Checking Satisfiability of CLTL without Automata

Achille Frigeri

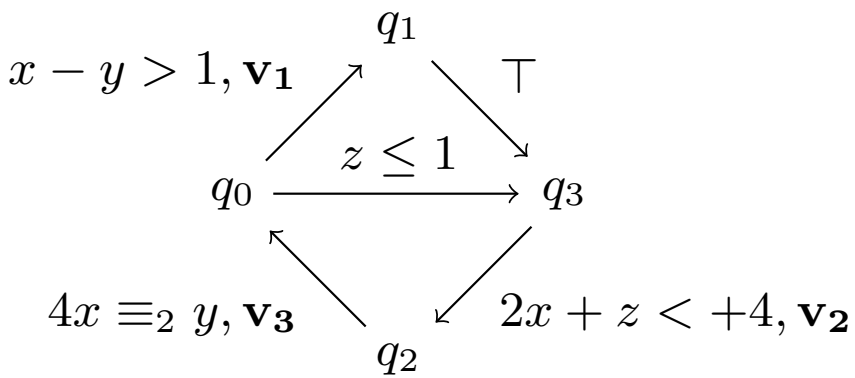
Dipartimento di Matematica “Francesco Brioschi”
Politecnico di Milano

joint work with Marcello M. Bersani

September 21, 2012

Verification of infinite state systems

- counter systems: finite state automata enriched with counters over infinite domains where transitions are labeled by formulae involving counters



- linear temporal language with arithmetical constraints: abstract propositions + arithmetic properties + time

$$(\mathrm{X}x > y + 3)\mathbf{U}\left((z = \mathrm{X}y) \wedge \mathbf{X}q_1\right)$$

Theoretical limit

- counter systems with two counters and zero-test simulate Minsky machines (and then Turing machines)
- temporal languages with arithmetical constraints can be enough expressive to represent runs of Minsky machines

Theoretical limit

- counter systems with two counters and zero-test simulate Minsky machines (and then Turing machines)
- temporal languages with arithmetical constraints can be enough expressive to represent runs of Minsky machines

Even basic problems become immediately undecidable!!

Our proposal

Verification approach based on **bounded representation**

- **generalization** of Bounded model-checking for LTL
- extended to infinite state systems
- and tailored to be implemented on SMT-solvers.

Our proposal

Verification approach based on **bounded representation**

- **generalization** of Bounded model-checking for LTL
- extended to infinite state systems
- and tailored to be implemented on SMT-solvers.

	BSAT	**BMC**	reduction
LTL	complete	complete	SAT
LTL+arith	complete (but...)	complete (but....)	SMT

bounded: infinite models are finitely represented

complete: solving a finite amount of bounded (w.r.t. time) problems, we can solve the non-bounded one

Satisfiability problem

Let $x, y \in D$

$$\varphi := \mathbf{G}(\mathbf{F}(\mathrm{X}x < y) \Rightarrow \mathbf{FG}(y \equiv_3 2 \wedge \mathrm{XX}y \geq \mathrm{Y}x))$$

Satisfiability problem

Let $x, y \in D$

$$\varphi := \mathbf{G}(\mathbf{F}(\mathrm{X}x < y) \Rightarrow \mathbf{FG}(y \equiv_3 2 \wedge \mathrm{XX}y \geq \mathrm{Y}x))$$

Models $\sigma \in (D^2)^\omega$ are sequences of assignments to vars

$x:$	0	3	1	-4	0	9	
$y:$	-5	5	5	-5	1	-4	...

Satisfiability problem

Let $x, y \in D$

$$\varphi := \mathbf{G}(\mathbf{F}(\mathrm{X}x < y) \Rightarrow \mathbf{FG}(y \equiv_3 2 \wedge \mathrm{XX}y \geq \mathrm{Y}x))$$

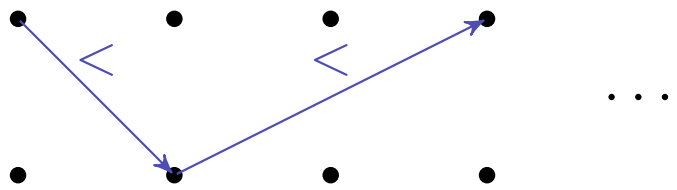
Models $\sigma \in (D^2)^\omega$ are sequences of assignments to vars

$$\begin{array}{lcccccc} x: & 0 & 3 & 1 & -4 & 0 & 9 \\ y: & -5 & 5 & 5 & -5 & 1 & -4 \quad \ldots \end{array}$$

