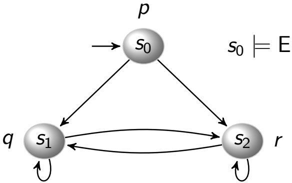
Introduction to Temporal Logics with Concrete Domains

Stéphane Demri
demri@lmf.cnrs.fr

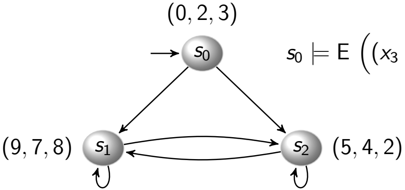
Étiolles, June 2023

Beyond Boolean Atomic Properties



$s_0 \models \mathsf{E}\left(\mathsf{X}q \wedge (\mathsf{GF}q \wedge \mathsf{GF}r)\right)$ (with $s_0 \to s_1 \to s_2 \to s_1 \to s_2 \cdots$)

(E ≈ "there Exists a path", GF ≈ "infinitely often")

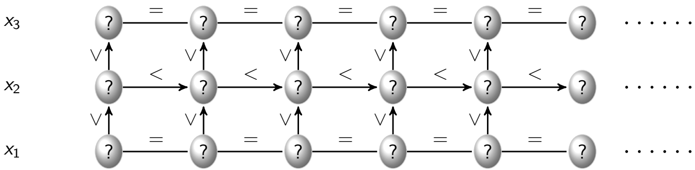


$s_0 \models \mathsf{E}\left((x_3 < \mathsf{X}x_3) \wedge (\mathsf{GF}(x_1 < \mathsf{X}x_2) \wedge \mathsf{GF}(x_3 > \mathsf{X}x_1))\right)$

$x_1 < \mathsf{X}x_2$: "current value of x_1 is smaller than the value of x_2 at the neXt position".

Introductory Example

Is $\underbrace{\mathsf{E}\ \mathsf{G}(x_1 = \mathsf{X} x_1 \ \wedge\ x_3 = \mathsf{X} x_3 \ \wedge\ x_1 < x_2 < \mathsf{X} x_2 < x_3)}_{=\ \phi}$ satisfiable?



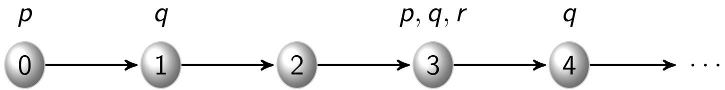
- $\begin{pmatrix} 1 \\ \frac{i+1}{i+2} \\ 0 \end{pmatrix}_{i\in\mathbb{N}} \models \phi$ with $(\mathbb{Q}, <)$.
- $\begin{pmatrix} \mathtt{b} \\ \mathtt{a}^{i+1} \\ \varepsilon \end{pmatrix}_{i\in\mathbb{N}} \models \phi$ with $\{\mathtt{a}, \mathtt{b}\}^*$ and lexico. ordering.
- No model for $(\mathbb{N}, <)$.

Linear-Time Temporal Logic LTL in a Nutshell

Specifying Properties on ω-sequences

- Linear-time temporal logic LTL. [Pnueli, FOCS'77]

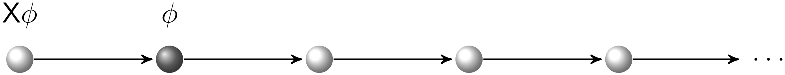
- LTL models ρ are ω-sequences of propositional valuations of the form $\rho : \mathbb{N} \to \mathcal{P}(\mathrm{PROP})$.



- LTL formulae:

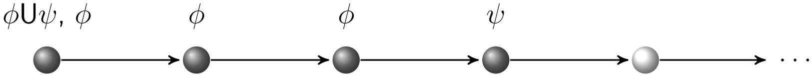
$$\phi, \psi ::= p \mid \neg\phi \mid \phi \wedge \psi \mid \phi \vee \psi \mid \mathsf{X}\phi \mid \phi \mathsf{U} \psi$$

- $\mathsf{X}\phi$ states that the next position satisfies ϕ:

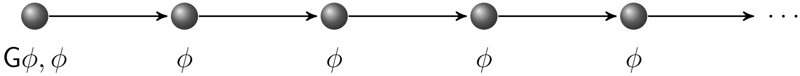


Linear-Time Temporal Operators

- $\phi \mathsf{U} \psi$ states that ϕ is true until ψ is true.



- $\mathsf{F}\phi$ states that some future position satisfies ϕ.



($\mathsf{G}\phi$ states that ϕ is always satisfied.)

Satisfaction Relation

- $\rho, i \models p \overset{\text{def}}{\Leftrightarrow} p \in \rho(i)$,
- $\rho, i \models \neg\phi \overset{\text{def}}{\Leftrightarrow} \rho, i \not\models \phi$,
- $\rho, i \models \phi_1 \wedge \phi_2 \overset{\text{def}}{\Leftrightarrow} \rho, i \models \phi_1$ and $\rho, i \models \phi_2$,
- $\rho, i \models \mathsf{X}\phi \overset{\text{def}}{\Leftrightarrow} \rho, i+1 \models \phi$,
- $\rho, i \models \phi_1 \mathsf{U} \phi_2 \overset{\text{def}}{\Leftrightarrow}$ there is $j \geq i$ such that $\rho, j \models \phi_2$ and $\rho, k \models \phi_1$ for all $i \leq k < j$.

$\mathsf{F}\phi \overset{\text{def}}{=} \top\mathsf{U}\phi \qquad \mathsf{G}\phi \overset{\text{def}}{=} \neg\mathsf{F}\neg\phi \qquad \phi\mathsf{R}\psi \overset{\text{def}}{=} \neg(\neg\phi\mathsf{U}\neg\psi)$

Examples

- ϕ holds infinitely often: $\mathsf{GF}\phi$.
- Liveness: $\mathsf{G}(\texttt{messageSent} \Rightarrow \mathsf{F}\ \texttt{messageReceived})$.
- Total correctness.

$$(\texttt{init} \wedge \texttt{precondition}) \Rightarrow \mathsf{F}(\texttt{end} \wedge \texttt{postcondition})$$

- Strong fairness.

$$\mathsf{GF}\ \texttt{processEnabled} \Rightarrow \mathsf{GF}\ \texttt{processExecuted}$$

Decision Problems

- Satisfiability problem for LTL.

  Input: LTL formula ϕ.

  Question: Is there any model ρ such that $\rho, 0 \models \phi$?

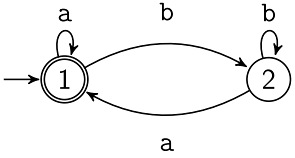
- Existential model-checking problem for LTL.

