Verification of gap-order constraint abstractions of counter systems

Laura Bozzelli[1] and Sophie Pinchinat[2]

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

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) [25]. GCS extend monotonicity constraint systems [4], integral relation automata [10], and constraint automata in [13]. First, we show that checking the existence of infinite runs in GCS satisfying acceptance conditions à la Büchi (fairness problem) is decidable and PSPACE-complete. Next, we consider a constrained branching-time logic, GCCTL*, obtained by enriching CTL* with GC, thus enabling expressive properties and subsuming the setting of [10]. 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 the verification problems investigated and shown to be decidable in [10], but for which no elementary upper bounds are known.

1 Introduction

Abstractions of Counter systems. Counter systems are a widely investigated complete computational model, used for instance to model broadcast protocols [17] and programs with pointer variables [6]. Though simple problems like reachability are already undecidable for 2-counter Minsky machines [22], interesting abstractions of counter systems have been studied, for which interesting classes of verification problems have been shown to be decidable. Many of these abstractions are in fact restrictions: examples include Petri nets [23], reversal-bounded counter machines [19], and flat counter systems [5, 11]. Genuine abstractions are obtained by approximating counting operations by non-functional fragments of Presburger constraints between the variables of the current state and the variables of the next state. Examples include the class of Monotonicity Constraint Systems (MCS) [4] and its variants, like constraint automata in [13], and integral relation automata (IRA) [10], for which the (monotonicity) constraints (MC) are boolean combinations of inequalities of the form $u < v$ or $u \leq v$, 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. [4]). Richer classes of non-functional fragments of Presburger constraints have been investigated, e.g. difference bound constraints [12], and their extension, namely octagon relations [8], 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 of flat counter systems). Size-change systems extended with difference bound constraints over the natural number domain have been investigated in [3]: there, the atomic difference constraints are of the form $x - y' \geq c$, 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. In order to specify behavioral properties of counter systems, standard temporal logics (like LTL or CTL*) 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 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. [13, 15], or by restricting the logical language, see e.g. [7, 11]. In particular, satisfiability and model checking (w.r.t. constraint automata) of standard LTL extended with MC are decidable and PSPACE-complete [13] (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 [10], where it is shown that model checking IRA against its existential and universal fragments, E–MCCTL* and A–MCCTL*, is decidable (by contrast, model checking for full MCCTL* is undecidable, even for its CTL-like fragment[1]). As done in [15], adding periodicity constraints and the ability for a fixed $k \geq 1$, to compare the variable values at states of a run at distance at most k, decidability of the above problems is preserved [9]. However, no elementary upper bounds for these problems are known [10, 9]. Moreover, it is shown in [14] that model checking a subclass of 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, 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) [25]. These constraints are positive boolean combinations of inequalities of the form $u - v \geq k$, 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 [25], and also have found applications in the

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

analysis of safety properties for parameterized systems [1, 2] and for determining state invariants in counter systems [18]. As pointed 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 [13]). This because GC extend MC and, differently from MC, are closed under existential quantification (but not under negation).[2] 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 constraints of the form $u - v \geq -k$, with $k \in \mathbb{N}$, then the resulting class of systems can trivially emulate Minsky counter machines, leading to undecidable basic decision problems.

Our results are as follows. First, we 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. 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. Next, we address verification problems of GCS against a *strict* extension, denoted by GCCTL*, of the logic MCCTL* (given in *complete* positive normal form) [10] obtained by adding transitional GC (we also allow existential quantification over variables in the underlying constraint language). 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 A–GCCTL* of GCCTL* is undecidable, model checking GCS against the existential fragment E–GCCTL* of GCCTL*, and satisfiability of both A–GCCTL* and E–GCCTL* are instead decidable and PSPACE-complete (which matches the complexity of model checking and satisfiability for the existential and universal fragments of standard CTL* [21]). Note that E–GCCTL* and A–GCCTL* are not dual. Moreover, for a given GCS $\mathcal{S}$ and E–GCCTL* formula φ, the set of states in $\mathcal{S}$ satisfying φ is *effectively* GC representable.

Since E–GCCTL* subsumes E–MCCTL*, and E–MCCTL* and A–MCCTL* are dual, our results imply PSPACE-completeness for model-checking (w.r.t. IRA or GCS) of both E–MCCTL* and A–MCCTL*. Hence, in particular, we solve complexity issues left open in [10] (see also [9]). Due to space reasons, many proofs are in Appendix.

[2] Hence, GC are closed under composition which captures the reachability relation in GCS for a fixed path in the control graph.

2 Preliminaries

Let $\mathbb{Z}$ (resp., $\mathbb{N}$) be the set of integers (resp., natural numbers). We fix a finite set *Var* $= \{x_1, \ldots, x_r\}$ of variables, a finite set of constants *Const* $\subseteq \mathbb{Z}$ such that $0 \in$ *Const*, and a fresh 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 a valuation ν, by convention, we define $\nu(c) = c$ for all $c \in \mathbb{Z}$.

Definition 1. *[25]* A *gap-order constraint* (GC) over V and *Const* is a conjunction ξ of inequalities of the form $u - v \geq k$, 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 $u - v \geq k$ for some k. A valuation $\nu : V \to \mathbb{Z}$ *satisfies* ξ if for each conjunct $u - v \geq k$ of ξ, $\nu(u) - \nu(v) \geq k$. We denote by *Sat*(ξ) the set of such valuations.

Definition 2. *[10]* A (*gap-order*) *monotonicity graph* (MG) 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 s.t.: if $u \xrightarrow{k} v$ and $u \xrightarrow{k'} v$ are edges of G, then $k = k'$. The set *Sat*(G) of *solutions* of G is the set of valuations ν over V s.t. for each $u \xrightarrow{k} v$ in G, $\nu(u) - \nu(v) \geq k$. 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*(ξ).[3]

The notation $G \models u < v$ means that there is an edge in G from v to u with weight $k > 0$. Moreover, $G \models u \leq v$ means that there is an edge of G from v to u, and $G \models u = v$ means $G \models u \leq v$ and $G \models v \leq u$. Also, we write $G \models u_1 \lhd_1 \ldots \lhd_{n-1} u_n$ to mean that $G \models u_i \lhd_i u_{i+1}$ for each $1 \leq i < n$, where $\lhd_i \in \{<, \leq, =\}$. A *transitional* GC (resp., *transitional* MG) is a GC (resp., MG) over *Var* $\cup$ *Var*$'$ and *Const*. For valuations $\nu, \nu' :$ *Var* $\to \mathbb{Z}$, we denote by $\nu \oplus \nu'$ the valuation over *Var* $\cup$ *Var*$'$ defined as follows: $(\nu \oplus \nu')(x_i) = \nu(x_i)$ and $(\nu \oplus \nu')(x'_i) = \nu'(x_i)$ for $i = 1, \ldots, r$.

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.

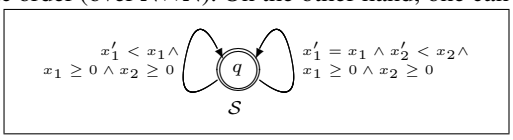
For a finite path $\wp$ of a GCS $\mathcal{S}$, $s(\wp)$ and $t(\wp)$ denote the source and target control points of $\wp$. For a finite path $\wp$ and a path $\wp'$ such that $t(\wp) = s(\wp')$, the composition of $\wp$ and $\wp'$, written $\wp\wp'$, is defined as usual.
The semantics of a GCS $\mathcal{S}$ is given by an infinite directed graph $[\![\mathcal{S}]\!]$ defined as:

- 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*(ξ). 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 $\mathcal{S}$.

[3] MG are called Positive Graphose Inequality Systems in [10]. A different constraint graph representation of GC can be found in [25].

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 of $\mathcal{S}$ is a path of $\mathcal{S}$ of non-null length. Let $\wp = q_0 \xrightarrow{\xi_0} q_1 \xrightarrow{\xi_1} q_2, \ldots$ be a path of $\mathcal{S}$. A run π of $\mathcal{S}$ is an *instance* of $\wp$ if π is of the form $\pi = (q_0, \nu_0) \rightarrow (q_1, \nu_1) \rightarrow (q_2, \nu_2), \ldots$ and for each i, $(q_i, \nu_i) \rightarrow (q_{i+1}, \nu_{i+1})$ is an instance of $q_i \xrightarrow{\xi_i} q_{i+1}$. Given $F \subseteq Q(\mathcal{S})$, an infinite run $(q_0, \nu_0) \rightarrow (q_1, \nu_1) \rightarrow \ldots$ of $\mathcal{S}$ is *fair w.r.t* F if for infinitely many $i \geq 0$, $q_i \in F$.

Example 1. The figure depicts a GCS $\mathcal{S}$ consisting of a unique control point q and two self-loops. Note that there is no infinite run since along any run, the pair (x_1, x_2) decreases strictly w.r.t. the lexicographic order (over $\mathbb{N} \times \mathbb{N}$). On the other hand, one can easily check that for each state (q, ν) with $\nu(x_1) > 0$ and $\nu(x_2) \geq 0$, the set of the lengths of the runs from (q, ν) is unbounded.



Convention: since we use MG representations to manipulate GC, we assume that the edge-labels in GCS are transitional MG.

2.1 Properties of monotonicity graphs

We recall some basic operations on MG [10] which can be computed in polynomial time. Furthermore, we define a sound and complete (w.r.t. satisfiability) approximation scheme of MG and show that the basic operations preserve soundness and completeness of this approximation. A different approximation scheme for GC can be found in [25].

A MG G is *satisfiable* if *Sat*$(G) \neq \emptyset$. Let G be a MG over V and *Const*. For $V' \subseteq V$, *the restriction of* G *to* V', written $G_{V'}$, is the MG 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* iff: (1) 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, and (2) for all constants $c_1, c_2 \in$ *Const*, $p_G(c_1, c_2) \leq c_1 - c_2$.

Proposition 1. [10] *Let G be a* MG *over V and Const. 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. *G is satisfiable $\Leftrightarrow$ G contains no loop with positive weight sum and for all $c_1, c_2 \in Const$, $p_G(c_1, c_2) \leq c_1 - c_2$ (this can be checked in polynomial time).*
3. *If G is satisfiable, then one can build in polynomial time an equivalent* normalized MG $\overline{G}$ *(i.e., Sat$(\overline{G})$ = Sat(G)), called the* closure *of G.*

According to Proposition 1, for a satisfiable MG G, we denote by $\overline{G}$ the closure of G. Moreover, for all unsatisfiable MG G over V and *Const*, we use a unique closure corresponding to some MG G_{nil} over V and *Const* 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*). Now, we recall some effective operations on MG. Let *Var*$'' = \{x_1'', \ldots, x_r''\}$ be an additional copy of *Var* $= \{x_1 \ldots, x_r\}$.

Definition 4. [10] Let G be a MG on V and *Const* and G' be a MG on V' and *Const*.

1. **Projection:** if $V' \subseteq V$, the *projection of* G *over* V' is the MG given by $(\overline{G})_{V'}$.
2. **Intersection:** the *intersection* $G \bigotimes G'$ *of* G *and* G' is the MG over $V \cup V'$ and *Const* defined as: $u \xrightarrow{k} v$ is an edge of $G \bigotimes G'$ 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'.
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 $G \bigotimes G''$ over *Var* $\cup$ *Var*$''$ by renaming any variable x''_i into x'_i.

By Definition 4 and Proposition 1, we easily obtain the following known result [10], which essentially asserts that MG (or, equivalently, GC) are closed under intersection and existential quantification.

Proposition 2. *Let* G *be a* MG *over* V *and Const and* G' *be a* MG *over* V' *and Const.*

1. ***Projection:*** *if* G' *is the projection of* G *over* V'*, then for* $\nu' : V' \to \mathbb{Z}$, $\nu' \in$ *Sat*(G') *iff* $\nu' = \nu|_{V'}$ *for some* $\nu \in$ *Sat*(G).
2. ***Intersection:*** *for* $\nu : V \cup V' \to \mathbb{Z}$, $\nu \in$ *Sat*$(G \bigotimes G')$ iff $\nu|_V \in$ *Sat*(G) *and* $\nu|_{V'} \in$ *Sat*(G'). *Hence, for* $V = V'$, $Sat(G \bigotimes G') =$ *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*$(G \bullet G')$ *iff* $\nu \oplus \nu'' \in$ *Sat*(G) *and* $\nu'' \oplus \nu' \in$ *Sat*(G') *for some* $\nu'' :$ *Var* $\to \mathbb{Z}$. *Moreover, the composition operator* $\bullet$ *is associative.*

Approximation scheme: let K stand for $\max(\{|c_1 - c_2| + 1 \mid c_1, c_2 \in Const\})$. Note that $K > 0$. For each $h \in \mathbb{N}$, let $\lfloor h \rfloor_K = h$ if $h \leq K$, and $\lfloor h \rfloor_K = K$ otherwise.

Definition 5 (K-bounded MG). A MG is *K-bounded* iff for each of its edges $u \xrightarrow{k} v$, $k \leq K$. For a MG G over V and *Const*, $\lfloor G \rfloor_K$ denotes the K-bounded MG over V and *Const* obtained from G by replacing each edge $u \xrightarrow{k} v$ of G with the edge $u \xrightarrow{\lfloor k \rfloor_K} v$.

The proofs of the following propositions are in Appendix A.1 and A.2, respectively.

Proposition 3. *Let* G *be a* MG *over* V *and Const. Then,* G *is satisfiable iff* $\lfloor G \rfloor_K$ *is satisfiable. Moreover,* $\lfloor \overline{G} \rfloor_K = \lfloor \overline{\lfloor G \rfloor_K} \rfloor_K$.

Proposition 4. *For transitional* MG G_1 *and* G_2, $\lfloor G_1 \bullet G_2 \rfloor_K = \lfloor \lfloor G_1 \rfloor_K \bullet \lfloor G_2 \rfloor_K \rfloor_K$.

2.2 Results on the reachability relation in GCS

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

Definition 6. *A transitional* MG G *is said to be* complete *if:*

- *for all* $u, v \in$ *Var* $\cup$ *Var*$' \cup$ *Const,* $G \models u \leq v \Rightarrow G \models u \lhd v$ *for some* $\lhd \in \{<, =\}$;
- *for all* $u, v \in$ *Var* $\cup$ *Const, either* $G \models u \leq v$ *or* $G \models v \leq u$;
- *for all* $u, v \in$ *Var*$' \cup$ *Const, either* $G \models u \leq v$ *or* $G \models v \leq u$.

A GCS $\mathcal{S}$ is *complete* iff each MG in $\mathcal{S}$ is complete. Fix a *complete* GCS $\mathcal{S}$. 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: for all $\nu, \nu' : \mathit{Var} \to \mathbb{Z}$, $\nu \rightsquigarrow_\wp \nu'$ 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 $\mathit{Sat}(G) = \{\nu \oplus \nu' \mid \nu \rightsquigarrow_\wp \nu'\}$. 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:

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

Note that the composition operator preserves completeness, and for a transitional MG G, G is complete iff $\lfloor G \rfloor_K$ is complete. Thus, by a straightforward induction on the length of the path $\wp$ and by using Propositions 2 and 4, we obtain the following.

Proposition 5. *For a non-null finite path $\wp$ of $\mathcal{S}$, $G_\wp = \overline{G_\wp}$, and $G_\wp$ is complete and characterizes the reachability relation $\rightsquigarrow_\wp$. Moreover, $G^{bd}_\wp = \lfloor G_\wp \rfloor_K$ and is complete.*

Let $\mathcal{G}^K_\mathcal{S} = \{(\lfloor G_\wp \rfloor_K, s(\wp), t(\wp)) \mid \wp \text{ is a non-null finite path and } G_\wp \text{ is satisfiable}\}$. Note that $\mathcal{G}^K_\mathcal{S}$ is finite since the set of transitional K-bounded MG is finite. By Proposition 5, $\mathcal{G}^K_\mathcal{S}$ 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 a simple transitive closure procedure. In particular, we obtain the following result (a proof is in Appendix A.3).

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

By [10] (see also [9]), 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 [25], 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 [10] (see also [9]), and applying the K-bounded approximation scheme, we easily obtain the following. For details, see Appendix A.4. Note that we are not able to give an upper bound on the cardinality of the set $\mathcal{P}_\mathcal{S}$.

Theorem 2. *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 $\mathcal{S}$ from q to q', there is a path $\wp \in \mathcal{P}_\mathcal{S}$ from q to q' so that $\lfloor G_{\wp'} \rfloor_K = \lfloor G_\wp \rfloor_K$, and $\rightsquigarrow_{\wp'}$ implies $\rightsquigarrow_\wp$.*

3 Checking Fairness

For a GCS $\mathcal{S}$ and a set F of control points of $\mathcal{S}$, we denote by $\mathit{Inf}_{\mathcal{S},F}$ the set of states of $\mathcal{S}$ from which there is an infinite run that is fair w.r.t. F. In this section, we show that the problem of checking for a given GCS $\mathcal{S}$ and set $F \subseteq Q(\mathcal{S})$, whether $\mathit{Inf}_{\mathcal{S},F} \neq \emptyset$ (*fairness problem*) is decidable and PSPACE-complete.

