 Formalization and verification of property specification patterns

Dmitriy Bryndin

MSU

December 6, 2010
Patterns:

- Property Patterns
  - Occurrence
    - Absence
    - Universality
    - Existence
  - Bounded Existence
- Order
  - Precedence
  - Response
  - Chain Precedence
  - Chain Response

Scopes:

- Globally
- Before $R$
- Between $Q$ and $R$
- After $Q$
- After $Q$ until $R$
Def: (Scope)

The scope consists of all states beginning with the starting delimiter state and up to but not including the ending delimiter state.

A scope is optional; if the delimiters are not present, then the specification is True.

Def: (Existence pattern)

A given state must occur within a scope.

LTL formulas are formal, scope/pattern definitions are not
Illustration for scopes, M.Dwyer et al.
Problem: Inconsistent graphical notation for scopes

∃P, Between Q and R:  □(Q ∧ ¬R → (¬R)W(P ∧ ¬R))

Illustration for Between Q and R scope (1 interval):

−− Q === Q ==== R − − − − >

Follows from LTL (2 intervals):

− − Q === Q ==== R − − − − >

Q ==== R

Q === R
Problem: Inconsistent graphical notation for scopes

\[ \exists P, \text{Between } Q \text{ and } R: \quad \Box(Q \land \neg R \rightarrow (\neg R) W (P \land \neg R)) \]

Illustration for Between \( Q \) and \( R \) scope (1 interval):

\[ \begin{array}{cccccccc}
- & - & Q = P = Q & \Rightarrow & \Leftarrow & R & - & - & - & >
\end{array} \]

Follows from LTL (2 intervals):

\[ \begin{array}{cccccccc}
- & - & Q = P = Q & \Rightarrow & \Leftarrow & R & - & - & - & >
\end{array} \]
\[ Q \Rightarrow \Leftarrow R \]
Problem: Inconsistent graphical notation for scopes

\[ \exists P, \text{ Between } Q \text{ and } R: \quad \square (Q \land \neg R \rightarrow (\neg R) \mathcal{W} (P \land \neg R)) \]

Illustration for Between \( Q \) and \( R \) scope (1 interval):

\[ - - Q = P = Q =\cdots = R - - - - \]

Follows from LTL (2 intervals):

\[ - - Q - P - Q =\cdots = R - - - - \quad \text{min, not max interval} \]
Problem: Inconsistent formulas

If the delimiters are not present, then the specification is *True* (M.Dwyer et al.).

\[ \exists P, \text{Before } R \quad \exists P, \text{Between } Q \text{ and } R \]
\[ R \quad \text{---} \quad (Q \land R) \quad \text{---} \quad > \]
\[ (\neg R) \ Diamond (P \land \neg R) \quad \Box (Q \land \neg R \rightarrow (\neg R) \ Diamond (P \land \neg R)) \]

*False* \quad *True*
Possible formalizations of scopes

Strong scopes, $S$: contain no empty intervals
Weak scopes, $S^W$: empty intervals are allowed

Example:

\[ (Q \land R) \implies S = \emptyset, \quad S^W = \{\emptyset\} \]

For all patterns, except the existence related, there are no difference between strong and weak scopes.

Strong and Weak versions of “Globally” and “After Q” scopes are the same.
Formal definitions: Weak Scopes

Weak scope is a set of *intervals*, where an interval is a sequence of consecutive numbers, corresponding to the indecies of the states in the execution.

\[
\begin{align*}
S_W^G &= \{ [0, \infty) \} \\
S_W^{BR} &= \{ [0, i) \mid i = \min(\{ k \geq 0 \mid s_k \models R \}) \} \\
S_W^{AQ} &= \{ [i, \infty) \mid i = \min(\{ k \geq 0 \mid s_k \models Q \}) \} \\
S_W^{BWQR} &= \{ [i, j) \mid s_i \models Q, j = \min(\{ k \geq i \mid s_k \models R \}) \} \\
S_W^{AUQR} &= S_{AUQR} \cup S_W^{BWQR}
\end{align*}
\]
Formal definitions: Strong Scopes

Strong scope is a set of nonempty intervals.

\[ S_G = \{ [0, \infty) \} \]

\[ S_{BR} = \{ [0, i) \mid s_0 \models \neg R, \; i = \min(\{ k > 0 \mid s_k \models R \}) \} \]

\[ S_{AQ} = \{ [i, \infty) \mid i = \min(\{ k \geq 0 \mid s_k \models Q \}) \} \]

\[ S_{BWQR} = \{ [i, j) \mid i \geq 0, \; s_i \models (Q \land \neg R), \; j = \min(\{ k > i \mid s_k \models R \}) \} \]

\[ S_{AUQR} = S_{BWQR} \cup \{ [i, \infty) \mid i \geq 0, \; s_i \models Q, (\forall j \geq i \cdot s_j \models \neg R) \} \]
Formal definitions: Patterns

Absence of $P$: $\forall I \in S, \forall n \in I \cdot s_n \models \neg P$

Existence of $P$: $\forall I \in S, \exists n \in I \cdot s_n \models P$

Strong Existence of $P$: $S \neq \emptyset, \forall I \in S, \exists n \in I \cdot s_n \models P$

Universally $P$: $\forall I \in S, \forall n \in I \cdot s_n \models P$

$S$ Precedes $P$: $\forall I \in S, \forall n \in I \cdot (s_n \models P \implies \exists m \in I \cdot (m \leq n, s_m \models S))$

$S$ Response to $P$: $\forall I \in S, \forall n \in I \cdot (s_n \models P \implies \exists m \in I \cdot (m \geq n, s_m \models S))$
Deriving LTL formulas using formal definitions

Absence of $P$, After $Q$ \iff $\forall I \in S_{AQ}, \forall n \in I \bullet s_n \models \neg P$

\forall I \in S_{AQ}, \forall n \in I \bullet s_n \models \neg P \iff

\forall i \geq 0 \bullet (i = \min(\{k \geq 0 \mid s_k \models Q\}) \implies \forall n \in [i, \infty) \bullet s_n \models \neg P)$

the RHS of the equivalence holds iff the following holds

\forall i \geq 0 \bullet (s_i \models Q \implies \forall n \in [i, \infty) \bullet s_n \models \neg P)$

this is the definition of $\square(Q \rightarrow \square(\neg P))$. 
Proof of correctness

Derived formulas for:

Patterns:
- Absence
- Existence
- Strong Existence
- Universality

Weak and Strong Scopes:
- Globally
- Before $R$
- After $Q$
- Between $Q$ and $R$
- After $Q$ until $R$

highlighted a few inconsistencies, fixed 1 typo, simplified several formulas
Everything is formal now

Before:
- Informal definitions of Patterns
- Informal, inconsistent definitions of Scopes
- LTL formulas reviewed, some are tested

After:
- Formal definitions of Patterns
- Two versions of formal definitions of Scopes
- Larger set of LTL formulas are proven to be correct
- Simplified LTL formulas