

Verifying linear temporal specifications of constant-rate multi-mode systems

Michael Blondin, Philip Offtermatt,
Alex Sansfaçon-Buchanan



Université de
Sherbrooke

Constant-rate multi-mode systems (MMS)

R. Alur et al. 2012

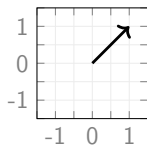
$$M \subset_{\text{finite}} \mathbb{R}^d$$

Constant-rate multi-mode systems (MMS)

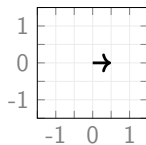
R. Alur et al. 2012

$$M \subset_{\text{finite}} \mathbb{R}^d$$

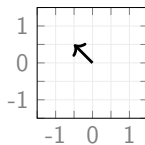
Example:



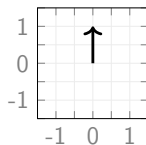
$$\mathbf{m}_1 = (1, 1)$$



$$\mathbf{m}_2 = \left(\frac{1}{2}, 0\right)$$



$$\mathbf{m}_3 = \left(-\frac{1}{2}, \frac{1}{2}\right)$$



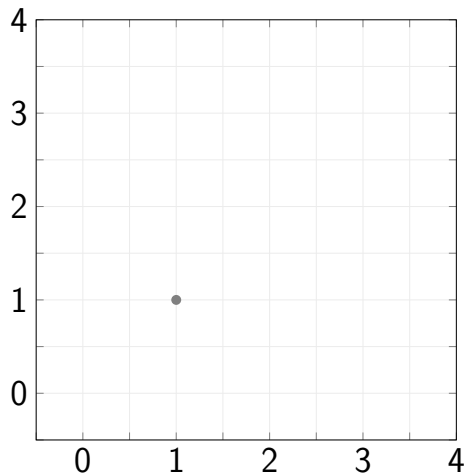
$$\mathbf{m}_4 = (0, 1)$$

$$m_1 = (1, 1)$$

$$m_2 = \left(\frac{1}{2}, 0\right)$$

$$m_3 = \left(-\frac{1}{2}, \frac{1}{2}\right)$$

$$m_4 = (0, 1)$$



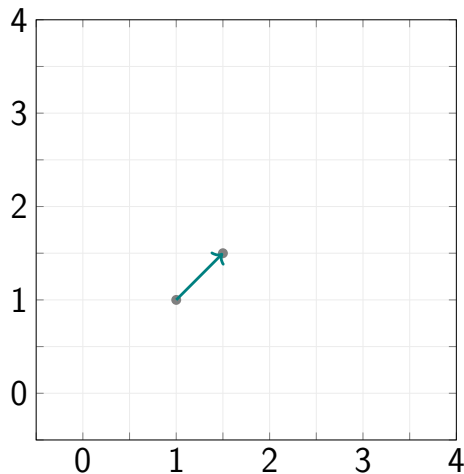
$$\sigma =$$

$$m_1 = (1, 1)$$

$$m_2 = \left(\frac{1}{2}, 0\right)$$

$$m_3 = \left(-\frac{1}{2}, \frac{1}{2}\right)$$

$$m_4 = (0, 1)$$



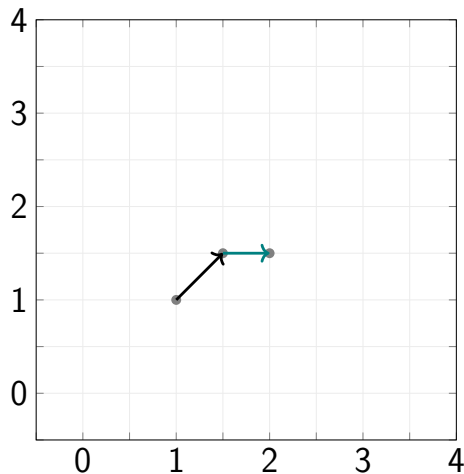
$$\sigma = \frac{1}{2}m_1$$

$$m_1 = (1, 1)$$

$$m_2 = \left(\frac{1}{2}, 0\right)$$

$$m_3 = \left(-\frac{1}{2}, \frac{1}{2}\right)$$

$$m_4 = (0, 1)$$



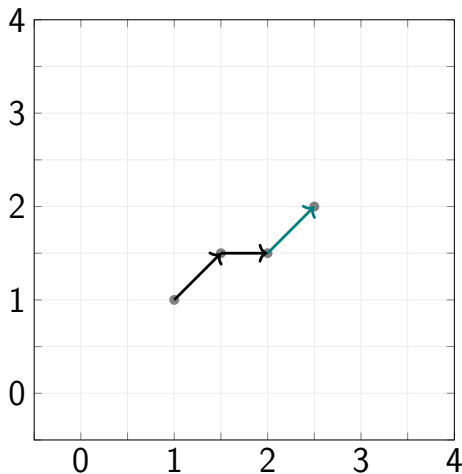
$$\sigma = \frac{1}{2} m_1 1 m_2$$

$$m_1 = (1, 1)$$

$$m_2 = \left(\frac{1}{2}, 0\right)$$

$$m_3 = \left(-\frac{1}{2}, \frac{1}{2}\right)$$

$$m_4 = (0, 1)$$



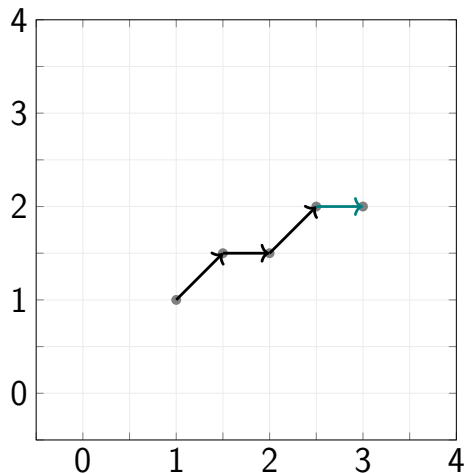
$$\sigma = \frac{1}{2}m_1 1 m_2 \frac{1}{2}m_1$$

