The Effects of Bounding Syntactic Resources on Presburger LTL (extended abstract)

S. Demri R. Gascon

LSV, ENS Cachan, CNRS, INRIA

TIME'07, June 28–30, 2007

Counter systems

- Verification of infinite-state systems by model-checking.
- Ubiquity of counter systems (CS)
  - Embedded systems/protocols, Petri nets, ...
  - Programs with pointer variables. [Bardin et al, AVIS 06; Bouajjani et al, CAV 06]
  - Broadcast protocols. [Leroux & Finkel, FSTTCS 02]
  - Logics for data words. [Bojańczyk et al, LICS 06]
- (High) undecidability
  - Checking safety properties for CS is undecidable.
  - Checking liveness properties for CS is Σ_1^1-hard.

Taming counter systems

- Classes with decidable reachability problems
  - Reversal-bounded CS. [Ibarra, JACM 78]
  - Flat relational CS. [Comon & Jurski, CAV 98]
  - Flat linear CS. [Boigelot, PhD 98; Finkel & Leroux, FSTTCS 02]
  - Petri nets. [Kosaraju, STOC 82]
- Decision procedures
  - Translation into Presburger arithmetic. [Ibarra, JACM 78, Comon & Jurski, CAV 98]
  - Well-structured transition systems. [Finkel & Schnoebelen, TCS 01]
- Tools: FAST, LASH, TREX, ...

Presburger arithmetic

- Decision
  - First-order theory of $\langle \mathbb{Z}, 0, + \rangle$.
  - Decidability shown in [Presburger 29].
  - Quantifier elimination in presence of modulo constraints.
  - Satisfiability in 3EXPTIME.

Presburger arithmetic

- Decision
  - First-order theory of $\langle \mathbb{Z}, 0, + \rangle$.
  - Decidability shown in [Presburger 29].
  - Quantifier elimination in presence of modulo constraints.
  - Satisfiability in 3EXPTIME.

- Fragments
  - DL: $\mathrm{E} ::= x \sim y + d \mid x \sim d \mid \mathrm{E} \wedge \mathrm{E} \mid \neg \mathrm{E}$. ($d \in \mathbb{Z}$, $\sim \in \{<, >, =\}$).
  - DL^+: $\mathrm{DL} + x \equiv_k c$, $x \equiv_k y + c$ ($c, k \in \mathbb{N}$).
  - QFP: $\mathrm{E} ::= \sum_{i \in I} a_i x_i \sim d \mid \sum_{i \in I} a_i x_i \equiv_k c \mid \mathrm{E} \wedge \mathrm{E} \mid \neg \mathrm{E}$. ($a_i \in \mathbb{Z}$)

Syntax for $\mathrm{CLTL}(L)$

- L is a fragment among DL, DL^+, QFP.
- Formulae:

  $$\phi ::= \mathrm{E}[x_1 \leftarrow \mathsf{X}^{l_1} x_{j_1}, \ldots, x_n \leftarrow \mathsf{X}^{l_n} x_{j_n}] \mid \phi \wedge \phi \mid \neg\phi \mid \mathsf{X}\phi \mid \phi \mathsf{U} \phi$$

  $(\mathrm{E} \in L)$

- $\overbrace{\mathsf{X}\mathsf{X}\cdots\mathsf{X}}^{i \text{ times}} x$ interpreted as the value of x at the ith next position.
- Definitions
  - One-step constraint: $l_1, \ldots, l_n \leq 1$.
  - X-length of ϕ: maximal i such that $\mathsf{X}^i x$ occurs in ϕ.

Semantics for Presburger LTL

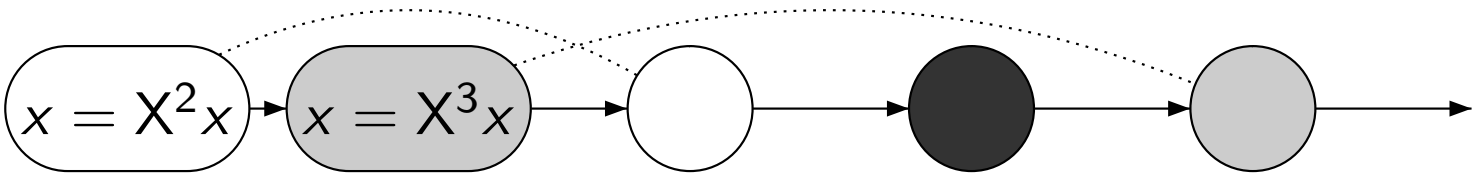
- Models: ω-sequences of valuations of the form $\mathrm{VAR} \to \mathbb{Z}$.

