Interval Temporal Logic

Antonio Cau and Ben Moszkowski

2019-05-10

Abstract

Interval Temporal Logic (ITL) is a flexible notation for both propositional and first-order reasoning about periods of time found in descriptions of hardware and software systems. Unlike most temporal logics, ITL can handle both sequential and parallel composition and offers powerful and extensible specification and proof techniques for reasoning about properties involving safety, liveness and projected time [129]. Timing constraints are expressible and furthermore most imperative programming constructs can be viewed as formulas in a slightly modified version of ITL [120]. Tempura provides an executable framework for developing and experimenting with suitable ITL specifications. In addition, ITL and its mature executable subset Tempura [152] have been extensively used to specify the properties of real-time systems where the primitive circuits can directly be represented by a set of simple temporal formulae. In addition, Tempura has been applied to hardware simulation and other areas where timing is important.
Contents

1 Finite Interval Temporal Logic 3
  1.1 Syntax ......................................................... 3
  1.2 Semantics ...................................................... 3
  1.3 Derived Constructs ............................................. 5
  1.4 Propositional proof system ................................. 7
  1.5 First order proof system ................................... 7

2 Finite and Infinite Interval Temporal Logic 8
  2.1 Syntax .......................................................... 8
  2.2 Semantics ........................................................ 8
  2.3 Derived Constructs ............................................ 11
  2.4 Propositional proof system ................................. 13
  2.5 First order proof system ................................... 13

3 Tools 14
  3.1 (Ana)Tempura ................................................ 14
  3.2 FLCheck: Fusion Logic decision Procedure .................. 21
  3.3 ITL library for Isabelle/HOL ................................ 23
  3.4 ITL Theorem Prover based on Prover9 ......................... 24
  3.5 ITL Proof Checker based on PVS ............................ 25
  3.6 Automatic Verification of Interval Temporal Logic ....... 25

4 ITL Related Publications 26
  4.1 Articles ....................................................... 26
  4.2 In Collections ................................................ 30
  4.3 Conference Papers ............................................. 32
  4.4 Books .......................................................... 40
  4.5 Theses .......................................................... 41
  4.6 Technical Reports ............................................. 42
Table 1: Syntax of finite ITL

### Integer Expressions
\[ ie ::= z | A | ig(ie_1, \ldots, ie_n) | \circ A | fin A \]

### Boolean Expressions
\[ be ::= b | Q | bg(be_1, \ldots, be_n) | \circ Q | fin Q \]

### Formulae
\[ f ::= true | h(e_1, \ldots, e_n) | \neg f | f_1 \land f_2 | \forall V \cdot f | fin f_1 ; f_2 | f^* \]

## 1 Finite Interval Temporal Logic

The key notion of ITL is an interval. An interval \( \sigma \) is considered to be a finite sequence of states \( \sigma_0 \ldots \sigma_k \).

### 1.1 Syntax

The syntax of finite ITL is defined in Table 1 where
- \( z \) denotes an integer value,
- \( A \) denotes a state integer variable,
- \( b \) denotes a Boolean value,
- \( Q \) denotes a state propositional variable,
- \( ig \) denotes an integer function symbol,
- \( bg \) denotes a Boolean function symbol,
- \( V \) denotes state (integer or Boolean) variable,
- \( e_i \) denotes a Boolean or integer expression,
- \( h \) denotes a predicate symbol.

### 1.2 Semantics

Each state \( \sigma_i \) is the union of the mapping from the set of integer variables \( \text{IntVar} \) to the set of integer values \( \mathbb{Z} \) and the mapping from propositional variables \( \text{PropVar} \) to the set of Boolean values \{\texttt{tt}, \texttt{ff}\}.

Each interval has at least one state. The length \( |\sigma| \) of an interval \( \sigma_0 \ldots \sigma_n \) is equal to \( n \), one less than the number of states in the interval (this has always been a convention in ITL), i.e., a one state interval has length 0. Let \( \sigma = \sigma_0 \sigma_1 \sigma_2 \ldots \) be an interval then

- \( \sigma_0 \ldots \sigma_k \) (where \( 0 \leq k \leq |\sigma| \)) denotes a prefix interval of \( \sigma \)
- \( \sigma_k \ldots \sigma_{|\sigma|} \) (where \( 0 \leq k \leq |\sigma| \)) denotes a suffix interval of \( \sigma \)
- \( \sigma_k \ldots \sigma_l \) (where \( 0 \leq k \leq l \leq |\sigma| \)) denotes a sub interval of \( \sigma \)

The informal semantics of the most interesting constructs are as follows:

- \( \circ A \): if the interval is non-empty then the value of \( A \) in the next state of that interval else an arbitrary value.
- \( \text{fin } A \): the value of \( A \) in the last state of the interval.
- \( \text{skip} \): unit interval (length 1).
- \( f_1 ; f_2 \): holds if the interval can be decomposed ("chopped") into a prefix and suffix interval, such that \( f_1 \) holds over the prefix interval and \( f_2 \) over the suffix interval.
Table 2: Semantics of finite ITL

<table>
<thead>
<tr>
<th>Formula</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>( E<a href="%5Csigma">z</a> )</td>
<td>( z )</td>
</tr>
<tr>
<td>( E<a href="%5Csigma">A</a> )</td>
<td>( \sigma_0(A) )</td>
</tr>
<tr>
<td>( E<a href="%5Csigma">ie_1, \ldots, ie_n</a> )</td>
<td>( \sigma_1(A) ) if (</td>
</tr>
<tr>
<td>( E<a href="%5Csigma">\bigcirc A</a> )</td>
<td>( \sigma_0(Q) )</td>
</tr>
<tr>
<td>( E<a href="%5Csigma">\text{fin } A</a> )</td>
<td>( \sigma_1(Q) ) if (</td>
</tr>
<tr>
<td>( E<a href="%5Csigma">\text{true}</a> )</td>
<td>( \sigma_{</td>
</tr>
</tbody>
</table>
| \( E[h(e_1, \ldots, e_n)](\sigma) \) | \( \text{tt} \) or \( \text{ff} \) if \( h(E[e_1](\sigma), \ldots, E[e_n](\sigma)) \)
| \( E[f](\sigma) \) | \( \text{tt} \) if \( f(\sigma) = \text{tt} \) otherwise not \( (M[f](\sigma) = \text{tt}) \) |
| \( E[f_1 \land f_2](\sigma) \) | \( \text{tt} \) if \( (M[f_1](\sigma) = \text{tt}) \) and \( (M[f_2](\sigma) = \text{tt}) \) |
| \( E[\text{skip}](\sigma) \) | \( \text{tt} \) if \( |\sigma| = 1 \) |
| \( E[\forall V \Phi \land f](\sigma) \) | \( \text{tt} \) if \( (\text{for all } \sigma' \text{ s.t. } \sigma \sim_{\Phi} \sigma', M[f](\sigma') = \text{tt}) \) |
| \( E[f_1 ; f_2](\sigma) \) | \( \text{tt} \) if \( (\text{exists } k, \text{ s.t. } M[f_1](\sigma_0 \ldots \sigma_k) = \text{tt} \text{ and } M[f_2](\sigma_k \ldots \sigma_{|\sigma|}) = \text{tt}) \) |
| \( E[f^*](\sigma) \) | \( \text{tt} \) if \( (\text{exists } l_0, \ldots, l_n \text{ s.t. } l_0 = 0 \text{ and } l_n = |\sigma| \text{ and for all } 0 \leq i < n, l_i < l_{i+1} \text{ and } M[f](\sigma_i \ldots \sigma_{l_{i+1}}) = \text{tt}) \) |

- \( f^* \) holds if the interval is decomposable into a finite number of intervals such that for each of them \( f \) holds.