$$m_1 = (1, 1)$$

$$m_2 = \left(\frac{1}{2}, 0\right)$$

$$m_3 = \left(-\frac{1}{2}, \frac{1}{2}\right)$$

$$m_4 = (0, 1)$$



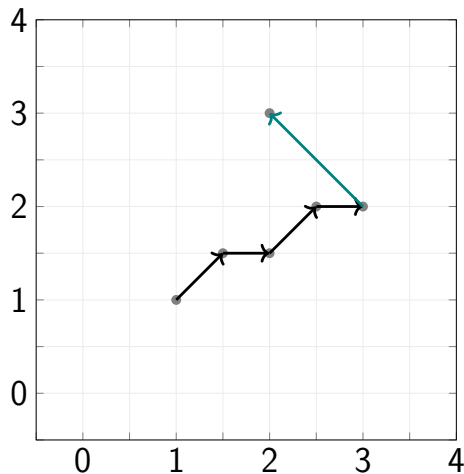
$$\sigma = \frac{1}{2}m_1 1 m_2 \frac{1}{2}m_1 1 m_2$$

$$m_1 = (1, 1)$$

$$m_2 = \left(\frac{1}{2}, 0\right)$$

$$m_3 = \left(-\frac{1}{2}, \frac{1}{2}\right)$$

$$m_4 = (0, 1)$$



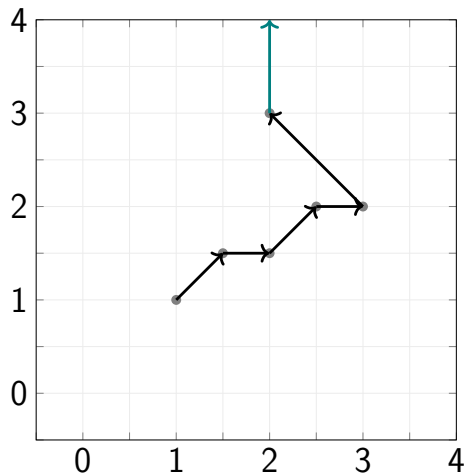
$$\sigma = \frac{1}{2}m_1 1 m_2 \frac{1}{2}m_1 1 m_2 2 m_3$$

$$m_1 = (1, 1)$$

$$m_2 = \left(\frac{1}{2}, 0\right)$$

$$m_3 = \left(-\frac{1}{2}, \frac{1}{2}\right)$$

$$m_4 = (0, 1)$$



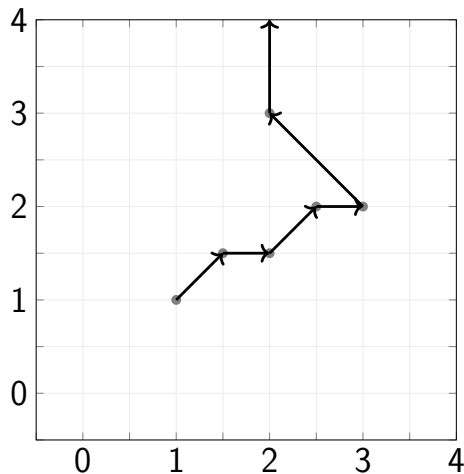
$$\sigma = \frac{1}{2}m_1 1 m_2 \frac{1}{2}m_1 1 m_2 2 m_3 1 m_4$$

$$m_1 = (1, 1)$$

$$m_2 = \left(\frac{1}{2}, 0\right)$$

$$m_3 = \left(-\frac{1}{2}, \frac{1}{2}\right)$$

$$m_4 = (0, 1)$$

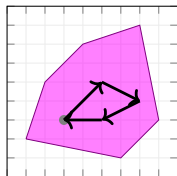


$$\sigma = \frac{1}{2}m_1 1 m_2 \frac{1}{2}m_1 1 m_2 2 m_3 1 m_4 \dots$$

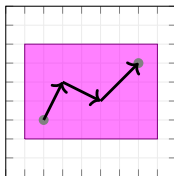
$$\sigma = \frac{1}{2}m_1 1 m_2 \frac{1}{2}m_1 1 m_2 2 m_3 1 m_4 \dots$$

Coefficients must sum to ∞ (non-Zeno)

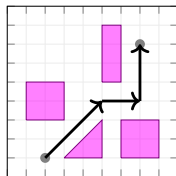
Safe scheduling



Safe reachability



Safe Planning



Green scheduling
PTIME

Motion planning
(Un)Decidable

Similar to problems on continuous Petri nets and vector addition systems (VAS)

Linear temporal logic (LTL)

Boolean logic:

true, *false*, \neg , \wedge , \vee , atomic propositions

Temporal operators:

$F\varphi$: φ is finally true

$G\varphi$: φ is always true

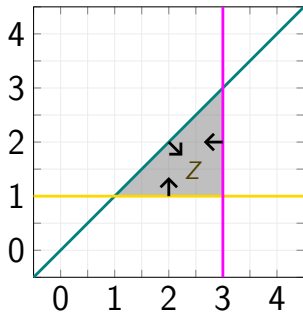
$\varphi_1 \text{ U } \varphi_2$: φ_1 is true until φ_2 is true

Atomic propositions (Zones)

Bounded convex polytope: $\mathbf{Ax} \leq \mathbf{b}$

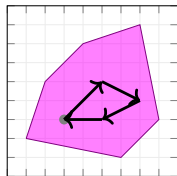
Example:

$$A = \begin{bmatrix} -1 & 1 \\ 0 & -1 \\ 1 & 0 \end{bmatrix}$$
$$b = \begin{bmatrix} 0 \\ -1 \\ 3 \end{bmatrix}$$