  Input: A finite transition system $\mathcal{S} = (S, \mathcal{R}, \mathfrak{v})$, $s \in S$ and an LTL formula ϕ.

  Question: Is there any infinite run ρ from s such that $\rho, 0 \models \phi$?

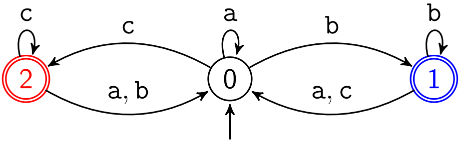
Büchi Automata on Infinite Words

- Büchi automata accepts ω-sequences in Σ^ω with acceptance condition F.



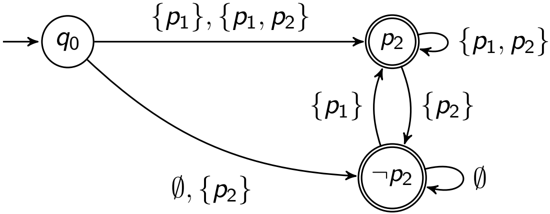
$$L(\mathbb{B}) = (\mathtt{b}^* \cdot \mathtt{a})^\omega$$

- Generalised Büchi automata accepts ω-sequences in Σ^ω with acceptance condition $F_1, F_2, \ldots, F_k$.



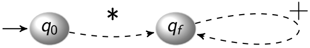
Büchi Automaton For $\mathsf{G}(p_1 \Leftrightarrow \mathsf{X}p_2)$

Letters are subsets of $\{p_1, p_2\}$.



A Selection of Nice Properties

- Nonemptiness problem for Büchi automata is $\textsc{NLogSpace}$-complete.



[Emerson & Lei, SCP 1987; Vardi & Wolper, IC 1994]

- Büchi automata and monadic second-order logic MSO recognize the same class of ω-languages. [Büchi, 1962]

- MSO is interpreted over $\rho : \mathbb{N} \to \Sigma$ using variable assignments $\mathcal{V} : (\mathrm{VAR}_1 \to \mathbb{N}) + (\mathrm{VAR}_2 \to \mathcal{P}(\mathbb{N}))$.

MSO Semantics

$$\phi := \mathsf{a}(x) \mid x < y \mid Y(x) \mid (\phi \wedge \phi) \mid \neg\phi \mid \exists x.\phi \mid \exists Y.\phi$$

$$\begin{array}{rcl}
\rho \models_{\mathcal{V}} \mathsf{a}(x) & \text{iff} & \rho(\mathcal{V}(x)) = \mathsf{a} \\
\rho \models_{\mathcal{V}} Y(x) & \text{iff} & \mathcal{V}(x) \in \mathcal{V}(Y) \\
\rho \models_{\mathcal{V}} \phi \wedge \psi & \text{iff} & \rho \models_{\mathcal{V}} \phi \text{ and } \rho \models_{\mathcal{V}} \psi \\
\rho \models_{\mathcal{V}} \exists x.\phi & \text{iff} & \text{there is } n \in \mathbb{N} \text{ s.t. } \rho \models_{\mathcal{V}[x \mapsto n]} \phi \\
\rho \models_{\mathcal{V}} \exists Y.\phi & \text{iff} & \text{there is } \mathcal{X}^{\dagger} \subseteq \mathbb{N} \text{ s.t. } \rho \models_{\mathcal{V}[Y \mapsto \mathcal{X}^{\dagger}]} \phi
\end{array}$$

- First-order logic FO over Σ^{ω} obtained by removing second-order variables in VAR_2.

Automata-Based Approach

- In general, to reduce logical problems to decision problems on automata. See e.g. [Büchi, 1962; Vardi & Wolper, IC 1994]

- Given an LTL formula ϕ over $\{p_1, \ldots, p_n\}$, design a Büchi automaton $\mathbb{B}_\phi$ over $\Sigma = \mathcal{P}(\{p_1, \ldots, p_n\})$ s.t.

  for all $\rho : \mathbb{N} \to \Sigma$, we have $\rho, 0 \models \phi$ iff $\rho \in \mathrm{L}(\mathbb{B}_\phi)$.

- Model-checking problem admits a similar reduction by checking $\mathrm{L}(\mathbb{B}_{\mathcal{S},s}) \cap \mathrm{L}(\mathbb{B}_\phi) \neq \emptyset$.

Preliminary Definitions

- ϕ in negation normal form (using release R dual of U), negation in front of propositional variables only.

- Closure set $cl(\phi)$ is the smallest set
  - containing ϕ and closed under subformulae,
  - $\phi_1 \mathsf{U} \phi_2 \in cl(\phi)$ implies $\mathsf{X}(\phi_1 \mathsf{U} \phi_2) \in cl(\phi)$,
  - $\phi_1 \mathsf{R} \phi_2 \in cl(\phi)$ implies $\mathsf{X}(\phi_1 \mathsf{R} \phi_2) \in cl(\phi)$.

- $\mathcal{X} \subseteq cl(\phi)$ is *propositionally consistent* iff
  - (for no propositional variable p, we have $\{p, \neg p\} \subseteq \mathcal{X}$,)
  - if $\phi_1 \vee \phi_2 \in \mathcal{X}$, then $\{\phi_1, \phi_2\} \cap \mathcal{X} \neq \emptyset$,
  - if $\phi_1 \wedge \phi_2 \in \mathcal{X}$, then $\{\phi_1, \phi_2\} \subseteq \mathcal{X}$,
  - if $\phi_1 \mathsf{U} \phi_2 \in \mathcal{X}$, then $\{\phi_1, \mathsf{X}(\phi_1 \mathsf{U} \phi_2)\} \subseteq \mathcal{X}$ or $\phi_2 \in \mathcal{X}$,
  - if $\phi_1 \mathsf{R} \phi_2 \in \mathcal{X}$, then $\{\phi_1, \mathsf{X}(\phi_1 \mathsf{R} \phi_2)\} \cap \mathcal{X} \neq \emptyset$ and $\phi_2 \in \mathcal{X}$.

A Construction of $\mathbb{B}_\phi$

- $\mathbb{B}_\phi = (Q, \Sigma, Q_{\text{in}}, \delta, F_1, \ldots, F_k)$.

- Q is the set of propositionally consistent subsets of $cl(\phi)$.

- $\Sigma = \mathcal{P}(\{p_1, \ldots, p_n\})$; $Q_{\text{in}} = \{\mathcal{X} \in Q \mid \phi \in \mathcal{X}\}$.