First, we give additional definitions. Let $\mathcal{S}$ be a GCS. We denote by $\lfloor \mathcal{S} \rfloor_K$ the GCS obtained from $\mathcal{S}$ by replacing each edge $q \xrightarrow{G} q'$ of $\mathcal{S}$ with the edge $q \xrightarrow{\lfloor G \rfloor_K} q'$.
A set U of states of $\mathcal{S}$ is MG *representable* if there is a family $\{\mathcal{G}_q\}_{q \in Q(\mathcal{S})}$ of finite sets of MG over *Var* and *Const* such that $\bigcup_{G \in \mathcal{G}_q} \mathit{Sat}(G) = \{\nu \mid (q, \nu) \in U\}$ for each $q \in Q(\mathcal{S})$. 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 $F \subseteq Q(\mathcal{S})$ and $q \in Q(\mathcal{S})$, $\mathit{Inf}^q_{\mathcal{S},F}$ denotes the set of states in $\mathit{Inf}_{\mathcal{S},F}$ of the form (q, ν) for some valuation ν. Moreover, $\mathit{Inf}_{\mathcal{S}}$ stands for $\mathit{Inf}_{\mathcal{S},Q(\mathcal{S})}$.
A MG G is *weakly normalized* if for all vertices u, v, $p_G(u, v) \geq 0$ (resp., $p_G(u, v) > 0$) implies $G \models v \leq u$ (resp., $G \models v < u$). Note that G is weakly normalized iff $\lfloor G \rfloor_K$ is weakly normalized. A transitional MG G is *(weakly) idempotent* iff $\lfloor G \bullet G \rfloor_K = \lfloor G \rfloor_K$.

3.1 Checking Fairness for simple GCS

In this section, we solve the fairness problem for a restricted class of GCS.

Definition 7 (Simple GCS). *A (satisfiable) simple* GCS *is a* GCS *consisting of just two edges of the form $q_0 \xrightarrow{G_0} q$ and $q \xrightarrow{G} q$ such that $q_0 \neq q$. Moreover, we require that $G_0 \bullet G$ is satisfiable, and G is complete,* weakly *normalized, and idempotent.*

To present our results on simple GCS, we need additional definitions.

Definition 8 (Lower and upper 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 $G \models y < \mathit{MIN}$ (resp., $G \models \mathit{MAX} < y$). Moreover, y is a *bounded variable* of G if $G \models \mathit{MIN} \leq y$ and $G \models y \leq \mathit{MAX}$.

Definition 9. A transitional MG is *balanced* iff for all $u, v \in \mathit{Var} \cup \mathit{Const}$ and $\lhd \in \{<, =\}$, $G \models u \lhd v$ iff $G \models u' \lhd v'$ (where for $u \in \mathit{Var} \cup \mathit{Const}$, we write u' to denote the corresponding variable in Var' if $u \in \mathit{Var}$, and u itself otherwise).

Fix a simple GCS $\mathcal{S}$ with edges $q_0 \xrightarrow{G_0} q$ and $q \xrightarrow{G} q$. Since G is idempotent, by the associativity of composition $\bullet$ and Proposition 4, we obtain that for each $k \geq 1$, $\lfloor G_0 \bullet \underbrace{G \bullet \ldots \bullet G}_{k \text{ times}} \rfloor_K = \lfloor G_0 \bullet G \rfloor_K$. Hence, $G_0 \bullet \underbrace{G \bullet \ldots \bullet G}_{k \text{ times}}$ and $\underbrace{G \bullet \ldots \bullet G}_{k \text{ times}}$ are satisfiable for each $k \geq 1$. Since G is complete, it follows that G is *balanced* as well. Moreover, since G is satisfiable and complete, a variable $y \in \mathit{Var} \cup \mathit{Var}'$ is either a lower variable, or an upper variable, or a bounded variable of G, where the "or" is exclusive. We denote by $\mathrm{L}_1, \ldots, \mathrm{L}_N$ (resp., $\mathrm{U}_1, \ldots, \mathrm{U}_M$) the lower (resp., the upper) variables of G in *Var*, and by $\mathrm{B}_1, \ldots, \mathrm{B}_H$ the bounded variables of G in *Var*. Hence, we can assume that

$$G \models \mathrm{L}_1 \lhd_2 \ldots \lhd_N \mathrm{L}_N < \mathrm{B}_1 \lhd'_2 \ldots \lhd'_H \mathrm{B}_H < \mathrm{U}_1 \lhd''_2 \ldots \lhd''_M \mathrm{U}_M$$

where $\lhd_2 \ldots \lhd_N, \lhd'_2 \ldots \lhd'_H, \lhd''_2 \ldots \lhd''_M \in \{<, =\}$. Since G is balanced it follows that the lower variables (resp., upper variables) of G in Var' are $\mathrm{L}'_1, \ldots, \mathrm{L}'_N$ (resp., $\mathrm{U}'_1, \ldots, \mathrm{U}'_M$), and the bounded variables of G in Var' are $\mathrm{B}'_1, \ldots, \mathrm{B}'_H$. Moreover,

$$G \models \mathrm{L}'_1 \lhd_2 \ldots \lhd_N \mathrm{L}'_N < \mathrm{B}'_1 \lhd'_2 \ldots \lhd'_H \mathrm{B}'_H < \mathrm{U}'_1 \lhd''_2 \ldots \lhd''_M \mathrm{U}'_M$$

Now, we define a polynomial-time checkable condition on simple GCS.

Definition 10 (termination condition). We say that G satisfies the termination condition iff one of the following holds:

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

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

Intuitively, the above condition asserts that either there is a lower (resp., upper) variable of G_{Var} whose value strictly increases (resp., decreases) along each run of $\mathcal{S}$, or there are two lower (resp., upper) variables of G_{Var} such that their distance strictly decreases along each run of $\mathcal{S}$. Let $\mathcal{TC}$ be the class of simple GCS satisfying the termination condition. By Definition 10, we easily obtain the following.

Proposition 6. *If* $\mathcal{S} \in \mathcal{TC}$, *then* $Inf_{\mathcal{S}} = \emptyset$.

It remains to consider the case when $\mathcal{S} \notin \mathcal{TC}$. We define two integers L and U as follows: L is the smallest $1 \leq i \leq N$ such that $G \models \mathrm{L}_i = \mathrm{L}'_i$ (if such an i does not exist, we set $L = N + 1$). Finally, U is the greatest $1 \leq i \leq M$ such that $G \models \mathrm{U}_i = \mathrm{U}'_i$ (if such an i does not exist, we set $U = 0$). Note that $1 \leq L \leq N + 1$ and $0 \leq U \leq M$. The set of *unconstrained variables* in Var, written *Unc*, consists of the lower variables L_i such that $1 \leq i < L$ and the upper variables U_j such that $U < j \leq M$. We denote by *Unc′* the corresponding subset in *Var′*. Evidently, the following holds.

Lemma 1. *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.*

The proof of the following lemma is in Appendix B.1. Essentially, the result follows from Lemma 1 and the following property (which is a consequence of the idempotence of G): if $\mathcal{S} \notin \mathcal{TC}$, then $G \not\models \mathrm{U}'_i \leq \mathrm{U}_j$ and $G \not\models \mathrm{L}_h \leq \mathrm{L}'_k$ for all upper variables $\mathrm{U}'_i, \mathrm{U}_j$ and lower variables $\mathrm{L}_h, \mathrm{L}'_k$ in *Unc* ∪ *Unc′*. In other terms, along a run of $\mathcal{S}$, the unconstrained upper (resp., lower) variables can increase (resp., decrease) arbitrarily.

Lemma 2. *Let* $\mathcal{S} \notin \mathcal{TC}$. *Then,* $(q, \nu_0) \in Inf_{\mathcal{S}}$ iff *there is a finite run* π *of* $\mathcal{S}$ *from* (q, ν_0) *of the form* $\pi = (q, \nu_0) \ldots (q, \nu) \ldots (q, \nu')(q, \nu'')$ *such that* $\nu''_{(Var \setminus Unc)} = \nu_{(Var \setminus Unc)}$.

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

Theorem 3. *Let* $\mathcal{S} \notin \mathcal{TC}$. *Then,* $Inf_{\mathcal{S}}$ *is* MG *representable and one can construct a* MG *representation of* $Inf_{\mathcal{S}}$, *written* $\sigma(\mathcal{S})$, *such that: (1)* $\lfloor \sigma(\mathcal{S}) \rfloor_K$ *can be computed in polynomial time, and (2)* $\lfloor \sigma(\mathcal{S}) \rfloor_K = \lfloor \sigma(\lfloor \mathcal{S} \rfloor_K) \rfloor_K$ ($\lfloor \mathcal{S} \rfloor_K$ *is simple and* $\lfloor \mathcal{S} \rfloor_K \notin \mathcal{TC}$).

Proof. By Theorem 2, one can compute a *finite* set $\mathcal{P}$ 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 $\rightsquigarrow_{\wp}$. Note that given $\wp \in \mathcal{P}$, the transitional MG $G_\wp$ (which characterizes the reachability relation $\rightsquigarrow_\wp$) has the form $\underbrace{G \bullet \ldots \bullet G}_{k \text{ times}}$ for some $k \geq 1$.

Let $G_=$ be the transitional MG corresponding to the GC given by $\bigwedge_{x \in Var \setminus Unc} x' = x$, and $\mathcal{G} = \{G_\wp \bullet (G_{\wp'} \bigotimes G_=) \mid \wp, \wp' \in \mathcal{P}\} \cup \{G_\wp \bigotimes G_= \mid \wp \in \mathcal{P}\}$. Then, $\sigma(\mathcal{S}) = \{\mathcal{G}^q, \mathcal{G}^{q_0}\}$, where $\mathcal{G}^q$ and $\mathcal{G}^{q_0}$ are defined as follows:

$\mathcal{G}^q = \{G' \mid G' \text{ is the projection of } G'' \text{ over } \mathit{Var} \text{ for some } G'' \in \mathcal{G}\}$

$\mathcal{G}^{q_0} = \{G' \mid G' \text{ is the projection of } G_0 \bullet G'' \text{ over } \mathit{Var} \text{ for some } G'' \in \mathcal{G}\}$

Correctness of the construction easily follows from Lemma 2. The second part of the theorem follows from Propositions 3–4, and the fact that for each $\wp \in \mathcal{P}$, $\lfloor G_\wp \rfloor_K = \lfloor G \rfloor_K$ (G is idempotent) and $\lfloor G_\wp \bigotimes G_= \rfloor_K = \lfloor \lfloor G_\wp \rfloor_K \bigotimes \lfloor G_= \rfloor_K \rfloor_K$ (see Proposition 7 in Appendix A.2). For details, see Appendix B.2. □

3.2 Checking fairness for unrestricted GCS

Fix a GCS $\mathcal{S}$. 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 $\wp\wp\ldots$. A infinite path $\wp$ of $\mathcal{S}$ of the form $\wp = \wp'(\wp'')^\omega$ is said to be *ultimately periodic*. By using Theorem 2 and Ramsey's Theorem (in its infinite version) [24], we show the following result.

Theorem 4 (Characterization Theorem). *Let $\mathcal{S}$ be a complete* GCS*, $F \subseteq Q(\mathcal{S})$, and $\mathcal{P}_\mathcal{S}$ be the finite set of non-null finite paths of $\mathcal{S}$ satisfying Theorem 2. Then, for each state s, $s \in \mathit{Inf}_{\mathcal{S},F}$* iff *there is an infinite run of $\mathcal{S}$ starting from s 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, $G_\wp$ is idempotent, and $G_{\wp_0}$ and $G_\wp$ are complete and normalized.*

Proof. The left implication $\Leftarrow$ is obvious. For the right implication $\Rightarrow$, assume that $s \in \mathit{Inf}_{\mathcal{S},F}$. Then, there is an infinite run π of $\mathcal{S}$ starting from s which visits infinitely often states whose control points are in F. Moreover, there is an infinite path $\wp_\infty$ of $\mathcal{S}$ such that π is an instance of $\wp_\infty$.

Let us consider the finite set $\mathcal{P}_\mathcal{S}$ of non-null finite paths of $\mathcal{S}$ satisfying the statement of Theorem 2. For each $\wp \in \mathcal{P}_\mathcal{S}$ from q to q', we denote by $[\wp]$ the set of non-null finite paths $\wp'$ of $\mathcal{S}$ from q to q' such that $\rightsquigarrow_{\wp'}$ 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 such an element of H must exist). Let us consider the infinite path $\wp_\infty$. Then, there is a control point $q \in F$ such that $\wp_\infty$ is of the form $\wp_\infty = \wp_0\wp_1\wp_2\ldots$, where for each $i \geq 1$, $\wp_i$ 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)[24], 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 $i \geq 1$, $\wp'_i \in [\wp]$ 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 4 and associativity of $\bullet$, we obtain that $\lfloor G_\wp \rfloor_K = \lfloor G_\wp \bullet G_\wp \rfloor_K$. Hence, $G_\wp$ is idempotent.

Let $\wp''_0 \in \mathcal{P}_\mathcal{S}$ such that $\wp'_0 \in [\wp''_0]$. Since π is an instance of $\wp_\infty = \wp'_0\wp'_1\ldots$, and $\wp'_i \in [\wp]$ for each $i \geq 1$, it follows that there is an infinite run π' starting from s which is an instance of the *ultimately periodic* path $\wp''_0(\wp)^\omega$. Moreover, $s(\wp) = q \in F$, $\wp''_0, \wp \in \mathcal{P}_\mathcal{S}$, $G_{\wp''_0} \cdot G_\wp$ is satisfiable, $G_\wp$ is idempotent, and by Proposition 5, $G_{\wp''_0}$ and $G_\wp$ are complete and normalized, which concludes. □

Theorem 5. *Let $\mathcal{S}$ be a* GCS *and $F \subseteq Q(\mathcal{S})$. Then, $Inf_{\mathcal{S},F}$ is* MG *representable and one can construct a* MG *representation of $Inf_{\mathcal{S},F}$, written $\sigma_F(\mathcal{S})$, such that:*

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

Sketched proof. (A detailed proof is in Appendix C.1). We assume that $\mathcal{S}$ is complete (the general case easily follows). Let $\mathcal{P}_\mathcal{S}$ be the computable finite set of non-null finite paths of $\mathcal{S}$ satisfying the statement of Theorem 2, and let $\mathcal{F}_\mathcal{S}$ be the finite set of *simple* GCS constructed as follows: $\mathcal{S}' \in \mathcal{F}_\mathcal{S}$ iff $\mathcal{S}' \notin \mathcal{TC}$ and $\mathcal{S}'$ is a simple GCS consisting of two edges of the form $(\natural, s(\wp_0)) \stackrel{G_{\wp_0}}{\rightarrow} t(\wp_0)$ and $s(\wp) \stackrel{G_\wp}{\rightarrow} t(\wp)$ such that $\wp_0, \wp \in \mathcal{P}_\mathcal{S}$ and $s(\wp) = t(\wp) \in F$. By Theorem 3, for each $\mathcal{S}' \in \mathcal{F}_\mathcal{S}$ one can compute a MG representation $\mathcal{G}_{\mathcal{S}', in(\mathcal{S}')}$ (resp., $\mathcal{G}_{\lfloor \mathcal{S}' \rfloor_K, in(\mathcal{S}')}$) of $Inf_{\mathcal{S}'}^{(\natural, in(\mathcal{S}'))}$ (resp., $Inf_{\lfloor \mathcal{S}' \rfloor_K}^{(\natural, in(\mathcal{S}'))}$), where $(\natural, in(\mathcal{S}'))$ is the initial control point of $\mathcal{S}'$. Moreover, $\lfloor \mathcal{G}_{\mathcal{S}', in(\mathcal{S}')} \rfloor_K = \lfloor \mathcal{G}_{\lfloor \mathcal{S}' \rfloor_K, in(\mathcal{S}')} \rfloor_K$. Then, $\sigma_F(\mathcal{S})$ is given by

$$\sigma_F(\mathcal{S}) = \{ \bigcup_{\{\mathcal{S}' \in \mathcal{F}_\mathcal{S} \mid in(\mathcal{S}') = q\}} \mathcal{G}_{\mathcal{S}', in(\mathcal{S}')} \}_{q \in Q(\mathcal{S})}$$

.