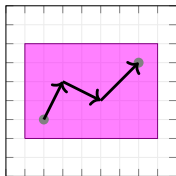
Linear temporal logic (LTL)

Safe scheduling



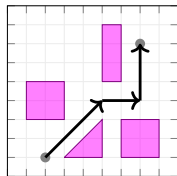
GZ

Safe reachability



$Z U \{x_{\text{target}}\}$

Safe Planning



$(\neg O_1 \wedge \dots \wedge \neg O_n) U \{x_{\text{target}}\}$

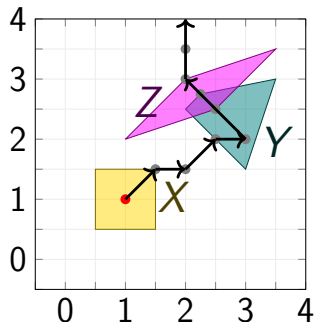
LTL interpreted over schedules

$$\sigma \models FZ$$

$$\sigma \not\models GX$$

$$\sigma \models F(X \wedge FY)$$

$$\sigma \not\models F(Y \wedge FX)$$

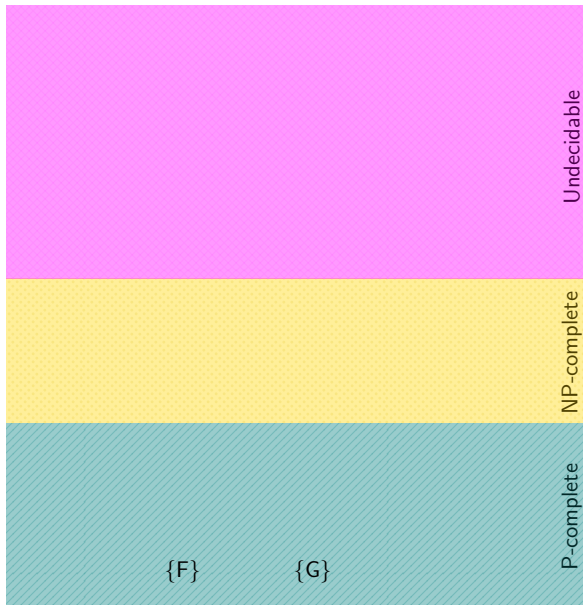


Model checking problem

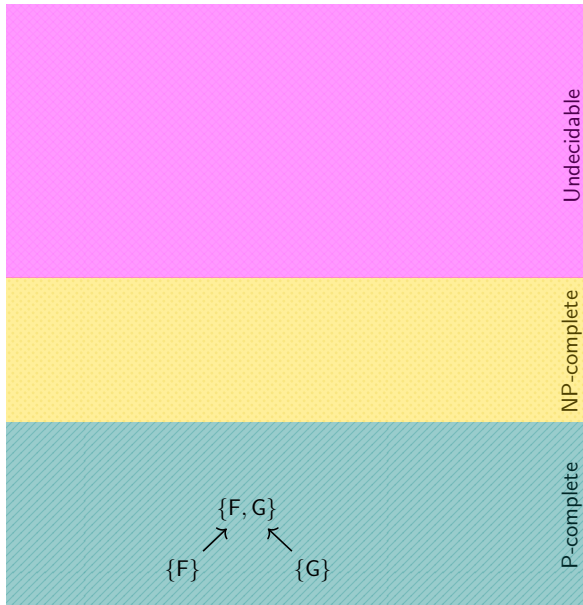
Given: LTL formula φ , point z , MMS M

Determine: whether there exists a schedule starting at z satisfying φ w.r.t M , i.e. $z \models_M \varphi$