Semantics for Presburger LTL

- Models: ω-sequences of valuations of the form $\mathrm{VAR} \to \mathbb{Z}$.
- Satisfaction relation:
  - $\sigma, i \models \mathrm{E}[x_1 \leftarrow \mathsf{X}^{l_1} x_{j_1}, \ldots, x_n \leftarrow \mathsf{X}^{l_n} x_{j_n}]$ iff $(\sigma(i + l_1)(x_{j_1}), \ldots, \sigma(i + l_n)(x_{j_n})) \models \mathrm{E}$ in PA,
  - $\sigma, i \models \mathsf{X}\phi$ iff $\sigma, i + 1 \models \phi$,
  - $\sigma, i \models \phi \mathsf{U} \phi'$ iff there is $j \geq i$ such that $\sigma, j \models \phi'$ and for every $i \leq k < j$, we have $\sigma, k \models \phi$.

Semantics for Presburger LTL

- Models: ω-sequences of valuations of the form $\mathrm{VAR} \to \mathbb{Z}$.
- Satisfaction relation:
  - $\sigma, i \models \mathrm{E}[x_1 \leftarrow \mathsf{X}^{l_1} x_{j_1}, \ldots, x_n \leftarrow \mathsf{X}^{l_n} x_{j_n}]$ iff $(\sigma(i + l_1)(x_{j_1}), \ldots, \sigma(i + l_n)(x_{j_n})) \models \mathrm{E}$ in PA,
  - $\sigma, i \models \mathsf{X}\phi$ iff $\sigma, i + 1 \models \phi$,
  - $\sigma, i \models \phi \mathsf{U} \phi'$ iff there is $j \geq i$ such that $\sigma, j \models \phi'$ and for every $i \leq k < j$, we have $\sigma, k \models \phi$.



Fragments $\mathrm{CLTL}_k^l(L)$

- $\mathrm{CLTL}_k^l(L)$ is the fragment of $\mathrm{CLTL}(L)$ with
  - atomic formulae built from constraints in L,
  - formulae use variables from $\{x_1, \ldots, x_k\}$,
  - the term $\mathsf{X}^i x$ can occur only if $i \leq l$.
- Examples
  - $x_1 = \mathsf{X}^8 x_2 + 1$ belongs to $\mathrm{CLTL}_2^8(\mathrm{DL})$,
  - $\mathsf{X}^2 x_1 \equiv_4 2$ belongs to $\mathrm{CLTL}_1^2(\mathrm{DL}^+) \cap \mathrm{CLTL}_1^2(\mathrm{QFP})$,
  - $\mathsf{XXX}(5\mathsf{X}x_1 + 2x_2 \geq 27)$ belongs to $\mathrm{CLTL}_2^1(\mathrm{QFP})$.

k-variable L-automata

- Definition:
  - Transitions of the form $q \xrightarrow{\mathrm{E}} q'$ for one-step constraint E in L. Examples: $q \xrightarrow{\mathsf{X}x>y+1} q'$, $q_0 \xrightarrow{x=0 \wedge y=0} q$, $q \xrightarrow{\top} q$.
  - Standard Büchi acceptance condition.
  - Accepting runs of the form $\mathbb{N} \to Q \times \mathbb{Z}^k$.
- σ realizes $\mathrm{E}_0 \cdot \mathrm{E}_1 \cdots$ iff for every i, we have $\sigma, i \models \mathrm{E}_i$.

k-$\mathbb{Z}$-counter automata

- Restriction of k-variable DL-automaton with constraints

$$\bigwedge_{i \in \{1 \ldots k\}} \mathrm{E}_{test^i} \wedge \bigwedge_{i \in \{1 \ldots k\}} \mathrm{E}_{update^i}$$

with

  - $\mathrm{E}_{test^i} \in \{\top\} \cup \{x_i \sim 0 \mid \sim \in \{<, >, =, \neq\}\}$,
  - $\mathrm{E}_{update^i} \in \{\mathsf{X}x_i = x_i + u \mid u \in \mathbb{Z}\}$

- Initial values of the counters are zero.
- Simple $\mathbb{Z}$-counter automata: updates in $\{0, -1, 1\}$.

