Introduction to
Temporal Logics with Concrete Domains

Stéphane Demri
demri@lmaf.cnrs.fr

Étiolles, June 2023
Beyond Boolean Atomic Properties

\[ s_0 \models E \left( Xq \land (GFq \land GFr) \right) \] (with \( s_0 \rightarrow s_1 \rightarrow s_2 \rightarrow s_1 \rightarrow s_2 \cdots \))

\((E \approx \text{“there Exists a path”, } GF \approx \text{“infinitely often”})\)

\[ s_0 \models E \left( (x_3 < x_3) \land (GF(x_1 < x_2) \land GF(x_3 > x_1)) \right) \]

\(x_1 < Xx_2: \text{ “current value of } x_1 \text{ is smaller than the value of } x_2 \text{ at the next position”}.\)
Introductory Example

Is $E \in G \left( x_1 = X x_1 \land x_3 = X x_3 \land x_1 < x_2 < X x_2 < x_3 \right)$ satisfiable?

$$\phi$$

\[
\begin{array}{llllllllllll}
\uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \ldots \ldots \\
\uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \ldots \ldots \\
\end{array}
\]

- \( \left( \begin{array}{c}
1 \\
\frac{i+1}{i+2} \\
0
\end{array} \right)_{i \in \mathbb{N}} \vdash \phi \) with \( (\mathbb{Q}, <) \).
- \( \left( \begin{array}{c}
b \\
a^{i+1} \\
e
\end{array} \right)_{i \in \mathbb{N}} \vdash \phi \) with \( \{a, b\}^* \) and lexico. ordering.
- No model for \( (\mathbb{N}, <) \).
Linear-Time Temporal Logic LTL in a Nutshell
Specifying Properties on $\omega$-sequences

- Linear-time temporal logic LTL.
  
- LTL models $\rho$ are $\omega$-sequences of propositional valuations of the form $\rho : \mathbb{N} \to \mathcal{P}(PROP)$.

  $\begin{array}{cccccc}
p & q & p, q, r & q \\
0 & 1 & 2 & 3 & 4 & \ldots
\end{array}$

- LTL formulae:

  $\phi, \psi ::= p \mid \neg \phi \mid \phi \land \psi \mid \phi \lor \psi \mid X\phi \mid \phi U \psi$

- $X\phi$ states that the next position satisfies $\phi$:
Linear-Time Temporal Operators

- $\phi U \psi$ states that $\phi$ is true until $\psi$ is true.

- $F \phi$ states that some future position satisfies $\phi$.

(G$\phi$ states that $\phi$ is always satisfied.)
Satisfaction Relation

- $\rho, i \models p \iff p \in \rho(i)$,

- $\rho, i \models \neg \phi \iff \rho, i \not\models \phi$,

- $\rho, i \models \phi_1 \land \phi_2 \iff \rho, i \models \phi_1$ and $\rho, i \models \phi_2$,

- $\rho, i \models X\phi \iff \rho, i + 1 \models \phi$,

- $\rho, i \models \phi_1 U \phi_2 \iff$ there is $j \geq i$ such that $\rho, j \models \phi_2$ and $\rho, k \models \phi_1$ for all $i \leq k < j$.

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

- $\phi$ holds infinitely often: $\mathsf{GF}\phi$.

- Liveness: $\mathsf{G(messageSent} \Rightarrow \mathsf{F messageReceived})$.

- Total correctness.
  
  \[(\mathsf{init} \land \mathsf{precondition}) \Rightarrow \mathsf{F(end} \land \mathsf{postcondition})\]

- Strong fairness.
  
  \[\mathsf{GF processEnabled} \Rightarrow \mathsf{GF processExecuted}\]
Decision Problems

• Satisfiability problem for LTL.
  Input: LTL formula $\phi$.
  Question: Is there any model $\rho$ such that $\rho, 0 \models \phi$?

• Existential model-checking problem for LTL.
  Input: A finite transition system $S = (S, \mathcal{R}, v)$, $s \in S$ and an LTL formula $\phi$.
  Question: Is there any infinite run $\rho$ from $s$ such that $\rho, 0 \models \phi$?
Büchi Automata on Infinite Words

- Büchi automata accepts $\omega$-sequences in $\Sigma^\omega$ with acceptance condition $F$.