Let \( \Sigma^+ \) denote the set of all finite intervals.
Let Expressions denote the set of (integer or Boolean) expressions.
Let Val denote the set of integer or Boolean values (\( \mathbb{Z} \cup \text{bool} \)).
Let \( E[\ldots](\ ) \) denote the meaning function from Formulae \( \times \Sigma^+ \) to Val.
Let Formulae denote the set of ITL formulae.
Let \( M[\ldots](\ ) \) denote the meaning function from Formulae \( \times \Sigma^+ \) to \( \text{bool} \) (set of Boolean values, \{tt, ff\}).
Let \( \sigma = \sigma_0 \sigma_1 \ldots \) denote an interval.
We write \( \sigma \sim_{\Psi} \sigma' \) if the intervals \( \sigma \) and \( \sigma' \) are identical with the possible exception of their mappings for the variable \( V \).
Let choose-any-from(Val) denote the choice function that selects an arbitrary value from Val.
The formal semantics is listed in Table 2.
1.3 Derived Constructs

Frequently used derived constructs are listed in Table 3–6.

Table 3: Frequently used non-temporal derived constructs

<table>
<thead>
<tr>
<th>Construct</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>false (\triangleq \neg\text{true})</td>
<td>false value</td>
</tr>
<tr>
<td>(f_1 \lor f_2) (\triangleq \neg(\neg f_1 \land \neg f_2))</td>
<td>or</td>
</tr>
<tr>
<td>(f_1 \supset f_2) (\triangleq \neg f_1 \lor f_2)</td>
<td>implies</td>
</tr>
<tr>
<td>(f_1 \equiv f_2) (\triangleq (f_1 \supset f_2) \land (f_2 \supset f_1))</td>
<td>equivalent</td>
</tr>
<tr>
<td>(\exists V \bullet f) (\triangleq \neg \forall V \bullet \neg f)</td>
<td>exists</td>
</tr>
</tbody>
</table>

Table 4: Frequently used temporal derived constructs

<table>
<thead>
<tr>
<th>Construct</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>(\bigcirc f) (\triangleq \text{skip} ; f)</td>
<td>next</td>
</tr>
<tr>
<td>more (\triangleq \bigcirc \text{true})</td>
<td>non-empty interval</td>
</tr>
<tr>
<td>empty (\triangleq \neg\text{more})</td>
<td>empty interval</td>
</tr>
<tr>
<td>(\diamond f) (\triangleq \text{true} ; f)</td>
<td>sometimes</td>
</tr>
<tr>
<td>(\square f) (\triangleq \neg\diamond \neg f)</td>
<td>always</td>
</tr>
<tr>
<td>(\bigotimes f) (\triangleq \neg\bigcirc \neg f)</td>
<td>weak next</td>
</tr>
<tr>
<td>(\diamond f) (\triangleq f ; \text{true})</td>
<td>some initial subinterval</td>
</tr>
<tr>
<td>(\boxdot f) (\triangleq \neg(\diamond \neg f))</td>
<td>all initial subintervals</td>
</tr>
<tr>
<td>(\diamond f) (\triangleq \text{true} ; f ; \text{true})</td>
<td>some subinterval</td>
</tr>
<tr>
<td>(\boxdot f) (\triangleq \neg(\diamond \neg f))</td>
<td>all subintervals</td>
</tr>
<tr>
<td>(\text{empty} \lor (\boxdot (f) ; \text{skip}))</td>
<td>all strict initial intervals</td>
</tr>
<tr>
<td>(\bigotimes (f)) (\triangleq \neg(\boxdot \neg f)))</td>
<td>some strict initial interval</td>
</tr>
<tr>
<td>(\bigtriangledown (f)) (\triangleq f \land \boxdot \neg f)</td>
<td>first occurrence</td>
</tr>
</tbody>
</table>
Table 5: Frequently used concrete derived constructs

<table>
<thead>
<tr>
<th>Construct</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>if then else</td>
<td>if ( f_0 ) then ( f_1 ) else ( f_2 ) \iff ( (f_0 \land f_1) \lor (\neg f_0 \land f_2) ) if then else</td>
</tr>
<tr>
<td>if then</td>
<td>if ( f_0 ) then ( f_1 ) \iff if ( f_0 ) then ( f_1 ) else true if then</td>
</tr>
<tr>
<td>fin ( f )</td>
<td>( \square (\text{empty} \supset f) ) final state</td>
</tr>
<tr>
<td>halt ( f )</td>
<td>( \square (\text{empty} \equiv f) ) terminate interval when</td>
</tr>
<tr>
<td>keep ( f )</td>
<td>( \Box (\text{skip} \supset f) ) all unit subintervals</td>
</tr>
<tr>
<td>keepnow ( f )</td>
<td>( \Diamond (\text{skip} \land f) ) initial unit subinterval</td>
</tr>
<tr>
<td>while ( f_0 ) do ( f_1 )</td>
<td>( (f_0 \land f_1)^* \land \text{fin} \neg f_0 ) while loop</td>
</tr>
<tr>
<td>repeat ( f_0 ) until ( f_1 )</td>
<td>( f_0 : (\text{while} \neg f_1 \text{ do } f_0) ) repeat loop</td>
</tr>
<tr>
<td>( f_1 \mapsto f_0 )</td>
<td>( \Box (f_1 \supset \text{fin} f_0) ) always followed by</td>
</tr>
<tr>
<td>( f_1 \leftrightarrow f_0 )</td>
<td>( \Box (f_1 \equiv \text{fin} f_0) ) strong followed by</td>
</tr>
</tbody>
</table>

Table 6: Frequently used derived constructs related to expressions

<table>
<thead>
<tr>
<th>Construct</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>( Y := e )</td>
<td>( (\Diamond Y) = e ) assignment</td>
</tr>
<tr>
<td>( Y \approx e )</td>
<td>( \Box (Y = e) ) equal in interval</td>
</tr>
<tr>
<td>( Y \leftarrow e )</td>
<td>( (\text{fin } Y) = e ) temporal assignment</td>
</tr>
<tr>
<td>( Y \text{ gets } e )</td>
<td>( \text{keep } (Y \leftarrow e) ) gets</td>
</tr>
<tr>
<td>stable ( Y )</td>
<td>( Y \text{ gets } Y ) stability</td>
</tr>
<tr>
<td>padded ( Y )</td>
<td>( (\text{stable } Y) ; \text{skip} \lor \text{empty} ) padded expression</td>
</tr>
<tr>
<td>( Y \lessdot e )</td>
<td>( (Y \leftarrow e) \land \text{padded } Y ) padded temporal assignment</td>
</tr>
<tr>
<td>intlen ( e )</td>
<td>( \exists I \cdot (I = 0) \land (I \text{ gets } I + 1) \land (I \leftarrow e) ) interval length</td>
</tr>
</tbody>
</table>
1.4 Propositional proof system

In Table 7 we list the propositional axioms and rules for finite ITL.