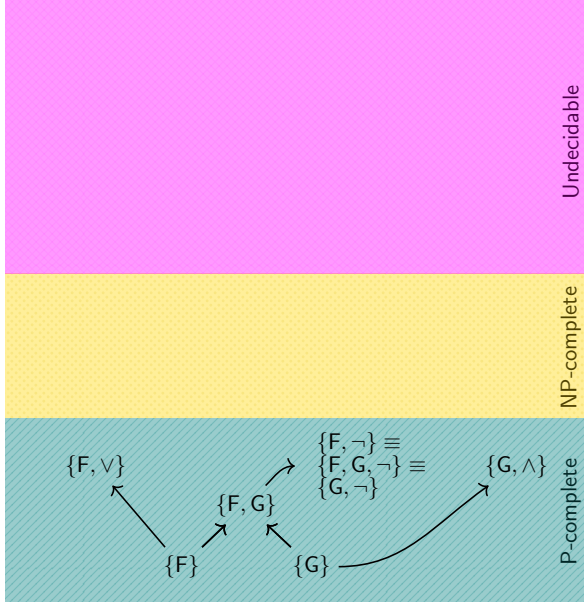
Contribution



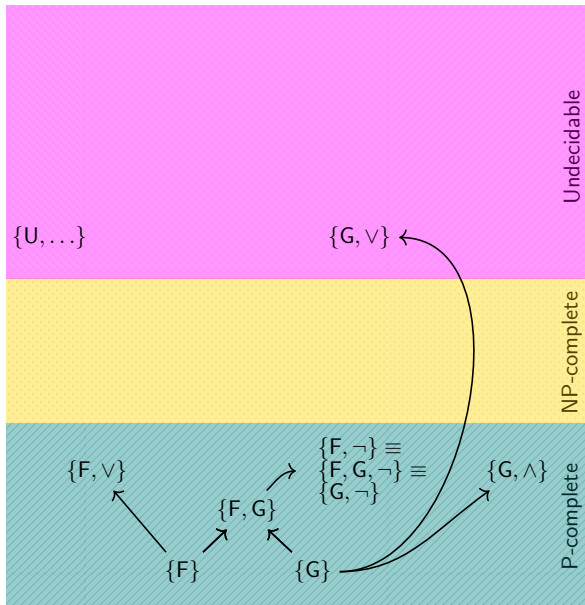
Contribution



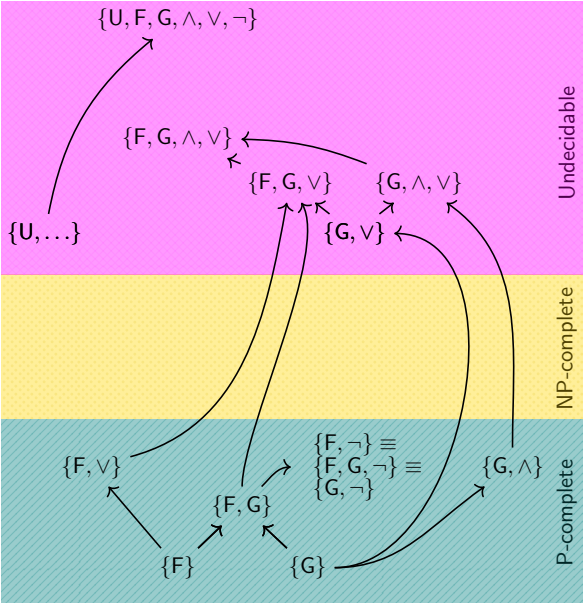
Contribution



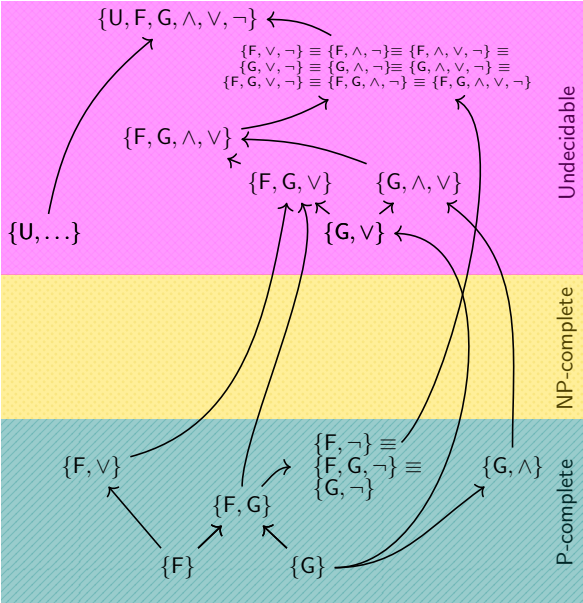
Contribution



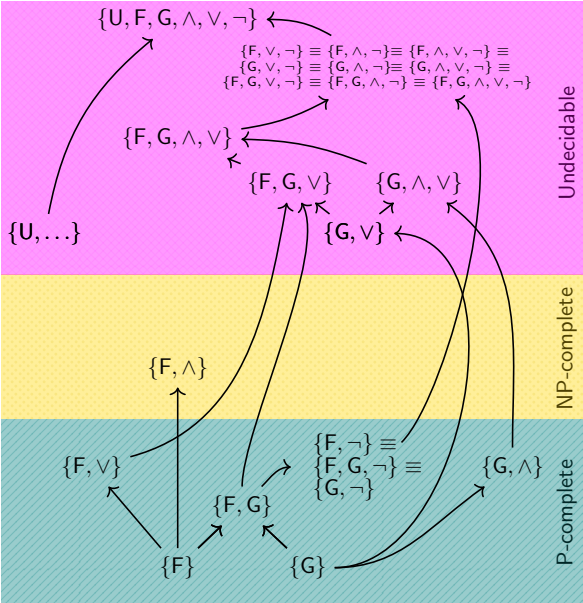
Contribution



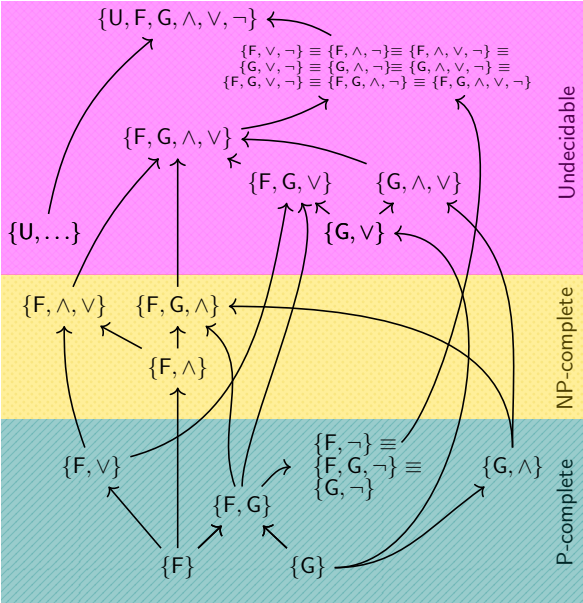
Contribution



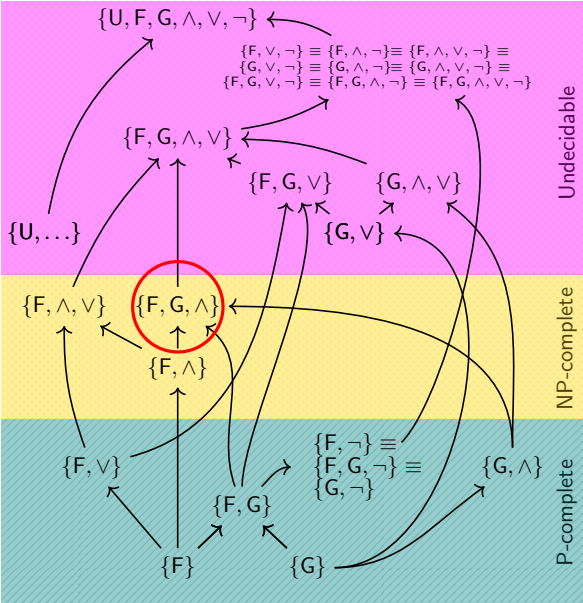
Contribution



Contribution



Contribution



$\{F, G, \wedge\}$ in NP: overview

- ① Flatten formula φ

$$\varphi \xrightarrow{\textcircled{1}} \text{flat}(\varphi)$$

$\{F, G, \wedge\}$ in NP: overview

- ① Flatten formula φ
- ② Create an almost acyclic automaton A_φ

$$\varphi \xrightarrow{\text{①}} \text{flat}(\varphi) \xrightarrow{\text{②}} A_\varphi$$

