Temporal Logics over Mazurkiewicz Traces

A Quick Tour

Madhavan Mukund
Chennai Mathematical Institute
92 G N Chetty Rd, Chennai 600 017, India
http://www.cmi.ac.in/~madhavan

Arcachon, 23 May 2002
Motivation

- Temporal logic — convenient specification language
- Formulas interpreted over sequences
  - For concurrent systems, sets of interleaved behaviours
  - Combinatorial explosion in verification
- Can we directly reason about a single structure that describes the entire behaviour of a concurrent system?
Mazurkiewicz traces

- An alphabet with an independence relation, \((\Sigma, I)\)

- Independent letters can be commuted.
  
  \[ \text{If } (a, b) \in I, \text{ then } wabw' \sim w'abw \]

- A trace is an equivalence class of words—a single concurrent behaviour with different, equivalent linearizations

- Traces faithfully model behaviour of concurrent systems with static architecture—e.g., safe Petri nets
Traces revisited

- Dependence alphabet \((\Sigma, D)\): \(D\) is the complement of \(I\)
  
  **Dependence graph:** e.g., \((\Sigma, D) = a \rightarrow b \rightarrow c \rightarrow d\)
  
  Here, \((a, c), (b, d), (a, d)\) are independent pairs

- A trace is a labelled partial order
  
  The trace \(\{abacbac, abcabac, \ldots, abcabea\}\) is the (set of linearizations of the) labelled partial order

\[
\begin{array}{ccc}
  & a & \\
  b & & a \\
  c & & b \\
  & a & \\
  & b & \\
  & c & \\
\end{array}
\]
Finite and infinite traces

\((\Sigma, D) = a \rightarrow b \rightarrow c \rightarrow d\)

Finite trace

Infinite trace
Traces as partial orders

A trace over \((\Sigma, D)\) is a labelled partial order \(t = (E, \leq, \lambda)\) such that

- \(e \not\leq f\) and \(f \not\leq e\) implies \((\lambda(e), \lambda(f)) \notin D\)

  Concurrent (unordered) events correspond to independent actions

- \(e \prec f\) implies \((\lambda(e), \lambda(f)) \in D\)

  The causality order on events is generated by \(D\)

- For all \(e \in E\), \(\downarrow e = \{f \mid f \leq e\}\) is finite

  Each event has a finite past (infinite traces are “real”)

**Key fact** For each \((\Sigma, D)\), the width of traces over \((\Sigma, D)\) is bounded.
Linear-time temporal logic over sequences

- Atomic propositions, boolean connectives, temporal modalities

\[ \Diamond \varphi \]

- Next

\[ \varphi \rightarrow \rho \rightarrow \varphi \rightarrow \varphi \rightarrow \cdots \]

\[ \varphi \]

- Until

\[ \varphi \leftarrow \varphi \rightarrow \varphi \rightarrow \cdots \rightarrow \varphi \rightarrow \varphi \rightarrow \cdots \]

\[ \varphi, \varphi, \varphi, \psi \]
Derived modalities

\[ \Diamond \psi \equiv T \bigcirc \psi \]

- Eventually

- Henceforth
Past modalities

- Previous

- Since
• **Theorem** (Kamp ’68)

  \( \text{LTL} \) has the same expressive power as \( FO(\mathbb{N}, <) \).

• **Theorem** (Gabbay, Pnueli, Shelah & Stavi ’80)

  \( \text{LTL} \) with only future modalities has the same expressive power as \( FO(\mathbb{N}, <) \).

• **Theorem** (Sistla & Clarke ’82)

  Model checking \( \text{LTL} \) is PSPACE-complete.

    – Do all sequences generated by a finite-state system \( S \) satisfy an \( \text{LTL} \) formula \( \varphi \)?
LTL over traces

- Points on a sequence $\Leftrightarrow$ prefixes of the sequence

- A prefix of a trace is a downward closed subset of events

- Interpret formulas at prefixes

- Prefixes can be ordered in the obvious way—$c \preceq c'$ iff $c \subseteq c'$
- Two prefixes may be unordered

- A prefix may have more than one “next” prefix
For a trace $t = (E, \leq, \lambda)$ over $(\Sigma, D)$, let $c \subseteq E$ be a prefix.

