Temporal Logics on Strings with Prefix Relation

Stéphane Demri
CNRS – Marie Curie Fellow

Joint work with Morgan Deters (NYU)

Corunna, February 2015

In Memoriam: Morgan Deters

LTL over Concrete Domains

Logics with Concrete Domains

- Temporal propositional logic $\mathfrak{L}$,
- Concrete domain $\mathcal{D} = \langle \mathfrak{D}, (\mathfrak{R}_i)_{i \in I} \rangle$,

$\Longrightarrow$

$\mathfrak{L}(\mathcal{D})$

- replacing propositional variables by domain-specific constraints,
- variables interpreted by elements of $\mathfrak{D}$.

Concrete Domains

- Concrete domain: $\mathcal{D} = \langle \mathfrak{D}, (\mathfrak{R}_i)_{i \in I} \rangle$.
- Interpretation domains for program variables.
- Atomic constraint: $\mathfrak{R}(\mathsf{x}_1, \ldots, \mathsf{x}_t)$.
- A $\mathfrak{D}$-valuation $v : \mathrm{VAR} \to \mathfrak{D}$.
- Examples:

$$\langle \mathbb{N}, \leq \rangle \quad \langle \{0,1\}^*, \preceq_p \rangle \quad \langle \mathbb{N}, =, +1 \rangle \quad \langle \mathbb{Q}, <, = \rangle$$

LTL over Concrete Domains

- Atomic term constraint $\mathfrak{R}(\mathsf{X}^{n_1}\mathsf{x}_1, \ldots, \mathsf{X}^{n_t}\mathsf{x}_t)$.

- X^i x interpreted as the value of x in the *i*th next state.

- $\phi ::= \mathfrak{R}(\mathsf{X}^{n_1}\mathsf{x}_1, \ldots, \mathsf{X}^{n_t}\mathsf{x}_t) \mid \mathsf{X}\phi \mid \phi \mathsf{U} \phi \mid \neg\phi \mid \ldots$

- Linear models: $\sigma : \mathbb{N} \rightarrow (\mathsf{VAR} \rightarrow \mathfrak{D})$.

$$\sigma, j \models \mathfrak{R}(\mathsf{X}^{n_1}\mathsf{x}_1, \ldots, \mathsf{X}^{n_t}\mathsf{x}_t)$$

iff

$$(\overbrace{\sigma(j+n_1)(\mathsf{x}_1)}^{\text{value of } \mathsf{x}_1 \text{ in the } (j+n_1)\text{th state}}, \ldots, \sigma(j+n_t)(\mathsf{x}_t)) \in \mathfrak{R}$$

i.e. values at different states can be compared.

A $\mathrm{LTL}(\mathbb{Q}, <, =)$-model

$$
\begin{array}{llllll}
x_1 & 0 & \frac{3}{8} & \frac{1}{9} & 3 & \dots \\
x_2 & \frac{1}{2} & \mathbf{0} & \frac{3}{4} & 2 & \dots \\
x_3 & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \mathbf{1} & \dots \\
x_4 & 1 & 2 & 3 & 4 & \dots
\end{array}
\models \mathsf{F}(x_2 < \mathsf{X}^2 x_3)
$$

Satisfiability of ϕ: is there σ such that $\sigma, 0 \models \phi$?

Spatio-Temporal Logics

- $\mathcal{D}$ is a spatial domain in spatio-temporal logics, see e.g. [Balbiani & Condotta, FROCOS'02; Wolter & Zakharyaschev, 2002]

- $\mathcal{D}$ is rather a class of domains.

- Example: RCC-8 [Randel & Cui & Cohn92, KR'92]
  Variables interpreted as regions
  Predicates: being "disconnected", "equal", "partial overlap", ...

LTL with Presburger Constraints

- Constraints on counters: $\mathsf{Xx} = \mathsf{x} + 1$, $\mathsf{x} < \mathsf{XXy}$.
- Satisfiability for LTL$(\mathbb{N}, =, +1)$ is undecidable.

LTL with Presburger Constraints

- Constraints on counters: $\mathsf{X}x = x + 1$, $x < \mathsf{XX}y$.

