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 $\Sigma_1^1$-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 $3\text{EXPTIME}$. 
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 $3\text{EXPTIME}$.

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

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

- Formulae:
  \[
  \phi ::= E[x_1 \leftarrow X^{l_1}x_{j_1}, \ldots, x_n \leftarrow X^{l_n}x_{j_n}] \mid \phi \land \phi \mid \neg \phi \mid X\phi \mid \phi U \phi
  \]
  \((E \in L)\)

  $i$ times

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

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

S. Demri, R. Gascon  
The Effects of Bounding Syntactic Resources on Presburger LTL
Semantics for Presburger LTL

- **Models**: $\omega$-sequences of valuations of the form $\text{VAR} \rightarrow \mathbb{Z}$. 
Semantics for Presburger LTL

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

- **Satisfaction relation:**
  
  - $\sigma, i \models E[x_1 \leftarrow X_1 l_1 x_{j_1}, \ldots, x_n \leftarrow X_n l_n x_{j_n}]$ iff $(\sigma(i + l_1)(x_{j_1}), \ldots, \sigma(i + l_n)(x_{j_n})) \models E$ 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:** \( \omega \)-sequences of valuations of the form \( \text{VAR} \rightarrow \mathbb{Z} \).

- **Satisfaction relation:**
  - \( \sigma, i \models E[ x_1 \leftarrow X_1 x_1, \ldots, x_n \leftarrow X_n x_n ] \) iff \( (\sigma(i + l_1)(x_1), \ldots, \sigma(i + l_n)(x_n)) \models E \) 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 \( \sigma, k \models \phi \).

![Diagram](image-url)
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 $\{x_1, \ldots, x_k\}$,
  - 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 $\text{CLTL}_1^2(\text{DL}^+) \cap \text{CLTL}_1^2(\text{QFP})$,
- $XXX(5Xx_1 + 2x_2 \geq 27)$ 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: $q \xrightarrow{x > y + 1} q'$, $q_0 \xrightarrow{x = 0 \land y = 0} q$, $q \xrightarrow{\top} q$.

- Standard Büchi acceptance condition.

- Accepting runs of the form $\mathbb{N} \to Q \times \mathbb{Z}^k$.

- $\sigma$ 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

\[
\bigwedge_{i \in \{1\ldots k\}} E_{test}^i \land \bigwedge_{i \in \{1\ldots k\}} E_{update}^i
\]

with

- $E_{test}^i \in \{\top\} \cup \{x_i \sim 0 \mid \sim \in \{<, >, =, \neq\}\}$,

- $E_{update}^i \in \{\forall x_i = x_i + u \mid u \in \mathbb{Z}\}$

- Initial values of the counters are zero.

- Simple $\mathbb{Z}$-counter automata: updates in $\{0, -1, 1\}$. 

S. Demri, R. Gascon

The Effects of Bounding Syntactic Resources on Presburger LTL
Model checking problems

- Model-checking $\text{CLTL}_k^1(L)$ formulae over a class $C$ of automata:
  - Input: a $k$-variable automaton $A$ in $C$ and a formula in $\text{CLTL}_k^1(L)$.
  - Question: Is there a model $\sigma$ that realizes a word accepted by $A$ and such that $\sigma, 0 \models \phi$?

- Model-checking $\text{CLTL}_3^1(\text{DL})$ over the class of 3-$\mathbb{N}$-automata is $\Sigma_1^1$-complete. [Alur & Henzinger, JACM 94]
$\mathcal{CLTL}_3^{1}(\mathcal{DL})$ satisfiability is $\Sigma^1_1$-complete

- Reduction from the recurring problem for nondeterministic Minsky machines.

- $\Sigma^1_1$-hardness from [Alur & Henzinger, JACM 94].