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

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

- Büchi automata accepts $\omega$-sequences in $\Sigma^\omega$ with acceptance condition $F$. 

- Generalised Büchi automata accepts $\omega$-sequences in $\Sigma^\omega$ with acceptance condition $F_1, F_2, \ldots, F_k$. 
Büchi Automaton For $G(p_1 \equiv Xp_2)$

Letters are subsets of $\{p_1, p_2\}$. 
A Selection of Nice Properties

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

  $\begin{array}{c}
  q_0 \quad * \quad q_f \\
  \end{array}$

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

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

• MSO is interpreted over $\rho : \mathbb{N} \rightarrow \Sigma$ using variable assignments $\mathcal{V} : (\text{VAR}_1 \rightarrow \mathbb{N}) + (\text{VAR}_2 \rightarrow \mathcal{P}(\mathbb{N}))$. 
**MSO Semantics**

\[ \phi := a(x) \mid x < y \mid Y(x) \mid (\phi \land \phi) \mid \neg \phi \mid \exists x.\phi \mid \exists Y.\phi \]

\[ \rho \models \forall a(x) \text{ iff } \rho(\forall(x)) = a \]

\[ \rho \models \forall Y(x) \text{ iff } \forall(x) \in \forall(Y) \]

\[ \rho \models \forall \phi \land \psi \text{ iff } \rho \models \forall \phi \text{ and } \rho \models \forall \psi \]

\[ \rho \models \forall \exists x.\phi \text{ iff there is } n \in \mathbb{N} \text{ s.t. } \rho \models \forall[x \mapsto n] \phi \]

\[ \rho \models \forall \exists Y.\phi \text{ iff there is } \mathcal{X}^\dagger \subseteq \mathbb{N} \text{ s.t. } \rho \models \forall[Y \mapsto \mathcal{X}^\dagger] \phi \]

- First-order logic $\mathcal{FO}$ over $\Sigma^\omega$ obtained by removing second-order variables in $\text{VAR}_2$.
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 \( \phi \) over \( \{p_1, \ldots, p_n\} \), design a Büchi automaton \( B_\phi \) over \( \Sigma = P(\{p_1, \ldots, p_n\}) \) s.t.

  for all \( \rho : \mathbb{N} \rightarrow \Sigma \), we have \( \rho, 0 \models \phi \) iff \( \rho \in L(B_\phi) \).

• Model-checking problem admits a similar reduction by checking \( L(B_\phi) \cap L(B_\psi) \neq \emptyset \).
Preliminary Definitions

• \( \phi \) 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 \( \phi \) and closed under subformulae,
  - \( \phi_1 U \phi_2 \in cl(\phi) \) implies \( X(\phi_1 U \phi_2) \in cl(\phi) \),
  - \( \phi_1 R \phi_2 \in cl(\phi) \) implies \( X(\phi_1 R \phi_2) \in cl(\phi) \).

• \( X \subseteq cl(\phi) \) is propositionally consistent iff
  - (for no propositional variable \( p \), we have \( \{p, \neg p\} \subseteq X \),)
  - if \( \phi_1 \lor \phi_2 \in X \), then \( \{\phi_1, \phi_2\} \cap X \neq \emptyset \),
  - if \( \phi_1 \land \phi_2 \in X \), then \( \{\phi_1, \phi_2\} \subseteq X \),
  - if \( \phi_1 U \phi_2 \in X \), then \( \{\phi_1, X(\phi_1 U \phi_2)\} \subseteq X \) or \( \phi_2 \in X \),
  - if \( \phi_1 R \phi_2 \in X \), then \( \{\phi_1, X(\phi_1 R \phi_2)\} \cap X \neq \emptyset \) and \( \phi_2 \in X \).
A Construction of $\mathcal{B}_\phi$

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

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

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

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

- If the U-formulae in $\phi$ are $\phi_1 U \psi_1, \ldots, \phi_k U \psi_k$,
  \[ F_i = \{\mathcal{X} \mid \psi_i \in \mathcal{X} \text{ or } \phi_i U \psi_i \notin \mathcal{X}\} \]
The location \( \mathcal{X} \) is understood as an obligation for the remaining of the \( \omega \)-word to satisfy all the formulae in \( \mathcal{X} \).