$t, c \models \Box \varphi$ if there exists a “next” prefix $c' = c \cup \{e\}$ such that $t, c' \models \varphi$

$t, c \models \varphi U \psi$ if $t, c' \models \psi$ for some prefix $c'$, $c \leq c'$, and for all $c''$ with $c \leq c'' \leq c'$, $t, c'' \models \psi$
Fix a trace alphabet \((\Sigma, D)\).

- When interpreted on traces over \((\Sigma, D)\), what is the expressive power of LTL\((\bigcirc, U)\) with respect to \(FO(<)\)?
  - LTL\((\bigcirc, U)\) is within \(FO(<)\) because width of a trace is bounded!

- **Theorem** (Thiagarajan & Walukiewicz, LICS '97)
  
  Expressively complete, if you add past formulas \(\ominus a\)
  
  - \(t, c \models \ominus a\) if \(c\) contains a maximal event labelled \(a\)

- **Theorem** (Diekert & Gastin, ICALP '00)
  
  Expressively complete with just \(\bigcirc\) and \(U\).
  
  Generalizes the GPSS '80 result from sequences to traces.
Unfortunately, . . .

- **Theorem** (Walukiewicz, ICALP ’98)

  Model checking is non elementary.
  
  “Too many” configurations between $\varphi$ and $\psi$.

![Diagram showing configurations between $\varphi$ and $\psi$.]
Global vs local configurations

- Local configuration represents local history of an event.
  - Events $e \in E \iff$ Local configurations $\downarrow e \subseteq E$

- Variables in $FO(<)$ are interpreted as events

- Can we evaluate temporal formulas at local configurations and still be as expressive as $FO(<)$?
Local logics on traces

Hasse diagram provides a natural local interpretation for $\bigcirc$.

Existential until

$\varphi$ holds on some path in the interval.

Universal until

$\varphi$ holds on every path in the interval.

Arcachon, 23 May 2002
Existential until is not first-order expressible

\[(\Sigma, D) = \begin{array}{c}
\begin{array}{c}
\quad h \\
\quad d \\
\quad g
\end{array}
\quad a \\
\quad b \\
\quad c \\
\quad f
\end{array}
\quad \quad \begin{array}{c}
\quad b \\
\quad e \\
\quad a
\end{array}
\begin{array}{c}
\quad h \\
\quad f
\end{array}
\end{array}\]

\[aht^2b^\omega = \begin{array}{c}
\begin{array}{c}
\quad a \\
\quad b \\
\quad c
\end{array}
\quad h \\
\quad e \\
\quad c \\
\quad a
\end{array}
\begin{array}{c}
\quad b \\
\quad e \\
\quad a
\end{array}
\quad \begin{array}{c}
\quad h \\
\quad f
\end{array}
\quad \begin{array}{c}
\quad b \\
\quad a \\
\quad b \\
\quad \cdots
\end{array}
\end{array}\]

Example (independently) due to Gastin and Walukiewicz
Existential until is not first-order expressible

\[(\Sigma, D) = d \triangleleft b \quad \text{and} \quad t = \]

\[aht^2b^\omega = \]

\[\varphi = a \lor b \lor c \lor d \lor b \]

Arcachon, 23 May 2002
Existential until is not first-order expressible

\[(\Sigma, D) = \begin{array}{c}
\text{h} \\
\text{a} \\
\text{e} \\
\text{b} \\
\text{d} \\
\text{g} \\
\text{c} \\
\text{f}
\end{array}
\]

\[t = \begin{array}{c}
\text{b} \\
\text{e} \\
\text{a} \\
\text{h} \\
\text{d} \\
\text{g} \\
\text{c} \\
\text{f}
\end{array}
\]

\[aht^1b^\omega = \begin{array}{c}
\text{a} \\
\text{h} \\
\text{b} \\
\text{c} \\
\text{a} \\
\text{h} \\
\text{b} \\
\text{b} \\
\text{d} \\
\text{g} \\
\text{c}
\end{array}
\]

