the upper bounds.

Upper bound for model checking GCS *against* E–GCCTL*: the proof is by a linear-time reduction to the problem of checking for a given GCS $\mathcal{S}$, control point q, and E–GCCTL* formula φ, whether $(\mathcal{G}(\mathcal{S}), (q, \nu)) \models \varphi$ for some valuation ν over *Var* (by Theorem 13, this last problem is in PSPACE). Fix a GCS $\mathcal{S}$, a state (q_0, ν_0) of $\mathcal{S}$, and an E–GCCTL* formula φ. W.l.o.g. we assume that φ does not contain occurrences of $\top$. Moreover, we can assume that $\nu_0(x) \in Const$ for each $x \in Var$ (otherwise, we extend *Const* by including the integers $\nu_0(x)$ with $x \in Var$). Let $G_{=}$ be the transitional MG corresponding to the GC given by $\bigwedge_{x \in Var} x = \nu_0(x)$ and $q'_0 \notin Q(\mathcal{S})$ be a fresh control point. We construct a new GCS $\mathcal{S}_0$ as follows: $\mathcal{S}_0$ is obtained from $\mathcal{S}$ by adding for each edge of $\mathcal{S}$ of the form $q_0 \xrightarrow{G} q$, the edge $q'_0 \xrightarrow{G \sqcap G_{=}} q$. We claim that $(q_0, \nu_0) \in [\![\varphi]\!]_{\mathcal{S}}$ iff $(q'_0, \nu) \in [\![\varphi]\!]_{\mathcal{S}_0}$ for some valuation ν over *Var*, hence the result follows. The claim directly follows from the following facts, which can be easily proved:

- Let T and T_0 be the unwindings of $[\![\mathcal{S}]\!]$ and $[\![\mathcal{S}_0]\!]$ starting from (q_0, ν_0) and (q'_0, ν_0), respectively. If we replace the label (q'_0, ν_0) of the root of T_0 with the label (q_0, ν_0), then the resulting labeled tree is isomorphic to T.
- For a valuation ν over *Var* such that $\nu \neq \nu_0$, (q'_0, ν) has no successors in $[\![\mathcal{S}_0]\!]$. Hence, $(q'_0, \nu) \notin [\![\varphi]\!]_{\mathcal{S}_0}$.

Upper bound for satisfiability of E–GCCTL*: the proof is by a linear-time reduction to the problem of checking for a given GCS $\mathcal{S}$, control point q, and E–GCCTL* formula φ, whether $(\mathcal{G}(\mathcal{S}), (q, \nu)) \models \varphi$ for some valuation ν over *Var*. Let S_0 be the GCS having a unique edge (which is a self-loop) of the form $q \xrightarrow{G} q$ such that G is equivalent to *true*. Evidently, given an E–GCCTL* formula φ, φ is satisfiable iff $(\mathcal{G}(\mathcal{S}_0), (q, \nu)) \models \varphi$ for some valuation ν over *Var*.

Upper bound for satisfiability of A–GCCTL*: in fact, we consider satisfiability of A–GCCTL* restricted to the class of labeled graphs admitting at least an infinite path (without this restriction, by the semantics of the universal path quantifier, each A–GCCTL* formula would be satisfiable). Formally, an A–GCCTL* formula φ is *strongly* satisfiable iff $(\mathcal{G}, s) \models \varphi$ for some labeled graph $\mathcal{G}$ and state s of $\mathcal{G}$ such that there is some infinite path of $\mathcal{G}$ from s. The upper bound for the considered problem is shown by a linear-time reduction to satisfiability of E–GCCTL*. Let φ be an A–GCCTL* formula, and let $\mathsf{E}\widetilde{\varphi}$ be the E–GCCTL* formula, where $\widetilde{\varphi}$ is obtained from φ by removing each occurrence of the universal path quantifier. Evidently, φ is strongly satisfiable iff $\mathsf{E}\widetilde{\varphi}$ is satisfiable. Hence, the result follows. □

7. Concluding remarks

We conclude by giving some future research directions.