- $\mathcal{X} \xrightarrow{\mathsf{a}} \mathcal{X}' \in \delta$ iff the conditions below hold.
  - $p \in \mathcal{X}$ implies $p \in \mathsf{a}$; $\neg p \in \mathcal{X}$ implies $p \notin \mathsf{a}$,
  - for all $\mathsf{X}\psi \in \mathcal{X}$, we have $\psi \in \mathcal{X}'$.

$$\{p, \neg q, p\mathsf{U}q, \mathsf{X}(p\mathsf{U}q)\} \xrightarrow{\{p,r\}} \{q, p\mathsf{U}q\}$$

- If the U-formulae in ϕ are $\phi_1\mathsf{U}\psi_1$, ..., $\phi_k\mathsf{U}\psi_k$,

$$F_i = \{\mathcal{X} \mid \psi_i \in \mathcal{X} \text{ or } \phi_i\mathsf{U}\psi_i \notin \mathcal{X}\}.$$

About $\mathbb{B}_\phi$

- The location $\mathcal{X}$ is understood as an obligation for the remaining of the ω-word to satisfy all the formulae in $\mathcal{X}$.

- Many other constructions exist ...

  See e.g. [Gastin & Oddoux, CAV'01]

- card(Q) is exponential in the size of ϕ.

- Nonemptiness of $\mathrm{L}(\mathbb{B}_\phi)$ can be checked in polynomial space in the size of ϕ.

Time to Wrap Up

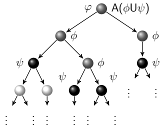
- Satisfiability problem for LTL is PSPACE-complete.
  [Sistla & Clarke, JACM 85]

- Model-checking problem for LTL is PSPACE-complete.
  [Sistla & Clarke, JACM 85]

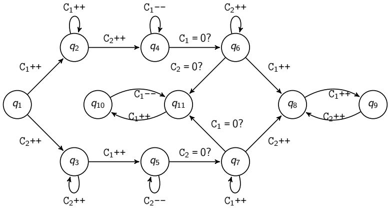
- LTL has good expressive power.
  - LTL expressively equivalent to FO. [Kamp, PhD 1968]
  - Other characterisations in [Diekert & Gastin, Chapter 2008]

Beyond plain LTL

- Branching-time temporal logics.



- Enriched operational models (counter machines, timed automata, pushdown systems).



- More linear-time temporal connectives, LTL games, . . .

LTL with Concrete Domains

Concrete Domains in TCS

- Constraint satisfaction problems (CSP).

- Satisfiability Modulo Theory (SMT) solvers.
  String theories, arithmetical theories, array theories, etc.
  See e.g. [Barrett & Tinelli, Handbook 2018]

- Description logics with concrete domains.
  [Baader & Hanschke, IJCAI'91, Lutz, PhD 2002]

- Temporal logics with arithmetical constraints.
  See e.g. [Bouajjani et al., LiCS 95; Comon & Cortier, CSL'00]

- Verification of database-driven systems.
  [Deutsch et al., SIGMOD 2014; Felli et al., AAAI'22]

A Fundamental Model: Data Words

(term coined by [Bouyer & Petit & Thérien, CONCUR'01])

- Timed word [Alur & Dill, TCS 1994]

a	b	c	a	a	b
0	0.3	1	2.3	3.5	3.51

- Runs from counter machines

q_0	q_2	q_3	q_2	q_3	q_2
0	0	1	2	3	4

- Abstract data words [Bouyer & Petit & Thérien, IC 03]

- Extension to trees, e.g. data trees for XML documents
  [Bojańczyk et al., PODS'06; Jurdzinski & Lazić, LiCS'07]

Concrete Domains

- Concrete domain $\mathcal{D} = (\mathbb{D}, R_1, R_2, \ldots)$: fixed non-empty domain with a family of relations.

- $(\mathbb{N}, <, +1)$, $(\mathbb{Q}, <, =)$, $(\mathbb{N}, <, =)$, $(\{0,1\}^*, \preceq_{\mathsf{pre}}, \preceq_{\mathsf{suf}})$.

- Concrete domain RCC8 with space regions in $\mathbb{R}^2$ contains topological relations between spatial regions.

  See e.g. [Wolter & Zakharyaschev, KR'00]

Constraints

- Terms are built from variables x.

- Constraint Θ: Boolean combination of atomic constraints of the form $R(\mathtt{t}_1, \ldots, \mathtt{t}_d)$.

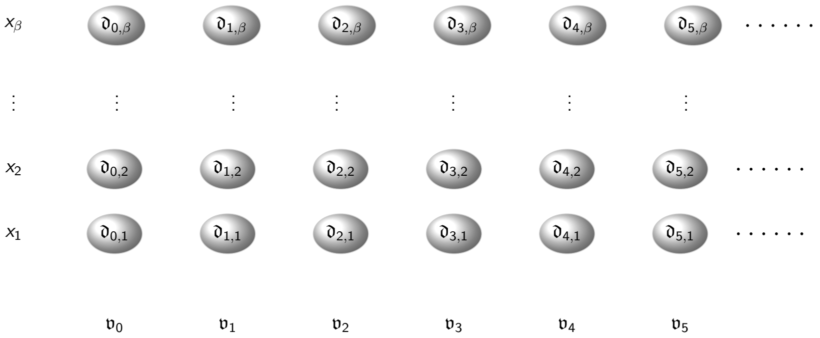
$$(x_1 = x_2 + x_3) \vee (x_1 > x_4)$$

- Constraints are interpreted on valuations $\mathfrak{v}$ that assign elements from $\mathbb{D}$ to the terms and

$$\mathfrak{v} \models R(\mathtt{t}_1, \ldots, \mathtt{t}_d) \ \text{ iff } \ (\mathfrak{v}(\mathtt{t}_1), \ldots, \mathfrak{v}(\mathtt{t}_d)) \in R^{\mathcal{D}}.$$

- A constraint Θ over $\mathcal{D}$ is satisfiable $\overset{\text{def}}{\Leftrightarrow}$ there is a valuation $\mathfrak{v}$ such that $\mathfrak{v} \models \Theta$.

Linear Models in $(\mathbb{D}^{\beta})^{\omega}$



$\mathfrak{v}_i : \{x_1, \ldots, x_\beta\} \to \mathbb{D}.$

$\mathrm{LTL}(\mathcal{D})$: LTL with Concrete Domain $\mathcal{D}$

$$\phi ::= R(\mathtt{t}_1, \ldots, \mathtt{t}_d) \mid \phi \wedge \phi \mid \neg\phi \mid \mathsf{X}\phi \mid \phi\mathsf{U}\phi$$

- The $\mathtt{t}_i$'s are terms of the form $\mathsf{X}^j x$ and '$\mathsf{X}x$' refers to the next value of x.
- $\mathrm{LTL}(\mathcal{D})$ model $\rho : \mathbb{N} \times \mathrm{VAR} \rightarrow \mathbb{D}$.

