Refutation of information flow interface for hyper linear temporal logic (LTL)

© Copyright 2020 by Colin James III  All rights reserved.

Abstract: We evaluate the final theorem and proof of the paper with both as not tautologous. Furthermore, the table result of the proof denial does not match that of the theorem denial. Therefore the stateful and stateless information flow conjecture is refuted. By extension temporal linear logic (TLL) and hyper temporal linear logic (HyperTLL) are also refuted. These results form a non tautologous fragment of the universal logic $VŁ₄$.

We assume the method and apparatus of Meth8/$VŁ₄$ with Tautology as the designated proof value, $F$ as contradiction, $N$ as truthity (non-contingency), and $C$ as falsity (contingency). The 16-valued truth table is row-major and horizontal, or repeating fragments of 128-tables, sometimes with table counts, for more variables. (See ersatz-systems.com.)

LET ~ Not $\neg$ ; + Or $\lor$ $\sqcup$ ; - Not Or $\lnot \lor$ ; & And $\land$ $\cap$ , , $\otimes$ ; \ Not And $\neg \land$ ; > Imply, greater than, $\rightarrow$, $\Rightarrow$, $\supset$, $\implies$ ; < Not Imply, less than, $\in$, $\subset$, $\ni$, $\notin$, $\leftarrow$, $\Leftarrow$ ; = Equivalent, $\equiv$, $\iff$, $\leftrightarrow$, $\triangleq$, $\equiv$ ; @ Not Equivalent, $\neq$, $\oplus$ ; % possibility, for one or some, $\exists$, $\exists$, $\Diamond$, $\exists$ ; # necessity, for every or all, $\forall$, $\square$, $\Box$; (z=z) T as tautology, T, ordinal 3; (z@z) F as contradiction, $\emptyset$, Null, $\bot$, zero; (%z>@z) N as non-contingency, $\Delta$, ordinal 1; (%z<@z) C as contingency, $\nabla$, ordinal 2; ~($y < x$) ($x \leq y$), ($x \subseteq y$), ($x \subseteq y$); (A=B) (A~B).

Note for clarity, we usually distribute quantifiers onto each designated variable.


Abstract … Our framework provides a refinement relation and a composition operation that support both incremental design and independent implementability. We develop our theory for both stateless and stateful interfaces. We … provide three plausible trace semantics to stateful information-flow interfaces and we show that only two correspond to temporal logics for specifying hyperproperties, while the third defines a new class of hyperproperties that lies between the other two classes.

Theorem 55. $[F_t]\not\subseteq [F_t]_a \not\subseteq [F_t]_u$.

Proof. $T_u \in [F_t]_u$ but $T_u \notin [F_t]_a$. And, $T_u \in [F_t]_a$ but $T_u \notin [F_t]_u$.

<table>
<thead>
<tr>
<th>t=0</th>
<th>t=1</th>
<th>1 &lt; t</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x$</td>
<td>$y$</td>
<td>$z$</td>
</tr>
<tr>
<td>$x$</td>
<td>$y$</td>
<td>$z$</td>
</tr>
<tr>
<td>$x$</td>
<td>$y$</td>
<td>$z$</td>
</tr>
</tbody>
</table>

Table 1 Set of traces $T_u$.

<table>
<thead>
<tr>
<th>t=0</th>
<th>t=1</th>
<th>1 &lt; t</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x$</td>
<td>$y$</td>
<td>$z$</td>
</tr>
<tr>
<td>$x$</td>
<td>$y$</td>
<td>$z$</td>
</tr>
<tr>
<td>$x$</td>
<td>$y$</td>
<td>$z$</td>
</tr>
</tbody>
</table>

Table 2 Set of traces $T_a$.

Linear temporal logic [28] (LTL) cannot express the properties introduced in Definition 54 [8, 7]. LTL extended with knowledge (linear time epistemic logic [5]) can express the strong no-flow interpretation of $F_t$ [5]. The unstructured no-flow semantics can be specified in HyperLTL [7]. HyperLTL extends LTL by allowing quantification over traces, which occur at the beginning of the formula. Epistemic temporal logic and HyperLTL have incomparable expressive power [5]. To the best of our knowledge, there is no temporal formalism that supports the structure-aware semantics.

Remark 55.1: Theorem 55 is numbered as (55.1.1).
LET p, q, s, t, u: [F], a, s, t, u.

\[\neg((p \land u) \land u) < ((p \land u) \land q) < ((p \land u) \land s) = (s = s) ;\]

\[
\begin{array}{cccc}
F & F & F & F \\
T & F & F & F \\
F & F & F & F \\
\end{array} \quad (2) \quad (55.1.2)
\]

Remark 55.2: The proof for Theorem 55 is numbered (55.2.1).

\[\neg((t \land u) < ((p \land u) \land u)) < ((t \land u) < ((p \land u) \land q)) \land \neg((t \land q) < ((p \land u) \land q)) < ((t \land q) < ((p \land u) \land s)) ;\]

\[
\begin{array}{cccc}
T & T & T & T \\
T & F & F & F \\
T & T & T & T \\
T & F & F & F \\
\end{array} \quad (55.2.2)
\]

Remark 55.3: Eqs. 55.1.2 and 55.2.2 are not tautologous. This means Theorem 55 and its proof are refuted. Furthermore, the table result of the proof denial does not match that of the theorem denial. Therefore the stateful and stateless information flow conjecture is refuted, and by extension temporal linear logic (TLL) and hyper temporal linear logic (HyperTLL) are also refuted.