- Satisfiability for LTL$(\mathbb{N}, =, +1)$ is undecidable.

- LTL$(\mathbb{Z}, =, <)$ is PSPACE-complete.

[Demri & D'Souza, IC 07]

See also [Segoufin & Toruńczyk, STACS'11]

LTL with Presburger Constraints

- Constraints on counters: $\mathsf{X}x = x + 1$, $x < \mathsf{XX}y$.
- Satisfiability for LTL$(\mathbb{N}, =, +1)$ is undecidable.
- LTL$(\mathbb{Z}, =, <)$ is PSPACE-complete.

[Demri & D'Souza, IC 07]

See also [Segoufin & Toruńczyk, STACS'11]

- Variants of LTL with Presburger constraints in:
  - [Bouajjani et al., LICS 95], [Comon & Cortier, CSL'00],
  - [Dang & Ibarra & San Pietro, FST&TCS'01].

What is the problem with $\mathrm{LTL}(\mathcal{D})$?

- Local satisfiability is constrained.
  - $\mathrm{p}_1, \ldots, \mathrm{p}_n$ can hold independently of each other.
  - $x_0 < x_1, \ldots, x_{n-1} < x_n$ are not independent.
- Global satisfiability is constrained.
  - $\mathrm{G}\mathrm{p}$ is satisfiable in LTL.
  - $\mathrm{G}(\mathrm{X}x < x)$ is not satisfiable in $\mathrm{LTL}(\mathbb{N}, <)$.
- How formulae define ω-regular classes of models ?

Temporal Logics on Strings

Reasoning about Strings

- Need for string reasoning: program verification, analysis of web applications, etc.
- Theory solvers for strings.
  [Liang et al. – Abdulla et al., CAV'14; Hutagalung & Lange, CSR'14]
- Solving word equations.
  [Makanin, Math. 77; Plandowski, JACM 04]
- What about reasoning on sequences of strings ?

LTL on Strings: $\mathrm{LTL}(\Sigma^*, \preceq_p)$

- String variables $\mathrm{SVAR} = \{x_1, x_2, \ldots\}$.
- Terms: $\mathtt{t} \quad ::= \quad \mathfrak{w} \mid x \mid Xx \qquad\qquad (x \in \mathrm{SVAR}, \mathfrak{w} \in \Sigma^*)$
- Formulae:

$$\phi \quad ::= \quad \mathtt{t} \preceq_p \mathtt{t}' \mid \neg\phi \mid \phi \wedge \phi \mid X\phi \mid \phi \, U \, \phi$$

- Example:

$$GF((001 \preceq_p x) \vee (x \preceq_p 1001)) \wedge G(\neg(x \preceq_p Xx))$$

A Model with $\Sigma = \{0, 1\}$

x_1	000	011110	ε	1111	...
x_2	101	**010001**	010001	00	...
x_3	00	111	**010001101**	ε	...

$\models \mathsf{F}(x_2 \preceq_p \mathsf{X}x_3)$

The Case $\Sigma = \{0\}$

- $\mathrm{LTL}(\mathbb{N}, \leq) \stackrel{\text{def}}{=} \mathrm{LTL}(\Sigma^*, \preceq_p)$ with $\Sigma = \{0\}$.

- Satisfiability problem for $\mathrm{LTL}(\mathbb{N}, \leq)$ is PSPACE-complete.

  [Demri & D'Souza, IC 07; Demri & Gascon, TCS 08]

  See also [Segoufin & Torunczyk, STACS'11]

- The PSPACE upper bound is preserved with several LTL extensions or with richer numerical constraints.
  (but no successor relation).