A possible direction is connected to the termination analysis of GCS. In particular, in termination analysis of programs, a classical method is the ranking function argument. In this method, the goal is finding a witness for uniform termination, i.e. a mapping (global ranking function) that associates a rank to every state of the program over a well-founded ordered domain (such as the set of natural numbers) and such that every transition of the program decreases the rank. For applications, an explicit ranking expression may provide an easy-to-verify witness for termination, since verification only amounts to checking it against every transition. Moreover, since a ranking function provides a witness for a termination proof, it is interesting for program certification. For example, for the class of MCS, A. Ben-Amram in [8] provides a procedure to

construct explicit global ranking functions in singly exponential time. It would be interesting to generalize the approach proposed by Ben-Amram for the more expressive class of GCS.

Regarding the logic GCCTL*, an intriguing question left open is the decidability status for satisfiability of full GCCTL*. We think that this is an important issue that deserves future investigation. Notice that the argument used for undecidability of model-checking MCS or IRA against CTL extended with MC [16] relies on the observation that existential and universal quantification over counter variables can be simulated by the path quantifiers of the logic and by using the fact that the formalism is infinite-branching (in particular, one can ensure that a variable assumes all the possible values in the successors of a given state). The "infinitely-branching requirement" which is crucial in the undecidability argument for model-checking cannot be applied to the satisfiability problem, and in fact, one can show that the logic GCCTL* satisfies the bounded-tree model property. Hence, establishing the decidability status for satisfiability of GCCTL* seems challenging.

Moreover, it would be interesting to investigate extensions of GCCTL* with mechanisms allowing one to compare variables at states arbitrarily far away from each other. In logical languages, these mechanisms are usually expressed by the use of *freeze* quantifiers and register variables. The freeze mechanism allows one to store a value in a register and to test later the value in the register with a current value. This operator is useful to compare values at distinct states of Kripke-like structures and has found applications in many logical frameworks such as real-time logics, hybrid logics, and regular linear-time logic LTL extended with Presburger constraints. However, it is well-known that the freeze operator can easily lead to undecidability. Thus, a goal is to individuate weak and still interesting "freeze" mechanisms which may lead to decidable and possibly tractable logics. For the logic GCCTL*, a possibility would be to permit atomic formulas of the form $x - \Diamond y \geqslant k$, or $\Diamond y - x \geqslant k$, or $x - \Box y \geqslant k$, or $\Box y - x \geqslant k$ ($k \in \mathbb{N}$), where $\Diamond y$ means "for some future value of y" and $\Box y$ means "for each future value of y". Thus, for example, $x - \Box y \geqslant 1$ asserts that the future values of y remain below the current value of x. We conjecture that for this extension, Theorem 14 still holds. Our intuition is that for the existential fragment of this extension, model checking GCS might be solved by using an approach similar to the one proposed in [5] for model checking timed automata against metric temporal logic without singular intervals.

Finally, there are other important questions left open in this paper. We have shown that it is possible to compute Presburger representations for the sets of terminating, strong terminating, and fair states of a GCS. The same holds for the set of states of a GCS satisfying a given E–GCCTL* formula. The possibility of computing these representations is crucially based on Theorem 2, or, equivalently, on the possibility of computing an MG representation of the binary reachability relation of a GCS. In particular, an elementary algorithm (for example, a singly exponential time algorithm) for constructing the finite set of sample paths of Theorem 2 would lead to elementary algorithms for computing the above Presburger representations. On the other hand, we are not able to give an upper bound on the time complexity of the proposed algorithm that computes the set of sample paths (the algorithm is based on a fixpoint iteration whose termination is guaranteed by a suitable decidable well-quasi-ordering defined over the set of transitional MG). This means that our method cannot be trivially extended in order to show that the above Presburger representations can be computed in elementary time/space. Moreover, we believe that answering these questions is not trivial, due to analogous questions for other classes of infinite-state formalisms. For example, the computation of the finite set of sample paths is similar to the computation of the coverability graph of a Petri net, and it is known that the size of the coverability graph can be non-primitive-recursive [15].