$\{F, G, \wedge\}$ in NP: overview

- ① Flatten formula φ
- ② Create an almost acyclic automaton A_φ
- ③ Non-deterministically pick linear path scheme π

$$\varphi \xrightarrow{\textcircled{1}} \text{flat}(\varphi) \xrightarrow{\textcircled{2}} A_\varphi \xrightarrow{\textcircled{3}} \pi$$

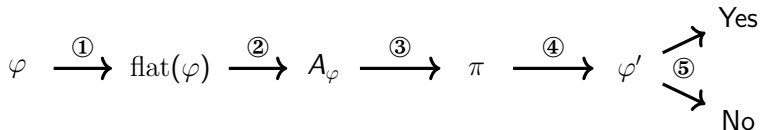
$\{F, G, \wedge\}$ in NP: overview

- ① Flatten formula φ
- ② Create an almost acyclic automaton A_φ
- ③ Non-deterministically pick linear path scheme π
- ④ Convert π into linear LTL formula φ'

$$\varphi \xrightarrow{\textcircled{1}} \text{flat}(\varphi) \xrightarrow{\textcircled{2}} A_\varphi \xrightarrow{\textcircled{3}} \pi \xrightarrow{\textcircled{4}} \varphi'$$

$\{F, G, \wedge\}$ in NP: overview

- ① Flatten formula φ
- ② Create an almost acyclic automaton A_φ
- ③ Non-deterministically pick linear path scheme π
- ④ Convert π into linear LTL formula φ'
- ⑤ Model check φ' through linear arithmetic



① Flat formulas

Definition

An LTL formula φ is *flat* if it has this form:

$$\psi \wedge G\psi' \wedge \bigwedge_{i \in I} GF\psi''_i \wedge \bigwedge_{j \in J} F\varphi_j,$$

where ψ , ψ' , ψ''_i are pseudo-atomic; and φ_j is flat.

① Flat formulas

Definition

$$\psi \wedge G\psi' \wedge \bigwedge_{i \in I} GF\psi''_i \wedge \bigwedge_{j \in J} F\varphi_j,$$

Example

non-flat formula	equivalent flat formula
$GF(a \wedge Gb \wedge Fc)$	$GFa \wedge FGb \wedge GFc$

① Flat formulas

Theorem

For every $\varphi \in \text{LTL}(\{F, G, \wedge\})$ there is an equivalent flat formula $\text{flat}(\varphi)$ of linear size.

Proof

It follows inductively with rewriting rules.

