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.

CNRS,
France.

Arnaud Sangnier

LIAFA, Université Paris Diderot,
Paris.

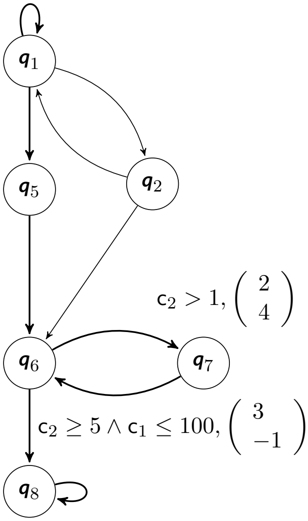
Model-Checking $\{\mathrm{CTL}^\star, \mathrm{CTL}, \mathrm{CTL}_{\mathsf{EF}}\}$

over Flat Counter Systems

is Equivalent to

Satisfiability of Presburger Arithmetic.

Models 〉 Counter Systems



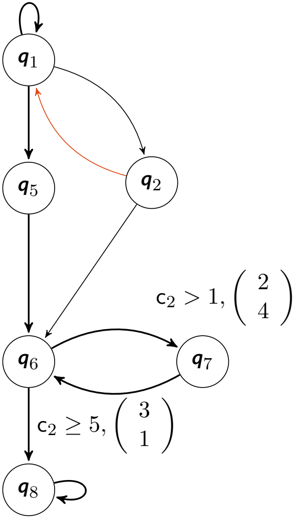
Counters : $\{c_1, c_2, \ldots, c_n\}$

Updates : $\mathbf{u} \in \mathbb{Z}^n$.

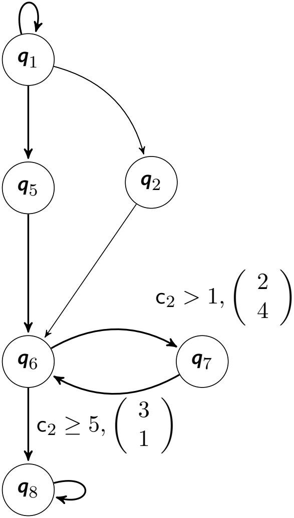
Guards : Boolean Combination of
arithmetic constraints
$2.c_1 + 5.c_2 - c_3 \;\; \{\leq, \geq, <, >\} \;\; 5.$

Models 〉 Flat Counter Systems

No intersecting/nested loops in the structure.



Non-Flat



Flat

Models 〉 Flat Counter Systems

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 $\mathrm{CTL}^{\star}$).
[Demri et al. - JANCL'10]

Optimal complexity of Model checking for many linear-time logics known (LTL with Past, FO, linear μ-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)

$\phi := \boldsymbol{p} \mid \mathsf{g} \mid \neg\phi \mid \phi \vee \phi \mid \mathsf{EX}\phi \mid \mathsf{AX}\phi \mid \mathsf{E}[\phi \mathsf{U} \phi] \mid \mathsf{A}[\phi \mathsf{U} \phi].$

Computation Tree Logic⋆ (CTL*)

$\phi := \boldsymbol{p} \mid \mathsf{g} \mid \neg\phi \mid \phi \vee \phi \mid \mathsf{X}\phi \mid \phi \mathsf{U} \phi \mid \mathsf{E}\phi.$

Computation Tree Logic with only EF (CTL$_{\mathsf{EF}}$)

$\phi := \boldsymbol{p} \mid \mathsf{g} \mid \neg\phi \mid \phi \vee \phi \mid \mathsf{EF}\phi.$

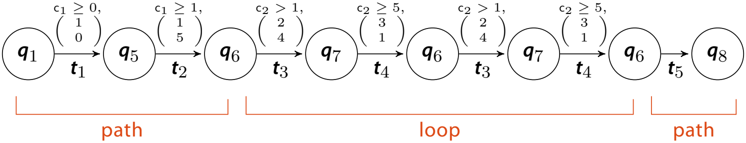
⋆ Each contains counter constraints

MC (L, FCS)

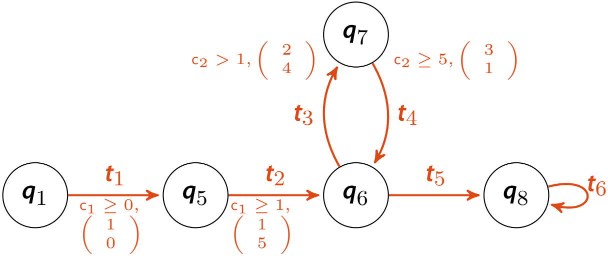
INPUT : A flat counter system $\boldsymbol{S}$, a specification $\mathcal{A}$ in logic L, a configuration $\langle \boldsymbol{q}_0, \mathbf{v}_0 \rangle$.

OUTPUT : Does there exists an execution ρ starting with $\langle \boldsymbol{q}_0, \mathbf{v}_0 \rangle$ in $\boldsymbol{S}$ such that $\rho, 0 \models \mathcal{A}$?

Simpler Models 〉 Path Schemas



Simpler Models 〉 Path Schemas



- Path Schemas - an alternating sequence of paths and loops -
  $\boldsymbol{P} = (\boldsymbol{t}_1\boldsymbol{t}_2)(\boldsymbol{t}_3\boldsymbol{t}_4)^+(\boldsymbol{t}_5)(\boldsymbol{t}_6)^\omega$
- A concise way of representing infinite runs = $\langle$Path schema, $\mathbf{m}\rangle$
  - **m** denotes the number of times loops are taken - $\langle \boldsymbol{P}, (2)\rangle$
- At most exponentially many *minimal* path schemas in flat counter systems [Leroux, Sutre - ATVA'05].