Many other constructions exist . . .

See e.g. [Gastin & Oddoux, CAV’01]

\[ \text{card}(Q) \] is exponential in the size of \( \phi \).

Nonemptiness of \( L(\mathcal{B}_\phi) \) can be checked in polynomial space in the size of \( \phi \).
Time to Wrap Up

- Satisfiability problem for LTL is \textsc{PSPACE}-complete.  
  \cite{SistlaClarke85}

- Model-checking problem for LTL is \textsc{PSPACE}-complete.  
  \cite{SistlaClarke85}

- LTL has good expressive power.
  - LTL expressively equivalent to FO.  \cite{KampPhD68}
  - Other characterisations in \cite{DiekertGastin08}
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

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

• Runs from counter machines

        q0    q2    q3    q2    q3    q2
        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.

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

- 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 $\Theta$: Boolean combination of atomic constraints of the form $R(t_1, \ldots, t_d)$.

\[(x_1 = x_2 + x_3) \lor (x_1 > x_4)\]

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

\[v \models R(t_1, \ldots, t_d) \iff (v(t_1), \ldots, v(t_d)) \in R^\mathbb{D}.\]

• A constraint $\Theta$ over $\mathcal{D}$ is satisfiable $\iff$ there is a valuation $v$ such that $v \models \Theta$. 
Linear Models in \((\mathbb{D}^\beta)^\omega\)

\[
x_{\beta} \quad \ldots \quad \quad \ldots \quad \quad \ldots \quad \quad \ldots \\
\vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \\
x_2 \quad \ldots \quad \quad \ldots \quad \quad \ldots \quad \quad \ldots \\
x_1 \quad \ldots \quad \quad \ldots \quad \quad \ldots \quad \quad \ldots \\
\vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \\
v_i : \{x_1, \ldots, x_\beta\} \rightarrow \mathbb{D}.
\]

\[
v_i : \{x_1, \ldots, x_\beta\} \rightarrow \mathbb{D}.
\]
**LTL(\(\mathcal{D}\)): LTL with Concrete Domain \(\mathcal{D}\)**

\[
\phi ::= R(t_1, \ldots, t_d) \mid \phi \land \phi \mid \neg \phi \mid X\phi \mid \phi U \phi
\]

- The \(t_i\)'s are terms of the form \(X^jx\) and ‘\(Xx\)’ refers to the next value of \(x\).

- **LTL(\(\mathcal{D}\)) model** \(\rho : \mathbb{N} \times \text{VAR} \to \mathcal{D}\).

**Satisfaction relation**

- \(\rho(i, X^jx) \overset{\text{def}}{=} \rho(i + j, x)\).

- \(\rho, i \models R(t_1, \ldots, t_d) \overset{\text{def}}{\iff} (\rho(i, t_1), \ldots, \rho(i, t_d)) \in R^\mathcal{D}\)

- \(\rho, i \models X\phi \overset{\text{def}}{\iff} \rho, i + 1 \models \phi\)

\[
\begin{array}{cccccc}
& x_1 & 0 & \frac{3}{8} & \frac{1}{9} & 3 & \ldots \\
& x_2 & \frac{1}{2} & 0 & \frac{3}{4} & 2 & \ldots \\
& x_3 & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & 1 & \ldots \\
& x_4 & 1 & 2 & 3 & 4 & \ldots \\
\end{array}
\]

\(\models F(x_2 < XXx_3)\)
Simple Properties

• “Infinitely often \( x \) is a prefix of the next value for \( y \)”

\[
GF(x \preceq_{\text{pre}} Xy)
\]

• “The value for \( x \) is strictly decreasing”

\[
G(x > Xx)
\]

