Strong termination for gap-order constraint abstractions of counter systems

Laura Bozzelli

[1]Technical University of Madrid (UPM), Spain

Int. Conference on Language and Automata Theory and Applications, 2012

Outline

Outline

Abstractions of counter systems

Counter systems: a complete computational formalism used to model broadcast protocols, programs with pointer variables, etc.
Abstractions of counter systems:

- Restrictions. Petri nets, reversal-bounded counter machines, flat counter systems, etc.
- Genuine abstractions. Counting operations $\rightsquigarrow$ non-functional Presburger fragments between the variables of current state and variables of next state (infinitely-branching formalisms).

Abstractions of counter systems

Counter systems: a complete computational formalism used to model broadcast protocols, programs with pointer variables, etc.
Abstractions of counter systems:

- Restrictions. Petri nets, reversal-bounded counter machines, flat counter systems, etc.
- Genuine abstractions. Counting operations $\rightsquigarrow$ non-functional Presburger fragments between the variables of current state and variables of next state (infinitely-branching formalisms).
  - Monotonicity Constraint Systems (MCS) [**Ben Amram 2010**], Constraint Automata [**Demri et al. 2007**], and Integral Relation Automata (IRA) [**Cerans 1994**]. Monotonicity constraints $u < v$ or $u \leq v$ with u, v variables or integer constants.
  - Richer classes of constraints. Difference bound constraints [**Comon et al. 1998**] and octagon relations [**Bozga et al. 2009**], where the transitive closure of a single constraint is Presburger definable.

Gap-order Constraint Systems (GCS)

An infinitely-branching abstract model of counter machines [**Bozzelli et al. VMCAI'12**]

- strictly extends Monotonicity Constraint Systems, IRA and Constraint Automata.
- gap-order constraints [**Revesz 1993**] between the variables of the source and target states.
  - Closed under existential quantification
  - but not under negation.

Outline

Gap-order constraints

Let *Const* $\subseteq \mathbb{Z}$ s.t. $0 \in$ *Const* be a finite set of integer constants and V be a finite set of variables.

Gap-order constraints (GC)

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

with $u, v \in V \cup Const$, $k \in \mathbb{N}$, and $x \in V$.

- Atomic GC of the form $u - v \geq k$ (k the lower bound).
- Write $\nu \models \eta$ when valuation $\nu : V \to \mathbb{Z}$ satisfies the GC η.
- $Sat(\eta) = \{\nu : V \to \mathbb{Z} \mid \nu \models \eta\}$ (the set of solutions of η).

Gap-order constraints

Let $Const \subseteq \mathbb{Z}$ s.t. $0 \in Const$ be a finite set of integer constants and V be a finite set of variables.

Gap-order constraints (GC)

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

with $u, v \in V \cup Const$, $k \in \mathbb{N}$, and $x \in V$.

- Atomic GC of the form $u - v \geq k$ (k the lower bound).
- Write $\nu \models \eta$ when valuation $\nu : V \to \mathbb{Z}$ satisfies the GC η.
- $Sat(\eta) = \{\nu : V \to \mathbb{Z} \,|\, \nu \models \eta\}$ (the set of solutions of η).

Conjunctive GC (cGC) [Revesz'93]

Conjunction ξ of atomic GCs.

Expressiveness of GC

- Lower and upper bounds on the values of individual variables, and equality, and gaps (minimal differences) between values of pairs of variables.
- Large class of protocols, where the behavior depends on the relative ordering of values among variables, rather than the actual values of these variables.
- Applications:
  - Constraint query languages (constraint Datalog) for deductive databases [**Revesz 1993**].
  - Safety property analysis for parameterized systems [**Abdulla et al. 2009**].
  - State invariants in counter systems [**Fribourg et al. 1996**].

Gap-order Constraint Systems

- Fix $Var = \{x, y, \ldots\}$ a finite set of variables and a primed copy $Var' = \{x', y', \ldots\}$.
- A transitional cGC is a cGC over $Var \cup Var'$.