A Richer and Auxiliary Logic $\mathrm{LTL}(\Sigma^*, \mathrm{clen})$

- $\mathrm{clen}(\mathfrak{w}, \mathfrak{w}')$: length of the longest common prefix between $\mathfrak{w}$ and $\mathfrak{w}'$ in Σ^*.

$$\sigma, i \models \mathrm{clen}(\mathtt{t}_0, \mathtt{t}'_0) \leq \mathrm{clen}(\mathtt{t}_1, \mathtt{t}'_1)$$

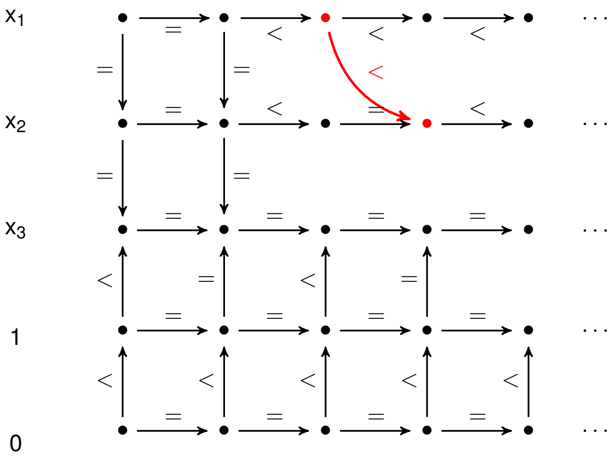
$$\stackrel{\text{def}}{\Leftrightarrow}$$

$$\mathrm{clen}([\mathtt{t}_0]_i, [\mathtt{t}'_0]_i) \leq \mathrm{clen}([\mathtt{t}_1]_i, [\mathtt{t}'_1]_i)$$

- Reduction from $\mathrm{LTL}(\Sigma^*, \preceq_p)$ to $\mathrm{LTL}(\Sigma^*, \mathrm{clen})$.
  $\mathtt{t} \preceq_p \mathtt{t}' \mapsto \mathrm{clen}(\mathtt{t}, \mathtt{t}) \leq \mathrm{clen}(\mathtt{t}, \mathtt{t}')$.

- In the sequel either $\Sigma = [0, k-1]$ for some $k \geq 1$ or $\Sigma = \mathbb{N}$.

Symbolic Models for $\mathrm{LTL}(\mathbb{N}, \leq)$



$\models_{\text{symb}} \mathsf{XX}(x_1 < \mathsf{X}x_2)$

+ Local consistency between two consecutive positions.

Rephrasing the Satisfiability Property

ϕ is $\mathrm{LTL}(\mathbb{N}, \leq)$ satisfiable

iff

there is a symbolic model σ such that

$\sigma \models_{\mathrm{symb}} \phi$ and σ has a concrete interpretation in $\mathbb{N}$

Characterisation for $\mathrm{LTL}(\mathbb{N}, \leq)$

- Usual notion of path π between two nodes.

- Strict length of the path π: $\mathrm{slen}(\pi)$ = number of edges labelled by $<$.

- Strict length between $\langle \mathsf{x}, i \rangle$ and $\langle \mathsf{x}', i' \rangle$:

$$\mathrm{slen}(\langle \mathsf{x}, i \rangle, \langle \mathsf{x}', i' \rangle) \stackrel{\text{def}}{=} \mathit{sup}\, \{\mathrm{slen}(\pi) : \text{ path } \pi \text{ from } \langle \mathsf{x}, i \rangle \text{ to } \langle \mathsf{x}', i' \rangle\}$$

Characterisation for $\mathrm{LTL}(\mathbb{N}, \leq)$

- Usual notion of path π between two nodes.

- Strict length of the path π: $\mathrm{slen}(\pi)$ = number of edges labelled by $<$.

- Strict length between $\langle \mathsf{x}, i \rangle$ and $\langle \mathsf{x}', i' \rangle$:

$$\mathrm{slen}(\langle \mathsf{x}, i \rangle, \langle \mathsf{x}', i' \rangle) \stackrel{\text{def}}{=} \mathit{sup} \, \{\mathrm{slen}(\pi) : \text{ path } \pi \text{ from } \langle \mathsf{x}, i \rangle \text{ to } \langle \mathsf{x}', i' \rangle\}$$

- Symbolic model σ has a concrete interpretation iff any pair of nodes has a finite strict length.