• “The value for \( x \) is equal to some future value of \( y \)”

\[
G(x^{\text{new}} = Xx^{\text{new}}) \land x = x^{\text{new}} \land F(x^{\text{new}} = y)
\]
Back to (Constraint) Automata

\[ Xx = x - 1 \]

\[ Xx = x + 1 \]

\[ x = 0 \land Xx = x \]

\[
\begin{align*}
q_2 & \xrightarrow{Xx=x-1} q_2 \xrightarrow{Xx>x} q_1 \xrightarrow{Xx=x+1} q_1 \xrightarrow{Xx=x-1} q_2 \xrightarrow{Xx>x} q_1 \xrightarrow{Xx=x+1} q_1 \ldots \\
3 & \rightarrow 2 \rightarrow 28 \rightarrow 29 \rightarrow 28 \rightarrow 35 \rightarrow 36 \ldots
\end{align*}
\]
Definition

- $\mathcal{D}$-automaton $A = (Q, \beta, Q_{\text{in}}, \delta, F)$ with $\beta$ 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,
  - $\delta$ is a finite subset of $Q \times \text{Bool}(\mathcal{D}, \beta) \times Q$, where
    $\text{Bool}(\mathcal{D}, \beta)$ is the set of $\mathcal{D}$-constraints over
    $\{x_1, \ldots, x_\beta\} \cup \{Xx_1, \ldots, Xx_\beta\}$.

- $v_0v_1 \cdots \in L(A) \iff$ there is $q_0 \xrightarrow{\Theta_0} q_1 \xrightarrow{\Theta_1} \cdots$ such that
  - $q_0 \in Q_{\text{in}}$ and some $q \in F$ occurs $\infty$-often in $q_0q_1q_2 \cdots$.
  - for all $i \in \mathbb{N}$, $q_i \xrightarrow{\Theta_i} q_{i+1} \in \delta$ and $v_i, v_{i+1} \models \Theta_i$. 
Decision Problems

• Nonemptiness problem for $\mathcal{D}$-automata.
  
  **Instance:** A $\mathcal{D}$-automaton $A$.
  
  **Question:** Is $L(A) \neq \emptyset$?

• Satisfiability problem for $\text{LTL(}\mathcal{D})$:
  
  **Instance:** A $\text{LTL(}\mathcal{D})$ formula $\phi$.
  
  **Question:** Is there a model $\rho$ such that $\rho, 0 \models \phi$?

• Existential model-checking problem for $\text{LTL(}\mathcal{D})$:
  
  **Instance:** A $\mathcal{D}$-automaton $A$ and a $\text{LTL(}\mathcal{D})$ formula $\phi$.
  
  **Question:** is there a model $\rho$ such that $\rho, 0 \models \phi$ and $\rho \in L(A)$?

• Satisfiability for $\text{LTL(}\mathbb{N}, =, +1)$ is undecidable.
  Flat Presburger $\text{LTL}$ is decidable. [Comon & Cortier, CSL’00]
Symbolic Models

• \( \text{Atoms}(\mathcal{D}, \beta) \): set of atomic constraints built over \( \{x_1, \ldots, x_\beta\} \) and \( \{Xx_1, \ldots, Xx_\beta\} \).

• \( \mathcal{X} \subseteq \text{Atoms}(\mathcal{D}, \beta) \) is understood as the constraint
  \[
  (\bigwedge_{\theta \in \mathcal{X}} \theta) \land (\bigwedge_{\theta \in (\text{Atoms}(\mathcal{D}, \beta) \setminus \mathcal{X})} \neg \theta).
  \]

• Symbolic model \( w : \mathbb{N} \rightarrow \mathcal{P}(\text{Atoms}(\mathcal{D}, \beta)) \).

• \( w \) is \( \mathcal{D} \)-satisfiable \( \iff \) there is \( \rho : \mathbb{N} \times \{x_1, \ldots, x_\beta\} \rightarrow \mathcal{D} \) such that for all \( i \), \( \{\theta \in \text{Atoms}(\mathcal{D}, \beta) \mid \rho, i \models \theta\} = w(i) \).

• \( \rho, i \models x = Xy \iff \rho(i, x) = \rho(i + 1, y) \).
A Selection of Problems

- \( L(\mathbb{A}) \neq \emptyset \) iff for some \( w : \mathbb{N} \rightarrow \mathcal{P}(\text{Atoms}(D, \beta)) \),
  - \( w \) is \( D \)-satisfiable and,
  - 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 \( w(i) \models \Theta_i \).