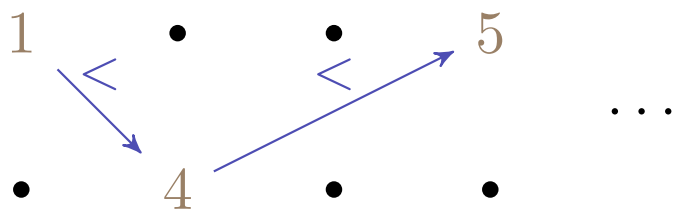
Is there a model $\sigma \in (D^n)^\omega$ satisfying φ?

Comparisons

- automata-based approach
  - verification procedure is *symbolic*; i.e., represents symbolic models ρ admitting arithmetic models σ



- finite amount of k-bounded satisfiability tests
  - verification procedure is "*concrete*"; i.e., represent a piece of arithmetic model σ and deduce its (infinite) symbolic model ρ
  - verification procedure is complete



The language of constraints

$(D, <, =)$, when

- $D \in \{\mathbb{N}, \mathbb{Z}\}$
- $D = \mathbb{R}$ or $D = \mathbb{Q}$ $<$ is a dense order without endpoints

Integer Periodic Constraints (IPC*) or subclasses.

$$\tau := \theta \mid x < y \mid \tau \wedge \tau \mid \neg\tau$$
$$\theta := x \equiv_c y + d \mid x = y \mid x < d \mid x = d \mid \theta \wedge \theta \mid \neg\theta \mid \exists x\theta$$

where $x, y \in V$, $c \in \mathbb{N}^+$ and $d \in \mathbb{Z}$.

Language from θ is IPC^{++}, but we consider its quantifier-free fragment.

CLTL with past-time operators (CLTLB)

Let x be a variable in V, an **arithmetical temporal term** τ is:

$$\tau := x \mid \mathrm{X}\tau \mid \mathrm{Y}\tau.$$

CLTL with past-time operators (CLTLB)

Let x be a variable in V, an **arithmetical temporal term** τ is:

$$\tau := x \mid \mathrm{X}\tau \mid \mathrm{Y}\tau.$$

Formulae of CLTLB(L) are:

$$\varphi := p \mid \gamma \mid \varphi \wedge \varphi \mid \neg\varphi \mid \mathbf{X}\varphi \mid \mathbf{Y}\varphi \mid \varphi\mathbf{U}\varphi \mid \varphi\mathbf{S}\varphi.$$

where $p \in AP$ is an atomic proposition and γ is a formula of the language of constraints L whose variables are the arithmetical temporal terms.

Semantics for CLTLB

The semantics of a formula φ of CLTLB(L) is defined w.r.t. a sequence of valuations $\sigma : \mathbb{Z} \times V \to D$.

The **satisfaction relation** $\models$ is defined for $i \geq 0$:

- atomic relations:

$$\sigma, i \models \tau_1 \sim \tau_2 \Leftrightarrow \sigma(i + |\tau_1|, x_{\tau_1}) \sim_L \sigma(i + |\tau_2|, x_{\tau_2})$$

$x:$	0	3		1	-4	0	9	
$y:$	-5	5		5	-5	1	-4	...
		$(\mathrm{X}x < \mathrm{Y}y)$						

  x_{τ_i} is the variable that appears in τ_i, $|\tau_i|$ is its depth.

- standard definition for LTL modalities

Symbolic valuations

A **symbolic valuation** sv is a **maximally consistent set** of formulae built from the original $\varphi \in \text{CLTLB}(L)$

$$\begin{array}{l|llll|llll} x\colon & 0 & 3 & 1 & -4 & 0 & 9 & \\ y\colon & -5 & 5 & 5 & 5 & 1 & -4 & \ldots \end{array}$$

$$sv = \{\mathrm{X}^2 x < y, x > \mathrm{X}x, x > \mathrm{X}^2 x, \mathrm{X}x < \mathrm{X}^2 y, \ldots\}$$

