SS 2017
Software Verification
From multimodal to temporal logic

Prof. Dr. Holger Schlingloff¹,²
Dr. Esteban Pavese¹

(1) Institut für Informatik der Humboldt Universität
(2) Fraunhofer Institut für offene Kommunikationssysteme FOKUS
Recap

- Parallel / distributed / concurrent computation? Interleaving?
- Is parallel composition idempotent?
- Given a nondeterministic labelled transition system, is there an equivalent deterministic one?
- What is equivalence of Kripke models?
- Give two nonisomorphic models which are equivalent!
- What is a simulation relation?
- What is a bisimulation relation?
- Relation between simulation and bisimulation?
Recap: Multimodal logic

- **Syntax:**
  
  \[
  \text{MML} ::= \top \mid \bot \mid (\text{MML} \to \text{MML}) \mid \langle A \rangle \text{MML}
  \]

- Captures precisely bisimulation on FSMs:
  - two FSMs are bisimilar iff they satisfy exactly the same MML-formulas

- Cannot talk about “transitive closure”
  - assume each transition is one step in a computation; how would you express “after a finite number of steps”?
  - If a call is made by the client, then eventually she will continue?

- Cannot even talk about “next time”
  - If a call is made, then the next step must be service?
• Solution: new operators

• Let \( \prec \) be the union of all accessibility relations in a model, and \(<\) and \(\leq\) the transitive and reflexive-transitive closure of \(\prec\)

• Define \textit{next}- and \textit{eventually}-operators by

  • \( w_0 \models X \varphi \) iff there exists \( w_1 \in U \) such that \( w_0 \prec w_1 \) and \( w_1 \models \varphi \),
  • \( w_0 \models F^+ \varphi \) iff there exists \( w_1 \in U \) such that \( w_0 < w_1 \) and \( w_1 \models \varphi \), and
  • \( w_0 \models F^* \varphi \) iff there exists \( w_1 \in U \) such that \( w_0 \leq w_1 \) and \( w_1 \models \varphi \).

• Example!
Dual Operators and Redundancy

\[ \begin{align*}
\text{X } \varphi & \triangleq \neg \text{X } \neg \varphi \\
G^+ \varphi & \triangleq \neg F^+ \neg \varphi \\
G^* \varphi & \triangleq \neg F^* \neg \varphi.
\end{align*} \]

\[ \text{G}^*(\text{req} \rightarrow F^+ \text{ack}). \]

\[(F^* \varphi \leftrightarrow \varphi \lor F^+ \varphi)\]
\[(F^+ \varphi \leftrightarrow \text{X } F^* \varphi)\]
\[F^+ \text{ is strictly more expressive than } F^*. \]

- In the literature, decorations + and * are omitted, since only one version of F and G is used.
- Furthermore, ◊ is used for X, ◊ for F and □ for G.
Some Axioms and Rules

- $|- G^* \phi \rightarrow \phi$
- $|- \phi \rightarrow F^* \phi$
- $|- G^* \phi \rightarrow G^* G^* \phi$
- $|- G^* G^* \phi \rightarrow G^* \phi$
- $|- F^* F^* \phi \rightarrow F^* \phi$
- $|- F^+ F^+ \phi \rightarrow F^+ \phi$
- $|- X \phi \rightarrow X \phi$ iff $\preceq$ is univalent (or deterministic): if $w \preceq w_1$ and $w \preceq w_2$, then $w_1 = w_2$
- $|- X \phi \rightarrow X \phi$ iff $\preceq$ is serial: for all $w$ in $U$ there is a $w'$ in $U$ such that $w \preceq w'$
- $|- X \phi \leftrightarrow X \phi$ iff $\preceq$ is linear (or functional): for all $w$ in $U$ there is exactly one $w'$ in $U$ such that $w \preceq w'$
Local vs. Global Validity

Recap: Semantics of MML:

• Let $M$ be an FSM and $s \in S$
  
  - $(M,s) \models \langle a \rangle \phi$ iff $\exists s' \in S$ s.t. $(s,a,s') \in R$ and $(M,s') \models \phi$
  
  - $M \models \phi$ iff $(M,s_0) \models \phi$

• This is called "initial semantics". Alternative: "global semantics"
  
  - $M \models \phi$ iff for all $s \in S$, $(M,s) \models \phi$
  
  - In the global semantics the necessitation rules hold:
    $\phi \models X\phi$ and $\phi \models G^+\phi$ and $\phi \models G^*\phi$

• In a tool, you have to be careful which semantics is used
  
  - in initial semantics you may have to write a $G^*$ in front of each specification formula
  
  - in global semantics, you may have to begin each specification formula with (start $\rightarrow$ ...)
The Glory of the Past

- Incidentally, the 0-ary operator “start” cannot be expressed in global semantics
  - The same holds for all modalities which “look backward”
  - However, this might be useful in specification
    “If the previous action was p, then the next action must be q”
    “If a request arrives, it must have been sent before”
    “Whenever a request arrives which hasn’t been served yet, the event handler is started”

- Solution: New operator $X^- / F^- / G^-
  - $(X^- p \rightarrow X q)$
  - $(\text{request} \rightarrow F^- \text{send})$
  - $G^*(\text{request} \land G^- \rightarrow \text{serve} \rightarrow \text{start_handling})$