<table>
<thead>
<tr>
<th>Propositional Axioms and Rules for finite ITL</th>
</tr>
</thead>
<tbody>
<tr>
<td>ChopAssoc</td>
</tr>
<tr>
<td>⊢ (f₀ ; f₁) ; f₂ ≡ f₀ ; (f₁ ; f₂)</td>
</tr>
<tr>
<td>OrChopImp</td>
</tr>
<tr>
<td>⊢ (f₀ ∨ f₁) ; f₂ ⊃ (f₀ ; f₂) ∨ (f₁ ; f₂)</td>
</tr>
<tr>
<td>ChopOrImp</td>
</tr>
<tr>
<td>⊢ f₀ ; (f₁ ∨ f₂) ⊃ (f₀ ; f₁) ∨ (f₀ ; f₂)</td>
</tr>
<tr>
<td>EmptyChop</td>
</tr>
<tr>
<td>⊢ empty ; f ≡ f</td>
</tr>
<tr>
<td>ChopEmpty</td>
</tr>
<tr>
<td>⊢ f ; empty ≡ f</td>
</tr>
<tr>
<td>BiBoxChopImpChop</td>
</tr>
<tr>
<td>⊢ □(f₀ ⊃ f₁) ∧ □(f₂ ⊃ f₃) ⊃ (f₀ ; f₂) ⊃ (f₁ ; f₃)</td>
</tr>
<tr>
<td>StateImpBi</td>
</tr>
<tr>
<td>⊢ w ⊃ □ w</td>
</tr>
<tr>
<td>NextImpNotNextNot</td>
</tr>
<tr>
<td>⊢ ⊗ f ⊃ ¬ ⊗ ¬ f</td>
</tr>
<tr>
<td>BoxInduct</td>
</tr>
<tr>
<td>⊢ f ∧ □(f ⊃ □ f) ⊃ □ f</td>
</tr>
<tr>
<td>ChopStarEqv</td>
</tr>
<tr>
<td>⊢ f* ≡ (empty ∨ ((f ∧ more) ; f*))</td>
</tr>
<tr>
<td>MP</td>
</tr>
<tr>
<td>⊢ f₀ ⊃ f₁, ⊢ f₀ ⇒ ⊢ f₁</td>
</tr>
<tr>
<td>BoxGen</td>
</tr>
<tr>
<td>⊢ f₀ ⇒ ⊢ □ f₀</td>
</tr>
<tr>
<td>BiGen</td>
</tr>
<tr>
<td>⊢ f₀ ⇒ ⊢ □ f₀</td>
</tr>
</tbody>
</table>

1.5 First order proof system

Some axioms for the first order case are shown in Table 8.

Let \( V \) denote a state variable.

We denote by \( f [e / V] \) that in formula \( f \) expression \( e \) is substituted for variable \( V \).

<table>
<thead>
<tr>
<th>Some First Order Axioms and Rules for finite ITL</th>
</tr>
</thead>
<tbody>
<tr>
<td>ForallSub</td>
</tr>
<tr>
<td>⊢ ∀V · f ⊃ f [e / V],</td>
</tr>
<tr>
<td>where the expression ( e ) has the same data</td>
</tr>
<tr>
<td>and temporal type as the variable ( V ) and</td>
</tr>
<tr>
<td>is free for ( V ) in ( f ).</td>
</tr>
<tr>
<td>ForallImplies</td>
</tr>
<tr>
<td>⊢ ∀V · (f₁ ⊃ f₂) ⊃ (f₁ ⊃ ∀V · f₂),</td>
</tr>
<tr>
<td>where ( V ) doesn’t occur freely in ( f₁ ).</td>
</tr>
<tr>
<td>SubstAxiom</td>
</tr>
<tr>
<td>⊢ □(V₁ = V₂) ⊃ f ≡ f [V₂ / V₁].</td>
</tr>
<tr>
<td>ExistsChopRight</td>
</tr>
<tr>
<td>⊢ ∃V · (f₁ ; f₂) ⊃ (∃V · f₁) ; f₂,</td>
</tr>
<tr>
<td>where ( V ) doesn’t occur freely in ( f₂ ).</td>
</tr>
<tr>
<td>ExistsChopLeft</td>
</tr>
<tr>
<td>⊢ ∃V · (f₁ ; f₂) ⊃ f₁ ; (∃V · f₂),</td>
</tr>
<tr>
<td>where ( V ) doesn’t occur freely in ( f₁ ).</td>
</tr>
<tr>
<td>ForallGen</td>
</tr>
<tr>
<td>⊢ f ⇒ ⊢ ∀V · f,</td>
</tr>
<tr>
<td>for any variable ( V ).</td>
</tr>
</tbody>
</table>
Table 9: Syntax of finite and infinite ITL

### Expressions
\[ ie ::= z \mid A \mid ig(ie_1, \ldots, ie_n) \mid \Box A \mid fin A \]

### Boolean Expressions
\[ be ::= b \mid Q \mid bg(be_1, \ldots, be_n) \mid \Box Q \mid fin Q \]

### Formulae
\[ f ::= \text{true} \mid h(e_1, \ldots, e_n) \mid \neg f \mid f_1 \land f_2 \mid \forall V \cdot f \mid \text{skip} \mid f_1 ; f_2 \mid f^* \]

## 2 Finite and Infinite Interval Temporal Logic

The key notion of ITL is an interval. An interval \( \sigma \) is considered to be a (in)finite sequence of states \( \sigma_0 \sigma_1 \ldots \).

### 2.1 Syntax

The syntax of ITL is defined in Table 9 where:
- \( z \) denotes an integer value,
- \( A \) denotes a state integer variable,
- \( b \) denotes a Boolean value,
- \( Q \) denotes a state propositional variable,
- \( ig \) denotes an integer function symbol,
- \( bg \) denotes a Boolean function symbol,
- \( V \) denotes state integer variable,
- \( e_i \) denotes a Boolean or integer expression,
- \( h \) denotes a predicate symbol.

### 2.2 Semantics

Each state \( \sigma_i \) is the union of the mapping from the set of integer variables IntVar to the set of integer values \( \mathbb{Z} \) and the mapping from propositional variables PropVar to set of Boolean values \( \{tt, ff\} \).

Each interval has at least one state. The length \( |\sigma| \) of an interval \( \sigma_0 \ldots \sigma_n \) is equal to \( n \), one less than the number of states in the interval (this has always been a convention in ITL), i.e., a one state interval has length 0. Let \( \sigma = \sigma_0 \sigma_1 \sigma_2 \ldots \) be an interval then

- \( \sigma_0 \ldots \sigma_k \) (where \( 0 \leq k \leq |\sigma| \)) denotes a prefix interval of \( \sigma \)
- \( \sigma_k \ldots \sigma_{|\sigma|} \) (where \( 0 \leq k \leq |\sigma| \)) denotes a suffix interval of \( \sigma \)
- \( \sigma_k \ldots \sigma_l \) (where \( 0 \leq k \leq l \leq |\sigma| \)) denotes a sub interval of \( \sigma \)

The informal semantics of the most interesting constructs are as follows:

- \( \Box A \): if interval is non-empty then the value of \( A \) in the next state of that interval else an arbitrary value.
- \( \text{fin } A \): if interval is finite then the value of \( A \) in the last state of that interval else an arbitrary value.
- \( \text{skip} \): unit interval (length 1).
• $f_1 \cdot f_2$ holds if the interval can be decomposed ("chopped") into a prefix and suffix interval, such that $f_1$ holds over the prefix and $f_2$ over the suffix, or if the interval is infinite and $f_1$ holds for that interval.

