Model Checking Flat Counter Systems

Amit Kumar Dhar

LIAFA, Univ Paris Diderot, Sorbonne Paris Cité, France

Phd Advisors:

Stéphane Demri (NYU,LSV)

Arnaud Sangnier (LIAFA)

MoVeP 2012, Student Session

Model Checking

Models (Abstraction of programs)

Labelled Transition Systems

Counter Systems

Multi-pushdown Systems

Model Checking

Models (Abstraction of programs)

Labelled Transition Systems

Counter Systems

Multi-pushdown Systems

Specification (Prop. of executions)

Logical Formulas

Automata

ω-regular expressions

Model Checking

Models (Abstraction of programs)

Labelled Transition Systems

Counter Systems

Multi-pushdown Systems

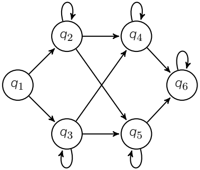
Specification (Prop. of executions)

Logical Formulas

Automata

ω-regular expressions

Model Checking



$\models \quad \phi$

$\mathrm{MC}(\mathrm{L}, \mathcal{C})$ -

Input:

a model *M*, (from $\mathcal{C}$)

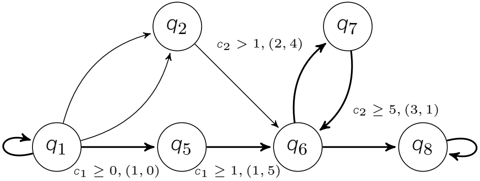
a specification ϕ (formula in logic L)

Output:

Does there exist an execution ρ of *M* such that $\rho \models \phi$ (or $\rho \in \mathcal{L}(\phi)$)?

Flat Counter Systems

Flat Counter System



$\langle Q, \mathsf{C}_n, \Delta, \mathbf{l} \rangle$:

C_n : n counters

$\mathbf{l} : Q \rightarrow 2^{\mathrm{AT}}$

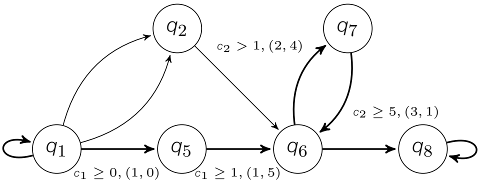
$\Delta \subseteq Q \times \mathtt{G}(\mathsf{C}_n) \times \mathbb{Z}^n \times Q$

$\mathtt{t} ::= a.\mathrm{x} \mid \mathtt{t} + \mathtt{t}$

$\mathtt{g} ::= \mathtt{t} \sim b \mid \mathtt{g} \wedge \mathtt{g} \mid \mathtt{g} \vee \mathtt{g}$

Flat Counter Systems

Flat Counter System



$\langle Q, \mathtt{C}_n, \Delta, \mathbf{l} \rangle$**:**

$\mathtt{C}_n$: n counters

$\mathbf{l} : Q \rightarrow 2^{\mathrm{AT}}$

$\Delta \subseteq Q \times \mathtt{G}(\mathtt{C}_n) \times \mathbb{Z}^n \times Q$

$\mathtt{t} ::= a.x \mid \mathtt{t} + \mathtt{t}$

$\mathtt{g} ::= \mathtt{t} \sim b \mid \mathtt{g} \wedge \mathtt{g} \mid \mathtt{g} \vee \mathtt{g}$

Runs in Flat Counter Systems

$$\langle q_1, (0,0) \rangle \longrightarrow \langle q_1, (0,0) \rangle \longrightarrow \langle q_5, (1,0) \rangle \longrightarrow \langle q_6, (2,5) \rangle \longrightarrow \langle q_7, (4,9) \rangle \longrightarrow \langle q_6, (7,10) \rangle$$

Specifications

Linear Temporal Logic with Past

Syntax

$\phi ::= p \mid \mathtt{g} \mid \neg\phi \mid \phi \wedge \phi' \mid \phi \vee \phi' \mid \mathtt{X}\phi \mid \phi\mathtt{U}\phi' \mid \mathtt{X}^{-1}\phi \mid \phi\mathtt{S}\phi'$
where, $p \in \mathrm{AT}, \mathtt{g} \in \mathtt{G}(\mathtt{C}_n)$

Semantics

$\sigma \in (Q \times \mathbb{N}^n)^\omega$
$\mathbf{l} : Q \to 2^{\mathrm{AT}}$

$\sigma, i \models p \Leftrightarrow p \in \mathbf{l}(\pi_1(\sigma(i)))$
$\sigma, i \models \mathtt{g} \Leftrightarrow \pi_2(\sigma(i)) \models \mathtt{g}$

Example

$(p \wedge \mathsf{x}_1 < 10)\mathtt{U}(\mathsf{x}_2 = 20)$

First Order Logic & Büchi Automata

Syntax

$\phi ::= P_a(z) \mid P_{\mathsf{g}}(z) \mid S(z_1, z_2) \mid z_1 < z_2 \mid z_1 = z_2 \mid \neg\phi \mid \phi \wedge \phi' \mid \exists z\, \phi(z)$
where, $a \in \mathrm{AT}$ and $\mathsf{g} \in \mathsf{G}(\mathsf{C}_n)$