Symbolic valuations

A **symbolic valuation** sv is a **maximally consistent set** of formulae built from the original $\varphi \in \text{CLTLB}(L)$

$$\begin{array}{l|llll|llll} x\colon & 0 & 3 & 1 & -4 & 0 & 9 & \\ y\colon & -5 & 5 & 5 & 5 & 1 & -4 & \ldots \end{array}$$

$$sv = \{\mathrm{X}^2 x < y, x > \mathrm{X}x, x > \mathrm{X}^2 x, \mathrm{X}x < \mathrm{X}^2 y, \ldots\}$$

symbolic satisfaction relation $\models_s$

$$sv \models_s \mathrm{X}^2 x \leq y$$

when val satisfies sv then val satisfies $\mathrm{X}^2 x \leq y$

- val assigns values of D to terms

Sequences of SVs

Definition

A (locally consistent) infinite **sequence of SVs** $\rho : \mathbb{N} \to SV(\phi)$ **admits a model** $(\sigma, 0 \models \rho)$ if there exists a model σ

$$\sigma, i \models \rho(i)$$

for every $i \geq 0$.

Definition

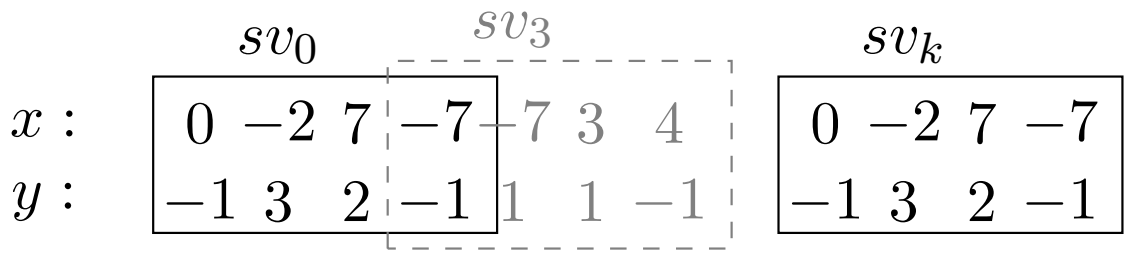
Given a formula φ, a sequence of SVs ρ is a **symbolic model** for φ when $\rho, 0 \models_s \varphi$.

- $\models_s$ naturally extends to symbolic models ρ

Ingredients

BSP is defined w.r.t.

- a partial model $\sigma_k : \{-l_{\mathrm{Y}}, \ldots, k + l_{\mathrm{X}}\} \times V \to D$,
- $\rho' \in SV(\phi)^{k+1}$, induced by σ_k



- a k-**bounded** satisfaction relation $\models_k$:

$$\sigma_k \models_k \rho' \text{ iff } \sigma_k, i \models \rho'(i) \text{ for } i \in [0, k].$$

The problem

Input: a CLTLB(L) formula φ, $k \in \mathbb{N}$;

Problem: is there an ultimately periodic sequence of SVs $\rho = \delta\pi^\omega$ such that

- $k + 1 = |\delta\pi|$ and $\rho, 0 \models_s \varphi$,
- and which admits a partial model σ_k such that $\sigma_k \models_k \rho'$?

k-bounded satisfiability is decidable

Polynomial time reduction from k-bounded satisfiability of CLTLB $\rightarrow$ satisfiability of formulae in the **combined theories**

- Equality and Uninterpreted Functions (EUF)
- Quantifier-free Integer/Real linear arithmetic IDL/RDL

k-bounded satisfiability is decidable

Polynomial time reduction from k-bounded satisfiability of CLTLB $\rightarrow$ satisfiability of formulae in the **combined theories**

- Equality and Uninterpreted Functions (EUF)
- Quantifier-free Integer/Real linear arithmetic IDL/RDL

Natural questions?

- what can we say when a formula is k-bounded satisfiable?
- when a formula is unsatisfiable?
  - k-bounded unsatisfiability does not immediately entail unsatisfiability

From k-bounded SAT to SAT

When $D \in \{\mathbb{Q}, \mathbb{R}\}$

Lemma (Demri&D'Souza IC07)

Let ρ be a locally consistent ultimately periodic sequence of SVs $\rho = \delta\pi^\omega$. Then ρ admits a model σ. (Exploit completion)

When a formula φ is k-bounded SAT then we know:

- its partial model σ_k
- an ultimately periodic symbolic model ρ

Then,

- φ is satisfiable
- we can build σ (complete arithmetic model) from σ_k by iterating suffix π infinitely many times

From k-bounded SAT to SAT

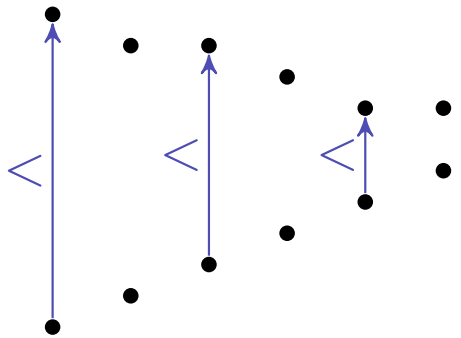
When $D \in \{\mathbb{N}, \mathbb{Z}\}$

Lemma (Demri&D'Souza IC07)

Let ρ be a locally consistent ultimately periodic sequence of SVs $\rho = \delta\pi^{\omega}$. Then ρ admits a model σ iff ρ satisfies a special condition C.