By Theorems 2 and 4, and Proposition 6, $\sigma_F(\mathcal{S})$ is a MG representation of $Inf_{\mathcal{S},F}$. Thus, the first part of the theorem holds. Now, let us consider Properties 1–3. Here, we focus on Property 1. Let $\mathcal{F}_{\mathcal{S},K}$ be the set of simple GCS $\mathcal{S}'$ such that $\mathcal{S}' = \lfloor \mathcal{S}'' \rfloor_K$ for some $\mathcal{S}'' \in \mathcal{F}_\mathcal{S}$. Since $\lfloor \mathcal{G}_{\mathcal{S}', in(\mathcal{S}')} \rfloor_K = \lfloor \mathcal{G}_{\lfloor \mathcal{S}' \rfloor_K, in(\mathcal{S}')} \rfloor_K$ for each $\mathcal{S}' \in \mathcal{F}_\mathcal{S}$, we obtain

$$\lfloor \sigma_F(\mathcal{S}) \rfloor_K = \{ \bigcup_{\{\mathcal{S}' \in \mathcal{F}_{\mathcal{S},K} \mid in(\mathcal{S}') = q\}} \lfloor \mathcal{G}_{\mathcal{S}', in(\mathcal{S}')} \rfloor_K \}_{q \in Q(\mathcal{S})}$$

Since for each $\mathcal{S}' \in \mathcal{F}_{\mathcal{S},K}$, $\lfloor \mathcal{G}_{\mathcal{S}', in(\mathcal{S}')} \rfloor_K$ can be computed in polynomial time in the size of $\mathcal{S}'$ (Theorem 3), it suffices to show that $\mathcal{F}_{\mathcal{S},K}$ can be computed in time $O(|E(\mathcal{S})| \cdot |Q(\mathcal{S})|^2 \cdot (K+2)^{(2|Var|+|Const|)^2})$. This last condition holds since: (i) for a GCS $\mathcal{S}'$, $\mathcal{S}'$ is simple iff $\lfloor \mathcal{S}' \rfloor_K$ is simple, (ii) for a simple GCS $\mathcal{S}''$, $\mathcal{S}'' \notin \mathcal{TC}$ iff $\lfloor \mathcal{S}'' \rfloor_K \notin \mathcal{TC}$, (iii) by Theorem 2, the set $\{(\lfloor G_\wp \rfloor_K, s(\wp), t(\wp)) \mid \wp \in \mathcal{P}_\mathcal{S}$ and $\lfloor G_\wp \rfloor_K$ is satisfiable$\}$ coincides with the set $\mathcal{G}_\mathcal{S}^K = \{(\lfloor G_\wp \rfloor_K, s(\wp), t(\wp)) \mid \wp$ is a non-null finite path of $\mathcal{S}$ and $\lfloor G_\wp \rfloor_K$ is satisfiable$\}$, and (iv) by Theorem 1, the set $\mathcal{G}_\mathcal{S}^K$ is computable in time $O(|E(\mathcal{S})| \cdot |Q(\mathcal{S})|^2 \cdot (K+2)^{(2|Var|+|Const|)^2})$. Thus, Property 1 holds. □

Corollary 1. *The fairness problem is* PSPACE*-complete.*

Proof. The upper bound easily follows from Property 3 in Theorem 5, and the fact that for each set $\mathcal{G}$ of MG, $\mathcal{G}$ contains a satisfiable MG iff $\lfloor \mathcal{G} \rfloor_K$ contains a satisfiable MG. Moreover, PSPACE-hardness follows from PSPACE-hardness of non-termination for Boolean Programs [20] and the fact that GCS subsume Boolean Programs. □

4 The constrained branching–time temporal logic (GCCTL*)

We introduce the *constrained branching–time temporal logic* (GCCTL*) and investigate the related satisfiability and model checking problems. The logic GCCTL* is an extension of standard logic CTL* [16], where the set of atomic propositions is replaced with a subclass of Presburger constraints whose atomic formulas correspond to transitional GC. Formally, for a set of variables V and a set of constants *Const*, the *language of constraints* η, denoted by $\exists$GC, over V and *Const* is defined as follows:

$$\eta := u - v \geq k \mid \eta \vee \eta \mid \eta \wedge \eta \mid \exists x.\, \eta$$

where $u, v \in V \cup \mathit{Const}$, $k \in \mathbb{N}$, and $x \in V$. For a $\exists$GC constraint η and a valuation $\nu : V \to \mathbb{Z}$ over V, the satisfaction relation $v \models \eta$ is defined as follows (we omit the standard clauses for conjunction and disjunction):

- $\nu \models u - v \geq k \stackrel{\text{def}}{\Leftrightarrow} \nu(u) - \nu(v) \geq k$;
- $\nu \models \exists x.\, \eta \stackrel{\text{def}}{\Leftrightarrow}$ there is $c \in \mathbb{Z}$ such that $\nu[x \leftarrow c] \models \eta$.

where $\nu[x \leftarrow c](y) = \nu(y)$ if $y \neq x$, and $\nu[x \leftarrow c](y) = c$ otherwise. Note that $\exists$GC constraints are not closed under negation. Moreover, by Proposition 1(3) and Proposition 2(1) (see also [25]), GC are closed under existential quantification and quantification elimination can be done in polynomial time.

Syntax and semantics of GCCTL*: for the fixed set of variables *Var* and set of constants *Const*, the *state formulas* φ and *path formulas* ψ of GCCTL* are defined as:

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

where $\top$ denotes "true", E ("for some path") and A ("for all paths") are path quantifiers, η is a $\exists$GC constraint over *Var* $\cup$ *Var'* and *Const*, and O ("next"), U ("until"), and $\Box$ ("always") are the usual linear temporal operators. Since $\exists$GC constraints are not closed under negation, the logic is not closed under negation as well.[4] 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. GCCTL* formulas are interpreted over directed graphs $\mathcal{G} = \langle S, \to, \mu \rangle$ augmented with a mapping μ assigning to each vertex (or state) a valuation over *Var*. For an infinite path $\pi = s_0, s_1, \ldots$ of $\mathcal{G}$, we denote the suffix $s_i, s_{i+1}, \ldots$ of π by π^i, and the i-th state of π by $\pi(i)$. Let $s \in S$ and π be a infinite path of $\mathcal{G}$. For a state (resp., path) formula φ (resp. ψ), the satisfaction relation $(\mathcal{G}, s) \models \varphi$ (resp., $(\mathcal{G}, \pi) \models \psi$), meaning that φ (resp., ψ) holds at state s (resp., holds along π) in $\mathcal{G}$, is defined as (we omit the clauses for conjunction and disjunction):

- $(\mathcal{G}, s) \models A\,\psi \stackrel{\text{def}}{\Leftrightarrow}$ for each infinite path π from s, $(\mathcal{G}, \pi) \models \psi$;
- $(\mathcal{G}, s) \models E\,\psi \stackrel{\text{def}}{\Leftrightarrow}$ there exists an infinite path π from s such that $(\mathcal{G}, \pi) \models \psi$;
- $(\mathcal{G}, \pi) \models \varphi \stackrel{\text{def}}{\Leftrightarrow} (\mathcal{G}, \pi(0)) \models \varphi$;
- $(\mathcal{G}, \pi) \models \eta \stackrel{\text{def}}{\Leftrightarrow} \mu(\pi(0)) \oplus \mu(\pi(1)) \models \eta$;
- $(\mathcal{G}, \pi) \models \mathsf{O}\psi \stackrel{\text{def}}{\Leftrightarrow} (\mathcal{G}, \pi^1) \models \psi$;

[4] If we allow negation, then the successor relation is definable and by [15], basic decision problems become undecidable.

– $(\mathcal{G},\pi) \models \Box\psi \stackrel{\text{def}}{\Leftrightarrow}$ for all $i \geq 0$, $(\mathcal{G},\pi^i) \models \psi$;
– $(\mathcal{G},\pi) \models \psi_1 \mathsf{U} \psi_2 \stackrel{\text{def}}{\Leftrightarrow}$ there is $i \geq 0$. $(\mathcal{G},\pi^i) \models \psi_2$ and for all $j < i$. $(\mathcal{G},\pi^j) \models \psi_1$.

Note that the *dual* until operator $\widetilde{\mathsf{U}}$ can be expressed in the logic since: $\psi_1 \widetilde{\mathsf{U}} \psi_2 \equiv \Box\psi_2 \vee \big(\psi_2 \mathsf{U}(\psi_1 \wedge \psi_2)\big)$. A GCCTL* formula ξ 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 2. 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

$$E\Box[((x'=0) \vee (x'-x) \geq k) \wedge ((y'=0) \vee (y'-y) \geq k')$$

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. For each $x \in$ *Var*, let us denote by ξ_x a special atomic formula (*unboundedness constraint*) that hold along an infinite run π iff the set of x-values along π is unbounded. Let E–GCCTL$^*_{Unb}$ be the extension of E–GCCTL* with these constraints. By the following result (whose proof is in Appendix D.1), it follows that model checking GCS against E–GCCTL$^*_{Unb}$ can be reduced in polynomial time to model checking GCS against E–GCCTL*.

Theorem 6. *Let $\mathcal{S}$ be a* GCS *over Var and φ be a* E–GCCTL$^*_{Unb}$ *formula over Var. Then, one can construct in polynomial-time an extension Var_{ext} of Var, a* GCS $\mathcal{S}_{ext}$ *over Var_{ext}, and a* E–GCCTL* *formula $f(\varphi)$ over Var_{ext} such that: for each state s of $\mathcal{S}$, one can compute in linear-time a state s_{ext} of $\mathcal{S}_{ext}$ so that*

$$(\mathcal{G}(\mathcal{S}),s) \models \varphi \text{ if and only if } (\mathcal{G}(\mathcal{S}_{ext}),s_{ext}) \models f(\varphi)$$

Decision procedures. By [10], model checking GCS against GCCTL* is undecidable. It is straightforward to extend this negative result to model checking GCS against A–GCCTL* (see Appendix D.2). 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.

Theorem 7. *Given a* GCS $\mathcal{S}$ *and a* E–GCCTL* *formula φ, $[\![\varphi]\!]_{\mathcal{S}}$ is* MG *representable and one can construct a* MG *representation of $[\![\varphi]\!]_{\mathcal{S}}$, written $\pi(\mathcal{S},\varphi)$, such that: (1) $\lfloor \pi(\mathcal{S},\varphi) \rfloor_K$ can be built in time $O(|E(\mathcal{S})| \cdot |Q(\mathcal{S})|^2 \cdot 2^{O(|\varphi|)} \cdot (K+2)^{O((2|Var|+|Const|)^2)})$, and (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 space polynomial in the sizes of $\mathcal{S}$ and φ.*

Sketched proof. (A detailed proof is in Appendix D.3). Fix a GCS $\mathcal{S}$. For a (state) E–GCCTL* formula φ, we construct $\pi(\mathcal{S},\varphi)$ and prove Properties 1–2 by induction on the structure of φ. Note that we can assume that each $\exists$GC constraint occurring in

φ is a disjunction of transitional GC. The non-trivial case is when $\varphi = E\,\psi$ for some path formula ψ. Let X be the set of state formulas θ such that there is an occurrence of θ in ψ which is not in the scope of E. By induction hypothesis, we can assume that the result holds for each formula in X. By a generalization of the standard construction for LTL model-checking, we show the following: one can build two GCS $\mathcal{S}_\varphi$ and $\mathcal{S}^{bd}_\varphi$ with set of control points $Q(\mathcal{S}) \times Q_\varphi$, where $Q_\varphi = O(2^{|\varphi|})$, and two subsets $Q^0_\varphi \subseteq Q_\varphi$ and $F \subseteq Q(\mathcal{S}_\varphi)$ such that the following holds:

Claim 1: $(q,\nu) \in [\![\varphi]\!]_{\mathcal{S}}$ *iff* $((q,q_0),\nu) \in \mathit{Inf}_{\mathcal{S}_\varphi,F}$ for some $q_0 \in Q^0_\varphi$.

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

Let $\sigma_F(\mathcal{S}_\varphi)$ be the *computable* MG representation of $\mathit{Inf}_{\mathcal{S}_\varphi,F}$ satisfying the statement of Theorem 5. Then, for each $q \in Q(\mathcal{S})$, the q-component of $\pi(\mathcal{S},\varphi)$ is the union of the (q,q_0)-components of $\sigma_F(\mathcal{S}_\varphi)$ such that $q_0 \in Q^0_\varphi$. By Claim 1, it follows that $\pi(\mathcal{S},\varphi)$ is a *computable* MG representation of $[\![\varphi]\!]_{\mathcal{S}}$. For the remaining part of the theorem, here, we focus on Property 1. By Claim 2, $\mathcal{S}^{bd}_\varphi = \lfloor\mathcal{S}_\varphi\rfloor_K$, hence, by Property 2 of Theorem 5, $\lfloor\sigma_F(\mathcal{S}_\varphi)\rfloor_K = \lfloor\sigma_F(\mathcal{S}^{bd}_\varphi)\rfloor_K$. Thus, since $Q(\mathcal{S}^{bd}_\varphi)$ has cardinality bounded by $|Q(\mathcal{S})|\cdot 2^{O(|\varphi|)}$, by Property 1 of Theorem 5, and Claim 2, Property 1 follows. □

Theorem 8. *Model checking* GCS *against* E–GCCTL* *and satisfiability of* E–GCCTL* *and* A–GCCTL* *are* PSPACE*-complete.*

Sketched proof. By Theorem 7, checking for a GCS $\mathcal{S}$, control point q, and E–GCCTL* formula φ, whether $(\mathcal{G}(\mathcal{S}),(q,\nu)) \models \varphi$ for some valuation ν, is in PSPACE. By an easy linear-time reduction to this last problem, the upper bound for model checking GCS against E–GCCTL* follows. The upper bounds for satisfiability of E–GCCTL* and A–GCCTL* easily follow by a linear-time reduction to the considered model checking problem. For details see Appendix D. Finally, 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., [21]). □

5 Concluding remarks

We focus on the logic GCCTL*. An intriguing question left open is the decidability status for satisfiability of full GCCTL*. Moreover, it would be interesting to investigate extensions of GCCTL* which allow to compare variables at states arbitrarily far away from each other. A possibility would be to permit atomic formulas of the form $x - \Diamond y \geq k$, or $\Diamond y - x \geq k$, or $x - \Box y \geq k$, or $\Box y - x \geq k$ ($k \in \mathbb{N}$), where $\Diamond y$ means "for some future value of y" and $\Box y$ means "for each future value of y". Thus, for example, $x - \Box y \geq 1$ asserts that the future values of y remain below the current value of x. We conjecture that with this extension, Theorem 8 still holds.

References

1. P.A. Abdulla and G. Delzanno. On the coverability problem for constrained multiset rewriting. In *Proc. 5th AVIS*, 2006.

2. P.A. Abdulla, G. Delzanno, and A. Rezine. Approximated parameterized verification of infinite-state processes with global conditions. *Formal Methods in System Design*, 34(2):126–156, 2009.
3. A.M. Ben-Amram. Size-change termination with difference constraints. *ACM Transactions on Programming Languages and Systems*, 30(3), 2008.
4. A.M. Ben-Amram. Size-change termination, monotonicity constraints and ranking functions. *Logical Methods in Computer Science*, 6(3), 2010.
5. B. Boigelot. *Symbolic methods for exploring infinite state spaces*. PhD thesis, Université de Liège, 1998.
6. A. Bouajjani, M. Bozga, P. Habermehl, R. Iosif, P. Moro, and T. Vojnar. Programs with Lists Are Counter Automata. In *Proc. 18th CAV*, volume 4144 of *LNCS*, pages 517–531. Springer, 2006.
7. A. Bouajjani, R. Echahed, and P. Habermehl. On the verification problem of nonregular properties for nonregular processes. In *LICS'95*, pages 123–133. IEEE Computer Society Press, 1995.
8. M. Bozga, C. Girlea, and R. Iosif. Iterating Octagons. In *Proc. 15th TACAS*, volume 5505 of *LNCS*, pages 337–351. Springer, 2009.
9. L. Bozzelli and R. Gascon. Branching-Time Temporal Logic Extended with Qualitative Presburger Constraints. In *LPAR'06*, volume 4246 of *LNCS*, pages 197–211. Springer, 2006.
10. Karlis Cerans. Deciding properties of integral relational automata. In *Proc. 21st ICALP*, LNCS 3921, pages 35–46. Springer, 1994.
11. H. Comon and V. Cortier. Flatness is not a weakness. In *Proc. 14th CSL*, volume 1862 of *LNCS*, pages 262–276. Springer, 2000.
12. H. Comon and Y. Jurski. Multiple Counters Automata, Safety Analysis and Presburger Arithmetic. In *Proc. 10th CAV*, volume 1427 of *LNCS*, pages 268–279. Springer, 1998.
13. S. Demri and Deepak D'Souza. An automata-theoretic approach to constraint LTL. *Information and Computation*, 205(3):380–415, 2007.
14. S. Demri, A. Finkel, V. Goranko, and G. van Drimmelen. Towards a Model-Checker for Counter Systems. In *ATVA'06*, volume 4218 of *LNCS*, pages 493–507. Springer, 2006.
15. S. Demri and R. Gascon. Verification of qualitative Z constraints. *Theoretical Computer Science*, 409(1):24–40, 2008.
16. E.A. Emerson and J.Y. Halpern. Sometimes and not never revisited: On branching versus linear time. *Journal of the ACM*, 33(1):151–178, 1986.
17. A. Finkel and J. Leroux. How to Compose Presburger-Accelerations: Applications to Broadcast Protocols. In *Proc. 22nd FSTTCS*, volume 2556 of *LNCS*, pages 145–156. Springer, 2002.
18. L. Fribourg and J. Richardson. Symbolic Verification with Gap-Order Constraints. In *Proc. 6th LOPSTR*, volume 1207 of *LNCS*, pages 20–37. Springer, 1996.
19. O. Ibarra. Reversal-bounded multicounter machines and their decision problems. *Journal of ACM*, 25(1):116–133, 1978.
20. Neil.D. Jonson. *Computability and Complexity from a Programming Perspective*. Foundations of Computing Series. MIT Press, 1997.
21. O. Kupferman and M.Y. Vardi. An automata-theoretic approach to modular model checking. *ACM Trans. Program. Lang. Syst.*, 22(1):87–128, 2000.
22. M. Minsky. *Computation: Finite and Infinite Machines*. Prentice Hall, 1967.
23. J.L. Peterson. *Petri Net Theory and the Modelling of Systems*. Prentice-Hall, 1981.
24. F. Ramsey. On a problem of formal logic. *Proceedings of the London Mathematical Society*, 30:264–286, 1930.
25. P.Z. Revesz. A Closed-Form Evaluation for Datalog Queries with Integer (Gap)-Order Constraints. *Theoretical Computer Science*, 116(1–2):117–149, 1993.