Semantics

$\sigma \in (Q \times \mathbb{N}^n)^\omega$
$\mathbf{l} : Q \to 2^{\mathrm{AT}}$

$\sigma \models_f P_a(z) \Leftrightarrow a \in \pi_1(\sigma(f(z)))$
$\sigma \models_f P_{\mathsf{g}}(z) \Leftrightarrow \pi_2(\sigma(f(z))) \models \mathsf{g}$

First Order Logic & Büchi Automata

Syntax

$\phi ::= P_a(\mathsf{z}) \mid P_{\mathsf{g}}(\mathsf{z}) \mid S(\mathsf{z}_1, \mathsf{z}_2) \mid \mathsf{z}_1 < \mathsf{z}_2 \mid \mathsf{z}_1 = \mathsf{z}_2 \mid \neg\phi \mid \phi \wedge \phi' \mid \exists \mathsf{z}\, \phi(\mathsf{z})$

where, $a \in \mathrm{AT}$ and $\mathsf{g} \in \mathsf{G}(\mathsf{C}_n)$

Semantics

$\sigma \in (Q \times \mathbb{N}^n)^\omega$

$\mathbf{l} : Q \to 2^{\mathrm{AT}}$

$\sigma \models_f P_a(\mathsf{z}) \Leftrightarrow a \in \pi_1(\sigma(f(\mathsf{z})))$

$\sigma \models_f P_{\mathsf{g}}(\mathsf{z}) \Leftrightarrow \pi_2(\sigma(f(\mathsf{z}))) \models \mathsf{g}$

Büchi Automata

$\mathcal{B} = \langle Q, \Sigma, q_0, \Delta, F \rangle$

$\Sigma = 2^{\mathrm{AT}} \times 2^{\mathsf{G}(\mathsf{C}_n)}$

$\sigma \in (2^{\mathrm{AT}} \times \mathbb{N}^n)^\omega$

$\sigma \models \mathcal{B}$ iff $\sigma \in \mathcal{L}(\mathcal{B})$

Main Contributions…

Contributions

Model Checking PLTL [DDS'12]

$\mathrm{MC}(\mathit{PLTL}, \mathtt{CFS})$ is NP-Complete.

Contributions

Model Checking PLTL [DDS'12]

$\mathrm{MC}(\mathit{PLTL}, \mathtt{CFS})$ is NP-Complete.

Model Checking Büchi Automaton

$\mathrm{MC}(\mathit{BA}, \mathtt{CFS})$ is NP-Complete.

Contributions

Model Checking PLTL [DDS'12]

$\mathrm{MC}(\mathit{PLTL}, \mathtt{CFS})$ is NP-Complete.

Model Checking Büchi Automaton

$\mathrm{MC}(\mathit{BA}, \mathtt{CFS})$ is NP-Complete.

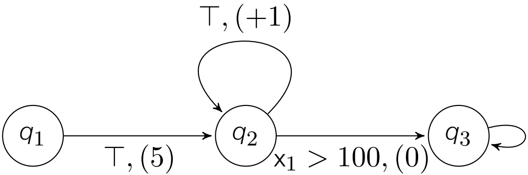
Model Checking FO

$\mathrm{MC}(\mathit{FO}, \mathtt{CFS})$ is PSpace-Complete.