Condition C guarantees that (infinite) symbolic models (ρ) admit arithmetic model (σ):

- no infinite (non-)strictly monotonic increasing sequence of values which is infinitely often less than an infinite (strictly) monotonic decreasing sequence.

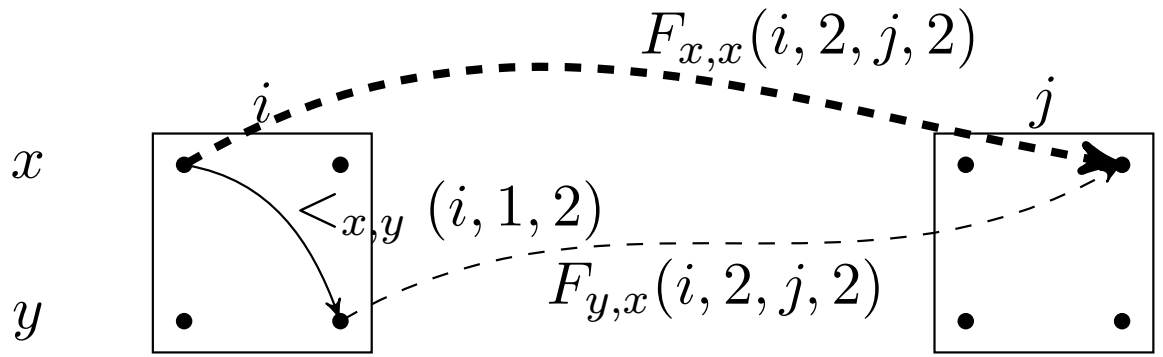


QF-EU$(\mathbb{Z}, <, =)$ encoding condition $\neg C$

Finite (non-)strict monotonic increasing sequences

- between two vars x, y
- at position h, m
- belonging to SV at position i and j

represented by predicates $F_{x,y}(i, h, j, m)$ in QF-EU$(\mathbb{Z}, \leq)$

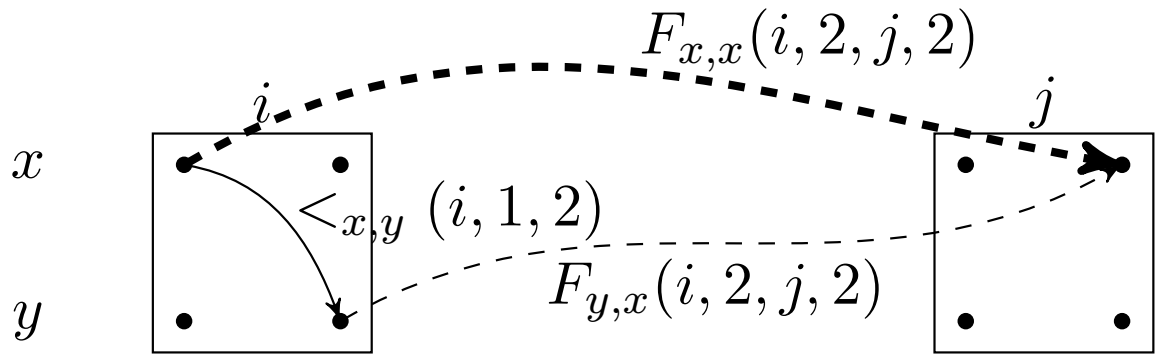


QF-EU$(\mathbb{Z}, <, =)$ encoding condition $\neg C$

Finite (non-)strict monotonic increasing sequences

- between two vars x, y
- at position h, m
- belonging to SV at position i and j

represented by predicates $F_{x,y}(i, h, j, m)$ in QF-EU$(\mathbb{Z}, \leq)$



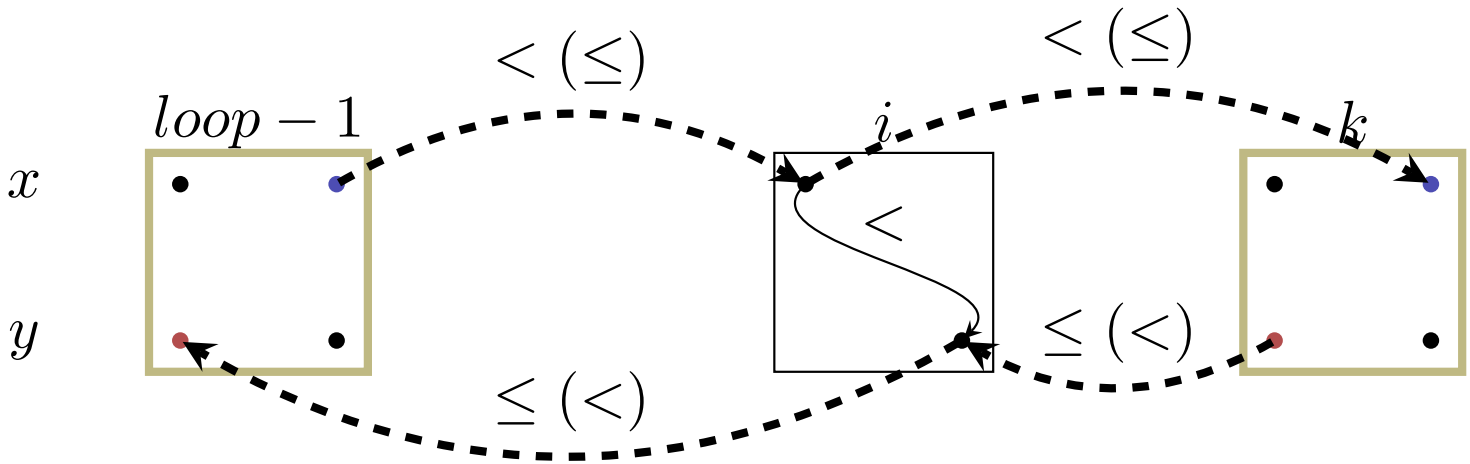
Finite (non-)strict monotonic decreasing sequences are represented analogously.

Encoding condition $\neg C$

Infinite sequences of relations are captured by the suffix π defining ultimately periodic model $\rho = \delta\pi^\omega$ relations between $sv(loop-1)$ and $sv(k)$

$$\rho = \underbrace{sv_0 sv_1 \dots sv_{loop-1}}_{\delta}\underbrace{(sv_{loop} \dots sv_k)}_{\pi}^{\omega}$$

where $sv(loop-1) = sv(k)$



From k-bounded SAT to SAT

When $D \in \{\mathbb{N}, \mathbb{Z}\}$

Lemma (Demri&D'Souza IC07)