• $f^*$ holds if the interval is decomposable into a finite number of intervals such that for each of them $f$ holds, or the interval is infinite and can be decomposed into an infinite number of finite intervals for which $f$ holds.

Let $\Sigma^+$ denote the set of all finite intervals and $\Sigma^\omega$ denotes the set of all infinite intervals.
Let Expressions denote the set of (integer or Boolean) expressions.
Let Val denote the set of integer or Boolean values ($\mathbb{Z} \cup \text{Bool}$).
Let $E[\ldots](\ )$ denote the meaning function from Expressions $\times (\Sigma^+ \cup \Sigma^\omega)$ to Val.
Let Formulae denote the set of ITL formulae.
Let $M[\ldots](\ )$ denote the meaning function from Formulae $\times (\Sigma^+ \cup \Sigma^\omega)$ to Bool (set of Boolean values, \{tt, ff\}).
Let $\sigma = \sigma_0\sigma_1\ldots$ denote an interval.
We write $\sigma \sim_V \sigma'$ if the intervals $\sigma$ and $\sigma'$ are identical with the possible exception of their mappings for the variable $V$.
Let choose-any-from(Val) denote the choice function that selects an arbitrary value from Val.
The formal semantics is listed in Table 10:
Table 10: Semantics of finite and infinite ITL

<table>
<thead>
<tr>
<th>Expression</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>$E<a href="%5Csigma">z</a>$</td>
<td>$z$</td>
</tr>
<tr>
<td>$E<a href="%5Csigma">A</a>$</td>
<td>$\sigma_0(A)$</td>
</tr>
<tr>
<td>$E<a href="%5Csigma">\text{ig}(i e_1, \ldots, i e_n)</a>$</td>
<td>$\text{ig}(E<a href="%5Csigma">i e_1</a>, \ldots, E<a href="%5Csigma">i e_n</a>)$</td>
</tr>
<tr>
<td>$E<a href="%5Csigma">\circ A</a>$</td>
<td>$\sigma_1(A)$ if $</td>
</tr>
<tr>
<td>$E<a href="%5Csigma">\text{fin } A</a>$</td>
<td>$\sigma_{</td>
</tr>
<tr>
<td>$E<a href="%5Csigma">b</a>$</td>
<td>$b$</td>
</tr>
<tr>
<td>$E<a href="%5Csigma">Q</a>$</td>
<td>$\sigma_0(Q)$</td>
</tr>
<tr>
<td>$E<a href="%5Csigma">\text{bg}(b e_1, \ldots, b e_n)</a>$</td>
<td>$\text{bg}(E<a href="%5Csigma">b e_1</a>, \ldots, E<a href="%5Csigma">b e_n</a>)$</td>
</tr>
<tr>
<td>$E<a href="%5Csigma">\circ Q</a>$</td>
<td>$\sigma_1(Q)$ if $</td>
</tr>
<tr>
<td>$E<a href="%5Csigma">\text{fin } Q</a>$</td>
<td>$\sigma_{</td>
</tr>
<tr>
<td>$M<a href="%5Csigma">\text{true}</a>$</td>
<td>$\text{tt}$</td>
</tr>
<tr>
<td>$M<a href="%5Csigma">h(e_1, \ldots, e_n)</a>$</td>
<td>$\text{tt}$ if $h(E<a href="%5Csigma">e_1</a>, \ldots, E<a href="%5Csigma">e_n</a>)$</td>
</tr>
<tr>
<td>$M<a href="%5Csigma">\neg f</a>$</td>
<td>$\text{tt}$ if $\neg (M<a href="%5Csigma">f</a> = \text{tt})$</td>
</tr>
<tr>
<td>$M<a href="%5Csigma">f_1 \land f_2</a>$</td>
<td>$\text{tt}$ if $(M<a href="%5Csigma">f_1</a> = \text{tt})$ and $(M<a href="%5Csigma">f_2</a> = \text{tt})$</td>
</tr>
<tr>
<td>$M<a href="%5Csigma">\text{skip}</a>$</td>
<td>$\text{tt}$ if $</td>
</tr>
<tr>
<td>$M<a href="%5Csigma">\text{V } f</a>$</td>
<td>$\text{tt}$ if $(\text{for all } \sigma' \text{ s.t. } \sigma \land \sigma', M<a href="%5Csigma'">f</a> = \text{tt})$</td>
</tr>
<tr>
<td>$M<a href="%5Csigma">f_1 : f_2</a>$</td>
<td>$\text{tt}$ if $(\text{exists } k \text{ s.t. } M[f_1](\sigma_0 \ldots \sigma_k) = \text{tt} \text{ and } M[f_2](\sigma_k \ldots \sigma_{</td>
</tr>
<tr>
<td>$M<a href="%5Csigma">f^*</a>$</td>
<td>$\text{tt}$ if $\sigma$ is finite then $(\text{exist } l_0, \ldots, l_n \text{ s.t. } l_0 = 0 \text{ and } l_n =</td>
</tr>
</tbody>
</table>
2.3 Derived Constructs

Frequently used derived constructs are listed in Table 11–14.

Table 11: Frequently used non-temporal derived constructs

<table>
<thead>
<tr>
<th>Construct</th>
<th>Definition</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>false</td>
<td>$\triangleq \neg \text{true}$</td>
<td>false value</td>
</tr>
<tr>
<td>$f_1 \lor f_2$</td>
<td>$\triangleq \neg(\neg f_1 \land \neg f_2)$</td>
<td>or</td>
</tr>
<tr>
<td>$f_1 \supset f_2$</td>
<td>$\triangleq \neg f_1 \lor f_2$</td>
<td>implies</td>
</tr>
<tr>
<td>$f_1 \equiv f_2$</td>
<td>$\triangleq (f_1 \supset f_2) \land (f_2 \supset f_1)$</td>
<td>equivalent</td>
</tr>
<tr>
<td>$\exists V \cdot f$</td>
<td>$\triangleq \neg \forall V \cdot \neg f$</td>
<td>exists</td>
</tr>
</tbody>
</table>