Satisfaction relation

- $\rho(i, \mathsf{X}^j x) \stackrel{\text{def}}{=} \rho(i + j, x)$.
- $\rho, i \models R(\mathtt{t}_1, \ldots, \mathtt{t}_d) \stackrel{\text{def}}{\Leftrightarrow} (\rho(i, \mathtt{t}_1), \ldots, \rho(i, \mathtt{t}_d)) \in R^{\mathcal{D}}$
- $\rho, i \models \mathsf{X}\phi \stackrel{\text{def}}{\Leftrightarrow} \rho, i + 1 \models \phi$

x_1	0	$\frac{3}{8}$	$\frac{1}{9}$	3	$\ldots$
x_2	$\frac{1}{2}$	$\mathbf{0}$	$\frac{3}{4}$	2	$\ldots$
x_3	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$\mathbf{1}$	$\ldots$
x_4	1	2	3	4	$\ldots$

$\models \mathsf{F}(x_2 < \mathsf{XX}x_3)$

Simple Properties

- "Infinitely often x is a prefix of the next value for y"

$$\mathsf{GF}(x \preceq_{\mathsf{pre}} \mathsf{X}y)$$

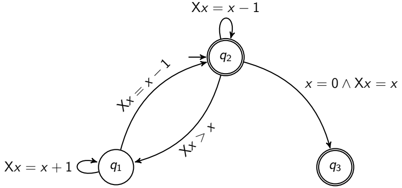
- "The value for x is strictly decreasing"

$$\mathsf{G}(x > \mathsf{X}x)$$

- "The value for x is equal to some future value of y"

$$\mathsf{G}(x^{new} = \mathsf{X}x^{new}) \wedge x = x^{new} \wedge \mathsf{F}(x^{new} = y)$$

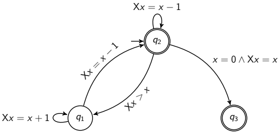
Back to (Constraint) Automata



$$q_2 \xrightarrow{\mathsf{X}x=x-1} q_2 \xrightarrow{\mathsf{X}x>x} q_1 \xrightarrow{\mathsf{X}x=x+1} q_1 \xrightarrow{\mathsf{X}x=x-1} q_2 \xrightarrow{\mathsf{X}x>x} q_1 \xrightarrow{\mathsf{X}x=x+1} q_1 \ldots$$

$$3 \longrightarrow 2 \longrightarrow 28 \longrightarrow 29 \longrightarrow 28 \longrightarrow 35 \longrightarrow 36 \ldots$$

Definition



- $\mathcal{D}$-automaton $\mathbb{A} = (Q, \beta, Q_{\text{in}}, \delta, F)$ with β variables:
  - Q is a non-empty finite set of locations,
  - Set $Q_{\text{in}} \subseteq Q$ of initial states; set $F \subseteq Q$ of accepting states,
  - δ is a finite subset of $Q \times \mathit{Bool}(\mathcal{D}, \beta) \times Q$, where $\mathit{Bool}(\mathcal{D}, \beta)$ is the set of $\mathcal{D}$-constraints over $\{x_1, \ldots, x_\beta\} \cup \{\mathrm{X}x_1, \ldots, \mathrm{X}x_\beta\}$.
- $\mathfrak{v}_0\mathfrak{v}_1 \cdots \in \mathrm{L}(\mathbb{A}) \overset{\text{def}}{\Leftrightarrow}$ there is $q_0 \overset{\Theta_0}{\to} q_1 \overset{\Theta_1}{\to} \cdots$ such that
  - $q_0 \in Q_{\text{in}}$ and some $q \in F$ occurs ∞-often in $q_0 q_1 q_2 \cdots$.
  - for all $i \in \mathbb{N}$, $q_i \overset{\Theta_i}{\to} q_{i+1} \in \delta$ and $\mathfrak{v}_i, \mathfrak{v}_{i+1} \models \Theta_i$.

Decision Problems

- Nonemptiness problem for $\mathcal{D}$-automata.

  Instance: A $\mathcal{D}$-automaton $\mathbb{A}$.
  Question: Is $\mathrm{L}(\mathbb{A}) \neq \emptyset$?

- Satisfiability problem for $\mathrm{LTL}(\mathcal{D})$:

  Instance: A $\mathrm{LTL}(\mathcal{D})$ formula ϕ.
  Question: Is there a model ρ such that $\rho, 0 \models \phi$?

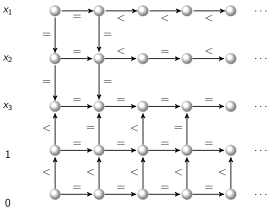
- Existential model-checking problem for $\mathrm{LTL}(\mathcal{D})$:

  Instance: A $\mathcal{D}$-automaton $\mathbb{A}$ and a $\mathrm{LTL}(\mathcal{D})$ formula ϕ.
  Question: is there a model ρ such that $\rho, 0 \models \phi$ and $\rho \in \mathrm{L}(\mathbb{A})$?

- Satisfiability for $\mathrm{LTL}(\mathbb{N}, =, +1)$ is undecidable.
  Flat Presburger LTL is decidable. [Comon & Cortier, CSL'00]

Symbolic Models

- $Atoms(\mathcal{D}, \beta)$: set of atomic constraints built over $\{x_1, \ldots, x_\beta\}$ and $\{\mathsf{X}x_1, \ldots, \mathsf{X}x_\beta\}$.
- $\mathcal{X} \subseteq Atoms(\mathcal{D}, \beta)$ is understood as the constraint $(\bigwedge_{\theta \in \mathcal{X}} \theta) \wedge (\bigwedge_{\theta \in (Atoms(\mathcal{D},\beta) \setminus \mathcal{X})} \neg\theta)$.
- Symbolic model $\mathtt{w} : \mathbb{N} \rightarrow \mathcal{P}(Atoms(\mathcal{D}, \beta))$.



- $\mathtt{w}$ is *$\mathcal{D}$-satisfiable* $\overset{\text{def}}{\Leftrightarrow}$ there is $\rho : \mathbb{N} \times \{x_1, \ldots, x_\beta\} \rightarrow \mathbb{D}$ such that for all i, $\{\theta \in Atoms(\mathcal{D}, \beta) \mid \rho, i \models \theta\} = \mathtt{w}(i)$.
- $\rho, i \models x = \mathsf{X}y$ iff $\rho(i, x) = \rho(i + 1, y)$.