Appendix

A Proofs from Section 2

A.1 Proof of Proposition 3

In order to prove Proposition 3, we recall [10] that the closure $\overline{G}$ of a *satisfiable* MG G over V and *Const* is the normalized MG over V and *Const* defined as: for all vertices $u, v \in V \cup \mathit{Const}$, 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 Property 2 of Proposition 1, $p_G(u,v) \neq \infty$).

Proposition 3. *Let G be a MG over V and $Const$. Then, 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 Property 2 of Proposition 1 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 Property 3 of Proposition 1, $\lfloor \overline{G} \rfloor_K$ 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:

Claim 1: for each edge $u \xrightarrow{k} v$ of $\overline{G}$, there is an edge $u \xrightarrow{k'} v$ of $\overline{\lfloor G \rfloor_K}$ s.t. $\lfloor k \rfloor_K = \lfloor k' \rfloor_K$;
Claim 2: for each edge $u \xrightarrow{k} v$ of $\overline{\lfloor G \rfloor_K}$, there is an edge $u \xrightarrow{k'} v$ of $\overline{G}$ s.t. $\lfloor k \rfloor_K = \lfloor k' \rfloor_K$.

Proof of Claim 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, $k \geq K$. 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 $k' \geq K$. Since $\lfloor k \rfloor_K = \lfloor k' \rfloor_K = K$, in this case Claim 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 $p_{\lfloor G \rfloor_K}(u,v) \leq p_G(u,v) = k$ and the weight sum of p is k, $u \xrightarrow{k} v$ must be also an edge of $\overline{\lfloor G \rfloor_K}$, and Claim 1 holds in this case as well. □

Proof of Claim 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 a MG and vertices u and v, there is at most one edge from u to v. Thus, by Claim 1, we obtain that $\lfloor k \rfloor_K = \lfloor k' \rfloor_K = K$, and Claim 2 follows. □

A.2 Proof of Proposition 4

In order to prove Proposition 4, we need the following preliminary result.

Proposition 7. *Let G_1 be a MG over V and Const and G_2 be a MG over V' and Const. Then, $\lfloor G_1 \otimes G_2 \rfloor_K = \lfloor \lfloor G_1 \rfloor_K \otimes \lfloor G_2 \rfloor_K \rfloor_K$.*

Proof. By definition of K-bounded MG it suffices to show the following:

Claim 1: for each edge $u \xrightarrow{k} v$ of $G_1 \bigotimes G_2$, there is an edge $u \xrightarrow{k'} v$ of $\lfloor G_1 \rfloor_K \bigotimes \lfloor G_2 \rfloor_K$ such that $\lfloor k \rfloor_K = \lfloor k' \rfloor_K$;

Claim 2: for each edge $u \xrightarrow{k} v$ of $\lfloor G_1 \rfloor_K \bigotimes \lfloor G_2 \rfloor_K$, there is an edge $u \xrightarrow{k'} v$ of $G_1 \bigotimes G_2$ such that $\lfloor k \rfloor_K = \lfloor k' \rfloor_K$.

Proof of Claim 1: Let $u \xrightarrow{k} v$ be an edge in $G_1 \bigotimes G_2$. By Definition 4, there are three cases:

- $u \xrightarrow{k} v$ is an edge of G_1 and there is no edge from u to v in G_2. It follows that $u \xrightarrow{\lfloor k \rfloor_K} v$ is an edge of $\lfloor G_1 \rfloor_K$ and there is no edge from u to v in $\lfloor G_2 \rfloor_K$. Hence, $u \xrightarrow{\lfloor k \rfloor_K} v$ is an edge of $\lfloor G_1 \rfloor_K \bigotimes \lfloor G_2 \rfloor_K$. Thus, in this case Claim 1 holds.
- $u \xrightarrow{k} v$ is an edge of G_2 and there is no edge from u to v in G_1. This case is similar to the previous one.
- G_1 has an edge $u \xrightarrow{k_1} v$, G_2 has an edge $u \xrightarrow{k_2} v$, and $k = \max(\{k_1, k_2\})$. It follows that there is an edge $u \xrightarrow{k'} v$ of $\lfloor G_1 \rfloor_K \bigotimes \lfloor G_2 \rfloor_K$ with $k' = \max(\{\lfloor k_1 \rfloor_K, \lfloor k_2 \rfloor_K\})$. One can easily check that $\lfloor \max(\{k_1, k_2\}) \rfloor_K = \lfloor \max(\{\lfloor k_1 \rfloor_K, \lfloor k_2 \rfloor_K\}) \rfloor_K$. Thus, Claim 1 holds in this case as well. □

Proof of Claim 2: Let $u \xrightarrow{k} v$ be an edge in $\lfloor G_1 \rfloor_K \bigotimes \lfloor G_2 \rfloor_K$. Then, there must be an edge of $G_1 \bigotimes G_2$ of the form $u \xrightarrow{k'} v$ for some k'. Recall that for a MG and its vertices u and v, there is at most one edge from u to v. Thus, by Claim 1, we obtain that $\lfloor k \rfloor_K = \lfloor k' \rfloor_K = K$, and Claim 2 follows. □

Now, we can prove Proposition 4.

Proposition 4. *For transitional* MG G_1 *and* G_2, $\lfloor G_1 \bullet G_2 \rfloor_K = \lfloor \lfloor G_1 \rfloor_K \bullet \lfloor G_2 \rfloor_K \rfloor_K$.

Proof. Let G_2' be obtained from G_2 by renaming any variable x_i' into x_i'' and x_i into x_i'. By Definition 4, and definition of K-bounded MG, it suffices to show that:

Claim: $\lfloor\ \overline{G_1 \bigotimes G_2'}\ \rfloor_K = \lfloor\ \overline{\lfloor G_1 \rfloor_K \bigotimes \lfloor G_2' \rfloor_K}\ \rfloor_K$

By Proposition 3, we obtain

$$\lfloor\ \overline{G_1 \bigotimes G_2'}\ \rfloor_K = \lfloor\ \overline{\lfloor G_1 \bigotimes G_2' \rfloor_K}\ \rfloor_K \tag{1}$$

$$\lfloor\ \overline{\lfloor G_1 \rfloor_K \bigotimes \lfloor G_2' \rfloor_K}\ \rfloor_K = \lfloor\ \overline{\lfloor \lfloor G_1 \rfloor_K \bigotimes \lfloor G_2' \rfloor_K \rfloor_K}\ \rfloor_K \tag{2}$$

By Proposition 7 it holds that $\lfloor G_1 \bigotimes G_2' \rfloor_K = \lfloor \lfloor G_1 \rfloor_K \bigotimes \lfloor G_2' \rfloor_K \rfloor_K$. Thus, by Equalities (1) and (2) above, the claim follows. □

A.3 Proof of Theorem 1

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

Proof. An upper bound on the cardinality of the finite set of K-bounded transitional MG is $(K+2)^{(2|Var|+|Const|)^2}$, as each transitional K-bounded 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 $u \xrightarrow{k} v$, where $k = 0, 1, \ldots, K$. It follows that the cardinality of $\mathcal{G}_{\mathcal{S}}^{K}$ is bounded by $|Q(\mathcal{S})|^2 \cdot (K+2)^{(2|Var|+|Const|)^2}$. By Proposition 5, $\mathcal{G}_{\mathcal{S}}^{K}$ is exactly the set $\{(G_{\wp}^{bd}, s(\wp), t(\wp)) \mid \wp \text{ is a non-null finite path and } G_{\wp}^{bd} \text{ is satisfiable}\}$. It follows that we can compute the set $\mathcal{G}_{\mathcal{S}}^{K}$ by the following transitive closure procedure: initialize a set B to $\{(\lfloor \overline{G} \rfloor_K, q, q') \mid q \xrightarrow{G} q' \text{ is an edge of } \mathcal{S} \text{ and } \lfloor G \rfloor_K \text{ is satisfiable}\}$ and repeat the following step until no more elements can be added to B (at this point $B = \mathcal{G}_{\mathcal{S}}^{K}$): for each $(G^{bd}, q, q') \in B$ and edge $q' \xrightarrow{G} q''$ of $\mathcal{S}$ include in B also $\lfloor G^{bd} \bullet \lfloor G \rfloor_K \rfloor_K$, unless it is unsatisfiable. Hence, the result follows. □

A.4 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 *partial order* iff, additionally, $y \preceq z$ and $z \preceq y$ imply $y = z$. Moreover, we say that $\preceq$ is a *well quasi-ordering* iff for every infinite sequence $y_0, y_1, y_2, \ldots$ of elements of S there exist indices $i < j$ such that $y_i \preceq y_j$. Let $\preceq$ be a partial order on S. For a subset $S' \subseteq S$, a *basis* of S' (w.r.t. $\preceq$) is a subset $B \subseteq S'$ satisfying the following:

- for all $y, z \in B$, $y \preceq z$ implies $y = z$;
- for each $y \in S'$, there is $z \in B$ such that $z \preceq y$.

It is easy to show that if S' is finite, then it admits a unique basis.

Definition 11 (Partial Order on transitional MG). *We define a partial order $\preceq$ on transitional* MG *such that $G \preceq G'$ iff $\lfloor G \rfloor_K = \lfloor G' \rfloor_K$, and for each edge $u \xrightarrow{k} v$ of G, there is an edge in G' of the form $u \xrightarrow{k'} v$ such that $k' \geq k$.*

Proposition 8. *Partial order $\preceq$ is a well quasi-ordering on the set of transitional* MG*.*

Proof. Since the set of K-bounded transitional MG is finite, the result follows from well-quasi ordering of the relation $\leq_h$ (for a fixed $h \in \mathbb{N}$) defined over the set of h-tuples of natural numbers as $(n_1, \ldots, n_h) \leq_h (m_1, \ldots, m_h)$ iff $n_i \leq m_i$ for each $1 \leq i \leq h$ [23]. □

Evidently, the following holds.

Proposition 9. *Let G, G', G'' be transitional* MG *such that $G \preceq G'$. Then, $Sat(G') \subseteq Sat(G)$ and $Sat(G' \bullet G'') \subseteq Sat(G \bullet G'')$.*

For a *finite* set $\mathcal{G}$ of transitional MG, $Min(\mathcal{G})$ denotes the unique basis of $\mathcal{G}$ w.r.t. the partial order $\preceq$ on its elements (note that given $\mathcal{G}$, $Min(\mathcal{G})$ can be effectively computed), and $Sat(\mathcal{G})$ denotes the set $\bigcup_{G \in \mathcal{G}} Sat(G)$. We also define a pre-order $\sqsubseteq$ over finite sets of transitional MG as follows: $\mathcal{G} \sqsubseteq \mathcal{G}'$ iff for each $G' \in \mathcal{G}'$ there is $G \in \mathcal{G}$ such that $G \preceq G'$. The following two Lemmata state some properties of $\sqsubseteq$.

Lemma 3. *Given two* finite *sets $\mathcal{G}$ and $\mathcal{G}'$ of transitional* MG*, the following holds:*

1. *if $\mathcal{G} \subseteq \mathcal{G}'$, then $\mathcal{G}' \sqsubseteq \mathcal{G}$;*
2. *if $\mathcal{G} \sqsubseteq \mathcal{G}'$, then Sat($\mathcal{G}'$) $\subseteq$ Sat($\mathcal{G}$);*
3. *$\mathcal{G} \sqsubseteq Min(\mathcal{G})$ and $Min(\mathcal{G}) \sqsubseteq \mathcal{G}$;*
4. *Sat($\mathcal{G}$) = Sat($Min(\mathcal{G})$);*
5. *if $Min(\mathcal{G}) \sqsubseteq Min(\mathcal{G}')$ and $Min(\mathcal{G}') \sqsubseteq Min(\mathcal{G})$, then $Min(\mathcal{G}) = Min(\mathcal{G}')$.*

Proof. Property 1 is obvious. Property 2 directly follows from the definition of the pre-order $\sqsubseteq$ and Proposition 9. Now, let us consider Property 3. Since $Min(\mathcal{G}) \subseteq \mathcal{G}$, by Property 1 we obtain that $\mathcal{G} \sqsubseteq Min(\mathcal{G})$. Moreover, since $Min(\mathcal{G})$ is the basis of $\mathcal{G}$, for any $G \in \mathcal{G}$ there is $G' \in Min(\mathcal{G})$ such that $G' \preceq G$. This means that $Min(\mathcal{G}) \sqsubseteq \mathcal{G}$. Therefore, Property 3 holds. Property 4 directly follows from Properties 2 and 3. Finally, let us consider Property 5. We show that $Min(\mathcal{G}) \subseteq Min(\mathcal{G}')$ (the other inclusion can be proved in the same way). Let $G \in Min(\mathcal{G})$. Since $Min(\mathcal{G}') \sqsubseteq Min(\mathcal{G})$, there is $G' \in Min(\mathcal{G}')$ such that $G' \preceq G$. Since $Min(\mathcal{G}) \sqsubseteq Min(\mathcal{G}')$, there is $G'' \in Min(\mathcal{G})$ such that $G'' \preceq G'$. Therefore, $G, G'' \in Min(\mathcal{G})$ and $G'' \preceq G$. Since $Min(\mathcal{G})$ is a basis, it follows that $G = G''$. Therefore, $G \preceq G'$ and $G' \preceq G$. Since $\preceq$ is a partial order, we conclude that $G = G'$, hence, $G \in Min(\mathcal{G}')$. □

Lemma 4. *Let $\mathcal{G}_1, \mathcal{G}_2, \ldots$ be an infinite sequence of finite sets of transitional* MG *such that $\mathcal{G}_{i+1} \sqsubseteq \mathcal{G}_i$ for each $i \geq 1$. Then, there is $k \geq 1$ such that $\mathcal{G}_k \sqsubseteq \mathcal{G}_{k+1}$.*

Proof. Assume the contrary and derive a contradiction. Hence, $\mathcal{G}_{i+1} \sqsubseteq \mathcal{G}_i$ and $\mathcal{G}_i \not\sqsubseteq \mathcal{G}_{i+1}$ for each $i \geq 1$. Then, we deduce the following:

Claim: for each $j > 1$, there is $G_j \in \mathcal{G}_j$ such that for all $i < j$ and $G \in \mathcal{G}_i$, $G \not\preceq G_j$.

By the claim above, we deduce the existence of an infinite sequence $G_1, G_2, \ldots$ of transitional MG such that $G_i \not\preceq G_j$ for all $1 \leq i < j$. Since $\preceq$ is a well-quasi ordering (Proposition 8), we obtain a contradiction, and the result follows.

Proof of the claim: assume the contrary and derive a contradiction. Then, there is $j > 1$ such that for each $G_j \in \mathcal{G}_j$, there is $i < j$ and $G_i \in \mathcal{G}_i$ so that $G_i \preceq G_j$. Since $\mathcal{G}_{j-1} \sqsubseteq \mathcal{G}_i$ for each $i < j$, it follows that for each $G_j \in \mathcal{G}_j$, there is $G \in \mathcal{G}_{j-1}$ so that $G \preceq G_j$. This means that $\mathcal{G}_{j-1} \sqsubseteq \mathcal{G}_j$, which is a contradiction. □

We extend the composition operator $\bullet$ to sets $\mathcal{G}$ and $\mathcal{G}'$ of transitional MG: $\mathcal{G} \bullet \mathcal{G}'$ is given by the set $\{G \bullet G' \mid G \in \mathcal{G},\ G' \in \mathcal{G}'\}$. Now, we can prove Theorem 2.

Theorem 2. *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 $\mathcal{S}$ from q to q', there is a path $\wp \in \mathcal{P}_\mathcal{S}$ from q to q' so that $\lfloor G_{\wp'} \rfloor_K = \lfloor G_\wp \rfloor_K$, and $\rightsquigarrow_{\wp'}$ implies $\rightsquigarrow_\wp$.*

Proof. For all $q, q' \in Q(\mathcal{S})$, let $\mathcal{G}_{q,q'} = \{G \mid q \xrightarrow{G} q' \text{ is an edge of } \mathcal{S}\}$. We inductively define a family of finite sets of transitional MG $\mathcal{G}^i_{q,q'}$, where $i \geq 1$ and $q, q' \in Q(\mathcal{S})$:

- $\mathcal{G}^1_{q,q'} = \{\overline{G} \mid q \xrightarrow{G} q' \text{ is an edge of } \mathcal{S}\}$;
- $\mathcal{G}^{i+1}_{q,q'} = Min(\{\mathcal{G}^i_{q,q''} \bullet \mathcal{G}_{q'',q'} \mid q'' \in Q(\mathcal{S})\} \cup \mathcal{G}^i_{q,q'})$.

Note that each $\mathcal{G}^i_{q,q'}$ can be effectively built. Moreover, by construction and Proposition 5, for each $G \in \mathcal{G}^i_{q,q'}$, there is a non-null path of $\mathcal{S}$ from q to q' of length at most i, denoted by $\wp_G$, such that G characterizes the reachability relation $\rightsquigarrow_{\wp_G}$. Moreover, $G = G_{\wp_G}$. Now, we prove two claims.

