SS 2017
Software Verification
Safety and Liveness

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

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

• Difference between LTL and CTL?
• Difference between $G^* F^* p$ and $AG^* EF^* p$?
• Difference between $AX \perp$ and $AX \perp$?
• How to formulate „infinitely often $p$“ in LTL (on natural models)?

• Which of the following are valid in LTL (on natural models)?
  - $(G^* G^* G^* \varphi \leftrightarrow G^* \varphi)$
  - $(F^* F^* \varphi \leftrightarrow F^* \varphi)$
  - $(G^* F^* \varphi \leftrightarrow F^* G^* \varphi)$
  - $(F^* G^* \varphi \rightarrow G^* F^* \varphi)$
  - $(F^* G^* F^* \varphi \leftrightarrow G^* F^* \varphi)$
  - $(G^* F^* G^* \varphi \leftrightarrow F^* G^* \varphi)$
Demo

Formula Syntax

Atom ::= a | b | c | ... | z
Formula ::= Atom
           TRUE | FALSE
           - formula (negation)

formula & formula (conjunction)
formula | formula (disjunction)
formula -> formula (implication)
formula <-> formula (double impl.)

X formula (next)
F formula (eventually)
G formula (always)
formula U formula (until)

Formula

Type below a PLTL-formula

Example: (F a) & (G ((a U b) -> (X a)))

Set

(F a) & (G ((a U b) -> (X a)))

Results

This is a model of Set:
State 0{a, b}
Cycle starts at the state 0

http://www.sc.ehu.es/jiwlucap/TTM.html
Coding a Model in LTL

- Given a finite Kripke model $M$, define a linear temporal formula $\varphi_M$ such that $M \models \psi$ iff $\models (\varphi_M \rightarrow \psi)$
- Reminder: $\models (\varphi_M \rightarrow \psi)$ iff $(\varphi_M \psi)$ is unsatisfiable
- Reduction of model checking to (temporal) satisfiability
- Bounded model checking uses this approach (e.g. nuSMV with Zchaff)
\begin{itemize}
  \item $\varphi$ is a \textit{safety property}, iff for every natural model $M$,
    \[
    M \models \varphi \text{ if } \forall i \in M' : \ [\ldots i] \circ M' \models \varphi
    \]
  \item $\varphi$ is a \textit{liveness property}, iff for every natural model $M$,
    \[
    \forall i \in M' : \ [\ldots i] \circ M' \models \varphi
    \]
\end{itemize}
Some Theorems

- Every LTL formula can be written in one of these forms (where p is a pure past formula)
  - Every LTL safety property is expressible as $G^*\varphi$ (where $\varphi$ is pure past)
  - Every LTL formula can be written as reactivity $\land(G^*F^*\varphi \lor F^*G^*\psi)$

- All the inclusions are strict

- All the non-inclusions are provable (dualities)
  - e.g. $F^*G^*p$ cannot be expressed as $G^*F^*\varphi$

- Conjunction and disjunction of a recurrence is a recurrence
  - $G^*F^*p \land G^*F^*q \rightarrow G^*F^*(p \land (\neg p)U\neg q)$ (there had been an error here, but its gone)
  - $G^*F^*p \lor G^*F^*q \leftrightarrow G^*F^*(p \lor q)$

- Obligations can be expressed as recurrences and persistences
  - $G^*p \leftrightarrow G^*F^*H^*p$, $F^*p \leftrightarrow G^*F^*P^*p$, where $H^*p \leftrightarrow \neg P^*\neg p$
Safety and Liveness Properties

- Safety properties are closed under finite unions and arbitrary intersections.
- Liveness properties are closed under arbitrary unions, but not under intersections.
- $\top$ is the only property which is both a safety and a liveness property.
- For any property $\varphi$ there exists a safety property $\varphi_S$ and a liveness property $\varphi_L$ such that $\varphi = (\varphi_S \cap \varphi_L)$.

Proof of decomposition theorem:
- $\varphi_s = \{w_0w_1\ldots \mid \text{for every } i, w_0w_1\ldots w_i \text{ is a prefix of } \varphi\}$
- $\varphi_l = \varphi \cup \{w_0w_1\ldots \mid \text{for some } i, w_0w_1\ldots w_i \text{ is not a prefix of } \varphi\}$
- show: $\varphi_s$ is safety, $\varphi_l$ is liveness, $\varphi = \varphi_s \cap \varphi_l$
Examples

- \((p \mathbf{U}^+ q) \iff ((p \mathbf{W}^+ q) \land \mathbf{F}^+ q)\)
- \(G^*(p \land F^*q) \iff (G^*p \land G^*F^*q)\)
- Total program correctness = invariance \land termination

4.4. Theorem. Every temporal formula built from literals with \(\bot, \top, \land, \lor\) and \(W^+\) defines a safety property.