Completeness for Bounded Satisfiability of LTL with arithmetical constraints

Marcello M. Bersani

DEI - Politecnico di Milano
Joint work with Achille Frigeri, Matteo Rossi and Pierluigi San Pietro

September 29, 2011

Motivations

Verification of infinite state systems: we want to use

counter systems: finite state automata enriched with counters over infinite domains where transitions are labeled by formulae involving counters

linear temporal languages where atomic formulae belong to arithmetical language

Theoretical limit:

- counter systems with two counters and zero-test simulate Minsky machines
- temporal languages over arithmetical language can be enough expressive to represent runs of Minsky machines

Our proposal

Verification approach based on **bounded representation**

- analogous to Bounded Model-Checking for LTL
- but extended to infinite state systems
- and tailored to be implemented on SMT-solvers.

Our proposal

Verification approach based on **bounded representation**

- analogous to Bounded Model-Checking for LTL
- but extended to infinite state systems
- and tailored to be implemented on SMT-solvers.

Given a LTL formula with arithm. atoms, we represent

- exactly, **relations** among counters over infinite (ultimately-periodic) runs/models $\delta\pi^\omega$,
  - $|\delta\pi| = k$
- partially, the **arithmetical assignments** satisfying $\delta\pi$

Our proposal

Verification approach based on **bounded representation**

- analogous to Bounded Model-Checking for LTL
- but extended to infinite state systems
- and tailored to be implemented on SMT-solvers.

Given a LTL formula with arithm. atoms, we represent

- exactly, **relations** among counters over infinite (ultimately-periodic) runs/models $\delta\pi^\omega$,
  - $|\delta\pi| = k$
- partially, the **arithmetical assignments** satisfying $\delta\pi$

The two models are still representative of an infinite "complete" model

Satisfiability problem

Let $x, y \in D$

$$\varphi = \mathbf{G}(\mathbf{F}(\mathrm{X}x < y) \Rightarrow \mathbf{FG}(y \equiv_3 2 \wedge \mathrm{XX}y \geq \mathrm{Y}x))$$

[1] [Demri&D'Souza IC07], [Demri&Gascon CONCUR05]

Satisfiability problem

Let $x, y \in D$

$$\varphi = \mathbf{G}(\mathbf{F}(\mathrm{X}x < y) \Rightarrow \mathbf{FG}(y \equiv_3 2 \wedge \mathrm{XX}y \geq \mathrm{Y}x))$$

Models are sequences of assignments to variables $\sigma \in (D^2)^\omega$

[1] [Demri&D'Souza IC07], [Demri&Gascon CONCUR05]

Satisfiability problem

Let $x, y \in D$

$$\varphi = \mathbf{G}(\mathbf{F}(\mathrm{X}x < y) \Rightarrow \mathbf{FG}(y \equiv_3 2 \wedge \mathrm{XX}y \geq \mathrm{Y}x))$$

Models are sequences of assignments to variables $\sigma \in (D^2)^\omega$

Is there a model $\sigma \in (\mathbb{Z}^n)^\omega$ satisfying φ?

[1] [Demri&D'Souza IC07], [Demri&Gascon CONCUR05]

Satisfiability problem

Let $x, y \in D$

$$\varphi = \mathbf{G}(\mathbf{F}(\mathrm{X}x < y) \Rightarrow \mathbf{FG}(y \equiv_3 2 \wedge \mathrm{XX}y \geq \mathrm{Y}x))$$

Models are sequences of assignments to variables $\sigma \in (D^2)^\omega$

Is there a model $\sigma \in (\mathbb{Z}^n)^\omega$ satisfying φ?

- automata-based approach[1] (without Y)
- finite amount of k-bounded satisfiability tests
  - verification procedure is complete

[1] [Demri&D'Souza IC07], [Demri&Gascon CONCUR05]

Language of atomic formulae

$(D, <, =)$, when

- $D \in \{\mathbb{N}, \mathbb{Z}\}$
- $D = \mathbb{R}$ or $D = \mathbb{Q}$ $<$ is a dense order without endpoints

Integer Periodic Constraints (IPC*) or subclasses.

$$\tau := \theta \mid x < y \mid \tau \wedge \tau \mid \neg\tau$$
$$\theta := x \equiv_c y + d \mid x = y \mid x < d \mid x = d \mid \theta \wedge \theta \mid \neg\theta \mid \exists x\theta$$

where $x, y \in V$, $c \in \mathbb{N}^+$ and $d \in \mathbb{Z}$.