Claim 1 Let $\wp$ be a non-null finite path of $\mathcal{S}$ from q to q'. Then, for $i = |\wp|$, there is $G \in \mathcal{G}^i_{q,q'}$ such that $\lfloor G_\wp \rfloor_K = \lfloor G \rfloor_K$ and $\rightsquigarrow_\wp$ implies $\rightsquigarrow_{\wp_G}$.

Claim 2 The sequence $\mathcal{G}^1_{q,q'}, \mathcal{G}^2_{q,q'}, \ldots$ stabilizes after a finite number of steps, i.e. there is $k_0 > 1$ such that $\mathcal{G}^i_{q,q'} = \mathcal{G}^{k_0}_{q,q'}$ for all $i \geq k_0$ and $q, q' \in Q(\mathcal{S})$. Moreover, k_0 can be effectively computed.

Proof of Claim 1: By induction on the length of $\wp$. For the base step, it suffices to observe that by construction for each finite path $\wp$ from q to q' of length 1, there is $G \in \mathcal{G}^1_{q,q'}$ such that $\wp_G = \wp$. Now, assume that $|\wp| = i + 1$ with $i \geq 1$. Then, $\wp$ can be written in the form $\wp = \wp'\wp''$ such that for some $q'' \in Q(\mathcal{S})$, $\wp'$ is a path of length i from q to q'' and $\wp''$ is a path of length 1 from q'' to q'. Let G'' be the MG labeling $\wp''$. Then, $G'' \in \mathcal{G}_{q'',q'}$, and by induction hypothesis, there is $G' \in \mathcal{G}^i_{q,q''}$ such that $\rightsquigarrow_{\wp'}$ implies $\rightsquigarrow_{\wp_{G'}}$, and $\lfloor G_{\wp'} \rfloor_K = \lfloor G' \rfloor_K$. It follows that $\rightsquigarrow_\wp$ implies $\rightsquigarrow_{\wp_{G'}\wp''}$ and $G' \bullet G''$ (resp., $G_{\wp'} \bullet G''$) characterizes the reachability relation $\rightsquigarrow_{\wp_{G'}\wp''}$ (resp., $\rightsquigarrow_\wp$). Moreover, $\lfloor G_\wp \rfloor_K = \lfloor G_{\wp'} \bullet G'' \rfloor_K = \lfloor \lfloor G_{\wp'} \rfloor_K \bullet \lfloor G'' \rfloor_K \rfloor_K = \lfloor \lfloor G' \rfloor_K \bullet \lfloor G'' \rfloor_K \rfloor_K = \lfloor G' \bullet G'' \rfloor_K$. Furthermore, by construction, there is $G \in \mathcal{G}^{i+1}_{q,q'}$ such that $G \preceq G' \bullet G''$, hence $\lfloor G \rfloor_K = \lfloor G' \bullet G'' \rfloor_K$. It follows that $\lfloor G \rfloor_K = \lfloor G_\wp \rfloor_K$, and $\rightsquigarrow_{\wp_{G'}\wp''}$ implies $\rightsquigarrow_{\wp_G}$. Hence, $\rightsquigarrow_\wp$ implies $\rightsquigarrow_{\wp_G}$, which concludes. □

Proof of Claim 2: First, we prove the following properties:

1. $\mathcal{G}^{i+1}_{q,q'} \sqsubseteq \mathcal{G}^i_{q,q'}$ for each $i \geq 1$;
2. if $\mathcal{G}^i_{q,q'} = \mathcal{G}^{i+1}_{q,q'}$ for all $q, q' \in Q(\mathcal{S})$, then $\mathcal{G}^j_{q,q'} = \mathcal{G}^i_{q,q'}$ for all $j \geq i$;
3. there is $k \geq 1$ such that $\mathcal{G}^k_{q,q'} \sqsubseteq \mathcal{G}^{k+1}_{q,q'}$ for all $q, q' \in Q(\mathcal{S})$.

Property 1 directly follows from construction and Properties 1 and 3 of Lemma 3. Property 2 directly follows from construction. Now, we prove Property 3. Assume on the contrary that Property 3 does not hold and derive a contradiction. Since the set $Q(\mathcal{S})$ is finite, we deduce that there are $q, q' \in Q(\mathcal{S})$ such that the set $I_{q,q'} = \{i > 1 \mid \mathcal{G}^i_{q,q'} \not\sqsubseteq \mathcal{G}^{i+1}_{q,q'}\}$ is infinite. By Property 1, it follows that there is an infinite chain

$$\mathcal{G}^{i_1}_{q,q'} \sqsupseteq \mathcal{G}^{i_2}_{q,q'} \sqsupseteq \ldots \sqsupseteq \mathcal{G}^{i_m}_{q,q'} \sqsupseteq \ldots$$

such that $i_1 < i_2 < \ldots < i_m < \ldots$ are elements of $I_{q,q'}$ and $\mathcal{G}^{i_j}_{q,q'} \not\sqsubseteq \mathcal{G}^{i_{j+1}}_{q,q'}$ for each $j \geq 1$. By Lemma 4, we obtain a contradiction. Thus, Property 3 holds. By Properties 1, 2 and 3, and Property 5 of Lemma 3, we deduce that it is defined the smallest $k_0 > 1$ such that $\mathcal{G}^{k_0}_{q,q'} = \mathcal{G}^{k_0+1}_{q,q'}$ (note that such a k_0 can be computed). Moreover, it holds that $\mathcal{G}^i_{q,q'} = \mathcal{G}^{k_0}_{q,q'}$ for all $i \geq k_0$ and $q, q' \in Q(\mathcal{S})$. Thus, Claim 2 holds. □

Let $k_0 > 1$ as in Claim 2 and let $\mathcal{P}_\mathcal{S}$ be the computable finite set of non-null finite paths of $\mathcal{S}$ given by $\mathcal{P}_\mathcal{S} = \{\wp_G \mid G \in \mathcal{G}^i_{q,q'}$ for some $i \leq k_0$ and $q, q' \in Q(\mathcal{S})\}$. By Claims 1 and 2, it follows that for each non-null finite path $\wp'$ of $\mathcal{S}$ from q to q', there is a path $\wp \in \mathcal{P}_\mathcal{S}$ from q to q' such that $\lfloor G_{\wp'} \rfloor_K = \lfloor G_\wp \rfloor_K$, and $\rightsquigarrow_{\wp'}$ implies $\rightsquigarrow_\wp$. Hence, the theorem follows. □

B Proofs from Subsection 3.1

B.1 Proof of Lemma 2

We need some additional definitions and preliminary results. Recall that the fixed transitional MG G labeling the self-loop of the fixed simple GCS $\mathcal{S}$ is complete, balanced, idempotent, satisfiable, and *weakly* normalized. Let L, U, and *Unc* as defined in Subsection 3.1. First, we give two technical lemmata, fundamental to understand the "interaction" between the variables in *Var* and those in *Var*$'$ for the fixed transitional MG G.

Lemma 5 (lower variables). *Let* $1 \leq i < j \leq N$. *Then, the following holds:*

1. *if* $G \models \mathrm{L}'_i \leq \mathrm{L}_j$, *then* either $G \models \mathrm{L}'_j \leq \mathrm{L}_j$ or $G \models \mathrm{L}'_i \leq \mathrm{L}_{j-1}$;
2. *if* $G \models \mathrm{L}_i \leq \mathrm{L}'_j$, *then* either $G \models \mathrm{L}_j \leq \mathrm{L}'_j$ or $G \models \mathrm{L}_i \leq \mathrm{L}'_{j-1}$.

Proof. First, we prove Condition 1. Assume that $G \models \mathrm{L}'_i \leq \mathrm{L}_j$ (where $i < j$). Then, since G is idempotent, $G \bullet G \models \mathrm{L}'_i \leq \mathrm{L}_j$. Hence, there is $u \in \mathit{Var} \cup \mathit{Const}$ such that $G \models u' \leq \mathrm{L}_j$ and $G \models \mathrm{L}'_i \leq u$.[5] Since $G \models u' \leq \mathrm{L}_j$, we deduce that u is a lower variable, hence $u = \mathrm{L}_h$ for some $h = 1, \ldots, N$. There are two cases:

- $h \geq j$. Since $G \models \mathrm{L}'_h \leq \mathrm{L}_j$ and $G \models \mathrm{L}'_j \leq \mathrm{L}'_h$, we obtain that $G \models \mathrm{L}'_j \leq \mathrm{L}_j$. Thus, in this case Condition 1 holds.
- $h < j$. Since $G \models \mathrm{L}'_i \leq \mathrm{L}_h$ and $G \models \mathrm{L}_h \leq \mathrm{L}_{j-1}$, we obtain that $G \models \mathrm{L}'_i \leq \mathrm{L}_{j-1}$. Thus, Condition 1 holds in this case as well.

This concludes the proof of Condition 1. Now, we prove Condition 2. Assume that $G \models \mathrm{L}_i \leq \mathrm{L}'_j$ (where $i < j$). Since G is idempotent, $G \bullet G \models \mathrm{L}_i \leq \mathrm{L}'_j$. Hence, there is $u \in \mathit{Var} \cup \mathit{Const}$ such that $G \models \mathrm{L}_i \leq u'$ and $G \models u \leq \mathrm{L}'_j$. Since $G \models u \leq \mathrm{L}'_j$, we deduce that u is a lower variable, hence $u = \mathrm{L}_h$ for some $h = 1, \ldots, N$. There are two cases:

- $h \geq j$. Since $G \models \mathrm{L}_h \leq \mathrm{L}'_j$ and $G \models \mathrm{L}_j \leq \mathrm{L}_h$, we obtain that $G \models \mathrm{L}_j \leq \mathrm{L}'_j$. Thus, in this case Condition 2 holds.
- $h < j$. Since $G \models \mathrm{L}_i \leq \mathrm{L}'_h$ and $G \models \mathrm{L}'_h \leq \mathrm{L}'_{j-1}$, we obtain that $G \models \mathrm{L}_i \leq \mathrm{L}'_{j-1}$. Thus, Condition 2 holds in this case as well.

This concludes the proof Condition 2, and we are done. □

Symmetric results hold for the upper variables (the proof is very similar to that of Lemma 5 and we omit it).

Lemma 6 (upper variables). *Let* $1 \leq i < j \leq M$. *Then, the following holds:*

1. *if* $G \models \mathrm{U}'_i \leq \mathrm{U}_j$, *then* either $G \models \mathrm{U}'_j \leq \mathrm{U}_j$ or $G \models \mathrm{U}'_i \leq \mathrm{U}_{j-1}$;
2. *if* $G \models \mathrm{U}_i \leq \mathrm{U}'_j$, *then* either $G \models \mathrm{U}_j \leq \mathrm{U}'_j$ or $G \models \mathrm{U}_i \leq \mathrm{U}'_{j-1}$.

Lemma 7. *Assume that* $\mathcal{S} \notin \mathcal{TC}$. *Then, the following holds:*

Lower Variables: *for all* $1 \leq i, j < L$, $G \not\models \mathrm{L}_i \leq \mathrm{L}'_j$;

[5] where u' denotes the corresponding variable in *Var*$'$ if $u \in \mathit{Var}$, and u itself otherwise.

Upper Variables: *for all* $U < i, j \leq M$, $G \not\models \mathrm{U}'_i \leq \mathrm{U}_j$*;*

Proof. **Lower Variables.** Assume that the result does not hold and derive a contradiction. Then, there are $1 \leq i, j < L$ such that $G \models \mathrm{L}_i \leq \mathrm{L}'_j$. There are two cases:

- $j \leq i$: since $G \models \mathrm{L}'_j \leq \mathrm{L}'_i$ and $G \models \mathrm{L}_i \leq \mathrm{L}'_j$, it follows that $G \models \mathrm{L}_i \leq \mathrm{L}'_i$.
- $j > i$: since $G \models \mathrm{L}_i \leq \mathrm{L}'_j$, by applying repeatedly Condition 2 of Lemma 5, it follows that there is $i \leq h \leq j$ such that $G \models \mathrm{L}_h \leq \mathrm{L}'_h$.

Thus, in both cases we obtain that $G \models \mathrm{L}_k \leq \mathrm{L}'_k$ for some $k < L$. 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 and the fact that $\mathcal{S} \notin \mathcal{TC}$. Hence, the result follows.

Upper Variables. Assume that the result does not hold and derive a contradiction. Then, there are $U < i, j, \leq M$ such that $G \models \mathrm{U}'_i \leq \mathrm{U}_j$. There are two cases:

- $j \leq i$: since $G \models \mathrm{U}'_j \leq \mathrm{U}'_i$ and $G \models \mathrm{U}'_i \leq \mathrm{U}_j$, it follows that $G \models \mathrm{U}'_j \leq \mathrm{U}_j$.
- $j > i$: since $G \models \mathrm{U}'_i \leq \mathrm{U}_j$, by applying repeatedly Condition 1 of Lemma 6, it follows that there is $i \leq h \leq j$ so that $G \models \mathrm{U}'_h \leq \mathrm{U}_h$.

Thus, in both cases we obtain that $G \models \mathrm{U}'_k \leq \mathrm{U}_k$ for some $U < k \leq M$. Since G is complete, it follows that $G \models \mathrm{U}'_k \lhd \mathrm{U}_k$ for some $\lhd \in \{=, <\}$, which is a contradiction by definition of U and the fact that $\mathcal{S} \notin \mathcal{TC}$. Hence, the result follows. □

Now, we define a partial order $\succeq_G$ (depending on the MG G) on the set of valuations over *Var* as follows: $\nu' \succeq_G \nu$ iff the following properties are satisfied:

- for each $\mathrm{B}_i \in B$, $\nu'(\mathrm{B}_i) = \nu(\mathrm{B}_i)$ (B is the set of bounded variables of G in *Var*);
- for all $u, v \in \mathit{Var} \cup \mathit{Const}$ and $\lhd \in \{<, =\}$, $\nu(u) \lhd \nu(v)$ iff $\nu'(u) \lhd \nu'(v)$;
- for all $u, v \in \mathit{Var} \cup \mathit{Const}$, if $\nu(u) - \nu(v) \geq 0$, then $\nu'(u) - \nu'(v) \geq \nu(u) - \nu(v)$.

Lemma 8 (Simulation lemma). *Let* $\nu_1 \oplus \nu_2 \in \mathit{Sat}(G)$ *and* $\nu'_1 \succeq_G \nu_1$*. Then,* $\nu'_1 \oplus \nu'_2 \in \mathit{Sat}(G)$ *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. Moreover, since $\nu_1 \oplus \nu_2 \in \mathit{Sat}(G)$, $\nu_1 \oplus \nu_2$ induces an ordering of the upper and lower variables in $\mathit{Var} \cup \mathit{Var}'$ 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 $\nu'_1 \oplus \nu'_2 \in \mathit{Sat}(G)$ and satisfying the above additional constraint w.r.t. ν_2 (i.e., ensuring $\nu'_2 \succeq_G \nu_2$) easily follows. □

For two valuations $\nu : V \to \mathbb{Z}$ and $\nu' : V' \to \mathbb{Z}$ such that $V \cap V' = \emptyset$, $\nu \uplus \nu'$ denotes the unique valuation over $V \cup V'$ extending both ν and ν'.

Lemma 9 (Pumping lemma). *Assume that* $\mathcal{S} \notin \mathcal{TC}$*. Let* $\nu : \mathit{Var} \to \mathbb{Z}$ *and* $\nu' : (\mathit{Var} \setminus \mathit{Unc}) \to \mathbb{Z}$ *be valuations such that* $\nu \oplus \nu'$ *is a solution of the restriction of* G *to* $\mathit{Var} \cup (\mathit{Var}' \setminus \mathit{Unc}')$*. Then, for each valuation* $\nu_0 : \mathit{Unc} \to \mathbb{Z}$ *such that* $\nu' \uplus \nu_0 \in \mathit{Sat}(G_{\mathit{Var}})$*,* ν' *can be extended to a valuation* ν'' *over Var in such a way that:* $\nu \oplus \nu''$ *is a solution of* G *and* $\nu'' \succeq_G (\nu' \uplus \nu_0)$*.*

Proof. Let ν_0, ν, and ν' as in the statement of the lemma. Let $\mathrm{U}_0 = \mathrm{U}'_0 = \mathit{MAX}$ and $\mathrm{L}_{N+1} = \mathrm{L}'_{N+1} = \mathit{MIN}$. Recall that $\mathit{Unc} = \{\mathrm{L}_1, \ldots, \mathrm{L}_{L-1}, \mathrm{U}_{U+1}, \ldots, \mathrm{U}_M\}$ and $\mathit{Unc}' = \{\mathrm{L}'_1, \ldots, \mathrm{L}'_{L-1}, \mathrm{U}'_{U+1}, \ldots, \mathrm{U}'_M\}$. Let $K \in \mathbb{N}$ such that $K \geq |[\nu' \uplus \nu_0](u) - [\nu' \uplus \nu_0](v)|$ for all $u, v \in \mathit{Var} \cup \mathit{Const}$ and $K \geq \Delta$, where Δ is the maximum of the set of edge weights of G. Let $\nu'_0 : \mathit{Unc} \to \mathbb{Z}$ be any valuation over Unc such that (w.l.o.g., we assume that the sets of upper and lower variables are not empty):

1. for all $u, v \in \mathit{Unc}$, $G \models u = v$ implies $\nu'_0(v) = \nu'_0(u)$;
2. for all $u, v \in \mathit{Unc}$, $G \models u < v$ implies $\nu'_0(v) - \nu'_0(u) > K$;
3. for each $\mathrm{U}_i \in \mathit{Unc}$, $\nu'_0(\mathrm{U}_i) - \nu'(\mathrm{U}_U) > K$ and $\nu'_0(\mathrm{U}_i) - \nu(\mathrm{U}_M) > K$;
4. for each $\mathrm{L}_i \in \mathit{Unc}$, $\nu'(\mathrm{L}_L) - \nu'_0(\mathrm{L}_i) > K$ and $\nu(\mathrm{L}_1) - \nu'_0(\mathrm{L}_i) > K$.