- \( w(i) \models \Theta_i \) def
  \[ (\bigwedge_{\theta \in w(i)} \theta) \land (\bigwedge_{\theta \in (\text{Atoms}(D, \beta) \setminus w(i))} \neg \theta) \Rightarrow \Theta_i \text{ is valid.} \]

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

- Can the class of \( D \)-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 $Xx$’s.

\[ x < XXy \iff G(y_1 = xy_0 \land y_2 = xy_1) \land x < y_2 \]

- Given $\phi \in \text{LTL}(\mathcal{D})$, there is a $\mathcal{D}$-automaton $A_\phi$ such that

\[ L(A_\phi) = \{ \rho : \mathbb{N} \times \{x_1, \ldots, x_\beta\} \rightarrow \mathbb{D} \mid \rho, 0 \models \phi \} \]
Automata Construction

- \( \phi \) 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.

- \( A_\phi = (Q, \beta, Q_{in}, \delta, F_1, \ldots, F_k) \).

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

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

\[
\{ x < Xy, \neg(z = 0), X(x < Xy U \neg(z = 0)) \} \xrightarrow{x < Xy \land \neg(z = 0)} \{ \neg(z = 0), x < Xy U \neg(z = 0) \}
\]
Three Ways for Deciding $\text{LTL}(D)$
Dense and Open \((\mathbb{Q}, <, \equiv)\): the Easy Way

- Symbolic model \(w\) is \(\mathbb{Q}\)-satisfiable iff for all \(i \in \mathbb{N}\),
  
  \(\text{(LocalSat)}\) \((\bigwedge_{\theta \in w(i)} \theta) \land (\bigwedge_{\theta \in (\text{Atoms}(\mathcal{D}, \beta) \setminus w(i))} \neg \theta)\) is satisfiable,

  \(\text{(OneShift)}\) \(\{Xx_1, \ldots, Xx_\beta\}\) in \(w(i)\) and \(\{x_1, \ldots, x_\beta\}\) in \(w(i + 1)\) coincide.

- The set of \(\mathbb{Q}\)-satisfiable symbolic models is \(\omega\)-regular.

- \(\text{SAT}(\text{LTL}(\mathbb{Q}, <, \equiv))\) is \(\text{PSPACE}\)-complete.
  
  \([\text{Balbiani & Condotta, FroCoS’02}]\)

- \(\text{SAT}(\text{LTL}(\text{RCC8}))\) is \(\text{PSPACE}\)-complete too.
  
  \([\text{Balbiani & Condotta, FroCoS’02}]\)
How to Handle Non-$\omega$-Regularity?

- Given $(\mathbb{N}, <, =)$, the set $\text{SatSMod}(\mathbb{N})$ of $\mathbb{N}$-satisfiable symbolic models is not $\omega$-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 $D$-satisfiable symbolic models for $D = (\mathbb{N}, <, =)$.

• 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 \((\mathbb{N}, <, \leq)\)

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

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

\[
\begin{array}{c}
\text{x} \\
\uparrow < \\
\text{y}
\end{array} \quad \begin{array}{c}
\text{=} \\
\uparrow < \\
\text{=} \\
\uparrow < \\
\text{=} \\
\uparrow < \\
\text{=} \\
\quad \quad \quad \text{\ldots \ldots}
\end{array} \quad \begin{array}{c}
\text{=} \\
\uparrow < \\
\text{=} \\
\uparrow < \\
\text{=} \\
\uparrow < \\
\text{=} \\
\quad \quad \quad \text{\ldots \ldots}
\end{array}
\]

- Strict length of the finite path \(\pi\):

\[\text{slen}(\pi) \overset{\text{def}}{=} \text{number of edges labelled by } <.\]

- Strict length of \((i, x)\):

\[\text{slen}((i, x)) \overset{\text{def}}{=} \text{sup} \{\text{slen}(\pi) : \text{finite path } \pi \text{ leading to } (i, x)\}\]
\(\mathbb{N}\)-Satisfiable Symbolic Models