Appendix A

A.1. Proof of Theorem 2

In order to prove Theorem 2, we need additional preliminary results. Recall that for a set S, a *pre-order* $\preceq$ over S is a reflexive and transitive (binary) relation on S. The pre-order $\preceq$ is a *well-quasi-ordering* if, additionally, for every infinite sequence $y_0, y_1, y_2, \ldots$ of elements of S, there exist indices $i < j$ such that $y_i \preceq y_j$.

Definition 20 *(Pre-order on transitional* MG*).* We define a pre-order $\preceq$ on transitional MG as follows: $G \preceq G'$ if *either* G' is unsatisfiable, *or* for each edge $u \xrightarrow{k} v$ of G, there is an edge in G' of the form $u \xrightarrow{k'} v$ such that $k' \geqslant k$. Note that $G \preceq G'$ implies $Sat(G') \subseteq Sat(G)$.

Definition 21 *(Pre-order on finite paths of a* GCS*).* Let $\mathcal{S}$ be a GCS. We denote by $\preceq_{\mathcal{S}}$ be the pre-order over the set of non-null finite paths of $\mathcal{S}$ defined as follows: $\wp \preceq \wp'$ if $s(\wp) = s(\wp')$, $t(\wp) = t(\wp')$, $\lfloor G_{\wp} \rfloor_K = \lfloor G_{\wp'} \rfloor_K$, and $G_{\wp} \preceq G_{\wp'}$. Moreover, given two finite sets $\mathcal{P}$ and $\mathcal{P}'$ of non-null finite paths of $\mathcal{S}$, we write $\mathcal{P} \sqsubseteq_{\mathcal{S}} \mathcal{P}'$ iff for each $\wp' \in \mathcal{P}'$ there is $\wp \in \mathcal{P}$ such that $\wp \preceq_{\mathcal{S}} \wp'$. Note that $\sqsubseteq_{\mathcal{S}}$ is a pre-order.

Lemma 22. *The pre-orders $\preceq$ and $\preceq_{\mathcal{S}}$ (for a* GCS *$\mathcal{S}$) are well-quasi-orderings.*

Proof. Since the set of K-bounded transitional MG is finite and the set of control points of a GCS $\mathcal{S}$ is finite, the result easily follows from well-quasi-ordering of the relation $\leqslant_h$ (for a fixed $h \in \mathbb{N}$) defined over the set of h-tuples of natural numbers as $(n_1, \ldots, n_h) \leqslant_h (m_1, \ldots, m_h)$ if $n_i \leqslant m_i$ for each $1 \leqslant i \leqslant h$ [29]. □

Lemma 23. *Let $\mathcal{S}$ be a* GCS *and $\wp \preceq_{\mathcal{S}} \wp'$. Then, for each non-null finite path $\wp''$ of $\mathcal{S}$ such that $s(\wp'') = t(\wp) = t(\wp')$, it holds that $\wp\wp'' \preceq_{\mathcal{S}} \wp'\wp''$.*

Proof. Let $\wp \preceq_{\mathcal{S}} \wp'$ and $\wp''$ as in the statement of the lemma. By the definition of the composition operator and definition of $\preceq$, for all transitional MG G, G', G'', $G \preceq G'$ implies $G \bullet G'' \preceq G' \bullet G''$. Thus, since $G_\wp \preceq G_{\wp'}$ (by hypothesis) and the composition operator is associative, we obtain that $G_{\wp\wp''} = G_\wp \bullet G_{\wp''} \preceq G_{\wp'} \bullet G_{\wp''} = G_{\wp'\wp''}$. Moreover, since $\lfloor G_\wp \rfloor_K = \lfloor G_{\wp'} \rfloor_K$ (by hypothesis), by Proposition 7, it follows that $\lfloor G_{\wp\wp''} \rfloor_K = \lfloor G_{\wp'\wp''} \rfloor_K$. Hence, the result follows. □