Model checking problems

- Model-checking $\mathrm{CLTL}^{I}_{k}(L)$ formulae over a class $\mathcal{C}$ of automata:
  - Input: a k-variable automaton $\mathcal{A}$ in $\mathcal{C}$ and a formula in $\mathrm{CLTL}^{I}_{k}(L)$.
  - Question: Is there a model σ that realizes a word accepted by $\mathcal{A}$ and such that $\sigma, 0 \models \phi$?

- Model-checking $\mathrm{CLTL}^{1}_{3}(\mathrm{DL})$ over the class of 3-$\mathbb{N}$-automata is Σ^{1}_{1}-complete. [Alur & Henzinger, JACM 94]

$\mathrm{CLTL}_3^1(\mathrm{DL})$ satisfiability is Σ_1^1-complete

- Reduction from the recurring problem for nondeterministic Minsky machines.
- Σ_1^1-hardness from [Alur & Henzinger, JACM 94].
- The instruction "$n : \mathtt{c}_1 := \mathtt{c}_1 + 1$; goto either n' or n''" is encoded by

  $$\mathsf{G}(x_{inst} = n \Rightarrow (\mathsf{X}x_1 = x_1 + 1 \wedge \mathsf{X}x_2 = x_2 \wedge (\mathsf{X}x_{inst} = n' \vee \mathsf{X}x_{inst} = n'')))$$

- Recurring condition: $\mathsf{GF}(x_{inst} = 1)$.

Taxonomy of subproblems

- Problems:
  - satisfiability,
  - model-checking L-automata,
  - model-checking $\mathbb{Z}$-counter automata.

Taxonomy of subproblems

- Problems:
  - satisfiability,
  - model-checking L-automata,
  - model-checking $\mathbb{Z}$-counter automata.

- Fragments: DL, DL^{+}, QFP.

Taxonomy of subproblems

- Problems:
  - satisfiability,
  - model-checking L-automata,
  - model-checking $\mathbb{Z}$-counter automata.
- Fragments: DL, DL^{+}, QFP.
- Bounding syntactic resources: X-length, number of variables.

Summary of results

($\mathrm{CLTL}^{l}_{k}(L)$: k variables, "next length" $\leq l$, fragment L)

	MC (DL)	SAT	MC (CA)
$\mathrm{CLTL}^{1}_{3}(\mathrm{DL})$	U	U	U
$\mathrm{CLTL}^{\omega}_{2}(\mathrm{DL})$	U	U	U
$\mathrm{CLTL}^{2}_{1}(\mathrm{DL})$	U	U	PSPACE-c
$\mathrm{CLTL}^{1}_{2}(\mathrm{DL})$	U	U	U
$\mathrm{CLTL}^{1}_{1}(\mathrm{DL}\text{ or }\mathrm{DL}^{+})$	PSPACE-c.	PSPACE-c.	PSPACE-c
$\mathrm{CLTL}^{1}_{1}(\mathrm{QFP})$	U	U	PSPACE-c
$\mathrm{CLTL}^{\omega}_{1}(\mathrm{QFP})$	U	U	PSPACE-c.

Symbolic model-checking for $\mathrm{CLTL}^1_1(\mathrm{DL})$

- Model-checking for $\mathrm{CLTL}^1_1(\mathrm{DL}^+)$ reduces to satisfiability for $\mathrm{CLTL}^1_1(\mathrm{DL}^+, \mathrm{PROP})$ (addition of propositions).
- Maps $\{x, \mathsf{X}x\} \to \mathbb{Z}$ are abstracted by finite sets of constraints depending on the syntactic resources of the formula to be checked.
- Symbolic models are ω-sequences of symbolic valuations.
- Satisfiability is reduced to nonemptiness problem for simple 1-$\mathbb{Z}$-counter automata over the alphabet of symbolic valuations.

