Verification of temporal logics on infinite-state systems

Lecture 5.2
Timed temporal logics

Stéphane Demri and Valentin Goranko

ESSLLI 2007, Trinity College, August 2007
Overview

**TPTL**
- Definition
- Decidable problems

**MTL**
- Definition
- Finitary problems are decidable
- Infinitary problems are undecidable
- Related issues

Few words about TCTL
Timed propositional temporal logic TPTL
Definition [Alur & Henzinger, JACM 94]

- **TPTL formulae:**
  \[
  \pi ::= x + k \mid k \\
  \phi ::= a \mid \pi_1 \leq \pi_2 \mid \pi_1 \equiv_d \pi_2 \mid \neg \phi \mid \phi \land \phi \mid X\phi \mid \phi U \phi \mid x \cdot \phi
  \]

- **TPTL model:** infinite timed word over \( \mathbb{N} \) without initialization condition.

- **Freeze formula** \( x \cdot \phi \): "Store in \( x \) the current time value and check whether \( \phi \) holds true".

- **Environment** \( env : \text{VAR} \rightarrow \mathbb{N} \) (assuming that the time domain is \( \mathbb{N} \)).
Satisfaction relation

- $\rho, i \models_{\text{env}} a$ iff $a = \sigma_i$.

- $\rho, i \models_{\text{env}} \pi_1 \leq \pi_2$ iff $\text{env}(\pi_1) \leq \text{env}(\pi_2)$ with $\text{env}(k) = k$ and
  $\text{env}(x + k) = \text{env}(x) + k$.

- $\rho, i \models_{\text{env}} \pi_1 \equiv_d \pi_2$ iff $\text{env}(\pi_1) \equiv_d \text{env}(\pi_2)$

- Clauses for $\neg$, $\land$, $X$, $U$ are standard.

- $\rho, i \models_{\text{env}} x \cdot \phi$ iff $\rho, i \models_{\text{env}[x \leftarrow \tau_i]} \phi$. 
Examples

- $G\ x \cdot (a \Rightarrow a U y \cdot (b \land y \leq x + 10))$

  $b \ a \ a \ a \ a \ b$

  0 6 6 7 8 15

- Synchronous real-time systems:

  $G x \cdot X y \cdot y = x + 1$
Satisfiability problem

- Satisfiability is $\text{ExpSpace}$-complete.
  
  [Alur & Henzinger, JACM 94]

- Ingredients of the automata-based decision procedure:
  - If $\phi$ has a model and $\Delta$ is the product of all constants in $\phi$, $\phi$ has a model in which two successive states do not increase more than $\Delta$.
  
  - Region-like abstractions for $\Delta$-bounded models.

- $\text{ExpSpace}$-hardness is a consequence of the fact that
  - imposing all over the model $Gx \cdot Xy \cdot y = x + 1$ and,
  - using $x = y + 2^n$
  allow to jump to the $2^n$th state, providing the possibility to have constraints on exponential-size tapes.
A model-checking problem

- Timed state graph:

- Timed state sequence

- Model-checking problem:
  - input: a timed graph state $G$ and a TPTL formula $\phi$
  - question: Do all the timed state sequences of $G$ satisfy $\phi$?

- Model-checking problem is $\text{ExpSpace}$-complete.

  [Alur & Henzinger, JACM 94]

  (upper bound obtained by a product construction)
Undecidable variants [Alur & Henzinger JACM 94]

- TPTL satisfiability by relaxing the monotonicity condition for timed sequences is $\Sigma_1^1$-complete.

- TPTL satisfiability extended to constraints with multiplication by 2 is $\Sigma_1^1$-complete.

- TPTL satisfiability with time interpreted over $\mathbb{Q}/\mathbb{R}$ is $\Sigma_1^1$-complete.
Metric temporal logic MTL
Definition [Koymans, RTS 90]

MTL formulae

\[ \phi ::= a \mid \phi \land \phi \mid \neg \phi \mid X_I \phi \mid \phi U_I \phi \]

with

- \( a \in \Sigma \),
- \( I \) is an open, closed, half-open interval with endpoints in \( \mathbb{N} \cup \{\infty\} \).

- \( G_I \phi \equiv \neg (\top U_I \neg \phi) \).

