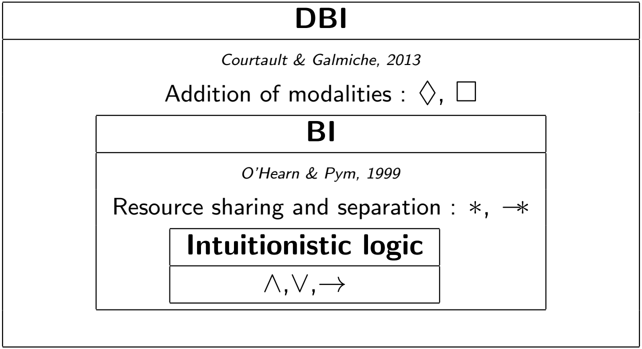
A temporal extension for BI

Pierre Kimmel

April 14, 2015

A temporal separation logic

Motivations



DBI

Courtault & Galmiche, 2013

Addition of modalities : $\Diamond$, $\Box$

BI

O'Hearn & Pym, 1999

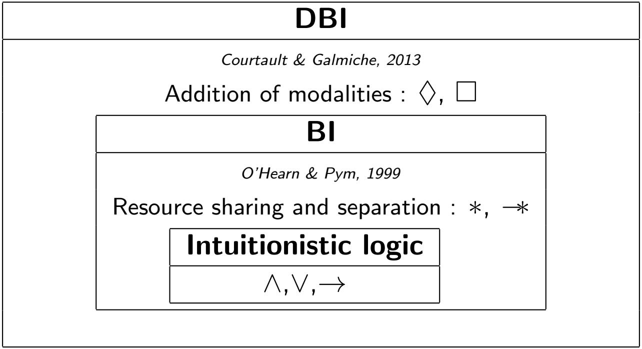
Resource sharing and separation : $*$, $-\!\!*$

Intuitionistic logic

$\wedge, \vee, \rightarrow$

A temporal separation logic

Motivations



DBI

Courtault & Galmiche, 2013

Addition of modalities : $\Diamond$, $\Box$

BI

O'Hearn & Pym, 1999

Resource sharing and separation : $*$, $-\!\!*$

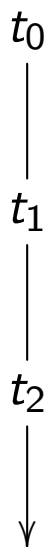
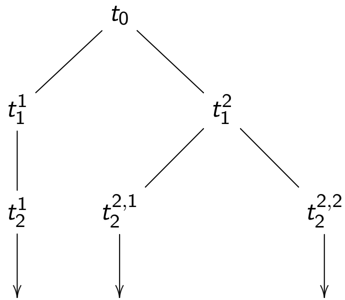
Intuitionistic logic

$\wedge,\vee,\rightarrow$

$\Rightarrow$ **A temporal extension for BI**

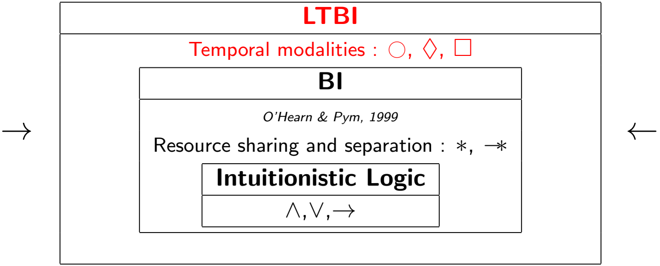
A temporal separation logic

Choice of the time

Linear time	**Branching time**
	
LTL	CTL*
G,**F**,**X**	**G**,**F**,**X** **E**, **A**
More documented	More expressive

A temporal separation logic

LTBI



DBI
Tableaux method with two labels (resource and state) →

LTBI

Temporal modalities : $\bigcirc$, $\Diamond$, $\Box$

BI

O'Hearn & Pym, 1999

Resource sharing and separation : $*$, $-\!*$

Intuitionistic Logic

$\wedge, \vee, \rightarrow$

← **LTL**
Tableaux method without labels

A temporal separation logic

Contributions

- A new temporal separation logic (LTBI)
  - Syntax - semantics
  - Models examples
- A tabeaux method (inspired by DBI)
  - Correction/Completeness
  - Counter-models extraction
- Another tableaux method(inspired by LTL)
- Comparison of the two methods