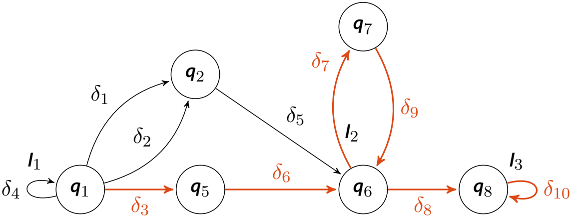
MC(CTL*,FCS) 〉 Reduction

MC(CTL*,FCS)

↓ **Reduction (modulo LogSpace)**

Satisfiability of Presburger Arithmetic

 Encoding Run

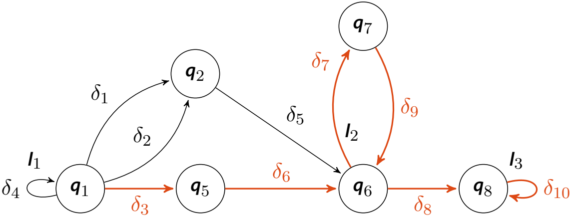


$$\delta_3 \cdot \delta_6 \cdot (l_2)^{146} \cdot \delta_8 \cdot (l_3)^{\omega} = \begin{cases} \mathbf{v}_p = (3,6,2,8,3,0,0,0,0,0,0,0,0) \\ \mathbf{v}_t = (0,0,1,0,1,0,0,0,0,0,0,0,0) \\ \mathbf{v}_{it} = (1,1,146,1,0,0,0,0,0,0,0,0,0) \end{cases}$$

ϕ_{ps} - Characterizing the properties of path schema

$$\bigvee_{i=1}^{8} ((\mathsf{x}_t^i = 1 \wedge \mathsf{x}_t^{i+2} = 1) \wedge (\mathsf{x}_p^i > 0 \wedge \mathsf{x}_p^{i+2} > 0)) \Rightarrow (\mathsf{x}_t^{i+1} = 0)$$

MC(CTL*,FCS) 〉 Encoding Run

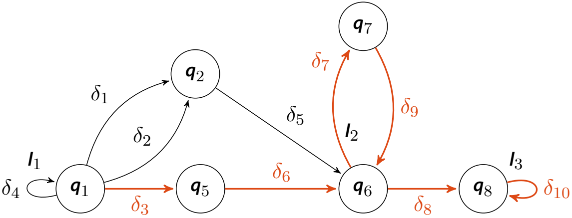


$$\delta_3 \cdot \delta_6 \cdot (l_2)^{146} \cdot \delta_8 \cdot (l_3)^{\omega} = \begin{cases} \mathbf{v}_p = (3,6,2,8,3,0,0,0,0,0,0,0,0) \\ \mathbf{v}_t = (0,0,1,0,1,0,0,0,0,0,0,0,0) \\ \mathbf{v}_{it} = (1,1,146,1,0,0,0,0,0,0,0,0,0) \end{cases}$$

ϕ_{run} - Characterizing the runs through path schema

$$\forall i > 0.\,update(\mathbf{v}_p, \mathbf{v}_t, \mathbf{v}_{it})[1 \ldots i] \geq 0$$

Encoding Run



$$\delta_3 \cdot \delta_6 \cdot (l_2)^{146} \cdot \delta_8 \cdot (l_3)^{\omega} = \begin{cases} \mathbf{v}_p = (3,6,2,8,3,0,0,0,0,0,0,0,0) \\ \mathbf{v}_t = (0,0,1,0,1,0,0,0,0,0,0,0,0) \\ \mathbf{v}_{it} = (1,1,146,1,0,0,0,0,0,0,0,0,0) \end{cases}$$

$\phi_{\mathrm{CTL}^\star}$ - Encoding the $\mathrm{CTL}^\star$ formula [Demri et al. - JANCL'10]

$$\phi = \exists \mathsf{x}_p^1 \cdots \mathsf{x}_p^{10}, \mathsf{x}_t^1 \cdots \mathsf{x}_t^{10}, \mathsf{x}_{it}^1 \cdots \mathsf{x}_{it}^{10}.(\phi_{ps} \wedge \phi_{run} \wedge \phi_{\mathrm{CTL}^\star})$$

Complexity

- 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.

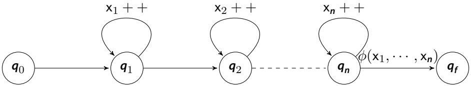
Satisfiability of Presburger Arithmetic

$$Q_1 x_1 Q_2 x_2 \cdots Q_n x_n \phi(x_1, x_2, \cdots, x_n)$$

Reduction

(modulo LogSpace)

MC(CTL$_{EF}$,FCS)



$\exists$	EF
$\forall$	AG

$\text{MC}(\textsc{ctl}^\star,\text{FCS})$

$\updownarrow$

$\text{MC}(\textsc{ctl},\text{FCS})$

$\updownarrow$

$\text{MC}(\textsc{ctl}_{\text{EF}},\text{FCS})$

$\updownarrow$

Satisfiability of Presburger arithmetic
[RP'14]

MC(Modal μ-calculus, FCS) ??

Thank You

For Your Kind Attention