Let ρ be a locally consistent ultimately periodic sequence of SVs $\rho = \delta\pi^\omega$. Then ρ admits a model σ iff ρ satisfies C.

When a formula φ is k-bounded SAT then we know:

- its partial model σ_k
- an ultimately periodic symbolic model ρ

Then,

- φ is satisfiable
- we can build σ (complete arithmetic model) from σ_k by iterating suffix π infinitely many times

So far, we can say that

- a formula is k-bounded satisfiable (for some $k \in \mathbb{N}$)
- if, and only if, it is satisfiable.

When a formula is k-bounded UNsatisfiable what can we deduce?

- the question is related to the completeness property...

So far, we can say that

- a formula is k-bounded satisfiable (for some $k \in \mathbb{N}$)
- if, and only if, it is satisfiable.

When a formula is k-bounded UNsatisfiable what can we deduce?

- the question is related to the completeness property...
- if we prove completeness then we can also decide when a formula is unsatisfiable

Towards completeness

Given a CLTL(L) formula φ, we can build an automaton[1] $\mathcal{A}_\varphi$ s.t. $\rho \in \mathcal{A}_\varphi$ if, and only if,

$$\rho \models_s \varphi \text{ and there exists } \sigma \text{ s.t. } \sigma \models \rho$$

$\mathcal{A}_\varphi$ is built by intersection of:

- $\mathcal{A}_s \rightarrow$ LTL symbolic models of φ
- $\mathcal{A}_\ell \rightarrow$ sequences of locally consistent SVs
- $\mathcal{A}_C \rightarrow$ sequences of SVs admitting a model σ. C is a condition on models of φ enforced by $\mathcal{A}_C$