- Symbolic model \(w\) is \(\mathbb{N}\)-satisfiable iff

\[
\text{(LocalSat)} \quad (\bigwedge_{\theta \in w(i)} \theta) \land (\bigwedge_{\theta \in \text{Atoms}(D, \beta) \setminus w(i)} \neg \theta) \text{ is satisfiable for all } i,
\]

\[
\text{(OneShift)} \quad \{Xx_1, \ldots, Xx_\beta\} \text{ in } w(i) \text{ and } \{x_1, \ldots, x_\beta\} \text{ in } w(i+1) \text{ coincide for all } i,
\]

\[
\text{(FiniteSLength)} \quad \text{any node has a finite strict length.}
\]

[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 \( \omega \)-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]

• \( \rho : \mathbb{N} \rightarrow \Sigma, \mathcal{V} : (\text{VAR}_1 \rightarrow \mathbb{N}) + (\text{VAR}_2 \rightarrow \mathcal{P}(\mathbb{N})) \).

• \( \rho \models_{\mathcal{V}} B Y.\phi \overset{\text{def}}{\iff} \) there is bound \( b \in \mathbb{N} \) such that whenever \( \rho \models_{\mathcal{V}}[Y \mapsto X^+] \phi \) for some finite set \( X^+ \subseteq \mathbb{N} \), \( \text{card}(X^+) \leq b \). [Bojańczyk, CSL’04]

• \( B \) well-designed to express (StrictSLength).
  (Idea: “for any node \( n \), any path labelled by \( (\lt \cup =)^+ \) leading to \( n \) has a bounded number of edges \( \xrightarrow{} \)”)
Decidable MSO Extensions with $B$

• Satisfiability $\text{MSO} + B$ is undecidable over $\omega$-words.  
  [Bojańczyk & Parys & Toruńczyk, STACS’16]

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

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

• Negation-closed $\mathcal{D}$ with $\text{EHD}(\text{BMW})$-property.  
  Satisfiability problem for $\text{CTL}^*(\mathcal{D})$ 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 $\mathcal{D}$.

\[(\neg (x = n) \iff \exists y (y = n) \land ((x < y) \lor (y < x)))\]

2) EHD(BMW) property for symbolic models.

There is $\phi_{SAT}$ in BMW for $\omega$-words such that

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

- EHD = “the Existence of a Homomorphism is Definable”.

- 2) EHD(BMW) property (complete version).

For every finite subsignature $\tau$, one can compute $\phi_\tau$ such that for every countable $\tau$-structure $S$,

there is an homomorphism from $S$ to $\mathcal{D}$ iff $S \models \phi_\tau$.

\approx \mathcal{D}$-satisfiability
New Decidability Results

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

- The satisfiability problem for 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 \(\mathcal{ALCF}_{P}(\mathbb{Z}, <, =, (=n)_{n \in \mathbb{Z}})\) is decidable.  
  [Carapelle & Turhan, ECAI’16]
\[ \mathbb{N} \text{-automata} \]

- EHD powerful for decidability, unsatisfactory for complexity!

- Concrete domains \( \mathcal{D} = (\mathbb{D}, <, P_1, \ldots, P_I, =_{o_1}, \ldots, =_{o_m}) \), 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.
**N-Automata: Extensible Lassos**

A has an accepting run iff there are finite runs $\pi, \lambda$ 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. "type($\vec{x}$) = type($\vec{y}$)", $\vec{x} \leq \vec{y}$ and $dv(\vec{x}) \leq dv(\vec{y})$.

\[
\begin{array}{c}
0 \ 7 \ 2 \ 9 \ 6 \ 15 \\
\end{array}
\]

$dv(\begin{pmatrix} 15 \\ 9 \\ 7 \end{pmatrix}) = \begin{pmatrix} 7 \\ 2 \\ 6 \end{pmatrix}$

\begin{flalign*}
\vec{x} & \quad \vec{y} \\
& < \\
& < \\
& < \\
& < \\
& \ldots \ldots \quad \ldots \ldots \\
& < \\
& < \\
\end{flalign*}

Conditions (2) and (3) allow us to repeat infinitely $\lambda$.