Table 12: Frequently used temporal derived constructs

<table>
<thead>
<tr>
<th>Construct</th>
<th>Definition</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\bigcirc f$</td>
<td>$\triangleq \text{skip} ; ; f$</td>
<td>next</td>
</tr>
<tr>
<td>more</td>
<td>$\triangleq \bigcirc \text{true}$</td>
<td>non-empty interval</td>
</tr>
<tr>
<td>empty</td>
<td>$\triangleq \neg \text{more}$</td>
<td>empty interval</td>
</tr>
<tr>
<td>inf</td>
<td>$\triangleq \text{true} ; ; \text{false}$</td>
<td>infinite interval</td>
</tr>
<tr>
<td>$\text{isinf}(f)$</td>
<td>$\triangleq \text{inf} \land f$</td>
<td>is infinite</td>
</tr>
<tr>
<td>finite</td>
<td>$\triangleq \neg \text{inf}$</td>
<td>finite interval</td>
</tr>
<tr>
<td>$\text{isfin}(f)$</td>
<td>$\triangleq \text{finite} \land f$</td>
<td>is finite</td>
</tr>
<tr>
<td>fmore</td>
<td>$\triangleq \text{more} \land \text{finite}$</td>
<td>non-empty finite interval</td>
</tr>
<tr>
<td>$\Diamond f$</td>
<td>$\triangleq \text{finite} ; ; f$</td>
<td>sometimes</td>
</tr>
<tr>
<td>$\Box f$</td>
<td>$\triangleq \neg \Diamond \neg f$</td>
<td>always</td>
</tr>
<tr>
<td>$\Diamond f$</td>
<td>$\triangleq \neg \bigcirc \neg f$</td>
<td>weak next</td>
</tr>
<tr>
<td>$\Diamond f$</td>
<td>$\triangleq f ; ; \text{true}$</td>
<td>some initial subinterval</td>
</tr>
<tr>
<td>$\Box f$</td>
<td>$\triangleq \neg(\Diamond \neg f)$</td>
<td>all initial subintervals</td>
</tr>
<tr>
<td>$\Diamond f$</td>
<td>$\triangleq \text{finite} ; ; f ; ; \text{true}$</td>
<td>some subinterval</td>
</tr>
<tr>
<td>$\Box f$</td>
<td>$\triangleq \neg(\Diamond \neg f)$</td>
<td>all subintervals</td>
</tr>
</tbody>
</table>
Table 13: Frequently used concrete derived constructs

<table>
<thead>
<tr>
<th>Construct</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{if } f_0 \text{ then } f_1 \text{ else } f_2$</td>
<td>$\triangleq (f_0 \land f_1) \lor (\neg f_0 \land f_2)$</td>
</tr>
<tr>
<td>$\text{if } f_0 \text{ then } f_1$</td>
<td>$\triangleq \text{if } f_0 \text{ then } f_1 \text{ else true}$</td>
</tr>
<tr>
<td>$\text{fin } f$</td>
<td>$\triangleq \Box (\text{empty} \supset f)$</td>
</tr>
<tr>
<td>$\text{sfin } f$</td>
<td>$\triangleq \neg (\text{fin } (\neg f))$</td>
</tr>
<tr>
<td>$\text{halt } f$</td>
<td>$\triangleq \Box (\text{empty} \equiv f)$</td>
</tr>
<tr>
<td>$\text{shalt } f$</td>
<td>$\triangleq \neg (\text{halt } (\neg f))$</td>
</tr>
<tr>
<td>$\text{keep } f$</td>
<td>$\triangleq \Box (\text{skip} \supset f)$</td>
</tr>
<tr>
<td>$f^\omega$</td>
<td>$\triangleq \text{isinf } (\text{isfin } (f)^*)$</td>
</tr>
<tr>
<td>$f^\ast$</td>
<td>$\triangleq \text{isfin } (\text{isfin } (f)^*) \lor$</td>
</tr>
<tr>
<td>$\text{while } f_0 \text{ do } f_1$</td>
<td>$\triangleq (f_0 \land f_1)^* \land \text{fin } \neg f_0$</td>
</tr>
<tr>
<td>$\text{repeat } f_0 \text{ until } f_1$</td>
<td>$\triangleq f_0 ; (\text{while } \neg f_1 \text{ do } f_0)$</td>
</tr>
</tbody>
</table>

Table 14: Frequently used derived constructs related to expressions

<table>
<thead>
<tr>
<th>Construct</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>$Y := e$</td>
<td>$\triangleq (\Box Y) = e$</td>
</tr>
<tr>
<td>$Y \approx e$</td>
<td>$\triangleq \Box (Y = e)$</td>
</tr>
<tr>
<td>$Y \leftarrow e$</td>
<td>$\triangleq \text{finite } \land (\text{fin } Y) = e$</td>
</tr>
<tr>
<td>$Y \text{ gets } e$</td>
<td>$\triangleq \text{keep } (Y \leftarrow e)$</td>
</tr>
<tr>
<td>$Y \text{ stable}$</td>
<td>$\triangleq Y \text{ gets } Y$</td>
</tr>
<tr>
<td>$Y \text{ padded}$</td>
<td>$\triangleq (\text{stable } (Y) ; \text{skip}) \lor \text{empty}$</td>
</tr>
<tr>
<td>$Y \approx e$</td>
<td>$\triangleq (Y \leftarrow e) \land \text{padded } Y$</td>
</tr>
<tr>
<td>$\text{intlen } (e)$</td>
<td>$\triangleq \exists I \cdot (I = 0) \land (I \text{ gets } I + 1) \land (I \leftarrow e)$</td>
</tr>
</tbody>
</table>

12
2.4 Propositional proof system

In Table 15 we list the propositional axioms and rules for finite and infinite ITL.

Table 15: Propositional Axioms and Rules for finite and infinite ITL.

<table>
<thead>
<tr>
<th>Rule</th>
<th>Formula</th>
</tr>
</thead>
<tbody>
<tr>
<td>ChopAssoc</td>
<td>( \vdash (f_0 ; f_1) ; f_2 \equiv f_0 ; (f_1 ; f_2) )</td>
</tr>
<tr>
<td>OrChopImp</td>
<td>( \vdash (f_0 \lor f_1) ; f_2 \lor (f_0 ; f_2) \lor (f_1 ; f_2) )</td>
</tr>
<tr>
<td>ChopOrImp</td>
<td>( \vdash f_0 ; (f_1 \lor f_2) \lor (f_0 ; f_1) \lor (f_0 ; f_2) )</td>
</tr>
<tr>
<td>EmptyChop</td>
<td>( \vdash \text{empty} ; f \equiv f )</td>
</tr>
<tr>
<td>ChopEmpty</td>
<td>( \vdash f ; \text{empty} \equiv f )</td>
</tr>
<tr>
<td>BiBoxChopImpChop</td>
<td>( \vdash \Box(f_0 \lor f_1) \land \Box(f_2 \lor f_3) \lor (f_0 ; f_2) \lor (f_1 ; f_3) )</td>
</tr>
<tr>
<td>StateImpBi</td>
<td>( \vdash w \lor \Box w )</td>
</tr>
<tr>
<td>NextImpNotNextNot</td>
<td>( \vdash \Diamond f \lor \neg \Diamond \neg f )</td>
</tr>
<tr>
<td>BoxInduct</td>
<td>( \vdash f \land \Box(f \lor \Box f) \lor \Box f )</td>
</tr>
<tr>
<td>InfChop</td>
<td>( \vdash (f \land \inf) ; g \equiv (f \land \inf) )</td>
</tr>
<tr>
<td>ChopStarEqv</td>
<td>( \vdash f^* \equiv (\text{empty} \lor ((f \land \more) ; f^*)) )</td>
</tr>
<tr>
<td>ChopstarInduct</td>
<td>( \vdash (\inf \land f \land \Box(f \lor (g \land \more) ; f)) \lor g^* )</td>
</tr>
<tr>
<td>MP</td>
<td>( \vdash f_0 \lor f_1, \vdash f_0 \Rightarrow \vdash f_1 )</td>
</tr>
<tr>
<td>BoxGen</td>
<td>( \vdash f_0 \Rightarrow \vdash \Box f_0 )</td>
</tr>
<tr>
<td>BiGen</td>
<td>( \vdash f_0 \Rightarrow \vdash \Box f_0 )</td>
</tr>
</tbody>
</table>

2.5 First order proof system

Some axioms for the first order case are shown in Table 16. Let \( V \) denote a state variable.

