A Tableau Calculus for a Temporal Logic with Temporal Connectives

Wolfgang May

Institut für Informatik

Universität Freiburg

Germany

June 8, 1999

Tableaux and Temporal Logics

- Modal Temporal Logics (LTL, CTL)
- Weaknesses:
  - temporal relationships between several transitions and states
  - no explicit use of time points/synchronization
- "if some state is reached s.t. a given predicate p has the same extension as now, then q holds in this state".
  Sorted First-Order Logic:

$$\forall s_1, s_2 : \\ (\forall x : p(x, s_1) \leftrightarrow p(x, s_2) \wedge s_1 < s_2) \rightarrow q(s_2) \ .$$

- other Formalisms:
  Event-Algebras, Transaction Logic:
  temporal connectives, e.g., sequential conjunction
- Synchronization: explicit use of state variables analogously to $\exists$ and $\forall$.

A Logic with Temporal Connectives and Quantification

- linear first-order Kripke structures

$$\boldsymbol{K} = (\boldsymbol{U}, \boldsymbol{M})$$

$$\boldsymbol{M} : \mathbb{N} \to \text{Interpretations over } \Sigma$$

  augmented by a *transition oracle* $\boldsymbol{N}$:

  Σ_A: *action names* similar to predicates

$$(u_1, \ldots u_k) \in (\boldsymbol{N}(n))(a) \;\Leftrightarrow$$

$$a(u_1, \ldots, u_k) \text{ is executed in}$$

$$\text{the transition } n \text{ to } n{+}1.$$

- *Action formulas*:
  First-order formulas over $\Sigma_A \cup \Sigma_{\textit{func}}$
  evaluated wrt. *transitions* $\boldsymbol{K}\langle i, i{+}1\rangle$:

$$(\boldsymbol{K}\langle n, n{+}1\rangle, \chi) \models a(t_1, \ldots, t_k) \;\Leftrightarrow$$

$$(\boldsymbol{M}(n)(t_1, \chi), \ldots, \boldsymbol{M}(n)(t_k, \chi)) \in \boldsymbol{N}(n)(a)\ .$$

The Logic

Formulas interpreted over segments $\boldsymbol{K}[i,j]$ of linear Kripke Structures

$$(\boldsymbol{K}[i,j], \chi, \zeta) \models \varphi$$

- assignment of variables to elements of the universe by $\chi : \mathsf{Var} \to \boldsymbol{U}$,
- synchronization points as *virtual* entities, universal and existential quantification by state variables,

$$\zeta : \mathsf{StateVars} \to \mathbb{N} \; .$$

The Logic: Base Cases

- For φ a first-order formula:
  $(\boldsymbol{K}[i,j],\chi,\zeta) \models \varphi \;:\Leftrightarrow\; i=j$ and $(\boldsymbol{I}_i,\chi) \models \varphi$
- For φ an action formula:
  $(\boldsymbol{K}[i,j],\chi,\zeta) \models \varphi \;:\Leftrightarrow\; j=i{+}1$ and
  $(\boldsymbol{K}\langle i,i{+}1\rangle,\chi) \models \varphi$
- $(\boldsymbol{K}[i,j],\chi,\zeta) \models \partial$ for all $i \leq j$
- $(\boldsymbol{K}[i,j],\chi,\zeta) \models \bot$ for no i,j

State Variables

- $(\boldsymbol{K}[i,j],\chi,\zeta) \models s \triangleright \mathrm{E} \;:\Leftrightarrow$
  $\zeta(s) = i$ and $(\boldsymbol{K}[i,j],\chi,\zeta) \models \mathrm{E}$, and
  $(\boldsymbol{K}[i,j],\chi,\zeta) \models \mathrm{E} \triangleleft s \;:\Leftrightarrow$
  $\zeta(s) = j \in \mathbb{N}$ and $(\boldsymbol{K}[i,j],\chi,\zeta) \models \mathrm{E}$