A Selection of Problems

- $\mathrm{L}(\mathbb{A}) \neq \emptyset$ iff for some $\mathtt{w} : \mathbb{N} \to \mathcal{P}(Atoms(\mathcal{D}, \beta))$,
  - $\mathtt{w}$ is $\mathcal{D}$-satisfiable and,
  - there is an accepting run $q_0 \stackrel{\Theta_0}{\to} q_1 \stackrel{\Theta_1}{\to} \cdots$ such that for all $i \in \mathbb{N}$, we have $\boxed{\mathtt{w}(i) \models \Theta_i}$.

- $\boxed{\mathtt{w}(i) \models \Theta_i} \stackrel{\text{def}}{\Leftrightarrow}$

  $$(\bigwedge_{\theta \in \mathtt{w}(i)} \theta) \wedge (\bigwedge_{\theta \in (Atoms(\mathcal{D},\beta) \setminus \mathtt{w}(i))} \neg\theta) \Rightarrow \Theta_i \text{ is valid.}$$

- Given $\mathcal{D}$, how to characterise the class of $\mathcal{D}$-satisfiable symbolic models? ($\{x > \mathsf{X}x\}^\omega$ not $\mathbb{N}$-satisfiable)

- Can the class of $\mathcal{D}$-satisfiable symbolic models be expressed with a given formalism? (e.g. with Büchi automata)

Automata-Based Approach Still Applies!

- In the presence of equality, renaming technique allows us to restrict to x's and $\mathsf{X}x$'s.

$$x < \mathsf{XX}y \mapsto \mathsf{G}(y_1 = \mathsf{X}y_0 \wedge y_2 = \mathsf{X}y_1) \wedge x < y_2$$

- Given $\phi \in \mathrm{LTL}(\mathcal{D})$, there is a $\mathcal{D}$-automaton $\mathbb{A}_\phi$ such that

$$\mathrm{L}(\mathbb{A}_\phi) = \{\rho : \mathbb{N} \times \{x_1, \ldots, x_\beta\} \rightarrow \mathbb{D} \mid \ \rho, 0 \models \phi\}$$

Automata Construction

- ϕ in negation normal form (using R), negation only in atomic constraints in $Bool(\mathcal{D}, \beta)$.

- Closure set $cl(\phi)$ and propositionally consistent sets defined as for LTL.

- $\mathbb{A}_\phi = (Q, \beta, Q_{\text{in}}, \delta, F_1, \ldots, F_k)$.

- Q is the set of propositionally consistent subsets of $cl(\phi)$, $Q_{\text{in}} = \{\mathcal{X} \in Q \mid \phi \in \mathcal{X}\}$ and the F_i's are defined as for LTL formulae.

- $\mathcal{X} \xrightarrow{\Theta} \mathcal{X}' \in \delta$ iff Θ is equal to $(\bigwedge_{\Theta' \in \mathcal{X}} \Theta')$ and for all $\mathsf{X}\psi \in \mathcal{X}$, we have $\psi \in \mathcal{X}'$.

$$\{x < \mathsf{X}y, \neg(z = 0), \mathsf{X}(x < \mathsf{X}y \mathsf{U} \neg(z = 0))\} \xrightarrow{x < \mathsf{X}y \wedge \neg(z=0)} \{\neg(z = 0), x < \mathsf{X}y \mathsf{U} \neg(z = 0)\}$$

Three Ways for Deciding $\mathrm{LTL}(\mathcal{D})$

Dense and Open $(\mathbb{Q}, <, =)$: the Easy Way

- Symbolic model $\mathtt{w}$ is $\mathbb{Q}$-satisfiable iff for all $i \in \mathbb{N}$,
  (LocalSat) $(\bigwedge_{\theta \in \mathtt{w}(i)} \theta) \wedge (\bigwedge_{\theta \in (Atoms(\mathcal{D},\beta) \setminus \mathtt{w}(i))} \neg\theta)$ is satisfiable,
  (OneShift) $\{\mathsf{X}x_1, \ldots, \mathsf{X}x_\beta\}$ in $\mathtt{w}(i)$ and $\{x_1, \ldots, x_\beta\}$ in $\mathtt{w}(i+1)$ coincide.

- The set of $\mathbb{Q}$-satisfiable symbolic models is ω-regular.

- $\mathrm{SAT}(\mathrm{LTL}(\mathbb{Q}, <, =))$ is $\mathrm{PS}\textsc{pace}$-complete.
  [Balbiani & Condotta, FroCoS'02]

- $\mathrm{SAT}(\mathrm{LTL}(\mathsf{RCC8}))$ is $\mathrm{PS}\textsc{pace}$-complete too.
  [Balbiani & Condotta, FroCoS'02]

How to Handle Non-ω-Regularity?

- Given $(\mathbb{N}, <, =)$, the set SatSMod($\mathbb{N}$) of $\mathbb{N}$-satisfiable symbolic models is not ω-regular. (forthcoming hints)

- Option 1: Go beyond Büchi automata (equivalently extend MSO with new features).

- Option 2: Perform an analysis on accepting runs for $\mathbb{N}$-constraint automata.

- Option 3: Stick to Büchi automata but use adequate approximations.

What's Next?

- Characterisation of $\mathcal{D}$-satisfiable symbolic models for $\mathcal{D} = (\mathbb{N}, <, =)$.

- EHD approach with MSO extensions. (Option 1)

- Analysis of runs in constraint $\mathbb{N}$-automata. (Option 2)

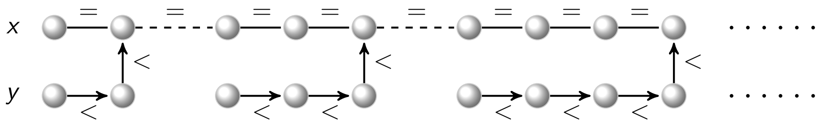
- Approximation condition (Approx) for $(\mathbb{N}, <, =)$ with ultimately periodic symbolic models. (Option 3)

- If time permits, global constraints on data values.

Characterisation for $(\mathbb{N}, <, =)$

- Symbolic model $\mathtt{w} : \mathbb{N} \to \mathcal{P}(Atoms(\mathbb{N}, \beta))$ understood as an infinite labelled graph on $\mathbb{N} \times \{x_1, \ldots, x_\beta\}$.

- A simple non $\mathbb{N}$-satisfiable symbolic model.