Lemma 24. *Let $\mathcal{S}$ be a* GCS *and $\mathcal{P}_1, \mathcal{P}_2, \ldots$ be an infinite sequence of finite sets of non-null finite paths of $\mathcal{S}$ such that $\mathcal{P}_{i+1} \sqsubseteq_{\mathcal{S}} \mathcal{P}_i$ for each $i \geqslant 1$. Then, there is $k \geqslant 1$ such that $\mathcal{P}_k \sqsubseteq_{\mathcal{S}} \mathcal{P}_{k+1}$.*

Proof. We assume the contrary and derive a contradiction. Hence, $\mathcal{P}_{i+1} \sqsubseteq_{\mathcal{S}} \mathcal{P}_i$ and $\mathcal{P}_i \not\sqsubseteq_{\mathcal{S}} \mathcal{P}_{i+1}$ for each $i \geqslant 1$. Then, we deduce the following:

Claim. *For each $j > 1$, there is $\wp_j \in \mathcal{P}_j$ such that for all $i < j$ and $\wp \in \mathcal{P}_i$, $\wp \not\preceq_{\mathcal{S}} \wp_j$.*

Proof of the claim. assume the contrary and derive a contradiction. Then, there is $j > 1$ such that for each $\wp_j \in \mathcal{P}_j$, there is $i < j$ and $\wp_i \in \mathcal{P}_i$ so that $\wp_i \preceq_{\mathcal{S}} \wp_j$. Since $\mathcal{P}_{j-1} \sqsubseteq_{\mathcal{S}} \mathcal{P}_i$ for each $i < j$, it follows that for each $\wp_j \in \mathcal{P}_j$, there is $\wp \in \mathcal{P}_{j-1}$ so that $\wp \preceq_{\mathcal{S}} \wp_j$. This means that $\mathcal{P}_{j-1} \sqsubseteq_{\mathcal{S}} \mathcal{P}_j$, which is a contradiction. □

By the claim above, we deduce the existence of an infinite sequence $\wp_1, \wp_2, \ldots$ of non-null finite paths of $\mathcal{S}$ such that $\wp_i \not\preceq_{\mathcal{S}} \wp_j$ for all $1 \leqslant i < j$. Since $\preceq_{\mathcal{S}}$ is a well-quasi-ordering, we obtain a contradiction, and the result follows. □

Now, we can prove Theorem 2.

Theorem 2. *Given a* GCS *$\mathcal{S}$, one can compute a finite set $\mathcal{P}_{\mathcal{S}}$ of non-null finite paths of $\mathcal{S}$ such that: for each non-null finite path $\wp'$ of $\mathcal{S}$, there is a path $\wp \in \mathcal{P}_{\mathcal{S}}$ so that $s(\wp) = s(\wp')$, $t(\wp) = t(\wp')$, $\lfloor G_\wp \rfloor_K = \lfloor G_{\wp'} \rfloor_K$, and $\rightsquigarrow_{\wp'}$ implies $\rightsquigarrow_\wp$ (hence, $Sat(G_{\wp'}) \subseteq Sat(G_\wp)$).*

Proof. For each $k \geqslant 1$, let $\mathcal{P}_k$ be the finite set of non-null finite paths of $\mathcal{S}$ of length at most k. First, we prove the following.

Claim. *Let $k \geqslant 1$. If $\mathcal{P}_k \sqsubseteq_{\mathcal{S}} \mathcal{P}_{k+1}$, then $\mathcal{P}_k \sqsubseteq_{\mathcal{S}} \mathcal{P}_h$ for each $h \geqslant k+1$.*