Gap-order Constraint Systems

- Fix $Var = \{x, y, \ldots\}$ a finite set of variables and a primed copy $Var' = \{x', y', \ldots\}$.
- A transitional cGC is a cGC over $Var \cup Var'$.

Definition

A Gap-order Constraint Systems (GCS) is a finite directed labeled graph $\mathcal{S}$ with

- the set of vertices $Q(\mathcal{S})$, called control points,
- each edge labeled by a transitional cGC.

Interpretation of GCS

The composition of two valuations ν and ν' is

$$\nu \oplus \nu' : Var \cup Var' \rightarrow \mathbb{Z}$$
$$(\nu \oplus \nu')(x) = \nu(x) \text{ and } (\nu \oplus \nu')(x') = \nu'(x')$$

A GCS $\mathcal{S}$ denotes a (infinite) directed graph $[\![\mathcal{S}]\!]$ where

- vertices (q, ν) with $q \in Q(\mathcal{S})$ and ν valuation over Var, called states;
- edge $(q, \nu) \rightarrow (q', \nu')$ whenever $q \xrightarrow{\xi} q'$ in $\mathcal{S}$ and $\nu \oplus \nu' \in Sat(\xi)$, for some ξ.

Interpretation of GCS

The composition of two valuations ν and ν' is

$$\nu \oplus \nu' : Var \cup Var' \to \mathbb{Z}$$
$$(\nu \oplus \nu')(x) = \nu(x) \text{ and } (\nu \oplus \nu')(x') = \nu'(x')$$

A GCS $\mathcal{S}$ denotes a (infinite) directed graph $[\![\mathcal{S}]\!]$ where

- vertices (q, ν) with $q \in Q(\mathcal{S})$ and ν valuation over Var, called states;
- edge $(q, \nu) \to (q', \nu')$ whenever $q \overset{\xi}{\to} q'$ in $\mathcal{S}$ and $\nu \oplus \nu' \in Sat(\xi)$, for some ξ.

A run of $\mathcal{S}$ is $\pi = (q_0, \nu_0) \to (q_1, \nu_1) \to (q_2, \nu_2), \ldots$, an instance of a path $q_0 \overset{\xi_0}{\to} q_1 \overset{\xi_1}{\to} q_2, \ldots$ of $\mathcal{S}$, *i.e.* $\nu_i \oplus \nu_{i+1} \in Sat(\xi_i), \forall i$.

Remarks

Extending the constraints by allowing negation, or, equivalently, atomic constraints of the form $u - v \geq -k$, with $k \in \mathbb{N}$, enables one to emulate Minsky counter machines with GCS.

Strong Termination

- State s of GCS $\mathcal{S}$ is terminating if there is no infinite run from s.
- State s of GCS $\mathcal{S}$ is strongly terminating if the set of lengths of finite runs from s is finite.

Strong Termination

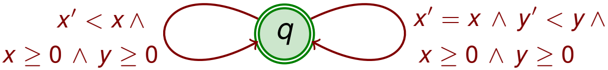
- State s of GCS $\mathcal{S}$ is terminating if there is no infinite run from s.
- State s of GCS $\mathcal{S}$ is strongly terminating if the set of lengths of finite runs from s is finite.

$$\text{Strong Termination} \Rightarrow \text{Termination}$$

Since GCS are infinitely-branching:

$$\text{Termination} \not\Rightarrow \text{Strong Termination}$$

GCS example



- there is no infinite run since the pair (x, y) decreases strictly w.r.t. the lexicographic order on $\mathbb{N} \times \mathbb{N}$.
- for each state (q, ν) with $\nu(x) > 0$ and $\nu(y) \geq 0$, the lengths of the runs from (q, ν) are unbounded.