- Still not expressive enough
Until and Unless

- $w_0 \models (\varphi U^k \psi)$ iff there exists $w_1 \in U$ with $w_0 < w_1$ and $w_1 \models \psi$, and for all $w_2 \in U$ with $w_0 < w_2$ and $w_2 < w_1$, we have $w_2 \models \varphi$.

\[
\text{G}^*(\text{req} \rightarrow (\text{req} U^+ \text{ack})).
\]

- $X \varphi \iff (\bot U^+ \varphi)$
- $F^+ \varphi \iff (\top U^+ \varphi)$

$(\varphi U^* \psi) \triangleq (\psi \lor \varphi \land (\varphi U^+ \psi))$

$(\varphi W^+ \psi) \triangleq \neg (\neg \psi U^+ \neg (\varphi \lor \psi))$

For natural models, $(\varphi W^+ \psi) \leftrightarrow ((\varphi U^+ \psi) \lor G^+ \varphi)$
Since

Expressiveness results:

• There are various theorems about the “disentangling” of until and since; e.g., \textbf{start} (= \textit{X}^{-} \perp) can replace \textit{U}^{-}

• Descriptive past and imperative future: every formula can be written as \textit{G}^{*}(\phi \rightarrow \psi), where \phi is pure-past and \psi is pure-future

• On linear structures with initial semantics, until is \textit{expressively complete}: For every first-order formula with one free variable there is a temporal formula (with \textit{U}^{+} as only operator)

• Most tools (e.g., SMV) support a subset or superset of operators

A note on notation: In SMV,
• \textit{U}^{-} = \textit{S} („since“),
• \textit{(pWq)} = \textit{(qVp)} („releases“),
• \textit{(pW^-q)} = \textit{(qTp)} („triggers“)
LTL

\[
\text{LTL ::= } \mathcal{P} \mid \bot \mid \text{LTL} \to \text{LTL} \mid \text{LTL} U^+ \text{LTL} \mid \text{LTL} U^- \text{LTL}
\]

- Usually interpreted on natural or on linearly ordered models
- Expressively equivalent to FOL (\(<\)) on linear orders
- Arguably more intuitive to use

\[
\begin{align*}
\text{FOL}((\neg \text{ack } U^\neg \text{ req }) U^+ \text{ack})) &= \exists t_1(t_0 < t_1 \land \text{ack}(t_1) \land \forall t_2(t_0 < t_2 < t_1 \rightarrow \text{FOL}((\neg \text{ack } U^\neg \text{ req }))\{t_0 := t_2\}))) \\
&= \exists t_1(t_0 < t_1 \land \text{ack}(t_1) \land \forall t_2(t_0 < t_2 < t_1 \rightarrow \\
&\quad \exists t_3(t_3 < t_2 \land \text{req}(t_3) \land \forall t_4(t_3 < t_4 < t_2 \rightarrow \neg \text{ack}(t_4))))).
\end{align*}
\]
SMV – LTL semantics

- $\mathbf{X} \ p$ is true at time $t$ if $p$ is true at time $t + 1$.
- $\mathbf{F} \ p$ is true at time $t$ if $p$ is true at some time $t' \geq t$.
- $\mathbf{F} [1, u] \ p$ is true at time $t$ if $p$ is true at some time $t + l \leq t' \leq t + u$.
- $\mathbf{G} \ p$ is true at time $t$ if $p$ is true at all times $t' \geq t$.
- $\mathbf{G} [1, u] \ p$ is true at time $t$ if $p$ is true at all times $t + l \leq t' \leq t + u$.
- $\mathbf{p U q}$ is true at time $t$ if $q$ is true at some time $t' \geq t$, and for all time $t''$ (such that $t \leq t'' < t'$) $p$ is true.
- $\mathbf{p V q}$ is true at time $t$ if $q$ holds at all time steps $t' \geq t$ up to and including the time step $t''$ where $p$ also holds. Alternatively, it may be the case that $p$ never holds in which case $q$ must hold in all time steps $t' \geq t$.
- $\mathbf{Y} \ p$ is true at time $t > t_0$ if $p$ holds at time $t - 1$. $\mathbf{Y} \ p$ is false at time $t_0$.
- $\mathbf{Z} \ p$ is equivalent to $\mathbf{Y} \ p$ with the exception that the expression is true at time $t_0$.
- $\mathbf{H} \ p$ is true at time $t$ if $p$ holds in all previous time steps $t' \leq t$.
- $\mathbf{H} [1, u] \ p$ is true at time $t$ if $p$ holds in all previous time steps $t - u \leq t' \leq t - l$.
- $\mathbf{O} \ p$ is true at time $t$ if $p$ held in at least one of the previous time steps $t' \leq t$.
- $\mathbf{O} [1, u] \ p$ is true at time $t$ if $p$ held in at least one of the previous time steps $t - u \leq t' \leq t - l$.
- $\mathbf{p S q}$ is true at time $t$ if $q$ held at time $t' \leq t$ and $p$ holds in all time steps $t''$ such that $t' < t'' \leq t$.
- $\mathbf{p T q}$ is true at time $t$ if $p$ held at time $t' \leq t$ and $q$ holds in all time steps $t''$ such that $t' \leq t'' \leq t$. Alternatively, if $p$ has never been true, then $q$ must hold in all time steps $t''$ such that $t_0 \leq t'' \leq t$. 