- MTL models: infinite timed words.
Satisfiability relation

- \( \rho, i \models a \) iff \( \sigma_i = a \)

- \( \rho, i \models X I \phi \) iff \( i < |\rho|, \tau_{i+1} - \tau_i \in I \) and \( \rho, i + 1 \models \phi \)

- \( \rho, i \models \phi_1 U I \phi_2 \) iff there is \( i \leq j < |\rho| - 1 \) such that \( \rho, j \models \phi_2, \tau_j - \tau_i \in I \) and for every \( i \leq k < j \), we have \( \rho, k \models \phi_1 \).

- \( L_f(\phi) \): set of finite timed words satisfying \( \phi \).
Examples from [Ouaknine & Worrell, LMCS]

- Events $\Sigma = \{\text{req}_i, \text{acq}_i, \text{rel}_i : i = A, B\}$ (request, acquire, release a lock).

- $B$ cannot acquire the lock less than 3 time units after $A$ acquires the lock:

  $$G_{[0,\infty)}(\text{acq}_A \Rightarrow G_{[0,3)} \neg \text{acq}_B)$$

- Whenever $A$ requests the lock, it acquires the lock within 2 time units and releases it exactly one time unit later:

  $$G_{[0,\infty)}(\text{req}_A \rightarrow F_{[0,2)}(\text{acq}_A \land F_1 \text{rel}_A))$$
In sequel, TPTL and MTL are over timed words with time domain $\mathbb{R}$.

$t(X_I \phi) = x \cdot X(t(\phi) \land y \cdot (y - x) \in I)$.

$t(\phi_1 U_I \phi_2) = x \cdot t(\phi_1)U(t(\phi_2) \land y \cdot (y - x) \in I)$.

TPTL is undecidable with the time domain $\mathbb{R}$.

What about MTL?
Finitary satisfiability for MTL is decidable

- Finitary satisfiability for MTL (with the pointwise semantics) is decidable [Ouaknine & Worrell, LICS 05].

- Reduction into the nonemptiness problem for one-clock timed alternating automata.

- Undecidable variant:
  - Finitary MTL satisfiability with the interval-semantics is undecidable. [Alur & Feder & Henzinger, PODC 91]
From MTL formula $\phi$ to ATA $A_\phi$

- Formula $\phi$ in negation normal form with dual until R and end (only atomic formulae can be in the scope of negation).

- $\phi_1 R I \phi_2 \equiv \neg (\neg \phi_1 U I \neg \phi_2)$ and $\text{end} \equiv \neg X_{[0,\infty)} \top$.

- $cl(\phi)$: set of subformulæ of $\phi$, and for each $X_I \phi$, we introduce the residual copy of $X_I \phi$ denoted by $(X_I \phi)^r$.

- The set of locations of $A_\phi$ is $cl(\phi)$. 
Transition relation

- $\delta(a, b) = \top$ if $a = b$.

- $\delta(\phi_1 \land \phi_2, a) = \delta(\phi_1, a) \land \delta(\phi_2, a)$.

- $\delta(X_I \psi, a) = x \cdot (X_I \psi)^r$.

- $\delta((X_I \psi)^r, a) = x \in I \land x \cdot \delta(\psi, a)$.

- $\delta(\psi_1 U_I \psi_2, a)$ is equal to
  $((x \cdot \delta(\psi_2, a)) \land x \in I) \lor ((x \cdot \delta(\psi_1, a)) \land (\psi_1 U_I \psi_2))$.

- $\delta(\text{end}, a) = \bot$.

- Dual clocks constraints for the other cases.
Satisfiability and model-checking problems

- Accepting locations: end and formulae with outermost connective $R_I$.
- $L_f(A_{\phi}) = L_f(\phi)$ [Ouaknine & Worrell, LICS 05].
- $\Rightarrow$ Finitary satisfiability for MTL (with the pointwise semantics) is decidable.
- Model-checking problem for MTL
  
  input: a timed automaton $A$ and a MTL formula $\phi$;
  question: $L_f(A) \subseteq L_f(\phi)$?

- $\Rightarrow$ Model-checking problem for MTL is decidable but . . . the proof relies of the construction of a well-structured transition system representing the execution of $A_{\phi}$ and $A$ in parallel.
Infinitary satisfiability for MTL is undecidable

- Infinitary satisfiability for MTL with the pointwise semantics is undecidable [Ouaknine & Worrell, FOSSACS 06].

- Reduction from the recurrent problem for gainy counter automata (see Lecture 3.2 on Wednesday).