Symbolic valuation

- $\langle \mathrm{E}_x, \mathrm{E}_m, \mathrm{E}'_x, \mathrm{E}'_m, \mathrm{E}_s \rangle \in \mathrm{C}_x \times \mathrm{Mod}_x \times \mathrm{C}_{\mathsf{X}x} \times \mathrm{Mod}_{\mathsf{X}x} \times \mathrm{C}_{\mathrm{step}}$.
- For $t \in \{x, \mathsf{X}x\}$
  - C_t:
    - $(d_i < t) \wedge (t < d_{i+1})$ for $i \in \{\mathsf{min}, .., \mathsf{max}-1\}$,
    - $t = d_i$ for $i \in \{\mathsf{min}, \ldots, \mathsf{max}\}$ + $t < d_{\mathsf{min}}$ and $d_{\mathsf{max}} < t$,
  - Mod_t: $t \equiv_K c$ for $c \in \{0, \ldots, K-1\}$,
  - $\mathrm{C}_{\mathrm{step}}$:
    - $x + e_i < \mathsf{X}x \wedge \mathsf{X}x < x + e_{i+1}$ for $i \in \{\mathsf{min}', \ldots, \mathsf{max}'-1\}$,
    - $\mathsf{X}x = x + e_i$ for $i \in \{\mathsf{min}', \ldots, \mathsf{max}'\}$ + $\mathsf{X}x < x + e_{\mathsf{min}'}$ and $x + e_{\mathsf{max}'} < \mathsf{X}x$.

Satisfiability and symbolic models

- Symbolic model $\langle \sigma, \rho \rangle$:
  - $\sigma : \mathbb{N} \to \mathrm{PROP}$,
  - $\rho : \mathbb{N} \to \Sigma$ (alphabet of symbolic valuations)
- ϕ is satisfiable iff there is a symbolic model $\langle \sigma, \rho \rangle$ such that
  (a) $\langle \sigma, \rho \rangle \models_{\mathit{symb}} \phi$ (as for LTL)
  (b) ρ is realized in some concrete model.

- Construction of
  - a Büchi automaton for (a) (almost as for LTL).
  - a simple 1-$\mathbb{Z}$-counter automata over Σ for (b).

- Synchronization and nonemptiness checking can be done on the fly in PSPACE.

Nonemptiness of simple 1-$\mathbb{Z}$-counter automata

- Büchi acceptance condition, interpretation in $\mathbb{Z}$, alphabet, zero and sign tests.
- Theorem: The nonemptiness problem for simple 1-$\mathbb{Z}$-counter automata is NLOGSPACE-complete.
- Structure of the proof:
  - Reduction to the nonemptiness problem for simple 1-$\mathbb{N}$-counter automata without alphabet and test $x \neq 0$.
  - Nonemptiness for this class of automata amounts to check the existence of paths of polynomial length.

$\mathrm{CLTL}^2_1(\mathrm{DL})$ satisfiability is Σ^1_1-hard

- Reduction from the rec. problem for 2-$\mathbb{N}$-counter automata.
- The recurring problem for 2-$\mathbb{N}$-counter automata that change the value of at least one counter by transition is also Σ^1_1-hard.
- A configuration $\langle q_i, c_1, c_2 \rangle$ is encoded by

$$\overbrace{c_1, c_1 + c_2 + 1, \ldots, c_1, c_1 + c_2 + 1}^{i \text{ times}}$$

- New configuration detected by 4 consecutive values c, d, c', d' with either $c \neq c'$ or $d \neq d'$.
- For instance, "$c_2 = 0$?" is encoded by $\mathsf{X}x = x + 1$.

$\mathrm{CLTL}_2^1(\mathrm{DL})$ is also undecidable

- $\mathrm{CLTL}_1^2(\mathrm{DL})$ reduces to $\mathrm{CLTL}_2^1(\mathrm{DL})$.
- the model $\star \bullet \bullet \bullet \star \circ \star \circ \bullet \cdots$ is transformed into

$$\begin{pmatrix} \star \\ \bullet \end{pmatrix} \begin{pmatrix} \bullet \\ \bullet \end{pmatrix} \begin{pmatrix} \star \\ \circ \end{pmatrix} \begin{pmatrix} \star \\ \circ \end{pmatrix} \cdots$$

- Formulae are translated accordingly.
- $\mathrm{CLTL}_2^1(\mathrm{DL})$ satisfiability is Σ_1^1-complete.

Conclusion

- Our main contributions:
  - Satisfiability for $\mathrm{CLTL}_1^2(\mathrm{DL})$ is Σ_1^1-complete.
  - Model-checking $\mathrm{CLTL}_1^1(\mathrm{DL}^+)$ over 1-variable DL-automata is PSPACE-complete.
  - Model-checking $\mathrm{CLTL}_1^\omega(\mathrm{QFP})$ over 1-$\mathbb{Z}$-counter automata is PSPACE-complete (not discussed in the talk).
- Extension of PSPACE results to extensions of LTL that translates into Büchi automata with the same complexity.
- Side open problem: complexity of nonemptiness for 1-$\mathbb{N}$-counter automata.