[1] [Demri&D'Souza IC07]

Towards completeness

Given a CLTL(L) formula φ, we can build an automaton[1] $\mathcal{A}_\varphi$ s.t. $\rho \in \mathcal{A}_\varphi$ if, and only if,

$$\rho \models_s \varphi \text{ and there exists } \sigma \text{ s.t. } \sigma \models \rho$$

$\mathcal{A}_\varphi$ is built by intersection of:

- $\mathcal{A}_s \rightarrow$ LTL symbolic models of φ
- $\mathcal{A}_\ell \rightarrow$ sequences of locally consistent SVs
- $\mathcal{A}_C \rightarrow$ sequences of SVs admitting a model σ. C is a condition on models of φ enforced by $\mathcal{A}_C$

Remark: $\mathcal{A}_C$ and $\mathcal{A}_\ell$ depends only on arithmetical language and the length of SVs but not on formula φ

[1] [Demri&D'Souza IC07]

Towards completeness

Our QF-EUL encoding represents:

- A_s by the fixpoint encoding of $\mathbf{X}, \mathbf{Y}, \mathbf{U}, \mathbf{S}$
- $\mathcal{A}_\ell$ because the encoding is inherently consistent
- $\mathcal{A}_C$ (previous section)

Given a formula $\varphi \in$ CLTLB(L), we verify if it is k-bounded satisfiable for all $k \in [1, c+1]$ where c is the length of the (**recurrence diameter**) longest loop-free path of $\mathcal{A}_\varphi$.

Towards completeness

Our QF-EUL encoding represents:

- A_s by the fixpoint encoding of $\mathbf{X}, \mathbf{Y}, \mathbf{U}, \mathbf{S}$
- $\mathcal{A}_\ell$ because the encoding is inherently consistent
- $\mathcal{A}_C$ (previous section)

Given a formula $\varphi \in$ CLTLB(L), we verify if it is k-bounded satisfiable for all $k \in [1, c+1]$ where c is the length of the (**recurrence diameter**) longest loop-free path of $\mathcal{A}_\varphi$.

Lemma

Formula φ is k-bounded satisfiable, for some $k \in [1, c+1]$, iff there exists an ultimately periodic model accepted by $\mathcal{A}_\varphi$.

k-bounded satisfiability is complete

- If φ is **k-bounded unsatisfiable** for all $k \in [1, c+1]$ then φ is **unsatisfiable**.
- Otherwise, there exists an ultimately periodic symbolic model ρ which admits a model σ.
  - σ is defined from σ_k by iterating infinitely many times the sequence of SVs in π

k-bounded satisfiability is complete

- If φ is **k-bounded unsatisfiable** for all $k \in [1, c+1]$ then φ is **unsatisfiable**.
- Otherwise, there exists an ultimately periodic symbolic model ρ which admits a model σ.
  - σ is defined from σ_k by iterating infinitely many times the sequence of SVs in π

Theorem

For constraint systems IPC^*, $(D, <, =)$, *where* D *is* $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$, *there exists a finite completeness threshold for* k*-bounded satisfiability problem.*

k-bounded satisfiability is complete

- If φ is **k-bounded unsatisfiable** for all $k \in [1, c+1]$ then φ is **unsatisfiable**.
- Otherwise, there exists an ultimately periodic symbolic model ρ which admits a model σ.
  - σ is defined from σ_k by iterating infinitely many times the sequence of SVs in π

Theorem

For constraint systems IPC^*, $(D, <, =)$, *where* D *is* $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$, *there exists a finite completeness threshold for* k*-bounded satisfiability problem.*

- the results holds also for k-bounded model-checking (when the reduction of model-checking to satisfiability is still a CLTLB formula of considered fragments)

How to estimate completeness threshold

We don't want to build the automaton $\mathcal{A}_\varphi$ but exploit directly the satisfiability of φ.

How to estimate completeness threshold

We don't want to build the automaton $\mathcal{A}_\varphi$ but exploit directly the satisfiability of φ.
Remark: rough estimation for the completeness bound

$$d \cdot |SV(\varphi)| \cdot 2^{|\varphi|}$$

- $d = |\mathcal{A}_C| = 4|V|^2|\lambda|^2$ or $d = 1$, depending on D
  - λ is the width of symbolic valuations (defined from φ)
- $|SV(\varphi)|$ witnesses $\mathcal{A}_\ell$ (exponential in the size of φ).