Outline

1. **Introduction**
   - Abstractions of counter systems
   - Gap-order constraint systems
   - Investigated Problems
2. **Preliminary Results**
   - Composition of transitional cGC
   - Approximation scheme
   - Constructive results on reachability relation in GCS
3. **Strong Termination Problem**
   - Main steps for solving the strong termination problem
   - Strong Termination for simple GCS
   - Strong termination for unrestricted GCS

Investigated Problems

The Strong Termination Problem

- Input: A GCS $\mathcal{S}$
- Answer: “Does it hold that all the states are strongly terminating?”

Variant for a designated state:

- Input: A GCS $\mathcal{S}$ and a state s
- Answer: “Is s strongly terminating?”

Strong termination analysis: basic tool in running-time analysis (based on GCS abstraction) of infinitely-branching systems (e.g., concurrent open systems).

Investigated Problems

The Strong Termination Problem

- Input: A GCS $\mathcal{S}$
- Answer: “Does it hold that all the states are strongly terminating?”

Variant for a designated state:

- Input: A GCS $\mathcal{S}$ and a state s
- Answer: “Is s strongly terminating?”

Strong termination analysis: basic tool in running-time analysis (based on GCS abstraction) of infinitely-branching systems (e.g., concurrent open systems).

Remark

Usual Termination of GCS is known to be decidable and PSPACE-complete [**Bozzelli et al. VMCAI’12**].

Outline

Composing transitional cGC's

The composition of two transitional cGC's ξ and ξ' is the transitional cGC $\xi \bullet \xi'$ satisfying

$$\nu \oplus \nu' \in \mathit{Sat}(\xi \bullet \xi')$$
iff
$$\nu \oplus \nu'' \in \mathit{Sat}(\xi) \text{ and } \nu'' \oplus \nu' \in \mathit{Sat}(\xi'), \text{ for some } \nu''$$

(Composition is associative and computable in polynomial time)

Composing transitional cGC's

The composition of two transitional cGC's ξ and ξ' is the transitional cGC $\xi \bullet \xi'$ satisfying

$$\nu \oplus \nu' \in \mathit{Sat}(\xi \bullet \xi')$$
iff
$$\nu \oplus \nu'' \in \mathit{Sat}(\xi) \text{ and } \nu'' \oplus \nu' \in \mathit{Sat}(\xi'), \text{ for some } \nu''$$

(Composition is associative and computable in polynomial time)

From $\wp = q_1 \xrightarrow{\xi_1} q_2 \ldots \xrightarrow{\xi_n} q_{n+1}$ in $\mathcal{S}$, build $\xi_\wp := \xi_1 \bullet \cdots \bullet \xi_n$.

$\xi_\wp$ characterizes reachability along $\wp$

$$\nu \oplus \nu' \in \mathit{Sat}(\xi_\wp)$$
iff
$$\nu \rightsquigarrow_\wp \nu'$$
i.e. there is an instance of the path $\wp$ from (q_1, ν) to (q_{n+1}, ν')

Outline

Finite abstraction of cGC's [Bozzelli et al. VMCAI'12]

Finite abstraction of cGC's [Bozzelli et al. VMCAI'12]

Let $K \in \mathbb{N}$.

- A cGC is *K*-bounded if the lower bounds in the atomic constraints are bounded by K.
- The *K*-bounded approximation $\lfloor \xi \rfloor_K$ of a cGC ξ is the K-bounded cGC obtained by replacing each $u - v \geq h$ by $u - v \geq min\{h, K\}$.
- The *K*-bounded approximation $\lfloor \mathcal{S} \rfloor_K$ of a GCS $\mathcal{S}$ is obtained by replacing each cGC ξ of $\mathcal{S}$ by $\lfloor \xi \rfloor_K$.

Finite abstraction of cGC's [Bozzelli et al. VMCAI'12]

Let $K \in \mathbb{N}$.

