

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 $\exists\text{EXPTIME}$.

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 $\exists\text{EXPTIME}$.

► Fragments

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

Syntax for CLTL(L)

- ▶ L is a fragment among DL, DL⁺, QFP.

- ▶ **Formulae:**

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

$$(E \in L)$$

- ▶ $\overbrace{XX \cdots X}^{i \text{ times}} x$ interpreted as the value of x at the i th next position.

- ▶ **Definitions**

- ▶ One-step constraint: $l_1, \dots, l_n \leq 1$.
- ▶ X-length of ϕ : maximal i such that $X^i x$ occurs in ϕ .

Semantics for Presburger LTL

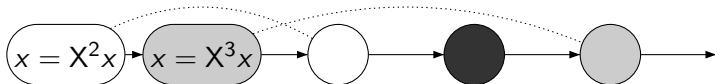
- ▶ **Models:** ω -sequences of valuations of the form $\text{VAR} \rightarrow \mathbb{Z}$.

Semantics for Presburger LTL

- ▶ **Models:** ω -sequences of valuations of the form $\text{VAR} \rightarrow \mathbb{Z}$.
- ▶ **Satisfaction relation:**
 - ▶ $\sigma, i \models E[x_1 \leftarrow X^{l_1} x_{j_1}, \dots, x_n \leftarrow X^{l_n} x_{j_n}]$ iff $(\sigma(i + l_1)(x_{j_1}), \dots, \sigma(i + l_n)(x_{j_n})) \models E$ in PA,
 - ▶ $\sigma, i \models X\phi$ iff $\sigma, i + 1 \models \phi$,
 - ▶ $\sigma, i \models \phi U \phi'$ 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 $\text{VAR} \rightarrow \mathbb{Z}$.
- ▶ **Satisfaction relation:**
 - ▶ $\sigma, i \models E[x_1 \leftarrow X^h x_{j_1}, \dots, x_n \leftarrow X^{l_n} x_{j_n}]$ iff $(\sigma(i + l_1)(x_{j_1}), \dots, \sigma(i + l_n)(x_{j_n})) \models E$ in PA,
 - ▶ $\sigma, i \models X\phi$ iff $\sigma, i + 1 \models \phi$,
 - ▶ $\sigma, i \models \phi U \phi'$ 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 $\text{CLTL}_k^l(L)$

- ▶ $\text{CLTL}_k^l(L)$ is the fragment of $\text{CLTL}(L)$ with
 - ▶ atomic formulae built from constraints in L ,
 - ▶ formulae use variables from $\{x_1, \dots, x_k\}$,
 - ▶ the term $X^i x$ can occur only if $i \leq l$.
- ▶ Examples
 - ▶ $x_1 = X^8 x_2 + 1$ belongs to $\text{CLTL}_2^8(\text{DL})$,
 - ▶ $X^2 x_1 \equiv_4 2$ belongs to $\text{CLTL}_1^2(\text{DL}^+) \cap \text{CLTL}_1^2(\text{QFP})$,
 - ▶ $\text{XXX}(5Xx_1 + 2x_2 \geq 27)$ belongs to $\text{CLTL}_2^1(\text{QFP})$.

k -variable L -automata

► Definition:

- Transitions of the form $q \xrightarrow{E} q'$ for one-step constraint E in L .
Examples: $q \xrightarrow{x > y + 1} q'$, $q_0 \xrightarrow{x = 0 \wedge y = 0} q$, $q \xrightarrow{\top} q$.
- Standard Büchi acceptance condition.
- Accepting runs of the form $\mathbb{N} \rightarrow Q \times \mathbb{Z}^k$.
- σ realizes $E_0 \cdot E_1 \cdots$ iff for every i , we have $\sigma, i \models E_i$.

k - \mathbb{Z} -counter automata

- ▶ Restriction of k -variable DL-automaton with constraints

$$\bigwedge_{i \in \{1 \dots k\}} E_{test^i} \wedge \bigwedge_{i \in \{1 \dots k\}} E_{update^i}$$

with

- ▶ $E_{test^i} \in \{\top\} \cup \{x_i \sim 0 \mid \sim \in \{<, >, =, \neq\}\}$,
- ▶ $E_{update^i} \in \{\neg x_i = x_i + u \mid u \in \mathbb{Z}\}$
- ▶ Initial values of the counters are zero.
- ▶ Simple \mathbb{Z} -counter automata: updates in $\{0, -1, 1\}$.