Since G is satisfiable and $G \models \mathrm{L}_i < \mathrm{U}_j$ for all upper variables $\mathrm{U}_j \in \mathit{Unc}$ and lower variables $\mathrm{L}_j \in \mathit{Unc}$, a valuation $\nu'_0 : \mathit{Unc} \to \mathbb{Z}$ satisfying the above conditions must exist. Since $\nu' \uplus \nu_0 \in \mathit{Sat}(G_{\mathit{Var}})$, $G \models \mathrm{U}_U < \mathrm{U}_j$ and $G \models \mathrm{L}_i < \mathrm{L}_L$ for all upper variables $\mathrm{U}_j \in \mathit{Unc}$ and lower variables $\mathrm{L}_i \in \mathit{Unc}$, and $G \models \mathrm{L}_L \leq x \leq \mathrm{U}_U$ for each $x \in \mathit{Var} \setminus \mathit{Unc}$, we deduce that $\nu'' = \nu' \uplus \nu'_0 \in \mathit{Sat}(G_{\mathit{Var}})$. Moreover, since G is complete, by definition of $\succeq_G$, we also deduce that $\nu'' \succeq_G (\nu' \uplus \nu_0)$.

By Lemma 7, $G \not\models \mathrm{U}'_i \leq \mathrm{U}_j$ and $G \not\models \mathrm{L}_h \leq \mathrm{L}'_k$ for all upper variables $\mathrm{U}'_i, \mathrm{U}_j$ and lower variables $\mathrm{L}_h, \mathrm{L}'_k$ in $\mathit{Unc} \cup \mathit{Unc}'$. Moreover, by definition of L and U, we have that $G \models \mathrm{U}_U = \mathrm{U}'_U < \mathrm{U}'_i$ and $G \models \mathrm{L}'_h < \mathrm{L}'_L = \mathrm{L}_L$ for all upper variables $\mathrm{U}'_i \in \mathit{Unc}'$ and lower variables $\mathrm{L}'_h \in \mathit{Unc}'$. Since G is balanced and complete and by hypothesis $\nu \oplus \nu'$ is a solution of the restriction of G to $\mathit{Var} \cup (\mathit{Var}' \setminus \mathit{Unc}')$, by construction of K and Conditions 1–4, it easily follows that $\nu \oplus \nu''$ is a solution of G, which concludes. □

Now, we can prove Lemma 2.

Lemma 2. *Let $\mathcal{S} \notin \mathcal{TC}$. Then, $(q, \nu_0) \in \mathit{Inf}_{\mathcal{S}}$* iff *there is a finite run π of $\mathcal{S}$ from (q, ν_0) of the form $\pi = (q, \nu_0) \ldots (q, \nu) \ldots (q, \nu')(q, \nu'')$ such that $\nu''_{(\mathit{Var} \setminus \mathit{Unc})} = \nu_{(\mathit{Var} \setminus \mathit{Unc})}$.*

Proof. For the right implication $\Rightarrow$, assume that $(q, \nu_0) \in \mathit{Inf}_{\mathcal{S}}$. Hence, there is an infinite run from (q, ν_0) in $\mathcal{S}$. Then, by Lemma 1, the result follows.

For the left implication $\Leftarrow$, assume that for a valuation ν_0 over Var, there is a finite run from (q, ν_0) of the form $\pi = (q, \nu_0) \ldots (q, \nu) \ldots (q, \nu')(q, \nu'')$ such that $\nu''_{(\mathit{Var} \setminus \mathit{Unc})} = \nu_{(\mathit{Var} \setminus \mathit{Unc})}$. Let us consider the suffix run of π, $(q, \nu) \ldots (q, \nu')(q, \nu'')$, where $\nu''_{(\mathit{Var} \setminus \mathit{Unc})} = \nu_{(\mathit{Var} \setminus \mathit{Unc})}$. Since $\nu' \oplus \nu''_{(\mathit{Var} \setminus \mathit{Unc})}$ is a solution of the restriction of G to $\mathit{Var} \cup (\mathit{Var}' \setminus \mathit{Unc}')$, $\nu \in \mathit{Sat}(G_{\mathit{Var}})$, and $\nu = \nu''_{(\mathit{Var} \setminus \mathit{Unc})} \uplus \nu_{\mathit{Unc}}$, by Lemma 9, $\nu''_{(\mathit{Var} \setminus \mathit{Unc})}$ can be extended to a valuation ν''' over Var such that $\nu''' \succeq_G (\nu''_{(\mathit{Var} \setminus \mathit{Unc})} \uplus \nu_{\mathit{Unc}}) = \nu$ and $\nu' \oplus \nu'''$ is a solution of G. It follows that there is a finite run π' in $\mathcal{S}$ of the form $\pi' = (q, \nu_0) \ldots (q, \nu) \ldots (q, \nu')(q, \nu''')$ where $\nu''' \succeq_G \nu$. By applying repeatedly Lemma 8, we obtain that there is an infinite run from (q, ν_0) in $\mathcal{S}$, which concludes. □

B.2 Detailed proof of Theorem 3

Theorem 3. *Let $\mathcal{S} \notin \mathcal{TC}$. Then, Inf_S is* MG *representable and one can construct a* MG *representation of Inf_S, written $\sigma(\mathcal{S})$, such that: (1) $\lfloor \sigma(\mathcal{S}) \rfloor_K$ can be computed in polynomial time, and (2) $\lfloor \sigma(\mathcal{S}) \rfloor_K = \lfloor \sigma(\lfloor \mathcal{S} \rfloor_K) \rfloor_K$ ($\lfloor \mathcal{S} \rfloor_K$ is simple and $\lfloor \mathcal{S} \rfloor_K \notin \mathcal{TC}$).*

Proof. 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 $\rightsquigarrow_{\wp}$. Note that given $\wp \in \mathcal{P}$, the transitional MG $G_{\wp}$ (which characterizes the reachability relation $\rightsquigarrow_{\wp}$) has the form $\underbrace{G \bullet \ldots \bullet G}_{k \text{ times}}$ for some $k \geq 1$.

Let $G_{=,\mathcal{S}}$ be the transitional MG (depending on $\mathcal{S}$) corresponding to the GC given by $\bigwedge_{x \in \mathit{Var} \setminus \mathit{Unc}} x' = x$. Moreover, let $\mathcal{G}_{\mathcal{S}}$ be the set of transitional MG given by

$$\mathcal{G}_{\mathcal{S}} = \{G_{\wp} \bullet (G_{\wp'} \bigotimes G_{=,\mathcal{S}}) \mid \wp, \wp' \in \mathcal{P}\} \cup \{G_{\wp} \bigotimes G_{=,\mathcal{S}} \mid \wp \in \mathcal{P}\}$$

Then, $\sigma(\mathcal{S}) = \{\sigma(\mathcal{S})_{q'}\}_{q' \in \{q_0, q\}}$ is defined as follows: the q-component $\sigma(\mathcal{S})_q$ and the q_0-component $\sigma(\mathcal{S})_{q_0}$ of $\sigma(\mathcal{S})$ are the finite sets of MG over *Var* and *Const* given by:

$$\sigma(\mathcal{S})_q = \{G' \mid G' \text{ is the projection of } G'' \text{ over } \mathit{Var} \text{ for some } G'' \in \mathcal{G}_{\mathcal{S}}\}$$

$$\sigma(\mathcal{S})_{q_0} = \{G' \mid G' \text{ is the projection of } G_0 \bullet G'' \text{ over } \mathit{Var} \text{ for some } G'' \in \mathcal{G}_{\mathcal{S}}\}$$

Correctness of the construction easily follows from Lemma 2. Now, we prove Property 1 in the statement of the theorem. By Definition 4, for all transitional MG G' and G'', $G' \bullet G'' = \overline{G' \bullet G''}$. Thus, $\sigma(\mathcal{S})_q$ and $\sigma(\mathcal{S})_{q_0}$ can be rewritten as:

$$\sigma(\mathcal{S})_q = \{(\overline{G'})_{\mathit{Var}} \mid G' \in \mathcal{G}_{\mathcal{S}}\} \text{ and } \sigma(\mathcal{S})_{q_0} = \{(G_0 \bullet G')_{\mathit{Var}} \mid G' \in \mathcal{G}_{\mathcal{S}}\}$$

Thus, by Propositions 3 and 4, we obtain

$$\lfloor \sigma(\mathcal{S})_q \rfloor_K = \{(\lfloor \overline{G'} \rfloor_K)_{\mathit{Var}} \mid G' \in \lfloor \mathcal{G}_{\mathcal{S}} \rfloor_K\} \tag{3}$$

$$\lfloor \sigma(\mathcal{S})_q \rfloor_K = \{(\lfloor \lfloor G_0 \rfloor_K \bullet G' \rfloor_K)_{\mathit{Var}} \mid G' \in \lfloor \mathcal{G}_{\mathcal{S}} \rfloor_K\} \tag{4}$$

Now, let us consider the set $\lfloor \mathcal{G}_{\mathcal{S}} \rfloor_K$. Since G is idempotent, by Proposition 4, we obtain that for each $\wp \in \mathcal{P}$, $\lfloor G_{\wp} \rfloor_K = \lfloor G \rfloor_K$. Moreover, by Proposition 7 in Appendix A.2, $\lfloor G_{\wp} \bigotimes G_{=,\mathcal{S}} \rfloor_K = \lfloor \lfloor G \rfloor_K \bigotimes \lfloor G_{=,\mathcal{S}} \rfloor_K \rfloor_K = \lfloor G \bigotimes G_{=,\mathcal{S}} \rfloor_K$. Thus, applying again Proposition 4, we obtain

$$\lfloor \mathcal{G}_{\mathcal{S}} \rfloor_K = \{\lfloor G \bullet (G \bigotimes G_{=,\mathcal{S}}) \rfloor_K \, , \, \lfloor G \bigotimes G_{=,\mathcal{S}} \rfloor_K\} \tag{5}$$

By equalities 3–5, Property 1 follows. Finally, let us consider Property 2. First, observe that $\lfloor \mathcal{S} \rfloor_K$ is a simple GCS and by Definition 10, $\mathcal{S} \notin \mathcal{TC}$ iff $\lfloor \mathcal{S} \rfloor_K \notin \mathcal{TC}$. 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 Proposition 7 in Appendix A.2 and Proposition 4, we obtain that $\lfloor \mathcal{G}_{\lfloor \mathcal{S} \rfloor_K} \rfloor_K = \lfloor \mathcal{G}_{\mathcal{S}} \rfloor_K$. Thus, by equalities 3–4, $\lfloor \sigma(\mathcal{S}) \rfloor_K = \lfloor \sigma(\lfloor \mathcal{S} \rfloor_K) \rfloor_K$, which concludes. □

C Proofs from Subsection 3.2

C.1 Detailed proof of Theorem 5

We need an additional result.

Proposition 10. *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 holds:*

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 $G' \in \mathcal{G}_b$, $G \otimes G'$ is complete. Furthermore, $Sat(G) = \bigcup_{G' \in \mathcal{G}_b} Sat(G \otimes G')$. Then, $\mathcal{C}(\mathcal{S})$ is obtained from $\mathcal{S}$ by replacing each edge $q \xrightarrow{G} q'$ with the edges $q \xrightarrow{G \otimes G'} q'$, 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 in Appendix A.2, we obtain that for each transitional MG G and $G' \in \mathcal{G}_b$, $\lfloor G \otimes G' \rfloor_K = \lfloor \lfloor G \rfloor_K \otimes G' \rfloor_K$. Hence, Property 2 holds as well, which concludes. □

Theorem 5. *Let $\mathcal{S}$ be a* GCS *and $F \subseteq Q(\mathcal{S})$. Then, $Inf_{\mathcal{S},F}$ is* MG *representable and one can construct a* MG *representation of $Inf_{\mathcal{S},F}$, written $\sigma_F(\mathcal{S})$, such that:*

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

Proof. We distinguish two cases:

- **$\mathcal{S}$ is complete:** Let $\mathcal{P}_\mathcal{S}$ be the computable finite set of non-null finite paths of $\mathcal{S}$ satisfying the statement of Theorem 2, and let $\mathcal{F}_\mathcal{S}$ be the finite set of *simple* GCS constructed as follows: $\mathcal{S}' \in \mathcal{F}_\mathcal{S}$ iff $\mathcal{S}' \notin \mathcal{TC}$ and $\mathcal{S}'$ is a simple GCS consisting of two edges of the form $(\natural, s(\wp_0)) \xrightarrow{G_{\wp_0}} t(\wp_0)$ and $s(\wp) \xrightarrow{G_\wp} t(\wp)$ such that $\wp_0, \wp \in \mathcal{P}_\mathcal{S}$ and $s(\wp) = t(\wp) \in F$. By Theorem 3, for each $\mathcal{S}' \in \mathcal{F}_\mathcal{S}$ one can compute a MG representation $\mathcal{G}_{\mathcal{S}', in(\mathcal{S}')}$ (resp., $\mathcal{G}_{\lfloor \mathcal{S}' \rfloor_K, in(\mathcal{S}')}$) of $Inf_{\mathcal{S}'}^{(\natural, in(\mathcal{S}'))}$ (resp., $Inf_{\lfloor \mathcal{S}' \rfloor_K}^{(\natural, in(\mathcal{S}'))}$), where $(\natural, in(\mathcal{S}'))$ is the initial control point of $\mathcal{S}'$. Moreover, $\lfloor \mathcal{G}_{\mathcal{S}', in(\mathcal{S}')} \rfloor_K = \lfloor \mathcal{G}_{\lfloor \mathcal{S}' \rfloor_K, in(\mathcal{S}')} \rfloor_K$. Then, $\sigma_F(\mathcal{S})$ is given by

$$\sigma_F(\mathcal{S}) = \{ \bigcup_{\{\mathcal{S}' \in \mathcal{F}_\mathcal{S} \mid in(\mathcal{S}') = q\}} \mathcal{G}_{\mathcal{S}', in(\mathcal{S}')} \}_{q \in Q(\mathcal{S})}$$

.

By Theorems 2 and 4, and Proposition 6, $\sigma_F(\mathcal{S})$ is a 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: Let $\mathcal{F}_{\mathcal{S},K}$ be the set of simple GCS $\mathcal{S}'$ such that $\mathcal{S}' = \lfloor \mathcal{S}'' \rfloor_K$ for some $\mathcal{S}'' \in \mathcal{F}_\mathcal{S}$. Since $\lfloor \mathcal{G}_{\mathcal{S}', in(\mathcal{S}')} \rfloor_K = \lfloor \mathcal{G}_{\lfloor \mathcal{S}' \rfloor_K, in(\mathcal{S}')} \rfloor_K$ for each $\mathcal{S}' \in \mathcal{F}_\mathcal{S}$, we obtain

$$\lfloor \sigma_F(\mathcal{S}) \rfloor_K = \{ \bigcup_{\{\mathcal{S}' \in \mathcal{F}_{\mathcal{S},K} | in(\mathcal{S}') = q\}} \lfloor \mathcal{G}_{\mathcal{S}', in(\mathcal{S}')} \rfloor_K \}_{q \in Q(\mathcal{S})}$$

Since for each $\mathcal{S}' \in \mathcal{F}_{\mathcal{S},K}$, $\lfloor \mathcal{G}_{\mathcal{S}', in(\mathcal{S}')} \rfloor_K$ can be computed in polynomial time in the size of $\mathcal{S}'$ (Theorem 3), it suffices to show that $\mathcal{F}_{\mathcal{S},K}$ can be computed in time $O(|E(\mathcal{S})| \cdot |Q(\mathcal{S})|^2 \cdot (K+2)^{(2|\mathit{Var}|+|\mathit{Const}|)^2})$. On the other hand, this last condition holds since: (i) for a GCS $\mathcal{S}'$, $\mathcal{S}'$ is simple iff $\lfloor \mathcal{S}' \rfloor_K$ is simple, (ii) for a simple GCS $\mathcal{S}''$, $\mathcal{S}'' \notin \mathcal{TC}$ iff $\lfloor \mathcal{S}'' \rfloor_K \notin \mathcal{TC}$, (iii) by Theorem 2, the set $\{(\lfloor G_\wp \rfloor_K, s(\wp), t(\wp)) \mid \wp \in \mathcal{P}_\mathcal{S}$ and $\lfloor G_\wp \rfloor_K$ is satisfiable$\}$ coincides with the set $\mathcal{G}^K_\mathcal{S} = \{(\lfloor G_\wp \rfloor_K, s(\wp), t(\wp)) \mid \wp$ is a non-null finite path of $\mathcal{S}$ and $\lfloor G_\wp \rfloor_K$ is satisfiable$\}$, and (iv) by Theorem 1, the set $\mathcal{G}^K_\mathcal{S}$ can be computed in time $O(|E(\mathcal{S})| \cdot |Q(\mathcal{S})|^2 \cdot (K+2)^{(2|\mathit{Var}|+|\mathit{Const}|)^2})$. Thus, Property 1 holds.