- A cGC is K-bounded if the lower bounds in the atomic constraints are bounded by K.
- The K-bounded approximation $\lfloor \xi \rfloor_K$ of a cGC ξ is the K-bounded cGC obtained by replacing each $u - v \geq h$ by $u - v \geq min\{h, K\}$.
- The K-bounded approximation $\lfloor \mathcal{S} \rfloor_K$ of a GCS $\mathcal{S}$ is obtained by replacing each cGC ξ of $\mathcal{S}$ by $\lfloor \xi \rfloor_K$.

Let K stand for $\max(\{|c_1 - c_2| + 1 \mid c_1, c_2 \in Const\})$

The number of K-bounded transitional cGC is finite and is bounded by $O((K + 2)^{(2|Var| + |Const|)^2})$.

Properties of K-bounded abstraction

- The approximation scheme is sound and complete:

  ξ is satisfiable iff $\lfloor \xi \rfloor_K$ is satisfiable

- Composition: $\lfloor \xi \bullet \xi' \rfloor_K = \lfloor \lfloor \xi \rfloor_K \bullet \lfloor \xi' \rfloor_K \rfloor_K$

Outline

Constructive results on reachability relation in GCS

Reachability in GCS for fixed source and target control points is effectively GC definable.

Theorem (Finite sampling of paths in GCS)

For a GCS $\mathcal{S}$, one can compute the set of sample paths of $\mathcal{S}$, $\mathcal{P}_{\mathcal{S}}$, such that:

- *$\mathcal{P}_{\mathcal{S}}$ is a finite set of non-null finite paths of $\mathcal{S}$,*
- *for each non-null finite path $\wp'$ from q to q′, there is $\wp \in \mathcal{P}_{\mathcal{S}}$ from q to q′ with $\lfloor \xi_{\wp'} \rfloor_K = \lfloor \xi_{\wp} \rfloor_K$, and $\rightsquigarrow_{\wp'}$ implies $\rightsquigarrow_{\wp}$*

Constructive results on reachability relation in GCS

Reachability in GCS for fixed source and target control points is effectively GC definable.

Theorem (Finite sampling of paths in GCS)

For a GCS $\mathcal{S}$, one can compute the set of sample paths of $\mathcal{S}$, $\mathcal{P}_{\mathcal{S}}$, such that:

- *$\mathcal{P}_{\mathcal{S}}$ is a finite set of non-null finite paths of $\mathcal{S}$,*
- *for each non-null finite path $\wp'$ from q to q', there is $\wp \in \mathcal{P}_{\mathcal{S}}$ from q to q' with $\lfloor \xi_{\wp'} \rfloor_K = \lfloor \xi_{\wp} \rfloor_K$, and $\rightsquigarrow_{\wp'}$ implies $\rightsquigarrow_{\wp}$*

No known elementary upper bound on the cardinality of $\mathcal{P}_{\mathcal{S}}$.

Outline

1. Introduction
   - Abstractions of counter systems
   - Gap-order constraint systems
   - Investigated Problems
2. Preliminary Results
   - Composition of transitional cGC
   - Approximation scheme
   - Constructive results on reachability relation in GCS
3. Strong Termination Problem
   - Main steps for solving the strong termination problem
   - Strong Termination for simple GCS
   - Strong termination for unrestricted GCS

Main steps

1. Solved for simple GCS.

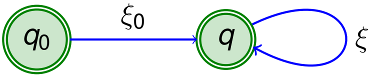
2. For an arbitrary GCS $\mathcal{S}$, construct a finite family $\mathcal{F}$ of simple GCS such that the set of strongly terminating states of $\mathcal{S}$ is the union of the sets of strongly terminating states of components in $\mathcal{F}$.

3. Compute separately and in exponential time the K-bounded abstractions of simple GCS in $\mathcal{F}$ which are sound and complete w.r.t. the existence of states which are not strongly terminating.