Language from θ is IPC^{++}[2] but we consider its quantifier-free fragment.

[2] IPC* and $(D, <, =)$ can be found in [Demri et al. TCS06-07, IC07]

CLTL with past-time operators (CLTLB$_{\mathrm{X,Y}}$)

Let $x \in D$
An **arithmetical temporal term** τ is:

$$\tau := x \mid \mathrm{X}\tau \mid \mathrm{Y}\tau.$$

CLTL with past-time operators ($\mathrm{CLTLB}_{\mathrm{X,Y}}$)

Let $x \in D$
An **arithmetical temporal term** τ is:

$$\tau := x \mid \mathrm{X}\tau \mid \mathrm{Y}\tau.$$

Formulae of $\mathrm{CLTLB}_{\mathrm{X,Y}}(L)$ are:

$$\varphi := \tau \sim \tau \mid \varphi \wedge \varphi \mid \neg\varphi \mid \mathbf{X}\varphi \mid \mathbf{Y}\varphi \mid \varphi\mathbf{U}\varphi \mid \varphi\mathbf{S}\varphi.$$

where $\sim$ is a relation from the language of constraints L.

Semantics for CLTLB$_{\mathrm{X,Y}}$

The semantics of a formula ϕ of CLTLB(L) is defined w.r.t. a sequence of valuations $\sigma : \mathbb{Z} \times V \to D$.

The **satisfaction relation** $\models$ is defined for $i \geq 0$:

$$
\begin{aligned}
\sigma, i \models \tau_1 \sim \tau_2 &\Leftrightarrow \sigma(i + |\tau_1|, x_{\tau_1}) \sim_L \sigma(i + |\tau_2|, x_{\tau_2}) \\
\sigma, i \models \neg\varphi &\Leftrightarrow \ldots \\
&\ldots \\
\sigma, i \models \mathbf{X}\varphi &\Leftrightarrow \sigma, i + 1 \models \varphi \\
\sigma, i \models \varphi \mathbf{U} \psi &\Leftrightarrow \ldots\ldots
\end{aligned}
$$

where x_{τ_i} is the variable that appears in τ_i.

Equivalence of $\mathrm{CLTLB}_{\mathrm{X,Y}}$ with $\mathrm{CLTLB}_{\mathrm{X}}$

The "previous" operator Y on terms can be removed.

$$(\mathrm{X}\mathbf{x} < \mathrm{Y}\mathbf{y})\mathbf{U}(\mathbf{y} = \mathbf{0}) \xrightarrow{r} (\mathrm{X}^2 x < y)\mathbf{U}(\mathrm{X}y = 0)$$

where r is a syntactic rewriting function

$$\begin{array}{lcc|ccc|ccc} x: & 0 & 3 & 1 & -4 & 0 & 9 & \\ y: & -5 & 5 & 5 & -5 & 1 & -4 & \ldots \end{array}$$

$$(\mathrm{X}\mathbf{x} < \mathrm{Y}\mathbf{y})$$

Equivalence of $\mathrm{CLTLB}_{\mathrm{X,Y}}$ with $\mathrm{CLTLB}_{\mathrm{X}}$

The “previous” operator Y on terms can be removed.

$$(\mathrm{X}x < \mathrm{Y}y)\mathbf{U}(y = 0) \xrightarrow{r} (\mathrm{X}^{\mathbf{2}}\mathbf{x} < \mathbf{y})\mathbf{U}(\mathrm{X}\mathbf{y} = \mathbf{0})$$

$$\begin{array}{llllllll}
x: & 0 & | \; 3 & 1 & -4 \; | & 0 & 9 & \\
y: & -5 & | \; 5 & 5 & -5 \; | & 1 & -4 & \ldots
\end{array}$$

$$(\mathrm{X}^{\mathbf{2}}\mathbf{x} < \mathbf{y})$$

Equivalence of $\mathrm{CLTLB}_{\mathrm{X,Y}}$ with $\mathrm{CLTLB}_{\mathrm{X}}$

The "previous" operator Y on terms can be removed.

$$(\mathrm{X}x < \mathrm{Y}y)\mathbf{U}(y = 0) \xrightarrow{r} (\mathrm{X}^{\mathbf{2}}\mathbf{x} < \mathbf{y})\mathbf{U}(\mathrm{X}\mathbf{y} = \mathbf{0})$$

$x:$	0	| 3	1	-4 |	0	9	
$y:$	-5	| 5	5	-5 |	1	-4	...

$$(\mathrm{X}^{\mathbf{2}}\mathbf{x} < \mathbf{y})$$

Values of terms before $i = 0$ are always defined.