We denote by \( f[e / V] \) that in formula \( f \) expression \( e \) is substituted for variable \( V \).

Table 16: Some First Order Axioms and Rules for ITL.

<table>
<thead>
<tr>
<th>Rule</th>
<th>Formula</th>
</tr>
</thead>
<tbody>
<tr>
<td>ForallSub</td>
<td>( \vdash \forall V \cdot f \lor f[e / V] ), where the expression ( e ) has the same data and temporal type as the variable ( V ) and is free for ( V ) in ( f ).</td>
</tr>
<tr>
<td>ForallImplies</td>
<td>( \vdash \forall V \cdot (f_1 \lor f_2) \lor (f_1 \lor \forall V \cdot f_2) ), where ( V ) doesn’t occur freely in ( f_1 ).</td>
</tr>
<tr>
<td>SubstAxiom</td>
<td>( \vdash \Box(V_1 = V_2) \lor f \equiv f[V_1 / V_2] ).</td>
</tr>
<tr>
<td>ExistsChopRight</td>
<td>( \vdash \exists V \cdot (f_1 ; f_2) \lor (\exists V \cdot f_1) ; f_2 ), where ( V ) doesn’t occur freely in ( f_2 ).</td>
</tr>
<tr>
<td>ExistsChopLeft</td>
<td>( \vdash \exists V \cdot (f_1 ; f_2) \lor f_1 ; (\exists V \cdot f_2) ), where ( V ) doesn’t occur freely in ( f_1 ).</td>
</tr>
<tr>
<td>ForallGen</td>
<td>( \vdash f \Rightarrow \vdash \forall V \cdot f ), for any variable ( V ).</td>
</tr>
</tbody>
</table>
3 Tools

3.1 (Ana)Tempura

Tempura, the C-Tempura interpreter version 2.7 developed originally by Roger Hale and now maintained by Antonio Cau and Ben Moszkowski, is an interpreter for executable Interval Temporal Logic formulae. The first Tempura interpreter was programmed in Prolog by Ben Moszkowski, and was operational around December 2, 1983. Subsequently he rewrote the interpreter in Lisp (mid Mar, 1984), and in late 1984 modified the program to handle a two-level memory and multi-pass scanning. The C-Tempura interpreter was written in early 1985 by Roger Hale at Cambridge University.

AnaTempura, which is built upon C-Tempura, is a tool for the runtime verification of systems using Interval Temporal Logic (ITL) and its executable subset Tempura. The runtime verification technique uses assertion points to check whether a system satisfies timing, safety or security properties expressed in ITL. The assertion points are inserted in the source code of the system and will generate a sequence of information (system states), like values of variables and timestamps of value change, while the system is running. Since an ITL property corresponds to a set of sequences of states (intervals), runtime verification is just checking whether the sequence generated by the system is a member of the set of sequences corresponding to the property we want to check. The Tempura interpreter is used to do this membership test.

Download Version:

- Version 3.4 (released 19/12/2017) gzipped tar file or zip file.
  - Initial support for monitoring rmi based Java programs.
  - Use internal variable runid to assign id to external processes.
  - Tempura commands stable and output now allows lists of variables, i.e., stable(V,W) and output(V,W).
  - Use kitcreator to generate the anatempura binaries. The windows binaries are generated using the mingw-w64 cross compiler.
  - Various other bug fixes, see ChangeLog for more details.

- Version 3.3 (released 07/06/2016) gzipped tar file or zip file.
  - The Tcl/Tk graphical user interface does not depend on Expect anymore.
  - The lexer/parser now throws an error on encountering a unknown character instead of silently discarding it.
  - The read-only State_number variable can be used in Tempura programs to determine the current state number.
  - The monitoring of C# programs does not need a Java wrapper anymore.
  - Support for monitoring of Java programs in the form of a jar file.
  - Support of time-stamps in the form of seconds and microseconds.
  - The GUI has now a different look/layout, history of commands window is gone, the most commonly used menu entries are now buttons and one interacts with Tempura using a shell-like interface.
  - Added template .anatempurarc .
  - Integers are now 64bits regardless of the machine architecture.
  - Windows binaries are compiled using the msys2-mingw32/64 system.
- For Windows we have 32 bit (XP and beyond) and 64 bit (7 and beyond) Tempura/AnaTempura binaries.
- Random numbers are now generated using xorshift128plus.
- Added support for monitoring Scala programs.
- Added option -stdio to start anatempura in cmdline mode.
- Various other bug fixes, see ChangeLog for more details.

• Version 3.2 (released 30/11/2015) gzipped tar file or zip file.

- Rewritten the Tempura output capture/processing routine.
- Rewritten the external program data capture/processing routine.
- New implementation of memory/framed variables, existsf V : f, is now used to indicate that V is memory/framed variable within f.
  The previous syntax mem(V) is now deprecated.
- Fix bugs in the implementation of prev(L) where L is a list.
- Added Tempura binary for Arduino-Yun and Raspberry Pi, i.e., tempura_mips_openwrt_linux and tempura_arm_linux_gnueabihf.
- Added elapsed time in the statistics output at the end of a run.
- Added plc and sql injection detection examples.
- Various other bug fixes see ChangeLog for more details.

• Version 3.1 (released 22/05/2015) gzipped tar file or zip file.

- Changed contact email address.
- Added pre-compiled MacOSX binary.
- Added frame(V) as alias for mem(V)
- Fixed some bugs in implementation of mem(V).
- Fixed some bugs in the help command.

• Version 3.0 (released 04/07/2013) gzipped tar file or zip file.

- Dropped pre-compiled Solaris binary.
- flex/bison based parser backward compatible with previous hard coded version but with stricter syntactic checks
- changed from cvs to svn as version control system
- improved syntax error messages
- fixed memory leaks
- tidy up format command
- startup file .anatempurname can also be in the current directory
- use kbs-0.4.4 to generate anatempura binaries
- anatempura binaries are using Tcl/Tk 8.6
- works again under Windows XP
- program assertions can have any symbol except control characters and !

• Version 2.18 (released 01/11/2012): gzipped tar file or zip file.
- Dropped tempura_macosx binary but added tempura_linux64 and anatempura_linux64 binaries.
- fixed some small bugs
- fixed memory leaks
- added command ‘winput’ that will wait for input from a file instead of switching to the keyboard.