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 $\vec{x}[j'] < \vec{x}[j]$.  

[Diagram of less-than relationships between vectors $\vec{x}$ and $\vec{y}$]
- Automata: Lasso Detection in PSpace

- Existence of finite runs $\pi, \lambda$ 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
  - $D_{\mathbb{Q}^*} = (\mathbb{Q}^*; \preceq_{\text{pre}}, \preceq_{\text{lex}}, =_{d_1}, \ldots, =_{d_m})$.
  - $D_{[1, \alpha]^*} = ([1, \alpha]^*; \preceq_{\text{pre}}, \preceq_{\text{lex}}, =_{d_1}, \ldots, =_{d_m}), \alpha \geq 2$. [Kartzow & Weidner, arXiv 2015]
Ultimately Periodic Models

• A symbolic model $w$ is ultimately periodic iff $w$ of the form

$$w(0) \cdots w(l - 1) \cdot (w(l) \cdots w(l + J))^\omega$$

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

• Reminder: $L(A) \neq \emptyset$ iff $\exists w : \mathbb{N} \rightarrow \mathcal{P}(Atoms(\mathbb{N}, \beta))$,

  1) $w$ 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 $w(i) \models \Theta_i$ (Büchi automaton $\mathbb{B}_2$).
Forthcoming Features of (Approx)

If

- Condition (Approx) is $\omega$-regular (Büchi automaton $B_1$).
- For all ultimately periodic symbolic models $w$, $w$ is $\mathbb{N}$-satisfiable iff $w$ satisfies (Approx).
- Symbolic models built from $(\mathbb{N}^\beta)^\omega$ satisfy (Approx).

Then

$$L(B_1) \cap L(B_2) \neq \emptyset \text{ iff } L(A) \neq \emptyset.$$
**Condition (Approx)**

Symbolic model $w$ satisfies the condition (Approx) iff

1. (LocalSat) and (OneShift).

2. There is no infinite $(j_1, z_1) \overset{a_1}{\rightarrow} (j_2, z_2) \overset{a_2}{\rightarrow} (j_3, z_3) \cdots$ s.t. $\{a_1, a_2, \ldots\} \subseteq \{=, >\}$ and infinitely often $a_j$'s equals $>$. 

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

\[
\begin{array}{cccccccc}
\star\star & =^* & \bullet & < & \bullet & =^* & \bullet & < & \bullet & =^* & \bullet & < & \bullet & < & \cdots \\
\downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \\
\star\star & =^* & \bullet & > & \bullet & =^* & \bullet & > & \bullet & =^* & \bullet & > & \bullet & =^* & \bullet & =^\omega
\end{array}
\]

with infinite amount of $\overset{\bowtie}{\rightarrow}$ from $\star\star$ on top path and finite amount of $\overset{\rightrightarrows}{\rightarrow}$ from $\dag\dag$ on bottom path

$(\text{LocalSat}) \land (\text{OneShift}) \land (\text{FiniteSL}) \Rightarrow (\text{Approx})$
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 \(\omega\)-regular.

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

• Results apply to \((\mathbb{Z}, <, =)\) with adequate adaptations.
SatSMod(\(\mathbb{N}\)) is Not \(\omega\)-Regular

- Non \(\mathbb{N}\)-satisfiable symbolic model \(w^*\) satisfying (Approx).
- \(\text{SatSMod}(\mathbb{N}) \cap \text{(Approx)}\) is \(\omega\)-regular and contains \(w^*\).
- \(\text{SatSMod}(\mathbb{N}) \cap \text{(Approx)}\) contains an ultimately periodic symbolic model \(w^{\dagger}\) satisfying (Approx).
- So, \(w^{\dagger}\) is \(\mathbb{N}\)-satisfiable, contradiction.