Sequential Conjunction

- $(\boldsymbol{K}[i,j],\chi,\zeta) \models \mathrm{E} \otimes \mathrm{F} \;:\Leftrightarrow$
  there is a $k \in \mathbb{N}$ s.t.
  $(\boldsymbol{K}[i,k],\chi,\zeta) \models \mathrm{E}$ and $(\boldsymbol{K}[k,j],\chi,\zeta) \models \mathrm{F}$

Connectives

- Parallel Conjunction:
  $(\boldsymbol{K}[i,j],\chi,\zeta) \models \mathrm{E} \times \mathrm{F} \;\; :\Leftrightarrow$
  $(\boldsymbol{K}[i,j],\chi,\zeta) \models \mathrm{E}$ and $(\boldsymbol{K}[i,j],\chi,\zeta) \models \mathrm{F}$
- Parallel Disjunction
  $(\boldsymbol{K}[i,j],\chi,\zeta) \models \sum_{1 \le m \le n} \mathrm{E}_m \;\; :\Leftrightarrow$
  there is a $1 \le k \le n$ s.t. $(\boldsymbol{K}[i,j],\chi,\zeta) \models \mathrm{E}_k$
- Temporal Implication
  $(\boldsymbol{K}[i,j],\chi,\zeta) \models (\mathrm{E} \rightsquigarrow \mathrm{F}) \;\; :\Leftrightarrow$
  $i = j$ and,
  if $(\boldsymbol{K}[i,\infty],\chi,\zeta) \models \mathrm{E} \otimes \partial$,
  then $(\boldsymbol{K}[0,\infty],\chi,\zeta) \models \mathrm{F} \otimes \partial$

Quantification

- Elements of the Universe

  $(\boldsymbol{K}[i,j],\chi,\zeta) \models \exists x : \mathrm{E} \;:\Leftrightarrow$

  there is a $d \in \boldsymbol{U}$ s.t. $(\boldsymbol{K}[i,j],\chi_x^d,\zeta) \models \mathrm{E}$

  $(\boldsymbol{K}[i,j],\chi,\zeta) \models \forall x : \mathrm{E} \;:\Leftrightarrow$

  for all $d \in \boldsymbol{U}$, $(\boldsymbol{K}[i,j],\chi_x^d,\zeta) \models \mathrm{E}$

- States

  $(\boldsymbol{K}[i,j],\chi,\zeta) \models \blacklozenge s : \mathrm{E} \;:\Leftrightarrow$

  there is a k s.t. $i \leq k \leq j$ and

  $(\boldsymbol{K}[i,j],\chi,\zeta_s^k) \models \mathrm{E}$, and

  $(\boldsymbol{K}[i,j],\chi,\zeta) \models \blacksquare s : \mathrm{E} \;:\Leftrightarrow$

  $j = \infty$ and for all $k \geq i$, $(\boldsymbol{K}[i,j],\chi,\zeta_s^k) \models \mathrm{E}$

Tableaux Representation

- every branch of the tableau corresponds to a linear Kripke structure with a transition oracle.
- information about the frame and the transitions has to be coded in tableau nodes.

... taken from the CTL calculus.

Entities to be described

- Elements of the universe. A new constant resp. function symbol is introduced by a δ-rule when an $\exists$-quantifier is processed
- States: States are introduced when required by an existence formula (instantiation of a synchronization point)
- Transitions
- The path

Tableaux Representation

- Tableau calculus with prefixes for states:

$$\boxed{\alpha : F}$$

- Explicit description of paths:

$$\boxed{[\alpha, F_1, \beta, F_2, \gamma, \ldots, \hat{\infty}]}$$

  - only relevant states are named,
  - requirements on states/transitions on path segments in-between

Naming of Entities

Elements of the universe:

δ-rule: $$\frac{\exists x : F}{F[\hat{f}(\mathsf{free}(T))/x]}$$; $\hat{f}$ new.

States:

prefix symbols $(\Sigma_F := \{\hat{\alpha}, \hat{\beta}, \hat{\gamma}, \ldots\})$

- prefixes (state descriptors): $\hat{\alpha}(t_1, \ldots, t_n)$.
  newly introduced states: $\hat{\alpha}(\mathsf{free}(T))$.
- Arguments of prefixes contain only function symbols which are interpreted state independently.