- Strict length of the finite path π:

$$\mathrm{slen}(\pi) \stackrel{\text{def}}{=} \text{number of edges labelled by } <.$$

- Strict length of (i, x):

$$\mathrm{slen}((i,x)) \stackrel{\text{def}}{=} sup \, \{\mathrm{slen}(\pi) : \text{ finite path } \pi \text{ leading to } (i,x)\}$$

$\mathbb{N}$-Satisfiable Symbolic Models

- Symbolic model $\mathtt{w}$ is $\mathbb{N}$-satisfiable iff

(LocalSat) $(\bigwedge_{\theta \in \mathtt{w}(i)} \theta) \wedge (\bigwedge_{\theta \in (Atoms(\mathcal{D},\beta) \setminus \mathtt{w}(i))} \neg\theta)$ is satisfiable for all i,

(OneShift) $\{\mathsf{X}x_1, \ldots, \mathsf{X}x_\beta\}$ in $\mathtt{w}(i)$ and $\{x_1, \ldots, x_\beta\}$ in $\mathtt{w}(i+1)$ coincide for all i,

(FiniteSLength) any node has a finite strict length.

[Cerans, ICALP'94; Demri & D'Souza, IC 07;Carapelle & Kartzow & Lohrey, CONCUR'13; Exibard & Filiot & Khalimov, STACS'21]

The EHD Approach

- The set of $\mathbb{N}$-satisfiable symbolic models is not ω-regular but can it be captured by decidable extensions of MSO?
- Starting point of the EHD approach with the bounding quantifier B. [Carapelle & Kartzow & Lohrey, CONCUR'13]
- $\rho : \mathbb{N} \rightarrow \Sigma$, $\mathcal{V} : (\mathrm{VAR}_1 \rightarrow \mathbb{N}) + (\mathrm{VAR}_2 \rightarrow \mathcal{P}(\mathbb{N}))$.
- $\rho \models_{\mathcal{V}} \mathsf{B} Y.\phi \overset{\text{def}}{\Leftrightarrow}$ there is bound $b \in \mathbb{N}$ such that whenever $\rho \models_{\mathcal{V}[Y \mapsto \mathcal{X}^{\dagger}]} \phi$ for some finite set $\mathcal{X}^{\dagger} \subseteq \mathbb{N}$, $\mathrm{card}(\mathcal{X}^{\dagger}) \leq b$.
  [Bojańczyk, CSL'04]
- B well-designed to express (StrictSLength).
  (Idea: "for any node $\mathfrak{n}$, any path labelled by $(< \cup =)^{+}$ leading to $\mathfrak{n}$ has a bounded number of edges $\overset{<}{\rightarrow}$")

Decidable MSO Extensions with B

- Satisfiability $\mathrm{MSO}+\mathrm{B}$ is undecidable over ω-words.
  [Bojańczyk & Parys & Toruńczyk, STACS'16]

- Satisfiability $\mathrm{WMSO}+\mathrm{B}$ is decidable over infinite trees of finite branching degree. [Bojańczyk & Toruńczyk, STACS'12]

- Boolean combinations of MSO and $\mathrm{WMSO}+\mathrm{B}$ (BMW) is decidable over infinite trees of finite branching degree.
  [Carapelle & Kartzow & Lohrey, JCSS 2016]

- Negation-closed $\mathcal{D}$ with EHD(BMW)-property.
  Satisfiability problem for $\mathrm{CTL}^*(\mathcal{D})$ is decidable.
  [Carapelle & Kartzow & Lohrey, JCSS 2016]
  (tree model property + decidability of BMW)

EHD Approach: Two Conditions

1) $\mathcal{D}$ negation-closed if complements of relations definable by positive existential first-order formulae over $\mathcal{D}$.
$(\neg(x = n) \Leftrightarrow \exists\, y\ (y = n) \wedge ((x < y) \vee (y < x)))$

2) EHD(BMW) property for symbolic models.
There is ϕ_{SAT} in BMW for ω-words such that

$$\mathtt{w} \text{ is } \mathbb{N}\text{-satisfiable iff } \mathtt{w} \models \phi_{\mathrm{SAT}}.$$

- EHD = "the Existence of a Homomorphism is Definable".

- 2) EHD(BMW) property (complete version).
  For every finite subsignature τ, one can compute ϕ_τ such that for every countable τ-structure $\mathcal{S}$,

$$\underbrace{\text{there is an homomorphism from } \mathcal{S} \text{ to } \mathcal{D}}_{\approx\ \mathcal{D}\text{-satisfiability}} \text{ iff } \mathcal{S} \models \phi_\tau.$$

New Decidability Results

- $(\mathbb{Z}, <, =, (=_n)_{n \in \mathbb{Z}})$ has the EHD(BMW)-property.

- The satisfability problem for $\mathrm{CTL}^*(\mathbb{Z}, <, =, (=_n)_{n \in \mathbb{Z}})$ is decidable. [Carapelle & Kartzow & Lohrey, JCSS 2016]

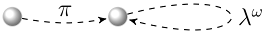
- Concept satisfiability w.r.t. general TBoxes for description logic $\mathcal{ALCF}^{\mathcal{P}}(\mathbb{Z}, <, =, (=_n)_{n \in \mathbb{Z}})$ is decidable. [Carapelle & Turhan, ECAI'16]

$\mathbb{N}$-automata

- EHD powerful for decidability, unsatisfactory for complexity!

- Concrete domains $\mathcal{D} = (\mathbb{D}, <, P_1, \ldots, P_l, =_{\mathfrak{d}_1}, \ldots, =_{\mathfrak{d}_m})$, where $(\mathbb{D}, <)$ is a linear ordering and the P_i's are unary relations. [Segoufin & Toruńczyk, STACS'11]

- Existence of accepting runs characterised by existence of extensible lassos.



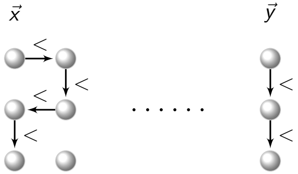
$\mathbb{N}$-Automata: Extensible Lassos

$\mathbb{A}$ has an accepting run iff there are finite runs π, λ s.t.

1. $\pi = (q_I, \vec{x}_0) \xrightarrow{*} (q_F, \vec{x})$ and $\lambda = (q_F, \vec{x}) \xrightarrow{+} (q_F, \vec{y})$

2. "$\mathrm{type}(\vec{x}) = \mathrm{type}(\vec{y})$", $\vec{x} \leq \vec{y}$ and $\mathrm{dv}(\vec{x}) \leq \mathrm{dv}(\vec{y})$.

$$0 \overset{7}{\frown} 7 \overset{2}{\frown} 9 \overset{6}{\frown} 15 \qquad \mathrm{dv}\left(\begin{pmatrix}15\\9\\7\end{pmatrix}\right) = \begin{pmatrix}7\\2\\6\end{pmatrix}$$



Conditions (2) and (3) allow us to repeat infinitely λ.