Ad absurdum, suppose SatSMod(\(\mathbb{N}\)) is \(\omega\)-regular.
Global Constraints on Data Values
Global Constraints

- So far, constraints have a local scope.

\[
\begin{array}{cccccccccccccc}
  x & 0 & 8 & 1 & 1 & < & 0 & 0 & 0 & 0 & \cdots & \cdots \\
y & 0 & 8 & 1 & 2 & 3 & = & 7 & 2 & \cdots & \cdots \\
z & 6 & 9 & 4 & 3 & 3 & 3 & 3 & 8 & \cdots & \cdots \\
\end{array}
\]

\[x < Xy \land XXz = Xy\]

- Global constraints have unbounded scope.

\[
\begin{array}{cccccccccccccc}
  x & 0 & 8 & 1 & 1 & 0 & 0 & 0 & 0 & \cdots & \cdots \\
y & 0 & 8 & 1 & 2 & 3 & 7 & 2 & \cdots & \cdots \\
z & 6 & 9 & 4 & 3 & 3 & 3 & 3 & 8 & \cdots & \cdots \\
\end{array}
\]

\[x = \langle \top \rangle z\]

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

\[G(\neg (x = \langle \top \rangle x))\]
LTL with Registers

- $\downarrow_{r=x} \phi$ states that freezing the value of $x$ in the register $r$ makes true the formula $\phi$.

- Registers in $RVAR = \{r, s, t, \ldots\}$.

- LTL↓$(\mathcal{D})$ formulae:
  $$\phi ::= R(t_1, \ldots, t_d) | \phi \land \phi | \neg \phi | \uparrow_{r=y} | \downarrow_{r=x} \phi | \mathbf{X}\phi | \phi \mathbf{U} \phi,$$

- Environment $env : RVAR \rightarrow \mathbb{D}$, $\rho : \mathbb{N} \times VAR \rightarrow \mathbb{D}$.

- $\rho, i \models_{env} \downarrow_{r=x} \phi \overset{\text{def}}{\iff} \rho, i \models_{env[r \mapsto \rho(i, x)]} \phi$.

- $\rho, i \models_{env} \uparrow_{r=y} \overset{\text{def}}{\iff} env(r) = \rho(i, y)$.

- We use $\uparrow_y$ and $\downarrow_x$ when there is a single register.

- All values for $x$ at distinct positions are distinct:
  $$G(\downarrow_x XG\neg \uparrow_x)$$
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 $\mathsf{LTL}^\downarrow(\mathbb{N}, =)$ restricted to one register and to the temporal operator $\mathsf{F}$ is undecidable.  
  [Figueira & Segoufin, MFCS'09]

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

- More results about $\mathsf{FO}$ over (infinite) data words.  
  [Bojańczyk et al., LiCS 06]
Repeating Values as a Storing Mechanism

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

\[
\begin{array}{cccccccccc}
x & 0 & 8 & 1 & 1 & 0 & 0 & 0 & 0 & \ldots \ldots \\
y & 0 & 8 & 1 & 2 & 3 & 7 & 2 & \ldots \ldots \\
z & 6 & 9 & 4 & 3 & 3 & 3 & & & \rightarrow 8 \ldots \ldots \\
\end{array}
\]

- \( x = \langle T \rangle z \)

- \( x = \langle T \rangle y \approx \downarrow_{r=x} \text{XF} \uparrow_{r=y} \).

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

[Carapelle, PhD 2015]
Repeating Values with \((\mathbb{N},=)\)

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

\[
\begin{array}{cccccccc}
  x & 0 & 8 & 8 & 8 & 0 & 8 & 0 & \cdots \\
  y & 0 & 8 & 1 & 2 & 3 & 3 & 2 & \cdots \\
  z & 6 & 9 & 4 & 3 & 4 & 4 & 8 & \cdots \\
\end{array}
\]

- **Satisfiability for LTL\(^\langle\rangle\)(\(\mathbb{N},=)\) is \(2\text{EXPSPACE}\)-complete.**
  
  \[\text{[Demri & Figueira & Praveen, LMCS 2016]}\]

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

\[
\begin{array}{cccccccccccc}
  4 & 6 & 28 & 17 & 14 & 6 & 0 & 1 & 11 & 23 & \ldots \\
  C_1 & C_2 & C_3 & C_4 & C_5 & C_6 & C_7 & C_8 & C_9 & C_{10} & \ldots \\
\end{array}
\]
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 $\omega$-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]