[Cerans, ICALP'94; Demri & D'Souza, IC 07]

[Gascon, PhD thesis 07;Carapelle & Kartzow & Lohrey, CONCUR'13]

When WMSO+U Enters Into the Play

- $\sigma \models \mathrm{U}\,\mathrm{X}\,\phi \stackrel{\text{def}}{\Leftrightarrow}$ for every $b \in \mathbb{N}$, there is a finite Y with $\mathrm{card}(Y) \geq b$ such that $\sigma \models \phi(Y)$.
  $\mathrm{B}\mathrm{X}\,\phi \stackrel{\text{def}}{=} \neg\mathrm{U}\,\mathrm{X}\,\phi$.
  [Bojańczyk, CSL'04; Bojańczyk & Colcombet, LICS'06]

- Symbolic models for $\mathrm{LTL}(\mathbb{N}, \leq)$ having a concrete interpretation can be characterized by a formula in Bool(MSO,WMSO+U).

- This leads to decidability of $\mathrm{CTL}^{\star}(\mathbb{N}, \leq)$.
  [Carapelle & Kartzow & Lohrey, CONCUR'13]
  (based on [Bojańczyk & Toruńczyk, STACS'12])
  See also decidable fragments in [Bozzelli & Gascon, LPAR'06]

Back to Strings
Simple but Essential Properties for $\mathrm{clen}(\cdot)$

$\mathfrak{w}_1$ **0 0 0** 1 0 2

$\mathfrak{w}_2$ **0 0 0** 0

$\longrightarrow \mathrm{clen}(\mathfrak{w}_1, \mathfrak{w}_2) \leq \mathrm{len}(\mathfrak{w}_1)$

Back to Strings
Simple but Essential Properties for $\mathrm{clen}(\cdot)$

$\mathfrak{w}_1$ **0 0 0** 1 0 2
$\mathfrak{w}_2$ **0 0 0** 0
$\longrightarrow \mathrm{clen}(\mathfrak{w}_1, \mathfrak{w}_2) \leq \mathrm{len}(\mathfrak{w}_1)$

$\mathfrak{w}_0$ **0 0 0** 1 0 2
$\mathfrak{w}_1$ **0 0 0** 0 1 3 5 6
$\mathfrak{w}_2$ **0 0 0** 2 1 4
...
$\mathfrak{w}_k$ **0 0 0** 3 1 3
$\longrightarrow \exists i, j \in [1, k]$ such that $\mathrm{clen}(\mathfrak{w}_0, \mathfrak{w}_1) < \mathrm{clen}(\mathfrak{w}_i, \mathfrak{w}_j)$
(Pigeonhole Principle – $\mathrm{card}(\Sigma) = k \geq 2$)

Back to Strings
Simple but Essential Properties for $\mathrm{clen}(\cdot)$

$\mathfrak{w}_1$ **0 0 0** 1 0 2
$\mathfrak{w}_2$ **0 0 0** 0
$\longrightarrow \mathrm{clen}(\mathfrak{w}_1, \mathfrak{w}_2) \leq \mathrm{len}(\mathfrak{w}_1)$

$\mathfrak{w}_0$ **0 0 0** 1 0 2
$\mathfrak{w}_1$ **0 0 0** 0 1 3 5 6
$\mathfrak{w}_2$ **0 0 0** 2 1 4
...
$\mathfrak{w}_k$ **0 0 0** 3 1 3
$\longrightarrow \exists i, j \in [1, k]$ such that $\mathrm{clen}(\mathfrak{w}_0, \mathfrak{w}_1) < \mathrm{clen}(\mathfrak{w}_i, \mathfrak{w}_j)$
(Pigeonhole Principle – $\mathrm{card}(\Sigma) = k \geq 2$)

$\mathfrak{w}_0$ **0 0 0** 1 0 2
$\mathfrak{w}_1$ **0 0 0** 0 1 3 5

and

$\mathfrak{w}_1$ **0 0 0 0** 1 3 5
$\mathfrak{w}_2$ **0 0 0 0** 1 4

$\longrightarrow \mathrm{clen}(\mathfrak{w}_0, \mathfrak{w}_1) = \mathrm{clen}(\mathfrak{w}_0, \mathfrak{w}_2)$