(we are not aware of any upper bound on the size of $\mathcal{F}$)

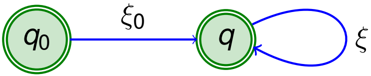
Outline

Simple GCS



q_0: initial control point

Simple GCS



q_0: initial control point

- $\xi_0 \bullet \xi$ is satisfiable.
- ξ_0 and ξ are complete, *i.e.* they induce a total ordering on $Var \cup Const$ (resp., $Var' \cup Const$).
- ξ is (weakly) idempotent, *i.e.* $\lfloor \xi \bullet \xi \rfloor_K = \lfloor \xi \rfloor_K$.

Upper and lower variables

For a transitional cGC ξ and $X = Var$ (resp., $X = Var'$), let

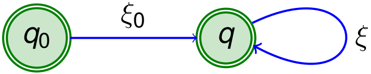
$$\mathit{Lower}(\xi, X) := \{\mathsf{L} \in X \mid \xi \models \mathsf{L} < \mathit{MIN}(\mathit{Const})\}$$
$$\mathit{Upper}(\xi, X) := \{\mathsf{U} \in X \mid \xi \models \mathsf{U} > \mathit{MAX}(\mathit{Const})\}$$

Upper and lower variables

For a transitional cGC ξ and $X = Var$ (resp., $X = Var'$), let

$$Lower(\xi, X) := \{\mathsf{L} \in X \mid \xi \models \mathsf{L} < MIN(Const)\}$$
$$Upper(\xi, X) := \{\mathsf{U} \in X \mid \xi \models \mathsf{U} > MAX(Const)\}$$

Fix a simple GCS $\mathcal{S}$:



q_0: initial control point

ξ is balanced: for all $x, y \in Var$,

$$\xi \models x \leq y < MIN(Const) \Leftrightarrow \xi \models x' \leq y' < MIN(Const)$$

$$\xi \models MAX(Const) < x \leq y \Leftrightarrow \xi \models MAX(Const) < x' \leq y'$$

Unboundedness criterium for simple GCS

For all $L_1, L_2 \in Lower(\xi, Var)$ and $L_0 \in Lower(\xi_0, Var)$

$$\left.\begin{array}{l} \xi \models L_1 < L_1' \\ \vee \\ \xi \models L_1 < L_2 \wedge \xi \models L_1 = L_1' \wedge \xi \models L_2' < L_2 \end{array}\right\} \Rightarrow \xi_0 \not\models L_0 \leq L_1'$$

Unboundedness criterium for simple GCS

For all $L_1, L_2 \in \mathit{Lower}(\xi, \mathit{Var})$ and $L_0 \in \mathit{Lower}(\xi_0, \mathit{Var})$

$$\left.\begin{array}{l} \xi \models L_1 < L_1' \\ \vee \\ \xi \models L_1 < L_2 \wedge \xi \models L_1 = L_1' \wedge \xi \models L_2' < L_2 \end{array}\right\} \Rightarrow \xi_0 \not\models L_0 \leq L_1'$$

For all $U_1, U_2 \in \mathit{Upper}(\xi, \mathit{Var})$ and $U_0 \in \mathit{Upper}(\xi_0, \mathit{Var})$

$$\left.\begin{array}{l} \xi \models U_2' < U_2 \\ \vee \\ \xi \models U_1 < U_2 \wedge \xi \models U_2 = U_2' \wedge \xi \models U_1 < U_1' \end{array}\right\} \Rightarrow \xi_0 \not\models U_2' \leq U_0$$

Strong Termination for simple GCS

Remark

- For a GCS $\mathcal{S}$, $\mathcal{S}$ is simple iff $\lfloor \mathcal{S} \rfloor_K$ is simple.
- For a simple GCS $\mathcal{S}$, $\mathcal{S}$ satisfies the unboundedness criterium iff $\lfloor \mathcal{S} \rfloor_K$ satisfies the unboundedness criterium.

Strong Termination for simple GCS

Remark

- For a GCS $\mathcal{S}$, $\mathcal{S}$ is simple iff $\lfloor \mathcal{S} \rfloor_K$ is simple.
- For a simple GCS $\mathcal{S}$, $\mathcal{S}$ satisfies the unboundedness criterium iff $\lfloor \mathcal{S} \rfloor_K$ satisfies the unboundedness criterium.