Tableau Semantics

- First-order part: $\{\boldsymbol{M}(i) \mid i \in \mathbb{N}\}$
- Action Symbols: Transition oracle $\boldsymbol{N}$
- Prefix symbols:

$$\pi : \ (\Sigma_F \cup \{\hat{\infty}\}) \to \boldsymbol{U}^m \to (\mathbb{N} \cup \{\infty\})$$

$$\Pi_{\boldsymbol{K}} := (\pi \cup K, \mathbb{N} \cup \{\infty\})$$

- evaluation of prefixes:

$$\Pi_{\boldsymbol{K}} : \ (\Gamma \cup \{\hat{\infty}\}) \times \mathrm{Term}_{\Sigma_L^c} \to \mathbb{N} \cup \{\infty\}$$

$$\Pi_{\boldsymbol{K}}(\gamma, \chi) := (\pi(\hat{\gamma}))(\boldsymbol{K}(t_1, \chi), \ldots, \boldsymbol{K}(t_n, \chi)) \ .$$

e.g. $\Pi_{\boldsymbol{K}}(\hat{\alpha}(t_1, \ldots, t_n), \chi) = 42$.

- for $f \in \Sigma$, γ a prefix:

$$(\boldsymbol{M}(n))(f_\gamma(t_1, \ldots, t_n), \chi) := \\ (\boldsymbol{M}(\Pi_{\boldsymbol{K}}(\gamma, \chi)))(f(t_1, \ldots, t_n), \chi) \ .$$

Tableau Formulas

- prefixed formulas,

$$\boxed{\gamma : \mathrm{E}}$$

- *path information formulas*:

$$\boxed{p : [\alpha, F_1, \beta, F_2, \gamma, \ldots, \hat{\infty}]}$$

A set $\mathcal{F}$ of path information formulas and prefixed formulas is *valid* in $\boldsymbol{K}$ under χ if there is a Π such that $(\boldsymbol{K}, \Pi, \chi) \Vdash \mathcal{F}$.

Semantics: Prefixed State Formulas

$$\gamma : \mathrm{E}$$

Prefixes in E: $\gamma_1, \ldots, \gamma_n$
$s_1, \ldots, s_n$ new state variables,
$\zeta = \{s_j \mapsto \Pi(\gamma_j, \chi) \mid 1 \leq j \leq n\}$.

$(\boldsymbol{K}, \Pi, \chi) \models\!\!\models \gamma{:}\mathrm{E} \;\; :\Leftrightarrow$

there is an $i \in \mathbb{N} \cup \{\infty\}$ s.t.

$(\boldsymbol{K}[\Pi(\gamma, \chi), i], \chi, \zeta) \models \mathrm{E}[s_1/\gamma_1, \ldots, s_n/\gamma_n]$.

In particular, for an action formula E,

$$
\begin{aligned}
(\boldsymbol{K}, \Pi, \chi) \Vdash \gamma : \mathrm{E} \quad &:\Leftrightarrow \\
&(\boldsymbol{K}\langle \Pi(\gamma,\chi), \Pi(\gamma,\chi)+1 \rangle, \chi) \models \mathrm{E}
\end{aligned}
$$

i.e., if the transition from $\Pi(\gamma,\chi)$ to $\Pi(\gamma,\chi)+1$ satisfies E under χ.

Semantics: Path Information Formulas

$$(\boldsymbol{K}, \Pi, \chi) \Vdash [\gamma_0, L_0, \gamma_1, L_1, \ldots, \gamma_n, L_n, \hat{\infty}]$$

$:\Leftrightarrow$ $\Pi(\gamma_0, \chi) = 0,$ and

for all $0 \leq i \leq n$:

$\Pi(\gamma_i, \chi) < \Pi(\gamma_{i+1}, \chi),$

and for all j s.t. $\Pi(\gamma_i, \chi) < j < \Pi(\gamma_{i+1}, \chi)$:

$(\boldsymbol{K}, \Pi \cup \{\hat{\delta} \mapsto j\}, \chi) \Vdash L_i$

$L_i =$ false implies $\Pi(\gamma_{i+1}, \chi) = \Pi(\gamma_i, \chi){+}1$.