Proof of the claim. let $\mathcal{P}_k \sqsubseteq_{\mathcal{S}} \mathcal{P}_{k+1}$. It suffices to show that $\mathcal{P}_{k+1} \sqsubseteq_{\mathcal{S}} \mathcal{P}_{k+2}$ (recall that $\sqsubseteq_{\mathcal{S}}$ is a pre-order). Let $\wp \in \mathcal{P}_{k+2}$. We need to show that there is $\wp' \in \mathcal{P}_{k+1}$ such that $\wp' \preceq_{\mathcal{S}} \wp$. If $\wp \in \mathcal{P}_{k+1}$, the result is obvious. Otherwise, $\wp$ can be written in the form $\wp = \wp_{k+1}\wp_1$ such that $\wp_{k+1} \in \mathcal{P}_{k+1}$ and $|\wp_1| = 1$. Since $\mathcal{P}_k \sqsubseteq_{\mathcal{S}} \mathcal{P}_{k+1}$, there is a path $\wp_k \in \mathcal{P}_k$ such that $\wp_k \preceq_{\mathcal{S}} \wp_{k+1}$. Let $\wp' = \wp_k\wp_1$. Note that $\wp'$ is well-defined and $\wp' \in \mathcal{P}_{k+1}$. Moreover, by Lemma 23, $\wp' \preceq \wp$. Hence, the result follows. □

Now, we can prove the theorem. Since $\mathcal{P}_k \subseteq \mathcal{P}_{k+1}$ for all $k \geqslant 1$, it holds that $\mathcal{P}_{k+1} \sqsubseteq_{\mathcal{S}} \mathcal{P}_k$ for all $k \geqslant 1$. Hence, by Lemma 24, it is defined the smallest $k_0 \geqslant 1$ such that $\mathcal{P}_{k_0} \sqsubseteq_{\mathcal{S}} \mathcal{P}_{k_0+1}$. Note that k_0 can be effectively computed. We set $\mathcal{P}_{\mathcal{S}}$ to the computable finite set $\mathcal{P}_{k_0}$. By the claim above, the definition of the pre-order $\sqsubseteq_{\mathcal{S}}$, and Proposition 8, it follows that $\mathcal{P}_{\mathcal{S}}$ satisfies the statement of the theorem, which concludes. □

References

[1] P.A. Abdulla, G. Delzanno, On the coverability problem for constrained multiset rewriting, in: Proc. 5th AVIS, 2006.
[2] P.A. Abdulla, G. Delzanno, A. Rezine, Approximated parameterized verification of infinite-state processes with global conditions, Form. Methods Syst. Des. 34 (2) (2009) 126–156.
[3] E. Albert, P. Arenas, S. Genaim, G. Puebla, Automatic inference of upper bounds for recurrence relations in cost analysis, in: Proc. 15th SAS, in: Lect. Notes Comput. Sci., vol. 5079, Springer, 2008, pp. 221–237.
[4] R. Alur, D.L. Dill, Automata for modeling real-time systems, in: Proc. 17th ICALP, in: Lect. Notes Comput. Sci., vol. 443, Springer, 1990, pp. 322–335.
[5] R. Alur, T. Feder, T.A. Henzinger, The benefits of relaxing punctuality, J. ACM 43 (1) (1996) 116–146.
[6] A.M. Ben-Amram, Size-change termination with difference constraints, ACM Trans. Program. Lang. Syst. 30 (3) (2008).
[7] A.M. Ben-Amram, Size-change termination, monotonicity constraints and ranking functions, Log. Methods Comput. Sci. 6 (3) (2010).
[8] A.M. Ben-Amram, Monotonicity constraints for termination in the integer domain, Log. Methods Comput. Sci. 7 (3) (2011).
[9] A.M. Ben-Amram, M. Vainer, Complexity analysis of size-change terminating programs, in: Second Workshop on Developments in Implicit Computational Complexity, 2011.
[10] B. Boigelot, Symbolic methods for exploring infinite state spaces, PhD thesis, Université de Liège, 1998.
[11] A. Bouajjani, M. Bozga, P. Habermehl, R. Iosif, P. Moro, T. Vojnar, Programs with lists are counter automata, in: Proc. 18th CAV, in: Lect. Notes Comput. Sci., vol. 4144, Springer, 2006, pp. 517–531.
[12] A. Bouajjani, R. Echahed, P. Habermehl, On the verification problem of nonregular properties for nonregular processes, in: LICS'95, IEEE Computer Society Press, 1995, pp. 123–133.
[13] M. Bozga, C. Girlea, R. Iosif, Iterating octagons, in: Proc. 15th TACAS, in: Lect. Notes Comput. Sci., vol. 5505, Springer, 2009, pp. 337–351.