- in the example, -1 is the new origin
- in practice, $[-1, \infty)$ is isomorphic to $\mathbb{N}$
  - translated formulae $r(\varphi)$ can be equivalently evaluated from 0

Symbolic valuations

A **symbolic valuation** sv is a **maximally consistent set** of formulae built from the original $\varphi \in$ CLTLB$_{\mathrm{X}}(L)$

x:	0	3	1	-4	0	9	
y:	-5	5	5	5	1	-4	...

$$sv = \{\mathrm{X}^2 x < y, x > \mathrm{X}x, x > \mathrm{X}^2 x, \mathrm{X}x < \mathrm{X}^2 y, \ldots\}$$

Symbolic valuations

Definition

A (locally consistent) infinite **sequence of SVs** $\rho : \mathbb{N} \rightarrow SV(\varphi)$ **admits a model** ($\sigma \models \rho$) if there exists a model σ of φ

$$\sigma, i \models \rho(i)$$

for every $i \geq 0$.

Symbolic valuations

Definition

A (locally consistent) infinite **sequence of SVs** $\rho : \mathbb{N} \to SV(\varphi)$ **admits a model** ($\sigma \models \rho$) if there exists a model σ of φ

$$\sigma, i \models \rho(i)$$

for every $i \geq 0$.

- ρ is a **symbolic model** for ϕ.
- $\models_s$ symbolic satisfaction relation for models ρ
  - the same as $\models$ except for atomic formulae

k-bounded satisfiability problem

k-BSP is defined by

- a partial model $\sigma_k : \{0, \ldots, k+l\} \times V \to D$,
- $\rho' \in SV(\varphi)^{k+1}$, a sequence of SVs of **length** $k+1$

$time:$	0	1	2	...	k	$k+l$
	sv$_0$				sv$_k$	
$x:$	1	3	-7	...	-1	1
$y:$	0	1	-1		1	-1

- a k-**bounded** satisfaction relation $\models_k$:

$$\sigma_k \models_k \rho' \text{ iff } \sigma_k, i \models_s \rho'(i) \text{ for all } 0 \leq i \leq k.$$

k-bounded satisfiability problem

k-BSP is defined by

- a partial model $\sigma_k : \{0, \dots, k+l\} \times V \to D$,
- $\rho' \in SV(\phi)^{k+1}$, a sequence of SVs of **length** $k+1$

$time:$	0	1	2	...	k	$k+l$
		sv$_1$			sv$_k$	
$x:$	7	3	-7	...	-1	1
$y:$	0	1	-1		1	-1

- a k**-bounded** satisfaction relation $\models_k$:

$$\sigma_k \models_k \rho' \text{ iff } \sigma_k, i \models_s \rho'(i) \text{ for all } 0 \le i \le k.$$

k-bounded satisfiability problem

k-BSP is defined by

- a partial model $\sigma_k : \{0, \ldots, k+l\} \times V \to D$,
- $\rho' \in SV(\phi)^{k+1}$, a sequence of SVs of **length** $k+1$

$$
\begin{array}{rccccccc}
time: & 0 & 1 & 2 & \ldots & k & k+l \\
 & & \boxed{\mathsf{sv}_1} & & & \boxed{\mathsf{sv}_k} & \\
x: & 7 & 3 & -7 & \ldots & -1 & 1 \\
y: & 0 & 1 & -1 & & 1 & -1
\end{array}
$$

- a k-**bounded** satisfaction relation $\models_k$:

$$\sigma_k \models_k \rho' \text{ iff } \sigma_k, i \models_s \rho'(i) \text{ for all } 0 \leq i \leq k.$$

Input: a $\mathrm{CLTLB}_{\mathrm{X}}(L)$ formula φ, $k \in \mathbb{N}$;