String Compatible Counter Valuations

- Counter valuation $\mathfrak{c} : \{\mathrm{clen}(\mathtt{t}, \mathtt{t}') : \mathtt{t}, \mathtt{t}' \in \mathtt{T}\} \rightarrow \mathbb{N}$.
- String-compatibility:

$$\bigwedge_{\mathtt{t},\mathtt{t}' \in \mathtt{T}} (\mathrm{clen}(\mathtt{t}, \mathtt{t}) \geq \mathrm{clen}(\mathtt{t}, \mathtt{t}'))$$

$$\bigwedge_{\mathtt{t}_0,\ldots,\mathtt{t}_k \in \mathtt{T}} ((\bigwedge_{i \in [0,k]} (\mathrm{clen}(\mathtt{t}_0, \mathtt{t}_1) < \mathrm{clen}(\mathtt{t}_i, \mathtt{t}_i))) \wedge \mathrm{clen}(\mathtt{t}_0, \mathtt{t}_1) = \cdots = \mathrm{clen}(\mathtt{t}_0, \mathtt{t}_k)$$

$$\Rightarrow (\bigvee_{i \neq j \in [1,k]} (\mathrm{clen}(\mathtt{t}_0, \mathtt{t}_1) < \mathrm{clen}(\mathtt{t}_i, \mathtt{t}_j)))$$

$$\bigwedge_{\mathtt{t},\mathtt{t}',\mathtt{t}'' \in \mathtt{T}} (\mathrm{clen}(\mathtt{t}, \mathtt{t}') < \mathrm{clen}(\mathtt{t}', \mathtt{t}'')) \Rightarrow (\mathrm{clen}(\mathtt{t}, \mathtt{t}') = \mathrm{clen}(\mathtt{t}, \mathtt{t}''))$$

- Size in $\mathcal{O}((q+r)^{k+2})$ with $\mathrm{card}(\mathtt{T}) = q + r$.

Characterisation

- String compatibility is equivalent to the existence of a string valuation witnessing the values of the counters $\mathrm{clen}(\mathtt{t}, \mathtt{t}')$.

- The exact statement is a bit more complex to be used after in the translation from $\mathrm{LTL}(\Sigma^*, \mathrm{clen})$ to $\mathrm{LTL}(\mathbb{N}, \leq)$.

Characterisation

- String compatibility is equivalent to the existence of a string valuation witnessing the values of the counters $\mathrm{clen}(\mathtt{t}, \mathtt{t}')$.

- The exact statement is a bit more complex to be used after in the translation from $\mathrm{LTL}(\Sigma^*, \mathrm{clen})$ to $\mathrm{LTL}(\mathbb{N}, \leq)$.

- Checking satisfiability of Boolean combinations of prefix constraints is NP-complete.
  (upper bound by reduction into QF Presburger arithmetic)

- PSPACE can be obtained using word equations and Plandowski's PSPACE upper bound.
  (suffix constraints can be added at no cost)

Translation

- Formula ϕ with constant strings $\mathfrak{w}_1, \ldots, \mathfrak{w}_q$ and, string variables $\mathsf{x}_1, \ldots, \mathsf{x}_r$.

- For all $i, j \in [1, q]$, $c_{i,j} \stackrel{\text{def}}{=} \mathrm{clen}(\mathfrak{w}_i, \mathfrak{w}_j)$.

- $\mathtt{T} \stackrel{\text{def}}{=} \{\mathsf{y}_1, \ldots, \mathsf{y}_q\} \cup \{\mathsf{x}_1, \ldots, \mathsf{x}_r\} \cup \{\mathsf{X}\mathsf{x}_1, \ldots, \mathsf{X}\mathsf{x}_r\}$.

- ϕ_1^{subst}: replace each $\mathfrak{w}_i$ by y_i.

- $\phi_2^{rig} \stackrel{\text{def}}{=} \mathsf{G}\ (\bigwedge_{i,j \in [1,q]} (\mathrm{clen}(\mathsf{y}_i, \mathsf{y}_j) = c_{i,j}))$.