Proof of Property 2: Since $\lfloor \mathcal{S} \rfloor_K$ is complete as well, it suffices to show that $\mathcal{F}_{\mathcal{S},K} = \mathcal{F}_{\lfloor \mathcal{S} \rfloor_K, K}$. By the proof of Property 1, for each GCS $\mathcal{S}'$, $\mathcal{S}' \in \mathcal{F}_{\mathcal{S},K}$ iff $\mathcal{S}'$ is a simple GCS not belonging to $\mathcal{TC}$ which consists of two edges of the form $s(\wp) \stackrel{\lfloor G_\wp \rfloor_K}{\rightarrow} t(\wp)$ and $(\natural, s(\wp_0)) \stackrel{\lfloor G_{\wp_0} \rfloor_K}{\rightarrow} t(\wp_0)$ such that $\wp_0$ and $\wp$ are non-null finite paths of $\mathcal{S}$ and $s(\wp) = t(\wp) \in F$. For a path $\wp = q_0 \stackrel{G_0}{\rightarrow} q_1 \stackrel{G_1}{\rightarrow} \ldots$ of $\mathcal{S}$, we denote by $\lfloor \wp \rfloor_K$ the sequence $\wp = q_0 \stackrel{\lfloor G_0 \rfloor_K}{\rightarrow} q_1 \stackrel{\lfloor G_1 \rfloor_K}{\rightarrow} \ldots$. Note that $\lfloor \wp \rfloor_K$ is a path of $\lfloor \mathcal{S} \rfloor_K$.

$\mathcal{F}_{\mathcal{S},K} \subseteq \mathcal{F}_{\lfloor \mathcal{S} \rfloor_K, K}$: let $\mathcal{S}' \in \mathcal{F}_{\mathcal{S},K}$. Then, there are two non-null finite paths $\wp_0, \wp$ of $\mathcal{S}$ such that $s(\wp) = t(\wp) \in F$, $\mathcal{S}'$ is a simple GCS not in $\mathcal{TC}$, and $\mathcal{S}'$ consists of the edges $(\natural, s(\wp_0)) \stackrel{\lfloor G_{\wp_0} \rfloor_K}{\rightarrow} t(\wp_0)$ and $s(\wp) \stackrel{\lfloor G_\wp \rfloor_K}{\rightarrow} t(\wp)$. By definition of $\lfloor \mathcal{S} \rfloor_K$, $\lfloor \wp_0 \rfloor_K$ and $\lfloor \wp \rfloor_K$ are paths of $\lfloor \mathcal{S} \rfloor_K$. Moreover, by Proposition 4 and associativity of $\bullet$, $\lfloor G_{\wp_0} \rfloor_K = \lfloor G_{\lfloor \wp_0 \rfloor_K} \rfloor_K$ and $\lfloor G_\wp \rfloor_K = \lfloor G_{\lfloor \wp \rfloor_K} \rfloor_K$. It follows that $\mathcal{S}' \in \mathcal{F}_{\lfloor \mathcal{S} \rfloor_K, K}$.

$\mathcal{F}_{\lfloor \mathcal{S} \rfloor_K, K} \subseteq \mathcal{F}_{\mathcal{S},K}$: let $\mathcal{S}' \in \mathcal{F}_{\lfloor \mathcal{S} \rfloor_K, K}$. Then, there are two non-null finite paths $\wp_0, \wp$ of $\lfloor \mathcal{S} \rfloor_K$ such that $s(\wp) = t(\wp) \in F$, $\mathcal{S}'$ is a simple GCS not in $\mathcal{TC}$, and $\mathcal{S}'$ consists of the edges $(\natural, s(\wp_0)) \stackrel{\lfloor G_{\wp_0} \rfloor_K}{\rightarrow} t(\wp_0)$ and $s(\wp) \stackrel{\lfloor G_\wp \rfloor_K}{\rightarrow} t(\wp)$. By definition of $\lfloor \mathcal{S} \rfloor_K$, there are two non-null finite paths $\wp'_0, \wp'$ of $\mathcal{S}'$ such that $\lfloor \wp'_0 \rfloor_K = \wp_0$ and $\lfloor \wp' \rfloor_K = \wp$. Moreover, by Proposition 4 and associativity of $\bullet$, $\lfloor G_{\wp_0} \rfloor_K = \lfloor G_{\wp'_0} \rfloor_K$ and $\lfloor G_\wp \rfloor_K = \lfloor G_{\wp'} \rfloor_K$. It follows that $\mathcal{S}' \in \mathcal{F}_{\mathcal{S},K}$.

Proof of Property 3: We outline a NPSPACE algorithm to check whether for a given $q \in Q(\mathcal{S})$ and K-bounded MG G over *Var*, G is in the q-component of $\lfloor \sigma_F(\mathcal{S}) \rfloor_K$. Since NPSPACE=PSPACE (by Savitch's theorem), the result follows. At each step, the nondeterministic algorithm guesses two non-null finite paths $\wp_0$ and $\wp$ of $\mathcal{S}$, and compute the GCS $\mathcal{S}'$ having the edges $(\natural, s(\wp_0)) \stackrel{\lfloor G_{\wp_0} \rfloor_K}{\rightarrow} t(\wp_0)$ and $s(\wp) \stackrel{\lfloor G_\wp \rfloor_K}{\rightarrow} t(\wp)$. 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 $\mathcal{S}'$ corresponds to a simple GCS such that $\mathcal{S}' \notin \mathcal{TC}$ and $s(\wp) \in F$ (i.e., $\mathcal{S}' \in \mathcal{F}_{\mathcal{S},K}$), and $s(\wp_0) = q$ and $G \in \lfloor \mathcal{G}_{\mathcal{S}', in(\mathcal{S}')} \rfloor_K$ (note that by Theorem 3, this check can be done in polynomial time in the size of $\mathcal{S}'$), then the algorithm terminates with success. Otherwise, the algorithm chooses two edges from control points $t(\wp_0)$ and $t(\wp)$, say $t(\wp_0) \stackrel{G_0}{\rightarrow} q_0$

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-write 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_0 and q, and the procedure is repeated.

– $\mathcal{S}$ **is not complete:** we can assume that the theorem holds for complete GCS. By Proposition 10, one can compute a complete GCS $\mathcal{C}(\mathcal{S})$ such that $[\![\mathcal{C}(\mathcal{S})]\!] = [\![\mathcal{S}]\!]$. Thus, we set $\sigma_F(\mathcal{S})$ to $\sigma_F(\mathcal{C}(\mathcal{S}))$, and the first part of the theorem holds. Now, let us consider Properties 1–3.

Proof of Property 1: since $\lfloor\sigma_F(\mathcal{C}(\mathcal{S}))\rfloor_K$ can be computed in time $O(|E(\mathcal{C}(\mathcal{S}))| \cdot |Q(\mathcal{C}(\mathcal{S}))|^2 \cdot (K+2)^{(2|\mathit{Var}|+|\mathit{Const}|)^2})$, by Proposition 10, it follows that $\lfloor\sigma_F(\mathcal{S})\rfloor_K$ can be computed in time $O(|E(\mathcal{S})| \cdot |Q(\mathcal{S})|^2 \cdot (K+2)^{(2|Var|+|Const|)^2})$.

Proof of Property 2: note that $\lfloor\mathcal{S}\rfloor_K$ is not complete. Then, $\lfloor\sigma_F(\lfloor\mathcal{S}\rfloor_K)\rfloor_K = \lfloor\sigma_F(\mathcal{C}(\lfloor\mathcal{S}\rfloor_K))\rfloor_K$ (Property 2 holds for complete GCS) $= \lfloor\sigma_F(\lfloor\mathcal{C}(\lfloor\mathcal{S}\rfloor_K)\rfloor_K)\rfloor_K$ (by Proposition 10) $= \lfloor\sigma_F(\lfloor\mathcal{C}(\mathcal{S})\rfloor_K)\rfloor_K$ (Property 2 holds for complete GCS) $= \lfloor\sigma_F(\mathcal{C}(\mathcal{S}))\rfloor_K = \lfloor\sigma_F(\mathcal{S})\rfloor_K$. Thus, Property 2 holds.

Proof of Property 3: note that by the proof of Proposition 10, an edge of $\mathcal{C}(\mathcal{S})$ is of the form $q \xrightarrow{G\otimes G'} q'$, 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 (see Subsection 3.2), the result easily follows.

This concludes the proof of the theorem. □

D Proofs from Section 4

D.1 Proof of Theorem 6

Theorem 6. *Let $\mathcal{S}$ be a* GCS *over Var and φ be a* E–GCCTL$^*_{Unb}$ *formula over Var. Then, one can construct in polynomial-time an extension Var_{ext} of Var, a* GCS $\mathcal{S}_{ext}$ *over Var_{ext}, and a* E–GCCTL* *formula $f(\varphi)$ over Var_{ext} such that: for each state s of $\mathcal{S}$, one can compute in linear-time a state s_{ext} of $\mathcal{S}_{ext}$ so that*

$$(\mathcal{G}(\mathcal{S}), s) \models \varphi \text{ if and only if } (\mathcal{G}(\mathcal{S}_{ext}), s_{ext}) \models f(\varphi)$$

Proof. For each $x \in \mathit{Var}$, let x_r and x_{prop} be fresh copies of 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. Let Var_{ext} be the extension of *Var* with these new variables. $\mathcal{S}_{ext}$ is defined as follows:

– for each $y \in \mathit{Var}$ and $q \in Q(\mathcal{S})$, let q_y be a fresh copy of q. Then, $Q(\mathcal{S}_{ext}) = Q(\mathcal{S}) \cup \bigcup_{q\in Q(\mathcal{S})} \bigcup_{y\in \mathit{Var}} \{q_y\}$.

– $E(\mathcal{S}_{ext})$ 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 $\xi' = \bigwedge_{x\in \mathit{Var}}(x'_r = x_r) \wedge (x_{prop} > 0)$;
- the edges $q_z \xrightarrow{\xi\wedge\xi''} p$ and $q_z \xrightarrow{\xi\wedge\xi''} p_y$, where $\xi'' = (z'_r = z) \wedge (z_{prop} = 0) \wedge \bigwedge_{x\in \mathit{Var}\setminus\{z\}}(x'_r = x_r) \wedge (x_{prop} > 0)$.

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. The 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:

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

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).

Now, we prove the correctness of the construction. 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: either $q' = q$ and $\nu(x_{prop}) > 0$ for each $x \in \mathit{Var}$, or for some $y \in \mathit{Var}$, $q' = q_y$, $\nu(y_{prop}) = 0$, and $\nu(x_{prop}) > 0$ for each $x \in \mathit{Var} \setminus \{y\}$. An *extension* of an infinite run π of $\mathcal{S}$ is an infinite run π' of $\mathcal{S}_{ext}$ such that for each $i \geq 0$, state $\pi'(i)$ is an extension of $\pi(i)$. A *well-formed mapping* is a function $\Upsilon : N \rightarrow \mathit{Var}$ such that: $N \subseteq \mathbb{N}$ and for each $x \in \mathit{Var}$, $\Upsilon^{-1}(x)$ is infinite. Evidently, the following holds:

Claim 1: Let $\xi_{x_1}, \ldots, \xi_{x_n}$ be unboundedness constraints over variables in *Var* and π be an infinite run of $\mathcal{S}$. Then, $\xi_{x_1} \wedge \ldots \wedge \xi_{x_n}$ holds along π *iff* there is a well-formed mapping $\Upsilon : N \rightarrow \mathit{Var}$ such that for each $1 \leq i \leq n$, the following holds:

- 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 $next(h)$ exists).

Now, we prove the following.

Claim 2: Let $\xi_{x_1}, \ldots, \xi_{x_n}$ be unboundedness constraints over variables in *Var*, π be an infinite run of $\mathcal{S}$ starting from (q, ν), and (q', ν') be an extension of (q, ν). Then, $\xi_{x_1} \wedge \ldots \wedge \xi_{x_n}$ holds along π *iff* there is an extension π' of π starting from (q', ν') such that $(\mathcal{G}(\mathcal{S}_{ext}), \pi') \models f(\xi_{x_1}) \wedge \ldots \wedge f(\xi_{x_n})$.

Proof of Claim 2:
$\Longrightarrow$) Assume that $\xi_{x_1} \wedge \ldots \wedge \xi_{x_n}$ holds along $\pi = (q_0, \nu_0), (q_1, \nu_1), \ldots$, where $(q_0, \nu_0) = (q, \nu)$. By Claim 1, there is a well-formed mapping $\Upsilon : N \rightarrow \mathit{Var}$ such that for each $1 \leq i \leq n$, the following holds:

A. 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 $\Upsilon(k) = x_i$.

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

By construction, Property A above, and definition of $\mathcal{S}_{ext}$, it easily follows that π' is an extension of π starting from (q', ν') such that $(\mathcal{G}(\mathcal{S}_{ext}), \pi') \models f(\xi_{x_1}) \wedge \ldots \wedge f(\xi_{x_n})$.

$\Longleftarrow$) Assume that π' is an extension of π starting from (q', ν') such that $(\mathcal{G}(\mathcal{S}_{ext}), \pi') \models f(\xi_{x_1}) \wedge \ldots \wedge f(\xi_{x_n})$. Then, by definitions of $\mathcal{S}_{ext}$ and formulas $f(\xi_{x_1}), \ldots, f(\xi_{x_n})$, it easily follows the existence of a well-formed mapping $\Upsilon : N \rightarrow \mathit{Var}$ such that for each $1 \leq i \leq n$, Property A above holds. Thus, by Claim 1, the result follows. □

Now, by using Claim 1, we show the following, hence correctness of the construction follows (since φ is an existential formula, we can assume that $\varphi = E\psi_1$ for some path formula ψ_1).

Claim 3: Let $E\psi$ be a subformula of φ. Then, for each state s of $\mathcal{S}$ and extension s_{ext} of s, $(\mathcal{G}(\mathcal{S}), s) \models E\psi$ *if and only if* $(\mathcal{G}(\mathcal{S}_{ext}), s_{ext}) \models f(E\psi)$

Proof of Claim 3:
The proof is by structural induction on $E\psi$. We use the notion of maximal subformula as defined in Appendix D.3. By induction hypothesis, we can assume that the result holds for each maximal state subformulas of ψ of the form $E\psi'$.

$\Longrightarrow$) Assume that $(\mathcal{G}(\mathcal{S}), s) \models E\psi$. 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 the set of all the unboundedness constraints over *Var* that hold along π. By Claim 2, there is an extension π' of π starting from s_{ext} such that $(\mathcal{G}(\mathcal{S}_{ext}), \pi') \models f(\xi_{x_1}) \wedge \ldots \wedge f(\xi_{x_n})$. Since for each suffix $(\pi')^i$ of π', $(\mathcal{G}(\mathcal{S}_{ext}), (\pi')^i) \models f(\xi_{x_1}) \wedge \ldots \wedge f(\xi_{x_n})$ 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 $i \geq 0$, $(\mathcal{G}(\mathcal{S}), \pi^i) \models \psi'$ implies $(\mathcal{G}(\mathcal{S}_{ext}), (\pi')^i) \models f(\psi')$. Hence, the result follows.

$\Longleftarrow$) Assume that $(\mathcal{G}(\mathcal{S}_{ext}), s_{ext}) \models f(E\psi)$. 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 the set of all the unboundedness constraints over *Var* such that $(\mathcal{G}(\mathcal{S}_{ext}), \pi') \models f(\xi_{x_1}) \wedge \ldots \wedge f(\xi_{x_n})$. By Claim 2, $\xi_{x_1}, \ldots, \xi_{x_n}$ hold along π. Since for each suffix $(\pi')^i$ of π', $(\mathcal{G}(\mathcal{S}_{ext}), (\pi')^i) \models f(\xi_{x_1}) \wedge \ldots \wedge f(\xi_{x_n})$ 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 $i \geq 0$, $(\mathcal{G}(\mathcal{S}_{ext}), (\pi')^i) \models f(\psi')$ implies $(\mathcal{G}(\mathcal{S}), \pi^i) \models \psi'$. Hence, the result follows. □

D.2 Undecidability of model checking GCS against A–GCCTL*

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* ∪ *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 ∃GC constraint over *Var* ∪ *Var*′ and *Const*. Now, we observe that positive boolean combinations of negations of transitional GC allow to express the successor relation. For example, $x' = x + 1$ is equivalent to $\neg(x' - x \geq 2) \wedge \neg(x - x' \geq 0)$, and $x = 0$ is equivalent to $\neg(x \geq 1) \wedge \neg(-x \geq 1)$. 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 DCMS against A–GCCTL* follows.

D.3 Proof of Theorem 7

In order to prove Theorem 7, we need additional definitions. Fix a *path* E–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 path quantifier E.

