Branching Time Logics & Flat Counter Systems

Amit Kumar Dhar
LIAFA, Université Paris Diderot, Paris.

Highlights Conference, 2014.

Joint Work With:

Stéphane Demri,
NYU, New York.

Arnaud Sangnier
LIAFA, Université Paris Diderot, Paris.
Model-Checking \(\{\text{CTL}^*, \text{CTL}, \text{CTL}_{\text{EF}}\}\) over Flat Counter Systems is Equivalent to

Satisfiability of Presburger Arithmetic.
Counters: \( \{c_1, c_2, \ldots, c_n\} \)

Updates: \( u \in \mathbb{Z}^n \).

Guards: Boolean Combination of arithmetic constraints

\[
2c_1 + 5c_2 - c_3 \quad \{\leq, \geq, <, >\}
\] 5.
No intersecting/nested loops in the structure.
Can still be used to model some systems e.g. Broadcast Protocols  
[Finkel, Leroux - FSTTCS'02, Fribourg, Olsén - LOPSTR'96]

Under-approximation of model-checking of counter systems.  
[Boigelot - 98, Comon, Jurski - CAV'98, Leroux, Sutre - ATVA'05]

Decidable Model checking for some logics (Presburger CTL*).  
[Demri et al. - JANCL’10]

Optimal complexity of Model checking for many linear-time logics known (LTL with Past, FO, linear $\mu$-calculus).  
[Demri, Dhar, sangnier - IJCAR’12, Demri, Dhar, Sangnier - ICALP’13]

Checking safety property on flat systems with octagonal loop is NP-Complete.  
[Bozga, Iosif, Konceny - VMCAI’14]
Specification ➔ Syntax

Computation Tree Logic (CTL)
\[ \phi := p \mid g \mid \neg \phi \mid \phi \lor \phi \mid \text{EX}\phi \mid \text{AX}\phi \mid E[\phi U \phi] \mid A[\phi U \phi]. \]

Computation Tree Logic* (CTL*)
\[ \phi := p \mid g \mid \neg \phi \mid \phi \lor \phi \mid \text{X}\phi \mid \phi U \phi \mid E\phi. \]

Computation Tree Logic with only EF (CTL_{EF})
\[ \phi := p \mid g \mid \neg \phi \mid \phi \lor \phi \mid \text{EF}\phi. \]

★ Each contains counter constraints
**Problem ▶ Model Checking**

**MC (L, FCS)**

**INPUT:** A flat counter system $s$, a specification $\mathcal{A}$ in logic L, a configuration $\langle q_0, v_0 \rangle$.

**OUTPUT:** Does there exists an execution $\rho$ starting with $\langle q_0, v_0 \rangle$ in $s$ such that $\rho, 0 \models \mathcal{A}$?
Simpler Models

Path Schemas

Path schemas are an alternating sequence of paths and loops, e.g.,

\[ \langle P; m \rangle + \langle P; (2) \rangle \]

A concise way of representing infinite runs, \( \langle \text{Path schema}; m \rangle \) denotes the number of times loops are taken.

At most exponentially many minimal paths schemas in flat counter systems [Leroux, Sutre-ATVA'05].
Path Schemas - an alternating sequence of paths and loops -
\[ P = (t_1 t_2)(t_3 t_4)^+(t_5)(t_6)^\omega \]

A concise way of representing infinite runs = \langle \text{Path schema}, m \rangle
- \( m \) denotes the number of times loops are taken - \langle P, (2) \rangle

At most exponentially many \textit{minimal} path schemas in flat counter systems [Leroux, Sutre - ATVA'05].
MC(CTL*, FCS) \rightarrow \text{Reduction}

MC(CTL*, FCS)

Reduction (modulo LogSpace)

Satisfiability of Presburger Arithmetic
\[ MC(\text{CTL}^*, \text{FCS}) \] 

**Encoding Run**

\[ \delta_3 \cdot \delta_6 \cdot (l_2)^{146} \cdot \delta_8 \cdot (l_3)^\omega = \begin{cases} 
    v_p = (3, 6, 2, 8, 3, 0, 0, 0, 0, 0, 0) \\
    v_t = (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \\
    v_{it} = (1, 1, 146, 1, 0, 0, 0, 0, 0, 0, 0) 
\end{cases} \]

\[ \phi_{ps} - \text{Characterizing the properties of path schema} \]

\[ \bigvee_{i=1}^{8} ((x_t^i = 1 \land x_t^{i+2} = 1) \land (x_p^i > 0 \land x_p^{i+2} > 0)) \Rightarrow (x_t^{i+1} = 0) \]
**MC(CTL*, FCS)**

**Encoding Run**

$$\MC(CTL^*, FCS) \xrightarrow{\text{Encoding Run}}$$

\[\phi_{\text{run}} - \text{Characterizing the runs through path schema}\]

$$\forall i > 0. update(v_p, v_t, v_{it})[1 \ldots i] \geq 0$$

\[
\begin{align*}
\delta_3 \cdot \delta_6 \cdot (l_2)^{146} \cdot \delta_8 \cdot (l_3)^{\omega} &= \begin{cases} 
v_p = (3, 6, 2, 8, 3, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) 
v_t = (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) 
v_{it} = (1, 1, 146, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \end{cases}
\end{align*}
\]
Encoding Run

\( \phi_{CTL^*} \) - Encoding the \( CTL^* \) formula [Demri et al. - JANCL’10]

\[
\phi = \exists x_p^1 \cdots x_p^{10}, x_t^1 \cdots x_t^{10}, x_{it}^1 \cdots x_{it}^{10} \cdot (\phi_{ps} \land \phi_{run} \land \phi_{CTL^*})
\]
Polynomial-time reduction compared to exponential time reduction known from [Demri et al. - JANCL’10].

- No enumeration of path schemas in formula.
- Encoding runs using a constant number of fixed size integer vectors.
- Utilizing the power of quantifiers in an essential way.
Satisfiability of Presburger Arithmetic

\[ Q_1 x_1 Q_2 x_2 \cdots Q_n x_n \phi(x_1, x_2, \ldots, x_n) \]

Reduction (modulo LogSpace)

MC(CTL_{EF}, FCS)

\[
\begin{align*}
q_0 & \rightarrow q_1 \xrightarrow{x_1++} q_1 \xrightarrow{x_2++} q_2 \xrightarrow{x_n++} q_n \\
\exists & \quad \text{EF} \\
\forall & \quad \text{AG}
\end{align*}
\]
Branching-Time Overview

\[ MC(\text{CTL}^*, \text{FCS}) \]
\[ \Downarrow \]
\[ MC(\text{CTL}, \text{FCS}) \]
\[ \Downarrow \]
\[ MC(\text{CTL}_{EF}, \text{FCS}) \]
\[ \Downarrow \]

Satisfiability of Presburger arithmetic
[RP'14]

MC(Modal \mu-calculus, FCS) ??
Thank You
For Your Kind Attention