Model checking problems

- ▶ Model-checking $\text{CLTL}'_k(L)$ formulae over a class \mathcal{C} of automata:
 - ▶ Input: a k -variable automaton \mathcal{A} in \mathcal{C} and a formula in $\text{CLTL}'_k(L)$.
 - ▶ Question: Is there a model σ that realizes a word accepted by \mathcal{A} and such that $\sigma, 0 \models \phi$?
- ▶ Model-checking $\text{CLTL}'_3(\text{DL})$ over the class of 3- \mathbb{N} -automata is Σ_1^1 -complete. [Alur & Henzinger, JACM 94]

CLTL₃¹(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 “ $n : C_1 := C_1 + 1$; goto either n' or n'' ” is encoded by

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

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

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

$(\text{CLTL}_k^l(L)$: k variables, “next length” $\leq l$, fragment L)

	MC (DL)	SAT	MC (CA)
$\text{CLTL}_3^1(\text{DL})$	U	U	U
$\text{CLTL}_2^\omega(\text{DL})$	U	U	U
$\text{CLTL}_1^2(\text{DL})$	U	U	PSPACE-c
$\text{CLTL}_2^1(\text{DL})$	U	U	U
$\text{CLTL}_1^1(\text{DL or DL}^+)$	PSPACE-c.	PSPACE-c.	PSPACE-c
$\text{CLTL}_1^1(\text{QFP})$	U	U	PSPACE-c
$\text{CLTL}_1^\omega(\text{QFP})$	U	U	PSPACE-c.

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

- ▶ Model-checking for $\text{CLTL}_1^1(\text{DL}^+)$ reduces to satisfiability for $\text{CLTL}_1^1(\text{DL}^+, \text{PROP})$ (addition of propositions).
- ▶ Maps $\{x, Xx\} \rightarrow \mathbb{Z}$ 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

- ▶ $\langle E_x, E_m, E'_x, E'_m, E_s \rangle \in C_x \times \text{Mod}_x \times C_{Xx} \times \text{Mod}_{Xx} \times C_{\text{step}}$.
- ▶ For $t \in \{x, Xx\}$
 - ▶ C_t :
 - ▶ $(d_i < t) \wedge (t < d_{i+1})$ for $i \in \{\min, \dots, \max - 1\}$,
 - ▶ $t = d_i$ for $i \in \{\min, \dots, \max\} + t < d_{\min}$ and $d_{\max} < t$,
 - ▶ Mod_t : $t \equiv_K c$ for $c \in \{0, \dots, K - 1\}$,
 - ▶ C_{step} :
 - ▶ $x + e_i < Xx \wedge Xx < x + e_{i+1}$ for $i \in \{\min', \dots, \max' - 1\}$,
 - ▶ $Xx = x + e_i$ for $i \in \{\min', \dots, \max'\} + Xx < x + e_{\min'}$ and $x + e_{\max'} < Xx$.

Satisfiability and symbolic models

- ▶ Symbolic model $\langle \sigma, \rho \rangle$:
 - ▶ $\sigma : \mathbb{N} \rightarrow \text{PROP}$,
 - ▶ $\rho : \mathbb{N} \rightarrow \Sigma$ (alphabet of symbolic valuations)
- ▶ ϕ is satisfiable iff there is a symbolic model $\langle \sigma, \rho \rangle$ such that
 - (a) $\langle \sigma, \rho \rangle \models_{\text{symb}} \phi$ (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.

CLTL₁²(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

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

- ▶ 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 $Xx = x + 1$.

CLTL₂¹(DL) is also undecidable

- ▶ CLTL₁²(DL) reduces to CLTL₂¹(DL).
- ▶ the model $\star \bullet \bullet \bullet \star \circ \star \circ \bullet \dots$ is transformed into

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

- ▶ Formulae are translated accordingly.
- ▶ CLTL₂¹(DL) satisfiability is Σ_1^1 -complete.

Conclusion

- ▶ Our main contributions:
 - ▶ Satisfiability for $\text{CLTL}_1^2(\text{DL})$ is Σ_1^1 -complete.
 - ▶ Model-checking $\text{CLTL}_1^1(\text{DL}^+)$ over 1-variable DL-automata is PSPACE-complete.
 - ▶ Model-checking $\text{CLTL}_1^\omega(\text{QFP})$ 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.