3. For all $j \in [1, k]$ such that $\vec{x}[j] = \vec{y}[j]$, there is no j' such that $\vec{x}[j'] < \vec{y}[j']$ and $\vec{x}[j'] < \vec{x}[j]$.

$\mathbb{N}$-Automata: Lasso Detection in PSpace

- Existence of finite runs π, λ can be checked in PSPACE.
- The non-emptiness problem for $(\mathbb{N}, <)$-automata is PSPACE-complete. [Segoufin & Toruńczyk, STACS'11]
- A similar method used in [Kartzow & Weidner, arXiv 2015].
- PSPACE-completeness with the concrete domains
  - $\mathcal{D}_{\mathbb{Q}^*} = (\mathbb{Q}^*; \preceq_{\mathsf{pre}}, \preceq_{\mathsf{lex}}, =_{\mathfrak{d}_1}, \ldots, =_{\mathfrak{d}_m})$.
  - $\mathcal{D}_{[1,\alpha]^*} = ([1, \alpha]^*; \preceq_{\mathsf{pre}}, \preceq_{\mathsf{lex}}, =_{\mathfrak{d}_1}, \ldots, =_{\mathfrak{d}_m})$, $\alpha \geq 2$.

[Kartzow & Weidner, arXiv 2015]

Ultimately Periodic Models

- A symbolic model $\mathtt{w}$ is ultimately periodic iff $\mathtt{w}$ of the form

$$\mathtt{w}(0) \cdots \mathtt{w}(I-1) \cdot \Big(\mathtt{w}(I) \cdots \mathtt{w}(I+J)\Big)^{\omega}$$

- Characterisation for $\mathbb{N}$-satisfiable ultimately periodic models might be simpler than the general case.

- Reminder: $\mathrm{L}(\mathbb{A}) \neq \emptyset$ iff $\exists\, \mathtt{w} : \mathbb{N} \to \mathcal{P}(\mathit{Atoms}(\mathbb{N}, \beta))$,
  1) $\mathtt{w}$ is $\mathbb{N}$-satisfiable and,
  2) there is an accepting run $q_0 \xrightarrow{\Theta_0} q_1 \xrightarrow{\Theta_1} \cdots$ such that for all $i \in \mathbb{N}$, we have $\mathtt{w}(i) \models \Theta_i$ (Büchi automaton $\mathbb{B}_2$).

Forthcoming Features of (Approx)

If

- Condition (Approx) is ω-regular (Büchi automaton $\mathbb{B}_1$).

- For all ultimately periodic symbolic models $\mathtt{w}$,

  $\mathtt{w}$ is $\mathbb{N}$-satisfiable iff $\mathtt{w}$ satisfies (Approx).

- Symbolic models built from $(\mathbb{N}^\beta)^\omega$ satisfy (Approx).

Then

$$\mathrm{L}(\mathbb{B}_1) \cap \mathrm{L}(\mathbb{B}_2) \neq \emptyset \text{ iff } \mathrm{L}(\mathbb{A}) \neq \emptyset.$$

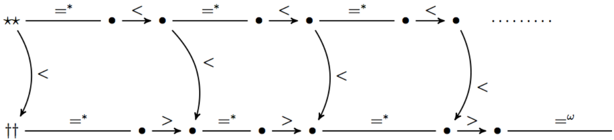
Condition (Approx)

Symbolic model $\mathtt{w}$ satisfies the condition (Approx) iff

1. (LocalSat) and (OneShift).

2. There is no infinite $(j_1, z_1) \xrightarrow{\mathsf{a}_1} (j_2, z_2) \xrightarrow{\mathsf{a}_2} (j_3, z_3) \cdots$ s.t. $\{\mathsf{a}_1, \mathsf{a}_2, \ldots\} \subseteq \{=, >\}$ and infinitely often a_j's equals $>$.

3. There do not exist nodes $\star\star$ and $\dagger\dagger$ such that



with infinite amount of $\xrightarrow{<}$ from $\star\star$ on top path and finite amount of $\xrightarrow{>}$ from $\dagger\dagger$ on bottom path

(LocalSat) $\wedge$ (OneShift) $\wedge$ (FiniteSLength) $\Rightarrow$ (Approx)

Properties of (Approx)

- Ultimately periodic symbolic model w. Equivalence btw.
  - w is $\mathbb{N}$-satisfiable.
  - w satisfies (Approx).

[Demri & D'Souza, IC 2007; Exibard & Filiot & Reynier, STACS'21]

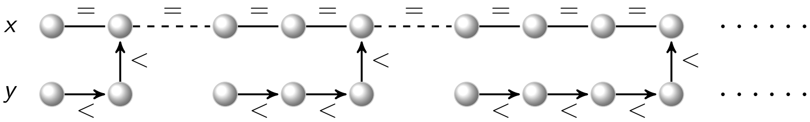
- The class of symbolic models satisfying (Approx) is ω-regular.

- By-products:
  - Non-emptiness problem for $\mathbb{N}$-automata is in PSPACE.
  - Satisfiability problem for $\mathrm{LTL}(\mathbb{N}, <, =)$ is in PSPACE.

- Results apply to $(\mathbb{Z}, <, =)$ with adequate adaptations.

SatSMod($\mathbb{N}$) is Not ω-Regular

- Non $\mathbb{N}$-satisfiable symbolic model $\mathtt{w}^\star$ satisfying (Approx).



- *Ad absurdum*, suppose SatSMod($\mathbb{N}$) is ω-regular.

- $\overline{\text{SatSMod}(\mathbb{N})} \cap \text{(Approx)}$ is ω-regular and contains $\mathtt{w}^\star$.

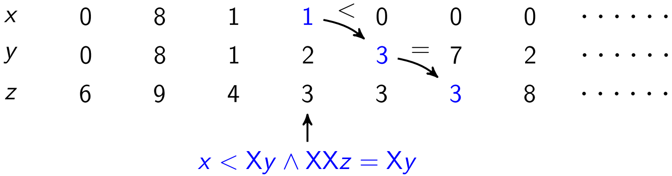
- $\overline{\text{SatSMod}(\mathbb{N})} \cap \text{(Approx)}$ contains an ultimately periodic symbolic model $\mathtt{w}^\dagger$ satisfying (Approx).

- So, $\mathtt{w}^\dagger$ is $\mathbb{N}$-satisfiable, contradiction.

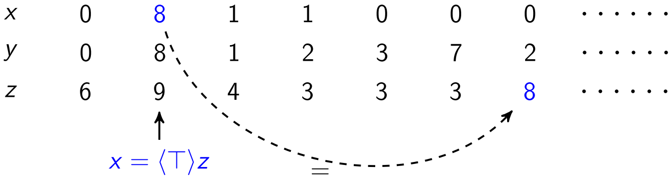
Global Constraints on Data Values

Global Constraints

- So far, constraints have a local scope.