• Version 2.17 (released 04/10/2011): gzipped tar file or zip file.
- initial support for MACOSX
- fixed gui bugs
- fixed some tempura bugs

• Version 2.16 (released 08/12/2009): gzipped tar file or zip file.
- added floats. Floats have the form $2.3e+10$ in Tempura. For output: output($2.3$) will be $2.3000e+00$, i.e., precision is 5 digits after the ‘.’. One can set this via the precision variable. With precision of 2 one gets $2.30e+00$. The format command can output floats in two forms: %f output will be of the form 2.33333, e output will be of the form 2.33333e+01. The following operations on floats are defined: unary, +, -; binary: +, -, div, mod, /, *, **, ceil, floor, sqrt, itof, exp, log, log10, sin, cos, tan, asin, acos, atan, atan2, sinh, cosh, tanh, fabs.
- anatempura is now using the new Tile interface
- when setting system variables with set, output both old and new values
- Added ’frandom’ and ’fRandom’ for float random number between [0.0,1.0)
- Added defaults command, X defaults 1 denotes when X is undefined then take as value for X the value 1.
- Added prev(X) operator, the value of X in the previous state.
- Added mem(X) operator, X is a ’memory’ variable, i.e., when undefined take the value in the previous state.
- Added #n history operator, used as option to exists when declaring a variable, it will keep a history of n previous values of a variable.
- Added nprev(X,n) operator, nprev(X,3) for instance is an abbreviation of prev(prev(prev(X))).
- When setting debug_level to 6 more useful information is displayed like the state of a variable and reduction rule being applied.
- Included tempura executables tempura_linux for Linux (compiled on Ubuntu 9.10), tempura_solaris for Solaris (compiled on Sparc Solaris 10u8), and tempura.exe for Windows (compiled on Windows XP SP3).
- Included anatempura executables anatempura_solaris, anatempura_linux and anatempura.exe. These were built using the Tclkit Kitgen build system (http://wiki.tcl.tk/18146). Now no need anymore to install tcl/tk and expect in order to run anatempura.
- changed copyright license to GPLv3.0

16

                        2.15******************************************************************************
- introduced various node accessor macros so that if one changes the node
structure we only have to change the macro.
- if formula can’t be reduced in the final state of the
prefix of a chop then we will evaluate ((prefix and empty);true)
and (suffix). This feature can be switched on/off with hopchop.
The default of hopchop is true.
- added integer overflow tests.
- unified/cleaned up the various node data structures.


                        2.14******************************************************************************
- work around a recent misfeature of windows when started an external program.
- added the io redirections, set infile="some file name", set
  outfile="some file name", where stdin and stdout can be used to
  redirect to standard keyboard and screen i/o.
- added the infinite and randlen constructs for respectively an
  infinite interval and a random length interval (less or equal
to max_randlen).


                        2.13******************************************************************************
- added reset in file menu to restart tempura.
- open and reload now also load the file into Tempura.
- added showstate Tempura command. This will display what is
  (un)defined in the current state.
- changed contact email address to tempura@dmu.ac.uk

• Version 2.12 (released 04/05/2007): gzipped tar file or zip file.

                        2.12******************************************************************************
This version is the first version that compiles both under
Windows and Unix/Linux type of machines. See Changelog for detailed
news/changes.

How to run AnaTempura?

• Use the pre-compiled binary:

  anatempura.exe: 32 bit binary and will run on Windows Xp, 7 and beyond, this will use tempura.exe
  in the current directory
  anatempura-win64.exe: 64 bit binary and will run on Windows 7 and beyond, this will use tempura-
  win64.exe in the current directory
  anatempura_linux: For 32bit Linux OS, this will use tempura_linux in the current directory
  anatempura_linux64: For 64bit Linux OS, this will use tempura_linux64 in the current directory
  anatempura_macosx: For MacOSX, this will use tempura_macosx in the current directory
Use anatempura.tcl:

you need to install Tempura, and Tcl/Tk (at least 8.5). Get Tcl/Tk and from Tcl/Tk site or use the ActiveTcl package.

Tempura can be compiled using the Gnu C compiler under a Unix like operating system like Ubuntu, GNU Debian, etc. For Windows you can use the MSYS2/MinGW-32/64 system, see their website for downloading and installation. Install the MSYS2 system, and then, using pacman, install the mingw-w64-i686-toolchain for compiling 32bit binaries and the mingw-w64-x86_64-toolchain for compiling 64bit binaries.

Compile Tempura using the following commands

./configure
make

For convenience the following pre-compiled Tempura binaries are included in the distribution:

32 bit Windows binary tempura.exe,
64 bit Windows binary tempura-win64.exe,
32 bit Linux binary tempura_linux,
64 bit Linux binary tempura_linux64,
MacOSX binary tempura_macosx,
Arduino-Yun binary tempura_mips_openwrt_linux,
Raspberry Pi binary tempura_arm_linux_gnuabihf.

Contact: Email cau.researcher@gmail.com in case of problems.

Publications:

• Analysing C programs is discussed in:

• Analysing Verilog programs is discussed in:

• A paper describing the run-time verification method used in AnaTempura:

• Slides of seminar talk about AnaTempura:

Overview: Figure 1 shows an overview of AnaTempura.
Figure 2 shows the interface of AnaTempura.
Figure 3 shows a graphical snapshot of a simulation of the EP/3 microprocessor specified in Tempura.
Figure 1: Overview of AnaTempura

Figure 2: Interface of AnaTempura
Figure 3: Graphical snapshot of simulation of the EP/3 microprocessor
3.2 FLCheck: Fusion Logic decision Procedure

Fusion Logic augments conventional Propositional Temporal Logic (PTL) with the fusion operator. Note: the fusion-operator is basically a “chop” that does not have an explicit negation on the left hand (for right fusion logic) side (as fusion expression) or the right hand (for left fusion logic). The negation is implicit, i.e., the negation is a derived fusion expression operator. The expressiveness of Fusion Logic is the same as Propositional Interval Temporal Logic. The main differences concern computational complexity, naturalness of expression for analytical purposes, and succinctness. Fusion Logic is closely related to Propositional Dynamic Logic (PDL).

We have implemented above decision procedure for Fusion Logic in Tcl/Tk and the CUDD BDD library. The tool allows one to check the validity or satisfiability of a Fusion Logic formula. If a formula is not valid it will produce a counter example and if a formula is satisfiable it will produce an example model. Figure 4 gives a screen dump of our tool which is available at

- FLCHECK version 1.2 (released 22/05/2015).
  Main Changes:
  - Added support for MacOSX.
  - Added pre-compiled binary for MacOSX.
- FLCHECK version 1.1 (released 04/07/2013).
  Main Changes:
  - Drop support for Solaris Sparc.
  - Added pre-compiled binaries for Windows (XP and 7) and Linux (Ubuntu 12.04, 32 and 64 bits).
- FLCHECK version 1.0 (released 23/01/2013).
  Main Changes:
  - Simplified ‘left always followed by’ operator.
  - Added more examples.
- FLCHECK version 0.9 (released 21/02/2012).
  Main Changes:
  - Introduction of left and right Fusion Logic which makes the specification of access control policies much simpler
  - Use of time reversal to rewrite left fusion logic formulae into right fusion logic formulae
  - Enforcement of policies expressed in left Fusion Logic
  - All examples come now with comments
- FLCHECK version 0.8 (released 26/03/2010).
  Initial release.
Publications:


Figure 4: FLCHECK fusion logic decision procedure
3.3 ITL library for Isabelle/HOL

Isabelle/HOL is a generic proof assistant. It allows mathematical formulas to be expressed in a formal language and provides tools for proving those formulas in a logical calculus.