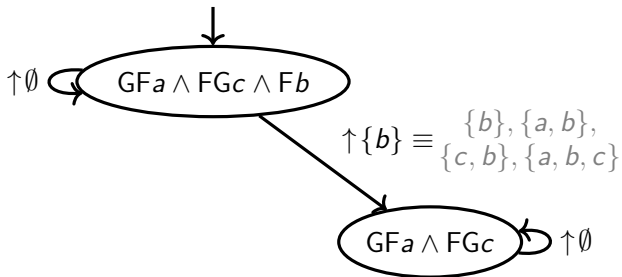
② Almost acyclic automata

$$GFa \wedge FGc \wedge Fb$$

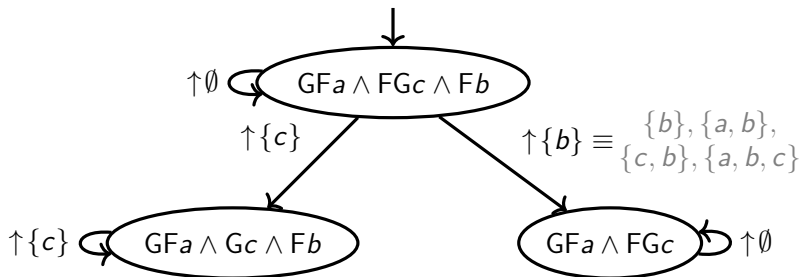
② Almost acyclic automata



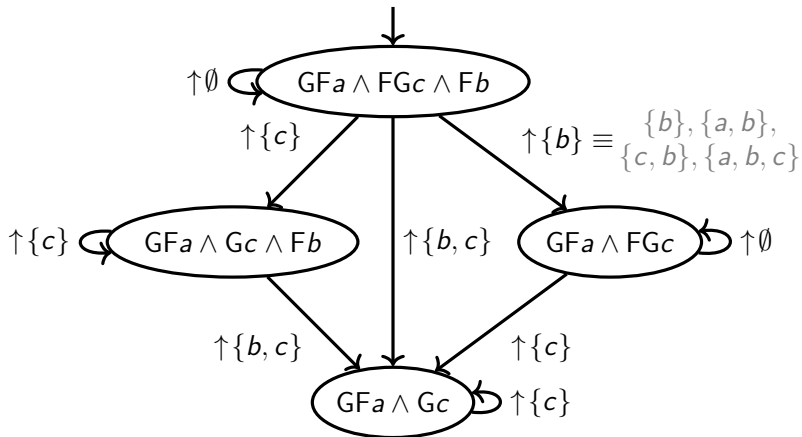
② Almost acyclic automata



② Almost acyclic automata



② Almost acyclic automata



② Almost acyclic automata

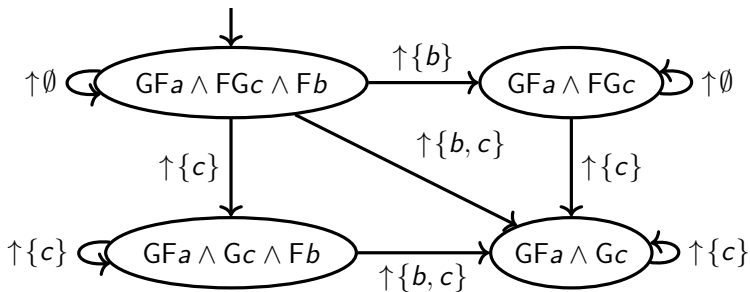
Theorem

Every formula $\varphi \in \text{LTL}(F, G, \wedge)$ has an almost acyclic automaton \mathcal{A}_φ such that $\varphi \equiv \mathcal{A}_\varphi$.

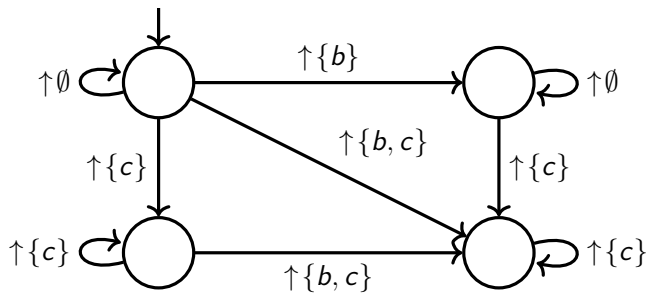
Proof

Inspired by unfoldings of Křetínský and Esparza 2012.

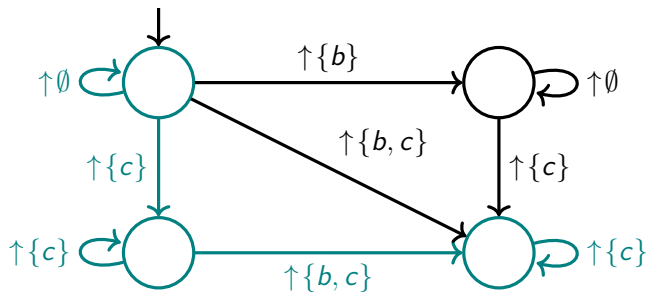
③ Linear path schemes (LPS)



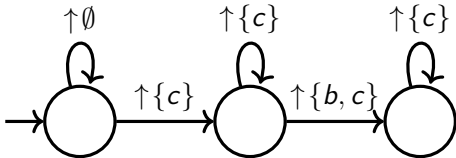
③ Linear path schemes (LPS)



③ Linear path schemes (LPS)

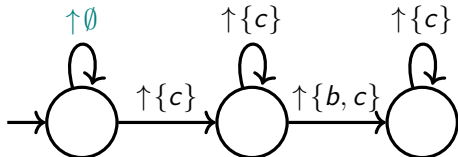


④ From LPS to linear LTL formulas



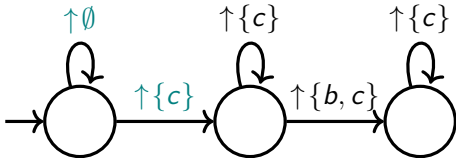
$true \ U \ (c \wedge (c \ U \ ((c \wedge b) \wedge Gc)))$

④ From LPS to linear LTL formulas



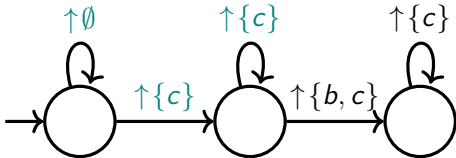
$true \text{ U } (c \wedge (c \text{ U } ((c \wedge b) \wedge Gc)))$

④ From LPS to linear LTL formulas



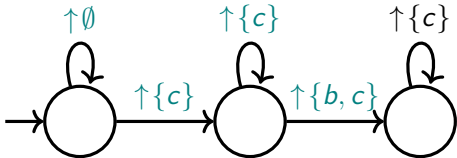
$true \text{ U } (c \wedge (c \text{ U } ((c \wedge b) \wedge Gc)))$

④ From LPS to linear LTL formulas



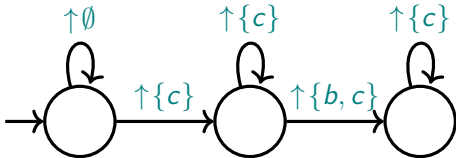
$true \text{ U } (c \wedge (c \text{ U } ((c \wedge b) \wedge Gc)))$

④ From LPS to linear LTL formulas



$true \text{ U } (c \wedge (c \text{ U } ((c \wedge b) \wedge Gc)))$

④ From LPS to linear LTL formulas



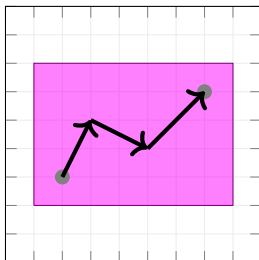
$true \text{ U } (c \wedge (c \text{ U } ((c \wedge b) \wedge Gc)))$

④ From LPS to linear LTL formulas

Proposition

Given an LPS S of \mathcal{A}_φ , one can construct, in poly time, a linear formula ψ s.t. $w \in L(S)$ iff $w \models \psi$.