- Global constraints have unbounded scope.



- "The variable x never takes twice the same value."

$$\mathsf{G}(\neg(x = \langle\top\rangle x))$$

LTL with Registers

- $\downarrow_{\mathtt{r}=x} \phi$ states that freezing the value of x in the register $\mathtt{r}$ makes true the formula ϕ.
- Registers in $\mathrm{RVAR} = \{\mathtt{r}, \mathtt{s}, \mathtt{t}, \ldots\}$.
- $\mathrm{LTL}^{\downarrow}(\mathcal{D})$ formulae:

  $\phi ::= R(\mathtt{t}_1, \ldots, \mathtt{t}_d) \mid \phi \wedge \phi \mid \neg \phi \mid \uparrow_{\mathtt{r}=y} \mid \downarrow_{\mathtt{r}=x} \phi \mid \mathsf{X}\phi \mid \phi \mathsf{U} \phi,$

- Environment $env : \mathrm{RVAR} \rightarrow \mathbb{D}$, $\rho : \mathbb{N} \times \mathrm{VAR} \rightarrow \mathbb{D}$.
- $\rho, i \models_{env} \downarrow_{\mathtt{r}=x} \phi \overset{\text{def}}{\Leftrightarrow} \rho, i \models_{env[\mathtt{r} \mapsto \rho(i,x)]} \phi$.
- $\rho, i \models_{env} \uparrow_{\mathtt{r}=y} \overset{\text{def}}{\Leftrightarrow} env(\mathtt{r}) = \rho(i, y)$.
- We use $\uparrow_y$ and $\downarrow_x$ when there is a single register.
- All values for x at distinct positions are distinct:

$$\mathsf{G}(\downarrow_x \mathsf{X}\mathsf{G} \neg \uparrow_x)$$

Similar Storing Mechanisms

- Freeze quantifier in hybrid logics.

  [Goranko 94; Blackburn & Seligman, JOLLI 95]

- Freeze quantifier in real-time logics.

  [Alur & Henzinger, JACM 94]

  $y \cdot \phi(y)$ binds the variable y to the current time t.

- Past LTL with Now operator (forgettable past).

  [Laroussinie & Markey & Schnoebelen, LiCS'02]

Complexity of Satisfiability Problems

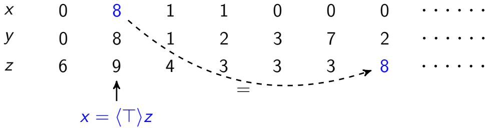
- Satisfiability for $\mathrm{LTL}^{\downarrow}(\mathbb{N}, =)$ restricted to one register and to the temporal operator F is undecidable.
  [Figueira & Segoufin, MFCS'09]

- Satisfiability for $\mathrm{LTL}^{\downarrow}(\mathbb{N}, =)$ restricted to one register and all occurrences of U are under an even number of negations is $\textsc{ExpSpace}$-complete. [Lazić, FSTTCS'11]

- More results about FO over (infinite) data words.
  [Bojańczyk et al., LiCS 06]

Repeating Values as a Storing Mechanism

- $\mathrm{LTL}^{\langle\top\rangle}(\mathcal{D})$: extension of $\mathrm{LTL}(\mathcal{D})$ with $x = \langle\top\rangle y$.



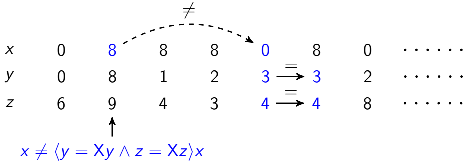
- $x = \langle\top\rangle y \approx \downarrow_{\mathtt{r}=x} \mathsf{XF} \ \uparrow_{\mathtt{r}=y}$.

- Satisfiability problem for $\mathrm{LTL}^{\langle\top\rangle}(\mathbb{N}, <, =)$ is undecidable.

  [Carapelle, PhD 2015]

Repeating Values with $(\mathbb{N}, =)$

- $\mathrm{LTL}^{\langle\rangle}(\mathbb{N}, =)$: extension of $\mathrm{LTL}(\mathbb{N}, =)$ with $x = \langle\phi\rangle y$ and $x \neq \langle\phi\rangle y$.



- $x = \langle\phi\rangle y \approx \downarrow_{\mathtt{r}=x} \mathsf{XF}\left(\uparrow_{\mathtt{r}=y} \wedge \phi\right)$.

- Satisfiability for $\mathrm{LTL}^{\langle\rangle}(\mathbb{N}, =)$ is 2EXPSPACE-complete.

  [Demri & Figueira & Praveen, LMCS 2016]

- Lower bound by reduction from control-state reachability for chained systems.

$$\begin{array}{cccccccccccc} 4 & 6 & 28 & 17 & 14 & 6 & 0 & 1 & 11 & 23 & \ldots \\ \mathtt{C}_1 & \mathtt{C}_2 & \mathtt{C}_3 & \mathtt{C}_4 & \mathtt{C}_5 & \mathtt{C}_6 & \mathtt{C}_7 & \mathtt{C}_8 & \mathtt{C}_9 & \mathtt{C}_{10} & \ldots \\ & & & & & \Uparrow & & & & & \end{array}$$

Conclusion

Recapitulation

- Introduction to LTL with concrete domain $\mathcal{D}$ and to constraint $\mathcal{D}$-automata.

- Presentation of several methods for handling classes of satisfiable symbolic models that are not ω-regular.
  1. Extending MSO while preserving decidability: EHD approach.
  2. Analysis of runs for $\mathcal{D}$-automata (for linear domains or string domains).
  3. Overapproximation using standard Büchi automata over finite alphabets.

- Brief introduction to global constraints including the freeze operator and its restrictions for repeating values.

Other Extensions

- Tree-like extensions, description logics.

[Bozzelli & Gascon, LPAR'06; Figueira, ToCL 2012; Labai et al., KR'20]

- More concrete domains such as string domains.

[Kartzow & Weidner, arXiv 2015; Peteler & Quaas, MFCS'22]
(N. Dumange –LMF– works on regularity constraints)

- Beyond satisfiability: model-checking, synthesis etc..

[Gascon, M4M'09; Bollig et al., LMCS 2019]
[Exibard et al., STACS'21; Bhaskar & Praveen, TIME'22]

- Relationships with counter machines, register automata, constraint automata, etc.

[Segoufin, CSL'06; Kartzow & Weidner, arXiv 2015]