We have given a deep embedding of propositional ITL and a shallow embedding of first order ITL in Isabelle/HOL. A shallow embedding represents ITL using Isabelle/HOL predicates, while a deep embedding would represent ITL formulas as mutually inductive datatypes. See, e.g., [96] for a discussion about deep vs. shallow embeddings in Isabelle/HOL. The shallow embedding of first order ITL uses techniques developed by Stefan Merz [175, 20] for the shallow embedding of Temporal Logic of Actions (TLA) in Isabelle/HOL.

- **Deep embedding**:
  Contains:
  - Propositional ITL, syntax, semantics (finite intervals), and axioms and proof rules.
  - The lemmas from Imperative Reasoning in Interval Temporal Logic by Ben Moszkowski.
  - Time Reversal operator and an extensive list of lemmas.
  - First operator and Monitors. All key theorems/lemmas/semantics in David Smallwood PhD thesis “ITL Monitor: Compositional Runtime Analysis with Interval Temporal Logic” have been verified.
  - Link with Georg Struth’s work on Kleene Algebra. This work is based on Interval Temporal Algebra (Section 3.4) but now re-encoded in Isabelle/HOL. So the work on ITL and Prover9 and PVS has now been superseded by the Isabelle/HOL library.

  Download:
  - Version 1.9 (16/03/2019), gzipped tar file.

  Changes:
  - Restructure First and Monitor Theories.
  - Added equivalence relation on monitors.
  - See ChangeLog for detailed changes.

  - Version 1.8 (08/12/2018, first public release), gzipped tar file.

- **Shallow embedding**:
  Contains:
  - First Order ITL, both quantification over state variables, added temporal variables (current, next, final, penultimate), syntax, semantics, and axioms and proof rules. The technique used is similar to that of Stephan Merz [175, 20] used for encoding TLA in Isabelle/HOL.
  - The lemmas from Imperative Reasoning in Interval Temporal Logic by Ben Moszkowski.
  - Time Reversal operator and an extensive list of lemmas included. Time reversal operator also works for temporal variables and quantification.
  - First operator and Monitors. All key theorems/lemmas/semantics in David Smallwood PhD thesis “ITL Monitor: Compositional Runtime Analysis with Interval Temporal Logic” have been verified.
Some concrete monitors have been specified and properties verified.
Some examples using quantification.

Download:

- Version 2.3 (16/03/2019, still work in progress), gzipped tar file.
  Changes:
  * Use Intensional.thy from Isabelle/HOL distribution.
  * Restructure First and Monitor Theories.
  * Added equivalence relation on monitors.
  * Restructure Example Theory.
  * See ChangeLog for detailed changes.
- Version 2.2 (08/12/2018, warning this is work in progress), gzipped tar file.

3.4 ITL Theorem Prover based on Prover9

Note: this work has been re-encoded in the deep embedding of propositional ITL in Isabelle/HOL.

Prover9 is a resolution/paramodulation automated theorem prover for first-order and equational logic developed by William McCune.

We have given an algebraic axiom system for Propositional Interval Temporal Logic (PITL): Interval Temporal Algebra. The axiom system is a combination of a variant of Kleene algebra and Omega algebra plus axioms for linearity and confluence.

This algebraic axiom system for PITL has been encoded in Prover9. So we can use Prover9 to prove the validity of various PITL theorems. The Prover9 encoding of PITL plus examples of more than 300 PITL theorems are available for download as

  - documentation updated to new semantics for chopstar and chop omega algebraic operators
- Version 1.7 (released 15/05/2009): gzipped tar file.
  - updated documentation in doc, to use new ITL semantics
- Version 1.6 (released 12/12/2008): gzipped tar file.
  - changed copyright license to GPLv3.0 and added the notice to all files

The README in this tar file contains instructions how to use Prover9 for proving PITL theorems.
3.5 ITL Proof Checker based on PVS

Note: this work has been superseded by the deep and shallow embedding of ITL in Isabelle/HOL.

PVS is an interactive environment, developed at SRI, for writing formal specifications and checking formal proofs. The specification language used in PVS is a strongly typed higher order logic. The powerful interactive theorem prover/proof checker of PVS has a large set of basic deductive steps and the facility to combine these steps into proof strategies. PVS is implemented in Common Lisp—with ancillary functions provided in C, Tcl/TK and LaTeX—and uses GNU Emacs for its interface. PVS is freely available for IBM RS6000 machines as well as Sun Sparcs under license from SRI. See PVS homepage for more information.

- The ITL library for PVS 4.0.
- The ITL library for PVS 3.2.
- The ITL library for PVS 2.4 patchlevel 1.
- The ITL library for PVS 2.3.
- The ITL library for PVS 2.2.
- The ITL library for PVS 2.1 patchlevel 2.417.

Publications:

- Technical report.

3.6 Automatic Verification of Interval Temporal Logic

Shinji Kono has developed an automatic theorem prover for propositional ITL (LITE). The implementation is in Prolog. Further information can be gathered at Shinji Kono’s Interval Temporal Logic page. Shinji Kono has also a Java version of LITE see CVS repository of JavaLite.
4 ITL Related Publications

Download BibTeX file

The book Executing Temporal Logic Programs by Dr. B. C. Moszkowski was originally published by Cambridge University Press in 1986. The publishers have kindly given the copyright back to the author. The pdf version of the book has now been made available.

4.1 Articles


URL: http://dx.doi.org/10.1093/logcom/exm006.

URL: http://dx.doi.org/10.1016/j.tcs.2005.01.017.


URL: http://dx.doi.org/10.1007/BF02944904.


URL: http://dx.doi.org/10.1016/S0166-218X(03)00201-4.

URL: http://dx.doi.org/10.3166/jancl.14.55-104.

URL: http://dx.doi.org/10.1093/logcom/13.2.195.

URL: http://dx.doi.org/10.1023/A:1016507527035.

URL: http://dx.doi.org/10.1109/32.910858.

URL: http://dx.doi.org/10.1002/1096-908X(200007/08)12:4<3C197::AID-SMR211>3.0.CO;2-X.


4.2 In Collections


### 4.3 Conference Papers


URL: http://dx.doi.org/10.14236/ewic/ics-csr2014.9.

URL: http://dx.doi.org/10.1007/978-3-642-34281-3_20.

URL: http://dx.doi.org/10.1109/SCET.2012.6342060.

URL: https://doaj.org/article/373d1feae6e04b2c90b7457634ddfe4d.


URL: http://dx.doi.org/10.1007/978-3-642-34281-3_5.

URL: http://dx.doi.org/10.1109/CRiSIS.2011.6061544.

URL: http://dx.doi.org/10.1109/TIME.2011.25.

URL: http://dx.doi.org/10.1109/SSIRI.2010.7.


4.4 Books


4.5 Theses

URL: https://www.dora.dmu.ac.uk/handle/2086/12490.

URL: https://www.dora.dmu.ac.uk/handle/2086/10406.

URL: https://www.dora.dmu.ac.uk/handle/2086/9488.

URL: https://www.dora.dmu.ac.uk/handle/2086/10076.

URL: https://www.dora.dmu.ac.uk/handle/2086/8237.

URL: https://www.dora.dmu.ac.uk/handle/2086/6900.

URL: https://www.dora.dmu.ac.uk/xmlui/handle/2086/4809.

URL: http://ethos.bl.uk/OrderDetails.do?uin=uk.bl.ethos.438868.

URL: http://www.cse.dmu.ac.uk/~fsiewe/papers/fsiewephd.pdf.


4.6 Technical Reports