$[\hat{\delta}/\triangledown]$

with $\hat{\delta}$ a new 0-ary prefix symbol.

$\triangledown$ as an auxiliary “generic prefix” on path segments,
is instantiated by a prefix when a state on the respective segment is explicitly named.

Examples:

$[0, \ldots \alpha, \triangledown : p(x), \beta, \ldots]$
$[0, \ldots, \alpha, \alpha : \sum_{i=1..n} \mathrm{E}_i \lhd \triangledown, \beta, \ldots]$

The Tableau Calculus

Initialization

$$\frac{}{\begin{array}{c}[\hat{0}, \mathsf{true}, \infty] \\ \hat{0} : F\end{array}}$$

+ Prefixed First-Order Calculus

Atomic Closure Rule

γ a prefix, A, B atomic formulas, σ a substitution,

σ_γ: replace every function symbol f by f_γ
(interpreted state-independently)

$$\frac{\begin{array}{c}\gamma : A \\ \gamma : B \\ \sigma(A) = \neg\sigma(B)\end{array}}{\perp}$$

apply σ_γ to the whole tableau.

Prefixed Event Formulas

$$\frac{\alpha : (\beta \rhd \mathrm{E})}{\begin{array}{c}\beta \equiv \alpha \\ \alpha : \mathrm{E}\end{array}}$$

Common Schema

... all other types formulas need consideration of the path information:

$$\frac{\begin{array}{c}\text{prefixed formula} \\ \text{path information formula}\end{array}}{\begin{array}{c}\text{prefixed formulas} \\ \text{path information formulas}\end{array}}$$

Postfixed Event Formulas

Synchronization point associated with the last elementary event of a formula

$$\frac{\alpha : \mathrm{E} \lhd \gamma \;,\; \mathsf{len}(\mathrm{E}) = \{1\} \;, \quad [..., \alpha, L, \beta, ...]}{\begin{array}{c}[..., \alpha, \mathsf{false}, \beta, ...] \\ \beta \equiv \gamma \\ \alpha : \mathrm{E}\end{array}}$$

$$\frac{\alpha : F \lhd \beta \;,\; \mathsf{len}(F) = \{0\}}{\begin{array}{c}\beta \equiv \alpha \\ \alpha : F\end{array}}$$

$$\frac{\alpha : \partial \lhd \beta \quad [..., \beta, ..., \alpha, ...]}{\perp}$$

Complex cases: by moving the postfix inside the outermost event connective.

Temporal Quantification

- linear ordering between states:
  every synchronization point must be integrated into this ordering.

$\Rightarrow$ synchronization points are shifted along path formulas;
systematic application of the γ- or δ-rules along the state sequence.

Universal Quantification

$$\frac{\alpha : \blacksquare s : \mathrm{E}}{\alpha : \blacksquare s_{\geq \alpha} : \mathrm{E}}$$

$$\frac{\begin{array}{c}\alpha : \blacksquare s_{\geq \beta} : \mathrm{E} \\ [\ldots, \beta, L, \gamma, \ldots]\end{array}}{\begin{array}{c}[\ldots, \beta, L \wedge \alpha : \mathrm{E}[\nabla / s], \gamma, \ldots] \\ \alpha : \mathrm{E}[\beta / s] \\ \text{if } \gamma \neq \infty\text{:}\ \ \alpha : \blacksquare s_{\geq \gamma} : \mathrm{E}\end{array}}$$

Existential Quantification

$$\frac{\alpha : \blacklozenge s : \mathrm{E}}{\alpha : \blacklozenge s_{\geq \alpha} : \mathrm{E}}$$