[14] L. Bozzelli, R. Gascon, Branching-time temporal logic extended with qualitative Presburger constraints, in: LPAR'06, in: Lect. Notes Comput. Sci., vol. 4246, Springer, 2006, pp. 197–211.
[15] E. Cardoza, Richard J. Lipton, Albert R. Meyer, Exponential space complete problems for Petri nets and commutative semigroups: Preliminary report, in: STOC, ACM, 1976, pp. 50–54.
[16] Karlis Cerans, Deciding properties of integral relational automata, in: Proc. 21st ICALP, in: Lect. Notes Comput. Sci., vol. 3921, Springer, 1994, pp. 35–46.
[17] H. Comon, V. Cortier, Flatness is not a weakness, in: Proc. 14th CSL, in: Lect. Notes Comput. Sci., vol. 1862, Springer, 2000, pp. 262–276.
[18] H. Comon, Y. Jurski, Multiple counters automata, safety analysis and Presburger arithmetic, in: Proc. 10th CAV, in: Lect. Notes Comput. Sci., vol. 1427, Springer, 1998, pp. 268–279.
[19] S. Demri, Deepak D'Souza, An automata-theoretic approach to constraint LTL, Inf. Comput. 205 (3) (2007) 380–415.
[20] S. Demri, A. Finkel, V. Goranko, G. van Drimmelen, Towards a model-checker for counter systems, in: ATVA'06, in: Lect. Notes Comput. Sci., vol. 4218, Springer, 2006, pp. 493–507.
[21] S. Demri, R. Gascon, Verification of qualitative Z constraints, Theor. Comput. Sci. 409 (1) (2008) 24–40.
[22] E.A. Emerson, J.Y. Halpern, Sometimes and not never revisited: On branching versus linear time, J. ACM 33 (1) (1986) 151–178.
[23] A. Finkel, J. Leroux, How to compose Presburger-accelerations: applications to broadcast protocols, in: Proc. 22nd FSTTCS, in: Lect. Notes Comput. Sci., vol. 2556, Springer, 2002, pp. 145–156.
[24] L. Fribourg, J. Richardson, Symbolic verification with gap-order constraints, in: Proc. 6th LOPSTR, in: Lect. Notes Comput. Sci., vol. 1207, Springer, 1996, pp. 20–37.
[25] O. Ibarra, Reversal-bounded multicounter machines and their decision problems, J. ACM 25 (1) (1978) 116–133.
[26] N.D. Jonson, Computability and Complexity from a Programming Perspective, Foundations of Computing Series, MIT Press, 1997.
[27] O. Kupferman, M.Y. Vardi, An automata-theoretic approach to modular model checking, ACM Trans. Program. Lang. Syst. 22 (1) (2000) 87–128.
[28] M. Minsky, Computation: Finite and Infinite Machines, Prentice–Hall, 1967.
[29] J.L. Peterson, Petri Net Theory and the Modelling of Systems, Prentice–Hall, 1981.
[30] A. Pnueli, The temporal logic of programs, in: Proc. 18th FOCS, IEEE Computer Society, 1977, pp. 46–57.
[31] F. Ramsey, On a problem of formal logic, Proc. Lond. Math. Soc. 30 (1930) 264–286.
[32] P.Z. Revesz, A closed-form evaluation for datalog queries with integer (gap)-order constraints, Theor. Comput. Sci. 116 (1–2) (1993) 117–149.
[33] M.Y. Vardi, P. Wolper, Reasoning about infinite computations, Inf. Comput. 115 (1) (1994) 1–37.