Problem: is there an ultimately periodic sequence of SVs $\rho = \delta\pi^\omega$ such that $k+1 = |\delta\pi|$ and $\rho, 0 \models_s \varphi$, and which admits a partial model σ_k such that $\sigma_k \models_k \rho'$ with $\rho' = \delta\pi$?

k-bounded satisfiability is decidable

Polynomial time reduction [Bersani et al. TIME10] from k-bounded satisfiability of CLTLB $\rightarrow$ satisfiability of formulae in the **combined theories**

- Equality and Uninterpreted Functions (EUF)
- quantifier-free Integer/Real linear arithmetic IDL/RDL

k-bounded satisfiability is decidable

Polynomial time reduction [Bersani et al. TIME10] from k-bounded satisfiability of CLTLB $\rightarrow$ satisfiability of formulae in the **combined theories**

- Equality and Uninterpreted Functions (EUF)
- quantifier-free Integer/Real linear arithmetic IDL/RDL

Natural questions?

- what can we say when a formula is k-bounded satisfiable?
- when a formula is unsatisfiable?
  - k-bounded unsatisfiability does not immediately entail unsatisfiability

Towards completeness

Given a CLTL(L) formula φ, we can build an automaton[3] $\mathcal{A}_\varphi$ s.t. $\rho \in \mathcal{A}_\varphi$ if, and only if,

$$\rho \models_s \varphi \text{ and there exists } \sigma \text{ s.t. } \sigma \models \rho$$

$\mathscr{L}(\mathcal{A}_\varphi) \subseteq SV(\varphi)^\omega$; it is the intersection of:

- $\mathcal{A}_s \rightarrow$ LTL symbolic models of φ (Vardi-Wolper)
- $\mathcal{A}_\ell \rightarrow$ sequences of locally consistent SVs
- $\mathcal{A}_C \rightarrow$ sequences of SVs admitting a model σ. C is a condition on models of φ enforced by $\mathcal{A}_C$

[3] [Demri&D'Souza IC07]

Towards completeness

Given a CLTL(L) formula φ, we can build an automaton[3] $\mathcal{A}_\varphi$ s.t. $\rho \in \mathcal{A}_\varphi$ if, and only if,

$$\rho \models_s \varphi \text{ and there exists } \sigma \text{ s.t. } \sigma \models \rho$$

$\mathscr{L}(\mathcal{A}_\varphi) \subseteq SV(\varphi)^\omega$; it is the intersection of:

- $\mathcal{A}_s \rightarrow$ LTL symbolic models of φ (Vardi-Wolper)
- $\mathcal{A}_\ell \rightarrow$ sequences of locally consistent SVs
- $\mathcal{A}_C \rightarrow$ sequences of SVs admitting a model σ. C is a condition on models of φ enforced by $\mathcal{A}_C$

Lemma

Locally consistent ultimately periodic sequence of SVs $\rho = \delta\pi^\omega$ admits models σ ($\sigma \models \rho$).

[3] [Demri&D'Souza IC07]

From k-bounded satisfiability to satisfiability

We represent:

- $\mathcal{A}_\ell$ by the formula $\varphi_\ell := \mathbf{G}(\bigvee_1^{|SV(\varphi)|} sv_i)$
- $\mathcal{A}_C$ by the formula $\varphi_{\mathcal{A}_C}$ ([Sistla&Clarke J. ACM 85])

Verify if the formula is k-boundedly satisfiable:

$$\Phi = \varphi \ \wedge \ \varphi_{\mathcal{A}_C} \ \wedge \ \varphi_\ell$$

for all $k \in [1, c+1]$ where c is the length of the (**recurrence diameter**) longest loop-free path of $\mathcal{A}_\varphi$.

From k-bounded satisfiability to satisfiability

We represent:

- $\mathcal{A}_\ell$ by the formula $\varphi_\ell := \mathbf{G}(\bigvee_1^{|SV(\varphi)|} sv_i)$
- $\mathcal{A}_C$ by the formula $\varphi_{\mathcal{A}_C}$ ([Sistla&Clarke J. ACM 85])

Verify if the formula is k-boundedly satisfiable:

$$\Phi = \varphi \ \wedge \ \varphi_{\mathcal{A}_C} \ \wedge \ \varphi_\ell$$

for all $k \in [1, c+1]$ where c is the length of the (**recurrence diameter**) longest loop-free path of $\mathcal{A}_\varphi$.