- Given an instance of a gainy counter automaton $A$, one can compute an MTL formula $\phi$ such that $A$ has an infinite computation (with some final location repeated infinitely often) iff $\phi$ is satisfiable in some infinite timed word.
Using MTL as a programming language

- Gainy counter automaton $A = (Q, q_0, k, \delta, F)$. 
  ($\delta \subseteq Q \times L \times Q$ with $L = \{inc, dec, ifzero\} \times \{1, \ldots, k\}$)

- MTL formula $\phi_A$ over the alphabet

$$Q \cup \{\bullet\} \cup \delta \cup \{[i, ]i : 1 \leq i \leq k\}$$

- Each configuration is encoded within $2k + 2$ states and counter $i$ is encoded within its interval $(2i - 1, 2i)$.

- Models of $\phi_A$ are strongly monotonic: $\phi_{sm} = GX_{>0} \top$.

- Büchi acceptance condition: $GF \bigvee_{q \in F} q$. 

Stéphane Demri and Valentin Goranko
Other formulae

- Locations occur every $2k + 2$-position:
  \[
  \phi_S = q_0 \land G(\bigvee Q \Rightarrow (F_{=2k+2} \bigvee Q \land G_{<2k+2} \neg \bigvee Q))
  \]

- Constraints on the occurrences of $[i, ]_i$ and $\bullet (\phi[i, \phi]_i, \phi\bullet)$
  e.g.,
  \[
  G(\bigvee Q \Rightarrow (G(2i,2i-1) \bullet \land G(2i,2i+1) \perp))
  \]

- Formula $\phi_\delta$ states which positions are marked by letters in $\delta$ whereas $\phi_\delta Q$ verifies the correct succession of locations wrt $\delta$.

- Copying formula: $\phi_{copy} = G_{(0,1)}(\bullet \Rightarrow F_{=2k+2}\bullet)$. 
Constraints on counter valuations

\[
G(\bigvee Q \Rightarrow \bigwedge_{\text{inst} \in L} (F=2k+1 \bigvee \{(−, l, −) \in \delta \Rightarrow \phi_l\}))
\]

\[
\phi(\text{ifzero}, i) = \bigwedge_{1 \leq j \leq k} F=2j−1 \\phi_{\text{copy}} \land G(2i−1, 2i) \perp
\]

\[
\phi(\text{inc}, i) = \bigwedge_{1 \leq j \leq k} F=2j−1 \\phi_{\text{copy}} \land F[2i−1, 2i)(X \setminus i) \land F=2k+2X \bullet
\]

\[
\phi(\text{dec}, i) = \bigwedge_{1 \leq j \leq k, j \neq i} F=2j−1 \\phi_{\text{copy}} \land F=2i−1X(\bullet \land \phi_{\text{copy}}).
\]

\[\phi_A\] is the conjunction of all the above formulae and \(A\) has a recurrent computation iff \(\phi\) has an infinite model.

[Ouaknine & Worrel, FOSSACS 06].
Related issues

- Safety MTL
  - every occurrence of $U_i$ with positive polarity has an interval $I$ of bounded length.
  - The model-checking problem for safety MTL over infinite words is decidable [Ouaknine & Worrell, LICS 05].

- Finitary satisfiability and model-checking for MTL have non-primitive recursive complexity.
  [Ouaknine & Worrell, LICS 05] (use of [Schnoebelen, IPL 02])

- Finitary satisfiability and model-checking for MTL restricted to nonsingular intervals (MITL) with interval-based semantics are $\text{ExpSpace}$-complete [Alur & Feder & Henzinger, JACM 96].

- TPTL is strictly more expressive than MTL.
  [Bouyer & Chevalier & Markey, FSTTCS 05]
Timed CTL
Timed CTL [Alur & Courcoubetis & Dill, IC 93]

- TCTL = CTL + time constraints.

- Until operators are replaced by

  \[ E \cdot U_{x \sim k} \cdot A \cdot U_{x \sim k} \cdot \]

  with \( \sim \in \{=, <, \geq, \leq, >\} \) and \( k \in \mathbb{N} \)

- Example: AG(problem ⇒ AF_{\leq 3} \text{ alarm})

- TCTL\textsubscript{h} is for TCTL what is TPTL for MTL.

- Model-checking problems for TCTL and TCTL\textsubscript{h} over timed automata are PSPACE-complete.
Incomplete bibliography

R. Alur, R. Courcoubetis, and D. Dill.
Model-checking in dense real-time.

The benefits of relaxing punctuality.

R. Alur and Th. Henzinger.
A really temporal logic.

J. Ouaknine and J. Worrell.
On Metric temporal logic and faulty Turing machines.