How We Do It…

Input

Flat Counter System

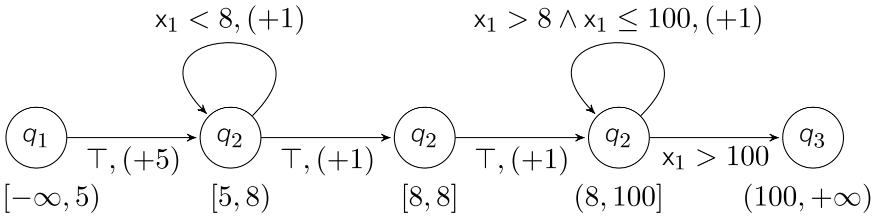


Formula with Counters

$\phi = \mathsf{F}(x_1 > 8 \wedge \mathsf{X}q_2)$

Eliminate Counters From Formula

Path Schema

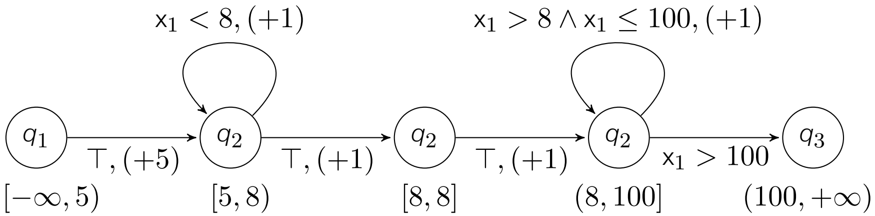


Formula with Counters

$\phi = \mathsf{F}(\mathsf{x}_1 > 8 \wedge \mathsf{X} q_2)$

Eliminate Counters From Formula

Path Schema

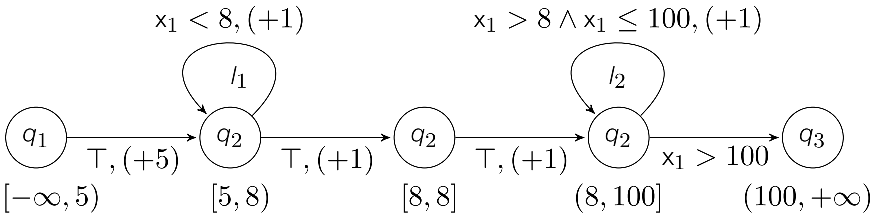


Formula without Counters

$\phi = \mathsf{F}(P_{\mathsf{x}_1>8} \wedge \mathsf{X}q_2)$

Applying Stuttering Theorem

Path Schema



Formula without Counters

$\phi = \mathsf{F}(P_{x_1 > 8} \wedge \mathsf{X} q_2)$

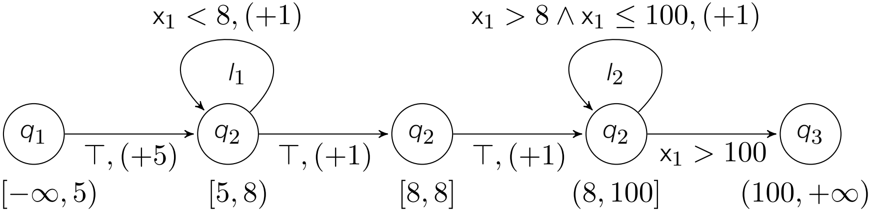
Stuttering Theorem

$l_1 \geq 0$

$l_2 \geq 2$

Applying Stuttering Theorem

Path Schema



Formula without Counters

$\phi = \mathsf{F}(P_{x_1 > 8} \wedge \mathsf{X} q_2)$

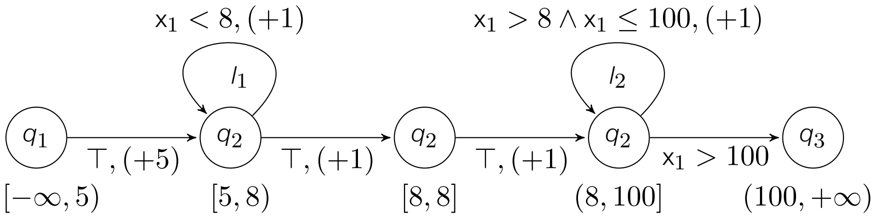
Stuttering Theorem

$l_1 = 2$

$l_2 = 9$

Constraint System

Path Schema



Formula without Counters

$\phi = \mathsf{F}(P_{x_1 > 8} \wedge \mathsf{X} q_2)$

Constraint System

$5 + 1.(l_1 - 1) < 8$

$5 + 1.(l_1) + 2 > 8$

$5 + 1.(l_1) + 2 \leq 100$

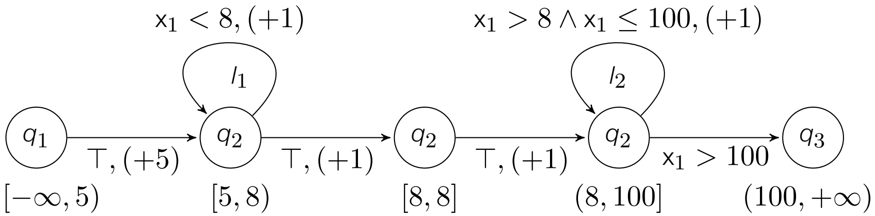
$5 + 1.(l_1) + 2 + 1.(l_2 - 1) > 8$

$5 + 1.(l_1) + 2 + 1.(l_2 - 1) \leq 100$

$l_2 \geq 9 \; , \; l_1 = 2$

Small Solution

Path Schema



Formula without Counters

$\phi = \mathsf{F}(P_{x_1 > 8} \wedge \mathsf{X} q_2)$

Small Solution

$$l_1 = 2$$
$$l_2 = 91$$

Constraint System

$$5 + 1.(l_1 - 1) < 8$$
$$5 + 1.(l_1) + 2 > 8$$
$$5 + 1.(l_1) + 2 \leq 100$$
$$5 + 1.(l_1) + 2 + 1.(l_2 - 1) > 8$$
$$5 + 1.(l_1) + 2 + 1.(l_2 - 1) \leq 100$$
$$l_2 \geq 9, l_1 = 2$$

Eventually…

Other Logics

Linear μ-Calculus (done),
Monadic Second Order Logic,
Branching Time Logics,
Freeze LTL…

Other Models

Affine Updates,
Relational Counter Systems,
etc.

Implementation

Implementing a prototype using the power of SMT Solvers.

Eventually...

Other Logics

Linear μ-Calculus (done),
Monadic Second Order Logic,
Branching Time Logics,
Freeze LTL...

Other Models

Affine Updates,
Relational Counter Systems,
etc.

Implementation

Implementing a prototype using the power of SMT Solvers.

Thank you for your attention.