$$\frac{\begin{array}{c}\alpha : \blacklozenge s_{\geq \beta} : \mathrm{E} \\ [..., \beta, L, \gamma, ...]\end{array}}{\begin{array}{c|c|c} \alpha : \mathrm{E}[\beta / s] & \begin{array}{r}[..., \beta, L \wedge \alpha : \mathrm{E}[\nabla / s] \rightsquigarrow \bot, \\ \hat{\delta}(\mathsf{free}(T)), L, \gamma, ...]\end{array} & \text{if } \gamma \neq \infty\text{:} \\ & L[\hat{\delta}(\mathsf{free}(T)) / \nabla] & [..., \beta, L \wedge \alpha : \mathrm{E}[\nabla / s] \rightsquigarrow \bot, \gamma, ...] \\ & \alpha : (\mathrm{E}[\beta / s] \rightsquigarrow \bot) & \alpha : \mathrm{E}[\beta / s] \rightsquigarrow \bot \\ & \alpha : \mathrm{E}[\hat{\delta}(\mathsf{free}(T)) / s] & \alpha : \blacklozenge s_{\geq \gamma} : \mathrm{E} \end{array}}$$

Alternative and parallel compositions

$$\frac{\alpha : \sum_{i=1\ldots n} \mathrm{E}_i}{\alpha : \mathrm{E}_1 \;\Big|\; \ldots \;\Big|\; \alpha : \mathrm{E}_n}$$

$$\frac{\alpha : \left(\mathrm{E}_1 \times \ldots \times \mathrm{E}_n\right)}{\begin{array}{c}\alpha : \mathrm{E}_1 \\ \vdots \\ \alpha : \mathrm{E}_n\end{array}}$$

Sequential Composition:

$$\mathrm{E} \otimes \mathrm{F}$$

Parentheses around composite events, e.g. $(\sum \ldots \mathrm{E}_i)$ and $(\mathrm{E}_1 \times \ldots \times \mathrm{E}_n)$ denote implicit synchronization (virtual entities):

$$\alpha : \mathrm{E} \otimes \mathrm{F} \equiv \alpha : \blacklozenge s : (\mathrm{E} \lhd s) \otimes (s \rhd \mathrm{F})$$

can be split into two parts ("sequential conjunction")

$$\frac{\alpha : \mathrm{E} \otimes \mathrm{F}}{\alpha : \blacklozenge s_{\geq \alpha} : (\mathrm{E} \lhd s) \otimes (s \rhd \mathrm{F})}$$

$$\frac{\alpha : (\mathrm{E} \lhd \beta) \otimes (\beta \rhd \mathrm{F})}{\begin{array}{c} \alpha : \mathrm{E} \lhd \beta \\ \beta : \mathrm{F} \end{array}}$$

Temporal Implication

When resolving constraints $\mathrm{E} \leadsto \mathrm{F}$, in the base case, E is a first-order formula or an action formula or a delay:

> for E a first-order formula
>
> or an action formula:
>
> $$\frac{\alpha : \mathrm{E} \leadsto \mathrm{F}}{\alpha : \neg \mathrm{E} \;\Big|\; \begin{array}{l} \alpha : \mathrm{E} \\ \hat{0} : \mathrm{F} \end{array}}$$
>
> $$\frac{\alpha : \partial \leadsto \mathrm{F}}{\hat{0} : \mathrm{F}}$$

Otherwise: equivalent rewriting of the formula.

Dealing with State Quantification

- every prefix symbol is introduced (and placed in the path information formula) exactly once, and there is exactly one prefix which is built from it $\Rightarrow$ Π well-defined.
- every prefix occurs also in the most recent path information formula of the same branch.
- there are no free state variables in the calculus (replaced by systematic state-γ-rule).

Correctness

(a) If a tableau $\mathcal{T}$ is satisfiable and $\mathcal{T}'$ is created from $\mathcal{T}$ by an application of any of the rules mentioned above, then $\mathcal{T}'$ is also satisfiable.

(b) If there is any closed tableau for $\mathcal{F}$, then $\mathcal{F}$ is unsatisfiable.

Properties

- the Logic is not compact,
- no calculus for it can be complete.
- The calculus is complete modulo inductive properties.

- the same tableau representation as for first-order CTL
- With $\blacksquare$ and $\blacklozenge$, the handling of state variables is closely related to the strategy for resolving the CTL modalities $\Box$ and $\Diamond$

$\Rightarrow$ representation both suitable for *modal temporal logics* and for logics using *temporal connectives* and *explicit temporal quantification*.

- potential integration of both calculi.