⑤ Safe reachability



$$x \rightarrow_z^* y \iff \varphi(x, y) \text{ holds where}$$

$\varphi \in \text{PTIME}$ fragment of $\text{FO}(\mathbb{R}, +, <)$ [B. & Haase '17]

⑤ From linear LTL to $\text{FO}(\mathbb{R}, +, <)$

$\text{true} \text{ U } (c \wedge (c \text{ U } ((c \wedge b) \wedge \text{G}c)))$

$x_0 \rightarrow^*$

⑤ From linear LTL to $\text{FO}(\mathbb{R}, +, <)$

$\text{true} \cup (c \wedge (c \cup ((c \wedge b) \wedge Gc)))$

$x_0 \rightarrow^* x_1 \in c$

⑤ From linear LTL to $\text{FO}(\mathbb{R}, +, <)$

$\text{true} \cup (c \wedge (c \cup ((c \wedge b) \wedge Gc)))$

$x_0 \rightarrow^* x_1 \in c \rightarrow_c^*$

⑤ From linear LTL to $\text{FO}(\mathbb{R}, +, <)$

$$\text{true} \cup (c \wedge (c \cup ((c \wedge b) \wedge Gc)))$$

$$x_0 \rightarrow^* x_1 \in c \rightarrow_c^* x_2 \in (c \cap b)$$

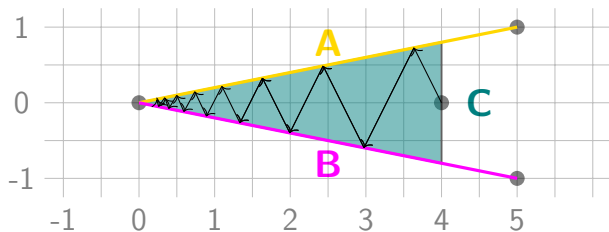
⑤ From linear LTL to FO($\mathbb{R}, +, <$)

$$true \text{ U } (c \wedge (c \text{ U } ((c \wedge b) \wedge Gc)))$$

$$x_0 \rightarrow^* x_1 \in c \rightarrow_c^* x_2 \in (c \cap b) \wedge x_2 \models_M Gc$$