- The instruction “$n : C_1 := C_1 + 1; \text{goto either } n' \text{ or } n''$” is encoded by

  $$G(x_{\text{inst}} = n \Rightarrow (Xx_1 = x_1 + 1 \land Xx_2 = x_2 \land (Xx_{\text{inst}} = n' \lor Xx_{\text{inst}} = n'')))$$

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

S. Demri, R. Gascon  The Effects of Bounding Syntactic Resources on Presburger LTL
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

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

<table>
<thead>
<tr>
<th></th>
<th>MC (DL)</th>
<th>SAT</th>
<th>MC (CA)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{CLTL}^1_3(DL)$</td>
<td>U</td>
<td>U</td>
<td>U</td>
</tr>
<tr>
<td>$\text{CLTL}^\omega_2(DL)$</td>
<td>U</td>
<td>U</td>
<td>U</td>
</tr>
<tr>
<td>$\text{CLTL}^2_1(DL)$</td>
<td>U</td>
<td>U</td>
<td>PSPACE-c</td>
</tr>
<tr>
<td>$\text{CLTL}^1_2(DL)$</td>
<td>U</td>
<td>U</td>
<td>U</td>
</tr>
<tr>
<td>$\text{CLTL}^1_1(DL \text{ or } DL^+)$</td>
<td>PSPACE-c.</td>
<td>PSPACE-c.</td>
<td>PSPACE-c</td>
</tr>
<tr>
<td>$\text{CLTL}^1_1(QFP)$</td>
<td>U</td>
<td>U</td>
<td>PSPACE-c</td>
</tr>
<tr>
<td>$\text{CLTL}^\omega_1(QFP)$</td>
<td>U</td>
<td>U</td>
<td>PSPACE-c.</td>
</tr>
</tbody>
</table>
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 $\omega$-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 \( t \in \{x, Xx\} \)
  - \( C_t: \)
    - \((d_i < t) \land (t < d_{i+1})\) for \( i \in \{\text{min}, \ldots, \text{max} - 1\},\)
    - \( t = d_i \) for \( i \in \{\text{min}, \ldots, \text{max}\} + t < d_{\text{min}} \) and \( d_{\text{max}} < t,\)
  - \( \text{Mod}_t: t \equiv_K c \) for \( c \in \{0, \ldots, K - 1\},\)
  - \( C_{\text{step}}: \)
    - \( x + e_i < Xx \land Xx < x + e_{i+1} \) for \( i \in \{\text{min}', \ldots, \text{max}' - 1\},\)
    - \( Xx = x + e_i \) for \( i \in \{\text{min}', \ldots, \text{max}'\} + Xx < x + e_{\text{min}'} \) and \( x + e_{\text{max}'} < Xx.\)
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)

- $\phi$ is satisfiable iff there is a symbolic model $\langle \sigma, \rho \rangle$ such that
  1. $\langle \sigma, \rho \rangle \models_{\text{symb}} \phi$ (as for LTL)
  2. $\rho$ 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 $\Sigma$ 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 $\text{NLOGSPACE}$-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.
\[ \text{CLTL}_1^2(\text{DL}) \text{ satisfiability is } \Sigma_1^1 \text{-hard} \]

- 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 \(\Sigma_1^1\)-hard.
- A configuration \(\langle q_i, c_1, c_2 \rangle\) is encoded by

\[
\begin{array}{c}
\text{i times} \\
\{ c_1, c_1 + c_2 + 1, \ldots, c_1, c_1 + c_2 + 1 \}
\end{array}
\]

- New configuration detected by 4 consecutive values \(c, d, c', d'\) with either \(c \neq c'\) or \(d \neq d'\).
- For instance, \(\text{“c}_2 = 0?\) “ is encoded by \(Xx = x + 1\).
\( \text{CLTL}^1_2(\text{DL}) \) is also undecidable

- \( \text{CLTL}^2_1(\text{DL}) \) reduces to \( \text{CLTL}^1_2(\text{DL}) \).
- the model \( \star \bullet \bullet \star \circ \circ \bullet \cdots \) is transformed into
  \[
  \left( \star \right) \left( \bullet \right) \left( \star \right) \left( \circ \right) \left( \circ \right) \cdots
  \]
- Formulae are translated accordingly.
- \( \text{CLTL}^1_2(\text{DL}) \) satisfiability is \( \Sigma^1_1 \)-complete.
Conclusion

Our main contributions:

- Satisfiability for $\text{CLTL}_1^2(\text{DL})$ is $\Sigma_1^1$-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.