Lemma

Formula Φ is satisfiable, for some $k \in [1, c+1]$, iff there exists an ultimately periodic model accepted by $\mathcal{A}_\varphi$.

k-bounded satisfiability is complete

- If Φ is k-boundedly unsatisfiable for all $k \in [1, c+1]$ then φ is unsatisfiable.
- Otherwise, there exists an ultimately periodic symbolic model ρ which admits a model σ.
  - σ is defined from σ_k by iterating infinitely many times the sequence of SVs in π, from $\rho' = \delta\pi$.

k-bounded satisfiability is complete

- If Φ is k-boundedly unsatisfiable for all $k \in [1, c+1]$ then φ is unsatisfiable.
- Otherwise, there exists an ultimately periodic symbolic model ρ which admits a model σ.
  - σ is defined from σ_k by iterating infinitely many times the sequence of SVs in π, from $\rho' = \delta\pi$.

Theorem

For languages IPC^*, $(D, <, =)$, where D is $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$, there exists a finite completeness threshold for k-bounded satisfiability problem.

k-bounded satisfiability is complete

- If Φ is k-boundedly unsatisfiable for all $k \in [1, c+1]$ then φ is unsatisfiable.
- Otherwise, there exists an ultimately periodic symbolic model ρ which admits a model σ.
  - σ is defined from σ_k by iterating infinitely many times the sequence of SVs in π, from $\rho' = \delta\pi$.

Theorem

For languages IPC^*, $(D, <, =)$, where D is $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$, there exists a finite completeness threshold for k-bounded satisfiability problem.

- the results holds also for k-bounded model-checking

k-bounded satisfiability in practice

Formula Φ can be simplified.

D	Φ
$\{\mathbb{N}, \mathbb{Z}\}$	$\varphi \wedge \varphi_{\mathcal{A}_C}$
$\{\mathbb{Q}, \mathbb{R}\}$	$\varphi \wedge \varphi_\ell$

- $D \in \{\mathbb{N}, \mathbb{Z}\}$, φ_ℓ can be removed thanks to the consistency of reduction from k-bounded SAT to (EUF$\cup L$) SAT
- $D \in \{\mathbb{Q}, \mathbb{R}\}$, φ_ℓ is necessary to define the sequence of locally consistent SVs ($\mathcal{A}_C$ is not needed anymore).

How to estimate completeness threshold

We don't want to build the automaton $\mathcal{A}_\varphi$ but exploit directly the satisfiability of Φ

- linear encoding of CLTLB [Bersani et al. TIME10]
- $\mathcal{A}_C$ and $\mathcal{A}_\ell$ depends only on the arithmetical language and the length of SVs but **not** on φ

D	Φ
$\{\mathbb{N}, \mathbb{Z}\}$	$\varphi \wedge \varphi_{\mathcal{A}_C}$
$\{\mathbb{Q}, \mathbb{R}\}$	$\varphi \wedge \varphi_\ell$

How to estimate completeness threshold

We don't want to build the automaton $\mathcal{A}_\varphi$ but exploit directly the satisfiability of Φ

- linear encoding of CLTLB [Bersani et al. TIME10]
- $\mathcal{A}_C$ and $\mathcal{A}_\ell$ depends only on the arithmetical language and the length of SVs but **not** on φ

D	Φ
$\{\mathbb{N}, \mathbb{Z}\}$	$\varphi \wedge \varphi_{\mathcal{A}_C}$
$\{\mathbb{Q}, \mathbb{R}\}$	$\varphi \wedge \varphi_\ell$

Remark: estimation for the completeness bound

$$d \cdot |SV(\varphi)| \cdot 2^{|\varphi|} \leq 2^{c|\varphi|}$$

- $d = |\mathcal{A}_C|$ or $d = 1$, depending on D
- $|SV(\varphi)|$ witnesses $\mathcal{A}_\ell$ (exponential in the size of φ).

Conclusions and Future works

- we introduced the notion of k-bounded satisfiability for temporal languages over constraints
- we give an example of temporal language over arithmetical constraints s.t. k-bounded satisfiability is complete
- we provide an effective method for verification using a bounded approach over SMT-solvers (implemented tool)

Future works: Mainly focus on

- discovering models which have properties of boundedness,
- adapting k-bounded satisfiability to model-checking and satisfiability problems.