Translation (II)

- Formula ϕ_3^{next}:

$$\mathsf{G}\ (\bigwedge_{\mathtt{t},\mathtt{t}' \in \{\mathsf{y}_1,\ldots,\mathsf{y}_q\} \cup \{\mathsf{X}\mathsf{x}_1,\ldots,\mathsf{X}\mathsf{x}_r\}} \mathrm{clen}(\mathtt{t},\mathtt{t}') = \mathsf{X}\ \mathrm{clen}(\mathtt{t} \setminus \mathsf{X}, \mathtt{t}' \setminus \mathsf{X}))$$

- Formulae ψ_{I}, ψ_{II} and ψ_{III} related to string-compatible counter valuations over $\mathtt{T}$.

- ϕ is satisfiable in $\mathrm{LTL}(\Sigma^*, \mathrm{clen})$ iff

$$\phi_1^{subst} \ \wedge\ \phi_2^{rig} \ \wedge\ \phi_3^{next} \ \wedge\ \psi_{\mathrm{I}} \ \wedge\ \psi_{\mathrm{II}} \ \wedge\ \psi_{\mathrm{III}}$$

is satisfiable in $\mathrm{LTL}(\mathbb{N}, \leq)$.

Complexity and Decidability

- Satisfiability problems for $\mathrm{LTL}(\Sigma^*, \preceq_p)$ and $\mathrm{LTL}(\Sigma^*, \mathrm{clen})$ are PSPACE-complete.

- This also holds for any LTL extension that behaves as LTL as far as the translation into Büchi automata is concerned (Past LTL, linear μ-calculus, ETL, etc.).

- For any satisfiable ϕ in LTL($\mathbb{N}^*$,clen), models with letters in $[0, N + 2 \times \mathrm{size}(\phi)]$ are sufficient (N max. letter in ϕ).

Lifting to Branching-Time Temporal Logics

- $\mathrm{CTL}^\star(\Sigma^*, \mathrm{clen})$: branching-time extension of $\mathrm{LTL}(\Sigma^*, \mathrm{clen})$.
- Translation can be extended for $\mathrm{CTL}^\star(\Sigma^*, \mathrm{clen})$.
- Proof is a bit more complex but the string characterisation is used similarly.
- The satisfiability problem for $\mathrm{CTL}^\star(\Sigma^*, \mathrm{clen})$ is decidable. By reduction into $\mathrm{CTL}^\star(\mathbb{N}, \leq)$ shown decidable in

  [Carapelle & Kartzow & Lohrey, CONCUR'13]

A Selection of Open Problems

- Complexity characterisation for uniform sat. problem.

  input: alphabet $\Sigma = [0, k-1]$ (k in unary) or $\Sigma = \mathbb{N}$,
  and a formula ϕ in $\mathrm{LTL}(\Sigma^*, \mathrm{clen})$

  question: is ϕ satisfiable in $\mathrm{LTL}(\Sigma^*, \mathrm{clen})$?

- Dec. status of LTL($\{0, 1\}^*$, $\preceq_p$, $\preceq_s$).

A Selection of Open Problems

- Complexity characterisation for uniform sat. problem.

  input: alphabet $\Sigma = [0, k-1]$ (k in unary) or $\Sigma = \mathbb{N}$, and a formula ϕ in $\mathrm{LTL}(\Sigma^*, \mathrm{clen})$

  question: is ϕ satisfiable in $\mathrm{LTL}(\Sigma^*, \mathrm{clen})$?

- Dec. status of LTL($\{0, 1\}^*$, $\preceq_p$, $\preceq_s$).

- Dec. status of LTL($\{0, 1\}^*$, $\preceq_p$, REG) with regularity tests.

A Selection of Open Problems

- Complexity characterisation for uniform sat. problem.

  input: alphabet $\Sigma = [0, k-1]$ (k in unary) or $\Sigma = \mathbb{N}$, and a formula ϕ in $\mathrm{LTL}(\Sigma^*, \mathrm{clen})$

  question: is ϕ satisfiable in $\mathrm{LTL}(\Sigma^*, \mathrm{clen})$?

- Dec. status of LTL($\{0,1\}^*$, $\preceq_p$, $\preceq_s$).

- Dec. status of LTL($\{0,1\}^*$, $\preceq_p$, REG) with regularity tests.

- Decidability status of LTL($\{0,1\}^*$, $\sqsubseteq$).