\[\varphi = a \lor b \lor c \lor d \cup \Box b\]
Existential until is not first-order expressible

\[(\Sigma, D) = \begin{array}{c}
h \\ d \\ g \\ c \\ f \\ a \\ e \\ b \\ \end{array} \]

\[t = \begin{array}{c}
b \\ e \\ a \\ h \\ d \\ g \\ c \\ f \\ \end{array} \]

\[aht^1b^\omega = \begin{array}{c}
a \\ b \\ c \\ a \\ h \\ b \\ \cdot \cdot \cdot \\ d \\ g \\ c \\ \end{array} \]

\[\varphi = a \lor b \lor c \lor d \cup \square b \]

\[aht^*b^\omega \cap \mathcal{L}(\varphi) = ah(t^2)^*b^\omega \]
Local logics on traces

Existential $\bigcirc$

Universal until

$\varphi$ holds on every path in the interval
• Need some way of globally combining local formulas to span disjoint components

Formula at \( e \) cannot “reach” the disconnected chain \( gfgfg \)

• Global formulas

Boolean combinations of \( EM \varphi \), \( \varphi \) a local formula

\( t \models EM \varphi \) if there is a minimal event \( e \) in \( t \) such that \( t, e \models \varphi \)
Pure future local logics are not sufficient

\( \varphi \) is a pure future formula if \( t, e \models \varphi \) implies that \( t', e \models \varphi \) for any \( t', t, e \)

Example (Walukiewicz)

The following traces over \( a \rightarrow b \rightarrow c \rightarrow d \) cannot be distinguished by pure future local formulas

\[
\begin{align*}
& a \rightarrow b \rightarrow c \rightarrow b \rightarrow \cdots \\
& d \rightarrow c \\
& d \rightarrow c \\
& a \rightarrow b \\
& d \rightarrow c \rightarrow b \rightarrow c \rightarrow \cdots \\
& d \rightarrow c \\
& a \rightarrow b
\end{align*}
\]
• For events $e \leq f$, the interval between $e$ and $f$ is more properly defined as $\downarrow f \setminus \downarrow e$
A stronger until

- For events $e \leq f$, the interval between $e$ and $f$ is more properly defined as $\downarrow f \setminus \downarrow e$

- This interval includes events that do not lie above $e$
- A **ternary** until

\[(\varphi_\parallel, \varphi_\prec) \mathcal{U}_\psi\]

- A weaker version — **filtered** until

\[\varphi \mathcal{U}_C \psi, \ C \subseteq \Sigma\]

- \(\varphi\) holds above \(e\) and below \(f\)
- No action from \(C\) occurs in \(\downarrow f \setminus \downarrow e\)
Filtered until can distinguish these traces

\[
\begin{align*}
a & \to b & c & \to b & \cdots \\
d & \to c \\
\end{align*}
\]

\[
\begin{align*}
d & \to c & \to b & \to c & \cdots \\
a & \to b \\
\end{align*}
\]

The formula $EMd U_{\{a\}}c$ is true in the first trace, but not in the second.
A dual modality — filtered since

\[ \varphi S_C \psi, \ C \subseteq \Sigma \]

- \( \varphi \) holds above \( f \) and below \( e \)
- No action from \( C \) occurs in \( \downarrow e \ \downarrow f \)
Theorem (Gastin & Mukund, ICALP ’02)

$LTL(\bigcirc, \Theta, U_C, S_C)$ has the same expressive power as $FO(<)$.

For each fixed alphabet $(\Sigma, D)$, the model-checking problem is in PSPACE (and hence PSPACE-complete).

Corollary

$FO_3(<)$, $FO$ with 3 variables, is as expressive as $FO(<)$ for traces.

Independent of the width of the trace!
Pure future modalities

Theorem (Diekert & Gastin, LPAR '01)

\( LTL(\bigcirc, \mathcal{U}) \), where \( \mathcal{U} \) is the universal pure future local until, has the same expressive power as \( FO(<) \) for cographs.

Cographs—traces where the alphabet \((\Sigma, D)\) is series-parallel.