Theorem (Strong Termination for simple GCS)

Let $\mathcal{S}$ be a simple GCS *with initial control point q_0.*

- *The set of valuations ν over Var such that (q_0, ν) is not strongly terminating is effectively* GC *representable.*
- *$\mathcal{S}$ satisfies the unboundedness criterium iff there is some state (q_0, ν) which is not strongly terminating.*

Outline

Characterization Theorem

Theorem (Characterization Theorem)

Let $\mathcal{S}$ be a GCS and (q_0, ν_0) be a state. Then, (q_0, ν_0) is strongly terminating iff there are $q \in Q(\mathcal{S})$, a path $\wp_0 \in \mathcal{P}_\mathcal{S}$ (the finite set of sample paths of $\mathcal{S}$) from q_0 to q, and $\wp \in \mathcal{P}_\mathcal{S}$ cyclic path from q to q such that

- *the GCS $\mathcal{S}'$ consisting of the edges $(q_0, \#) \overset{\xi_{\wp_0}}{\rightarrow} q$ and $q \overset{\xi_\wp}{\rightarrow} q$ is simple, and $((q_0, \#), \nu_0)$ is strongly-terminating for $\mathcal{S}'$.*

Proof.

By using Ramsey's Theorem in its infinite version. □

By Characterization Theorem, for a GCS $\mathcal{S}$,

- one can construct a finite family $\mathcal{F}$ of *simple* GCS such that the set of strongly terminating states of $\mathcal{S}$ corresponds to the union of the sets of strongly terminating states of components in $\mathcal{F}$.

Since for transitional cGC ξ and ξ', $\lfloor \xi \bullet \xi' \rfloor_K = \lfloor \lfloor \xi \rfloor_K \bullet \lfloor \xi' \rfloor_K \rfloor_K$,

- one can compute separately and in exponential time the K-bounded abstractions of the simple GCS in $\mathcal{F}$.

By Characterization Theorem, for a GCS $\mathcal{S}$,

- one can construct a finite family $\mathcal{F}$ of *simple* GCS such that the set of strongly terminating states of $\mathcal{S}$ corresponds to the union of the sets of strongly terminating states of components in $\mathcal{F}$.

Since for transitional cGC ξ and ξ', $\lfloor \xi \bullet \xi' \rfloor_K = \lfloor \lfloor \xi \rfloor_K \bullet \lfloor \xi' \rfloor_K \rfloor_K$,

- one can compute separately and in exponential time the K-bounded abstractions of the simple GCS in $\mathcal{F}$.

Thus, by results for simple GCS, we obtain the main result. . .

Main result

Theorem (Strong Termination for unrestricted GCS)

Let $\mathcal{S}$ be a GCS. Then, for each control point q,

1. *The set of valuations ν such that (q, ν) is not strongly terminating is effectively GC representable.*
2. *Checking whether (q, ν) is not strongly terminating for some valuation ν is in PSPACE and can be done in time $O(|E(\mathcal{S})| \cdot |Q(\mathcal{S})|^2 \cdot (K+2)^{(2|Var|+|Const|)^2})$.*

Main result

Theorem (Strong Termination for unrestricted GCS)

Let $\mathcal{S}$ be a GCS. Then, for each control point q,

1. *The set of valuations ν such that (q, ν) is not strongly terminating is effectively GC representable.*
2. *Checking whether (q, ν) is not strongly terminating for some valuation ν is in PSPACE and can be done in time $O(|E(\mathcal{S})| \cdot |Q(\mathcal{S})|^2 \cdot (K+2)^{(2|Var|+|Const|)^2})$.*

Corollary

The strong termination problem and the strong termination problem w.r.t. a designated state are PSPACE-complete.

Strong termination for unrestricted GCS

MANY THANKS!