The *closure* of ψ, denoted by $cl(\psi)$, is the set containing all the *maximal subformulas* of ψ, $\mathsf{O}(\psi_1 \mathsf{U} \psi_2)$ for each maximal subformula $\psi_1 \mathsf{U} \psi_2$ of ψ, and $\mathsf{O}(\Box \psi_1)$ for each maximal subformula $\Box \psi_1$ of ψ. Note that $\psi \in cl(\psi)$. An (LTL-)*atom* of ψ is a set $A \subseteq cl(\psi)$ satisfying the following properties:

- for $\psi_1 \vee \psi_2 \in cl(\psi)$, $\psi_1 \vee \psi_2 \in A$ iff either $\psi_1 \in A$ or $\psi_2 \in A$;
- for $\psi_1 \wedge \psi_2 \in cl(\psi)$, $\psi_1 \wedge \psi_2 \in A$ iff $\psi_1 \in A$ and $\psi_2 \in A$;
- for $\psi_1 \mathsf{U} \psi_2 \in cl(\psi)$, $\psi_1 \mathsf{U} \psi_2 \in A$ iff either $\psi_2 \in A$ or $\{\psi_1, \mathsf{O}(\psi_1 \mathsf{U} \psi_2)\} \subseteq A$;
- for $\Box \psi_1 \in cl(\psi)$, $\Box \psi_1 \in A$ iff $\{\psi_1, \mathsf{O} \Box \psi_1\} \subseteq A$.

Let $Atoms(\psi)$ be the set of atoms of ψ. Note that the size of $Atoms(\psi)$ is $O(2^{|\psi|})$. When an until-formula $\psi_1 \mathsf{U} \psi_2$ is asserted at a state along a run of the given GCS, we must make sure that the liveness requirement ψ_2 is eventually satisfied. This is done (as for LTL) using a generalized Büchi condition having a component for each until formula in $cl(\psi)$. Formally, we denote by $\mathcal{F}(\psi)$ the family of subsets of $Atoms(\psi)$ defined as: $\mathcal{F}(\psi) = \{F_{\psi_1 \mathsf{U} \psi_2}\}_{\psi_1 \mathsf{U} \psi_2 \in cl(\psi)}$, where for each until formula $\psi_1 \mathsf{U} \psi_2 \in cl(\psi)$, $F_{\psi_1 \mathsf{U} \psi_2}$ contains all and only the atoms A such that either $\psi_2 \in A$ or $\psi_1 \mathsf{U} \psi_2 \notin A$. Now, we give a detailed proof of Theorem 7.

Theorem 7. *Given a* GCS $\mathcal{S}$ *and a* E–GCCTL* *formula* φ, $[\![\varphi]\!]_{\mathcal{S}}$ *is* MG *representable and one can construct a* MG *representation of* $[\![\varphi]\!]_{\mathcal{S}}$*, written* $\pi(\mathcal{S}, \varphi)$*, such that: (1)* $\lfloor \pi(\mathcal{S}, \varphi) \rfloor_K$ *can be built in time* $O(|E(\mathcal{S})| \cdot |Q(\mathcal{S})|^2 \cdot 2^{O(|\varphi|)} \cdot (K+2)^{O((2|Var|+|Const|)^2)})$*, and (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 space polynomial in the sizes of* $\mathcal{S}$ *and* φ*.*

Proof. Fix a GCS $\mathcal{S}$. For a (state) E–GCCTL* formula φ, we construct $\pi(\mathcal{S}, \varphi)$ and prove Properties 1–2 by induction on the structure of φ. Note that by Proposition 1(3) and Proposition 2(1) (see also [25]), GC are closed under existential quantification and quantification elimination can be done in polynomial time. Thus, w.l.o.g. we can assume that each $\exists$GC constraint occurring in φ is a disjunction of transitional GC. If φ is or $\top$ or a conjunction or a disjunction of E–GCCTL* formulas, then the result easily follows from the induction hypothesis, Proposition 2, and Proposition 7 in Appendix A.2. The remaining case is when $\varphi = E\,\psi$ for some path formula ψ. Let X (resp., Y) be the set of state formulas (resp., atomic formulas) in $cl(\psi)$. By the induction hypothesis, we can assume that the result holds for each formula in X. We construct two GCS $\mathcal{S}_\varphi$ and $\mathcal{S}_\varphi^{bd}$ with set of control points $Q(\mathcal{S}) \times Atoms(\psi) \times \{0, \ldots, |\mathcal{F}(\psi)|\}$ and a subset $F \subseteq Q(\mathcal{S}_\varphi)$ such that:

Claim 1: $(q, \nu) \in [\![\varphi]\!]_{\mathcal{S}}$ *iff* $((q, A, 0), \nu) \in \mathit{Inf}_{\mathcal{S}_\varphi, F}$ for some atom A such that $\psi \in A$.

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

$\mathcal{S}_{\varphi}$, $\mathcal{S}^{bd}_{\varphi}$, and F are constructed as follows, where $\mathcal{F}(\psi)=\{F_1,\ldots,F_m\}$:

1. $Q(\mathcal{S}_{\varphi})=Q(\mathcal{S}^{bd}_{\varphi})=Q(\mathcal{S})\times Atoms(\psi)\times\{0,\ldots,m\}$. A control point of $Q(\mathcal{S}_{\varphi})$ and $Q(\mathcal{S}^{bd}_{\varphi})$ is a triple (q,A,i), where q is a control point of $\mathcal{S}$, A is an atom of ψ, which intuitively represents the set of maximal subformulas of ψ that hold at the current state (with control point q) of the current infinite run of $\mathcal{S}$, and i is a finite counter used to check the fulfillment of the generalized Büchi condition $\mathcal{F}(\psi)$.
2. $(q,A,i)\xrightarrow{G}(q',A',j)$ is an edge of $\mathcal{S}_{\varphi}$ (resp., $\mathcal{S}^{bd}_{\varphi}$) iff the following holds:
   2.1. for all $\mathsf{O}\psi'\in cl(\psi)$, $\mathsf{O}\psi'\in A$ iff $\psi'\in A'$ (i.e., the next-requirements in A are met in A');
   2.2. $j=i$ if $i<m$ and $A'\notin F_{i+1}$, and $j=(i+1)\ mod\ (m+1)$ otherwise;
   2.3. let $A\cap X=\{\theta_1,\ldots,\theta_k\}$ and $A\cap Y=\{\xi_1,\ldots,\xi_h\}$. Then, there are an edge of $\mathcal{S}$ of the form $q\xrightarrow{G_0}q'$ and for each $1\leq p\leq k$, a MG G_p belonging to the q-component of $\pi(\mathcal{S},\theta_p)$ (resp., the q-component of $\lfloor\pi(\mathcal{S},\theta_p)\rfloor_K$) such that
$$G=G_0\otimes G_1\otimes\ldots\otimes G_k\otimes G(\xi_1)\otimes\ldots\otimes G(\xi_h)$$
$$(resp., G=\lfloor\lfloor G_0\rfloor_K\otimes G_1\otimes\ldots\otimes G_k\otimes\lfloor G(\xi_1)\rfloor_K\otimes\ldots\otimes\lfloor G(\xi_h)\rfloor_K\rfloor_K)$$
3. $F=\{(q,A,m)\in Q(\mathcal{S}_{\varphi})\}$.

Now, by using Claims 1 and 2 (which are proved below), we construct a MG representation $\pi(\mathcal{S},\varphi)$ of $[\![\varphi]\!]_{\mathcal{S}}$ and show that it satisfies Properties 1 and 2 in the statement of the theorem. Let $\sigma_F(\mathcal{S}_{\varphi})$ be the *computable* MG representation of $\mathit{Inf}_{\mathcal{S}_{\varphi},F}$ satisfying the statement of Theorem 5. Then, for each $q\in Q(\mathcal{S})$, the q-component of $\pi(\mathcal{S},\varphi)$ is the union of the $(q,A,0)$-components of $\sigma_F(\mathcal{S}_{\varphi})$ such that $\psi\in A$. 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 5, $\lfloor\sigma_F(\mathcal{S}_{\varphi})\rfloor_K=\lfloor\sigma_F(\mathcal{S}^{bd}_{\varphi})\rfloor_K$. 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 $|E(\mathcal{S})|\cdot 2^{O(|\varphi|)}\cdot(K+2)^{(2|\mathit{Var}|+|\mathit{Const}|)^2}$ (the MG of $\mathcal{S}^{bd}_{\varphi}$ are K-bounded), by Property 1 of Theorem 5, and Claim 2, Property 1 follows. Now, let us consider Property 2. By the induction hypothesis, we can assume that Property 2 holds for each formula in X. Moreover, by the above considerations, it suffices to show that given a K-bounded MG G over *Var* and $q\in Q(\mathcal{S}^{bd}_{\varphi})$, checking whether G is in the q-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 5, 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 5, the nondeterministic algorithm that checks whether G is in the q-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 $s(e_0)$-component (resp., $s(e)$-component) of $\lfloor \pi(\mathcal{S}, \theta) \rfloor_K$, where $\theta \in X$. 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 check 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).

Now, 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 $\theta \in X$. Hence, the nondeterministic algorithm runs in space polynomial in the sizes of $\mathcal{S}$ and φ. Since NPSPACE=PSPACE , Property 2 follows.

It remains to prove Claims 1 and 2. Claim 2 easily follows from construction, the induction hypothesis, and Proposition 7 in Appendix A.2. Now, we prove Claim 1.

Proof of Claim 1: $\Longrightarrow$) Let $(q, \nu) \in [\![\varphi]\!]_{\mathcal{S}}$ (recall that $\varphi = E\,\psi$). We need to prove that $((q, A, 0), \nu) \in \mathit{Inf}_{S_\varphi, F}$ for some $A \in \mathit{Atoms}(\psi)$ such that $\psi \in A$. By hypothesis there is an infinite run π of $\mathcal{S}$ of the form $\pi = (q_0, \nu_0), (q_1, \nu_1), \ldots$ such that $(q_0, \nu_0) = (q, \nu)$ and $(\mathcal{G}(\mathcal{S}), \pi) \models \psi$. For each $i \geq 0$, we denote by A_i the set $\{\psi' \in \mathit{cl}(\psi) \mid (\mathcal{G}(\mathcal{S}), \pi^i) \models \psi'\}$. Note that A_i is an atom of ψ for each $i \geq 0$, and $\psi \in A_0$. Moreover, let $h_0, h_1, \ldots$ be the infinite sequence of integers in $\{0, \ldots, m\}$ defined as follows: $h_0 = 0$, and for all $i \geq 0$, $h_{i+1} = h_i$ if $h_i < m$ and $A_{i+1} \notin F_{h_i+1}$, and $h_{i+1} = (h_i + 1)\ mod\ (m + 1)$ otherwise. Let us consider the infinite sequence of states of $\mathcal{S}_\varphi$ given by $\pi_\varphi = ((q_0, A_0, h_0), \nu_0), ((q_1, A_1, h_1), \nu_1), \ldots$. We show that π_φ is an infinite run of $\mathcal{S}_\varphi$ such that for infinitely many $i \geq 0$, $(q_i, A_i, h_i) \in F$, hence the result follows (recall that $h_0 = 0$ and $\psi \in A_0$).

By the semantics of the until operator it follows that for each until formula $\psi_1 \mathsf{U} \psi_2 \in \mathit{cl}(\psi)$, the set $\{i \geq 0 \mid \text{either } \psi_2 \in A_i \text{ or } \psi_1 \mathsf{U} \psi_2 \notin A_i\}$ is infinite. Therefore, by definition of the sets $\mathcal{F}(\psi)$ and F, it follows that π_φ contains infinite occurrences of states whose corresponding control points belong to F. It remains to show that for each $i \geq 0$, $((q_i, A_i, h_i), \nu_i) \rightarrow ((q_{i+1}, A_{i+1}, h_{i+1}), \nu_{i+1})$ is an edge of $[\![\mathcal{S}_\varphi]\!]$. Let us consider the infinite run π and fix $i \geq 0$. Then, there is an edge of $\mathcal{S}$ of the form $q_i \xrightarrow{G^i_0} q_{i+1}$ such that $\nu_i \oplus \nu_{i+1} \in \mathit{Sat}(G^i_0)$. Let $A_i \cap X = \{\theta^i_1, \ldots, \theta^i_{k_i}\}$ and $A_i \cap Y = \{\xi^i_1, \ldots, \xi^i_{l_i}\}$. By definition of A_i, $(\mathcal{G}(\mathcal{S}), (q_i, \nu_i)) \models \theta^i_p$ for each $1 \leq p \leq k_i$, and $\nu_i \oplus \nu_{i+1} \in \mathit{Sat}(G(\xi^i_p))$ for each $1 \leq p \leq l_i$. Hence, for each $1 \leq p \leq k_i$, there is a MG G^i_p such that G^i_p belongs to the q_i-component of $\pi(\mathcal{S}, \theta^i_p)$ and $\nu_i \in \mathit{Sat}(G^i_p)$. Let $G^i = G^i_0 \otimes G^i_1 \otimes \ldots \otimes G^i_{k_i} \otimes G(\xi^i_1) \otimes \ldots \otimes G(\xi^i_{l_i})$. By definition of $\mathcal{S}_\varphi$, it follows that $(q_i, A_i, h_i) \xrightarrow{G^i} (q_{i+1}, A_{i+1}, h_{i+1})$ is an edge of $\mathcal{S}_\varphi$. Since $\nu_i \oplus \nu_{i+1} \in \mathit{Sat}(G^i)$, the result follows.

$\Longleftarrow$) Let $((q, A, 0), \nu) \in \mathit{Inf}_{\mathcal{S}_\varphi, F}$ such that $\psi \in A$. We need to show that $(q, \nu) \in [\![\varphi]\!]_{\mathcal{S}}$ (recall that $\varphi = E\,\psi$). By hypothesis there is an infinite run π_φ of $\mathcal{S}_\varphi$ of the form $\pi_\varphi =$

$((q_0, A_0, h_0), \nu_0)$, $((q_1, A_1, h_1), \nu_1), \ldots$ such that $((q_0, A_0, h_0), \nu_0) = ((q, A, 0), \nu)$ and for infinitely many $i \geq 0$, $(q_i, A_i, h_i) \in F$. For each $i \geq 0$, let $A_i \cap X = \{\theta^i_1, \ldots, \theta^i_{k_i}\}$ and $A_i \cap Y = \{\xi^i_1, \ldots, \xi^i_{l_i}\}$. By definition of $\mathcal{S}_\varphi$, for each $i \geq 0$, there is an edge of $\mathcal{S}$ of the form $q_i \xrightarrow{G^i_0} q_{i+1}$ and for each $1 \leq p \leq k_i$, there is a MG G^i_p belonging to the q_i-component of $\pi(\mathcal{S}, \theta^i_p)$ such that $\nu_i \oplus \nu_{i+1} \in \mathit{Sat}(G^i_0)$ and $\nu_i \in \mathit{Sat}(G^i_p)$ for each $1 \leq p \leq k_i$. Moreover, $\nu_i \oplus \nu_{i+1} \in \mathit{Sat}(G(\xi^i_p))$ for each $1 \leq p \leq l_i$. In particular, $\pi = (q_0, \nu_0), (q_1, \nu_1), \ldots$ is an infinite run of $\mathcal{S}$ starting from (q, ν). Since $\psi \in A_0 = A$, it suffices to show that for all $i \geq 0$ and $\psi' \in A_i$, $(\mathcal{G}(\mathcal{S}), \pi^i) \models \psi'$. We prove this by structural induction on ψ'. The induction step can be proved in the standard way. Therefore, we analyze only the cases in which either ψ' is an atomic formula (i.e., $\psi' \in Y$) or ψ' is a state formula (i.e, $\psi' \in X$). For the first case, assume that $\psi' \in Y \cap A_i$. Then, $\psi' = \xi^i_p$ for some $1 \leq p \leq l_i$. Since $\nu_i \oplus \nu_{i+1} \in \mathit{Sat}(G(\xi^i_p))$, we obtain that $(\mathcal{G}(\mathcal{S}), \pi^i) \models \psi'$. For the second case, assume that $\psi' \in X \cap A_i$. Then, $\psi' = \theta^i_p$ for some $1 \leq p \leq k_i$. Hence, $\nu_i \in \mathit{Sat}(G^i_p)$, where G^i_p belongs to the q_i-component of $\pi(\mathcal{S}, \theta^i_p)$. Since $\pi(\mathcal{S}, \theta^i_p)$ is a MG representation of $[\![\theta^i_p]\!]_{\mathcal{S}}$, we obtain that $(\mathcal{G}(\mathcal{S}), \pi^i) \models \psi'$, which concludes. □

D.4 Proof of Theorem 8

Theorem 8. *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., [21]). 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 7, this last problem is in PSPACE). Fix a GCS $\mathcal{S}$, a state (q_0, ν_0) of $\mathcal{S}$, and a E–GCCTL* formula φ. W.l.o.g. we assume that φ does not contain occurrences of $\top$. Moreover, we can assume that $\nu_0(x) \in \mathit{Const}$ for each $x \in \mathit{Var}$ (otherwise, we extend *Const* by including the integers $\nu_0(x)$ with $x \in \mathit{Var}$). Let $G_=$ be the transitional MG corresponding to the GC given by $\bigwedge_{x \in \mathit{Var}} x = \nu_0(x)$, 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 $q'_0 \xrightarrow{G \otimes G_=} q$. 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:

1. 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.
2. 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*: 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 of the form $q \xrightarrow{G} q$ such that G is equivalent to $true$. Evidently, given a 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 a A–GCCTL* formula, and let $E\widetilde{\varphi}$ 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 $E\widetilde{\varphi}$ is satisfiable. Hence, the result follows. □