- \((\Sigma, D)\) is built from singletons using
  - \( \Sigma_1 \cdot \Sigma_2 \) — all actions in \( \Sigma_1 \) are dependent on all actions \( \Sigma_2 \)
  - \( \Sigma_1 \parallel \Sigma_2 \) — all actions in \( \Sigma_1 \) are independent of all actions \( \Sigma_2 \)

- \((\Sigma, D)\) is N-free, does not embed \( a \rightarrow b \rightarrow c \rightarrow d \).

- Traces generated by \((\Sigma, D)\) are series-parallel graphs.
For arbitrary alphabets, you have only $U_C$, but not $S_C$?

Each trace is equipped with a special bottom element.

Can separate these traces using the pure future formula $\neg a \ U_C$ evaluated at $\bot$. 

Arcachon, 23 May 2002
Another point of view

- $(\Sigma, D)$ can be implemented as a distributed alphabet $(\Sigma_1, \ldots, \Sigma_n)$.
  - $\bigcup_{1 \leq i \leq n} \Sigma_i = \Sigma$
  - If $(a, b) \in D$, then for some $i$, $\{a, b\} \in \Sigma_i$

- Think of each $i$ as an agent or process in a distributed system.

- Example, can implement $a \rightarrow b \rightarrow c \rightarrow d$ with three agents.
  - Distributed alphabet is $(\{a, b\}, \{b, c\}, \{c, d\})$. 

Arcachon, 23 May 2002
Can redraw the trace

\[
\begin{align*}
    &a \rightarrow b \rightarrow a \rightarrow b \rightarrow a \\
    &b \rightarrow c \rightarrow b \rightarrow c
\end{align*}
\]

as

\[
\begin{align*}
    p_1 &= \{a, b\} \quad \quad a \quad b \quad a \\
    p_2 &= \{b, c\} \quad \quad b \quad c \quad b \\
    p_3 &= \{c, d\} \quad \quad c \quad c
\end{align*}
\]
The view that \( p_3 \) has of

\[
\begin{align*}
  p_1 &= \{a, b\} \\
  p_2 &= \{b, c\} \\
  p_3 &= \{c, d\}
\end{align*}
\]

is

\[
\begin{align*}
  p_1 &= \{a, b\} \\
  p_2 &= \{b, c\} \\
  p_3 &= \{c, d\}
\end{align*}
\]
The $p_1$ view of the $p_3$ view of

\begin{align*}
p_1 &= \{a, b\} \\
p_2 &= \{b, c\} \\
p_3 &= \{c, d\}
\end{align*}

is

\begin{align*}
p_1 &= \{a, b\} \\
p_2 &= \{b, c\} \\
p_3 &= \{c, d\}
\end{align*}
• Define local modalities based on processes

  \(\text{(TrPTL, Thiagarajan LICS '94)}\)

• \(t, e \models \Diamond_i \varphi\)

  With respect to the maximal \(i\)-event in \(\downarrow e\), the next \(i\)-event satisfies \(\varphi\)

• \(t, e \models \varphi U_i \psi\)

  Starting with the maximal \(i\)-event in \(\downarrow e\), the sequence of events along process \(i\) satisfies \(\varphi U \psi\).

• Boolean combination of assertions \(EM_i \varphi\) which say that there is a minimal \(i\)-event satisfying the local formula \(\varphi\).
• Is TrPTL equivalent to $FO(<)$?

  Probably not, but counterexample is elusive

• Using more explicit past assertions, it is possible to obtain a process-oriented temporal logic that is equivalent to $FO(<)$

  (Adsul & Sohoni, ICALP ’02)
Summary

- Temporal logics interpreted over the Hasse diagram of a trace
  - Without a special element $\bot$, to what extent are past modalities required?
  - With a special element $\bot$, are past modalities required at all?
- Temporal logics interpreted over the process view of a trace
  - Is TrPTL expressively complete?
- Not discussed at all in this talk
  - $\mu$-calculi on traces and expressive completeness with respect to MSO
    (Niebert '95, Walukiewicz '01)