Safe repeated reachability

$GC \wedge GF A \wedge GF B$

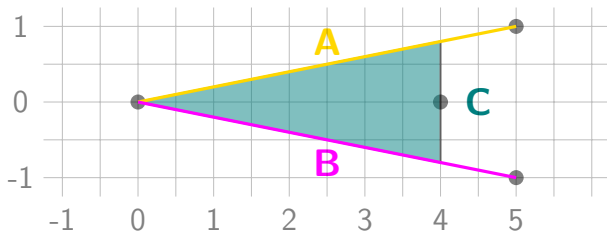


$$m_1 = (0, 0, 1), m_2 = (0, 0, -1),$$

$$m_3 = (-1, 2, 0), m_4 = (-1, -2, 0)$$

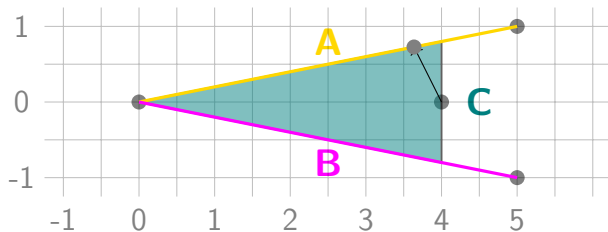
Safe repeated reachability

$$GC \wedge GF A \wedge GF B$$



Safe repeated reachability

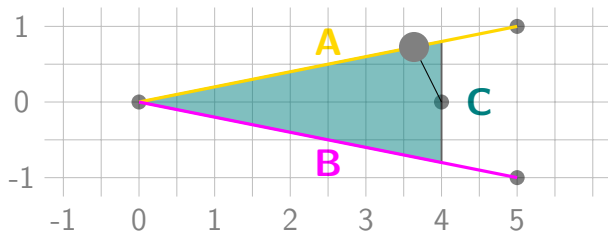
$$GC \wedge GF A \wedge GF B$$



$$\frac{4}{11} m_3$$

Safe repeated reachability

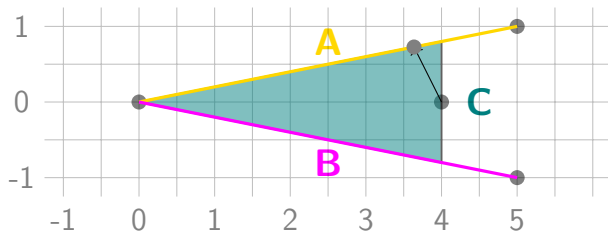
$GC \wedge GF A \wedge GF B$



$$\frac{4}{11} m_3 m_1$$

Safe repeated reachability

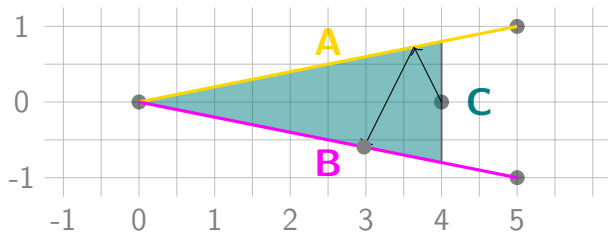
$GC \wedge GF A \wedge GF B$



$$\frac{4}{11} m_3 m_1 m_2$$

Safe repeated reachability

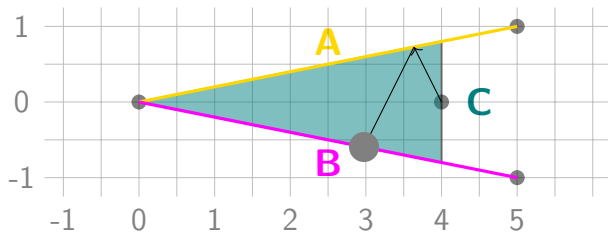
$GC \wedge GF A \wedge GF B$



$$\frac{4}{11} m_3 m_1 m_2 \frac{80}{121} m_4$$

Safe repeated reachability

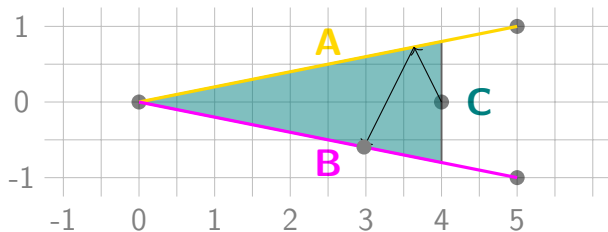
$GC \wedge GF A \wedge GF B$



$$\frac{4}{11} m_3 m_1 m_2 \frac{80}{121} m_4 m_1$$

Safe repeated reachability

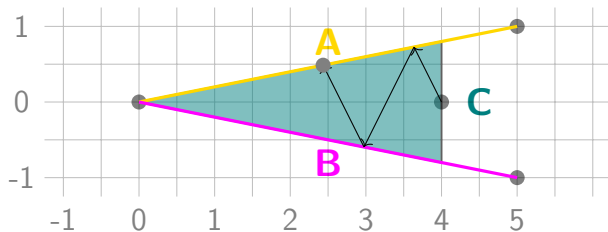
$GC \wedge GF A \wedge GF B$



$$\frac{4}{11} m_3 m_1 m_2 \frac{80}{121} m_4 m_1 m_2$$

Safe repeated reachability

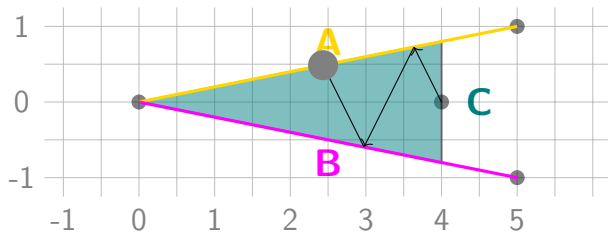
$GC \wedge GF A \wedge GF B$



$$\frac{4}{11} m_3 m_1 m_2 \frac{80}{121} m_4 m_1 m_2 \frac{720}{1331} m_3$$

Safe repeated reachability

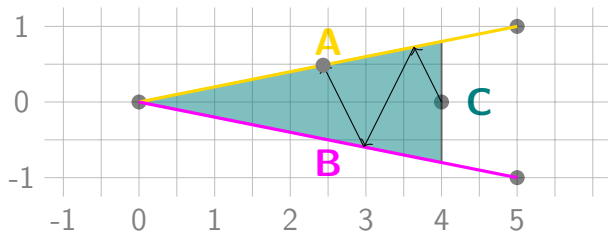
$GC \wedge GF A \wedge GF B$



$$\frac{4}{11} m_3 m_1 m_2 \frac{80}{121} m_4 m_1 m_2 \frac{720}{1331} m_3 m_1$$

Safe repeated reachability

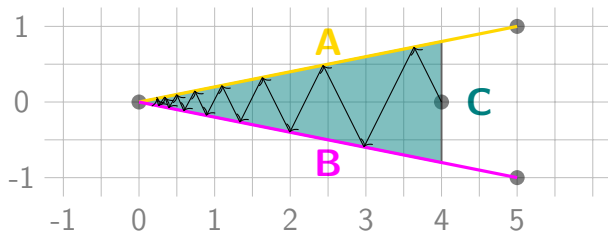
$GC \wedge GF A \wedge GF B$



$$\frac{4}{11} m_3 m_1 m_2 \frac{80}{121} m_4 m_1 m_2 \frac{720}{1331} m_3 m_1 m_2$$

Safe repeated reachability

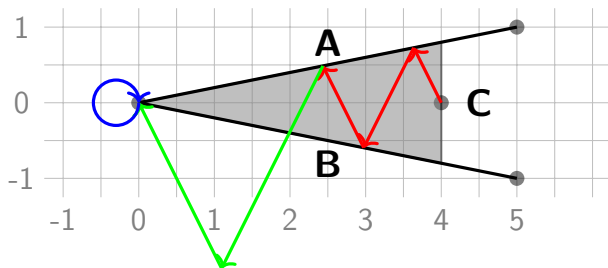
$GC \wedge GF A \wedge GF B$



$$\frac{4}{11} m_3 m_1 m_2 \frac{80}{121} m_4 m_1 m_2 \frac{720}{1331} m_3 m_1 m_2 \dots$$

Safe repeated reachability

$$GC \wedge GFA \wedge GFB$$



1. safe reach (SR),
2. loop reach (LR),
3. loop (L)

Safe repeated reachability

Informal theorem

There is a **safe reach (SR)** segment from x , a **loop reach (LR)** segment and a **loop (L)** segment where $\emptyset \neq \text{supp}(L) \subseteq \text{supp}(SR) = \text{supp}(LR)$

$$\iff x \models_M GC \wedge GFA \wedge GFB.$$

Proof sketch of (\Leftarrow)

(**SR**) follows by definition,
(**LR, L**) follows by Farkas' lemma.

Safe repeated reachability

Informal theorem

There is a **safe reach (SR)** segment from x , a **loop reach (LR)** segment and a **loop (L)** segment where $\emptyset \neq \text{supp}(L) \subseteq \text{supp}(SR) = \text{supp}(LR)$

$$\iff x \models_M GC \wedge GFA \wedge GFB.$$

Expressible in the PTIME logic of [B. and Haase '17]

Conclusion: summary

- ▶ Introduced LTL for MMS
- ▶ Classified every syntactic fragment as either P-complete, NP-complete or undecidable
- ▶ Generalized and unified work on MMS and continuous vector addition systems/Petri nets

Conclusion: future work

- ▶ Handling richer properties
- ▶ Implementing a solver for linear LTL
- ▶ Extending LTL to 2-player games

Thank you!