A temporal separation logic

Syntax

Constants		Additives (shared resources)		Multiplicatives (separated resources)		Temporals	
$\top$	Top	$\wedge$	And	$*$	And	$\bigcirc$	At the next state
$\bot$	Bottom	$\vee$	Ou			$\Box$	Always in the future
I	Multiplicative identity	$\rightarrow$	Implication (intuitionistic)	$-\!\!*$	Implication	$\Diamond$	One state in the future

Intuitionistic negation : $\neg X \equiv X \rightarrow \bot$

A temporal separation logic

Semantics

Definition (Linear resource model)

A *linear resource model* is a triplet $\mathcal{K} = (\mathcal{M}, [\![\cdot]\!], \vDash_{\mathcal{K}})$ such as $\mathcal{M} = (R, \bullet, e, \pi, \sqsubseteq, S)$ is a linear resource monoïd, $[\![\cdot]\!]$ is a linear interpretation and $\vDash_{\mathcal{K}}$ is a *forcing relation* on $R \times S \times \mathcal{L}$ defined as follows :

- $r, s \vDash_{\mathcal{K}} \phi \wedge \psi$ iff $r, s \vDash_{\mathcal{K}} \phi$ and $r, s \vDash_{\mathcal{K}} \psi$
- $r, s \vDash_{\mathcal{K}} \phi * \psi$ iff $\exists r', r'' \in R \cdot r' \bullet r'' \sqsubseteq r$ iff $r', s \vDash_{\mathcal{K}} \phi$ and $r'', s \vDash_{\mathcal{K}} \psi$
- $r, s \vDash_{\mathcal{K}} \Box\phi$ iff $\forall s' \in S$, if $s \preceq s'$ then $r, s' \vDash_{\mathcal{K}} \phi$
- $r, s \vDash_{\mathcal{K}} \bigcirc\phi$ iff $r, \sigma(s) \vDash_{\mathcal{K}} \phi$
- $\ldots$

A formula ϕ is *valid*, an we note $\vDash \phi$, if $e, s_0 \vDash_{\mathcal{K}} \phi$ for all linear resource models $\mathcal{K}$.

A temporal separation logic

Models: delayed consumption of resources

Instant consumption with BI :

$$(sent \wedge encoded) * (sent \mathrel{-\!\!*} received) \vDash_{BI} received$$

Delayed consumption with LTBI :

$$(sent \wedge encoded) * (sent \mathrel{-\!\!*} \Diamond received) \vDash_{BI} \Diamond received$$

$$(sent \wedge encoded) * (sent \mathrel{-\!\!*} \Diamond received) \nvDash_{BI} received$$

A temporal separation logic

Models : partitioned system

R is a set of places (buildings, rooms,...), $\sqsubseteq$ is the inclusion for places, $\bullet$ is the separation of places.

$b, t_0 \models_{\mathcal{K}} \phi$ means "ϕ is in b at time t_0".

Somebody changes place :

$$\phi = (A \wedge B \wedge \bigcirc A) * (\bigcirc B)$$

A temporal separation logic

Models : a new branching time logic ?

A formula that discriminates linear and branching time :

$$\Diamond A \wedge \Diamond B \rightarrow \Diamond(A \wedge \Diamond B) \vee \Diamond(B \wedge \Diamond A)$$

(valid in linear time, non linear in branching time)

An LTBI version with explicit branches :

$$\Diamond A * \Diamond B \rightarrow \Diamond(A \wedge \Diamond B) \vee \Diamond(B \wedge \Diamond A)$$

A tableaux method for LTBI

Resource labels and constraints

Definition (Resource labels)

L_r is a set of *resource labels* built by :

$$X ::= 1 \mid c_i \mid X \circ X$$

A *resource constraint* is a statement of the form $x \leq y$.

Definition (Closure of resource constraints set)

The *closure* of $\mathcal{C}_r$ ($\overline{\mathcal{C}_r}$) is the smaller relation closed by the following rules and such as $\mathcal{C}_r \subseteq \overline{\mathcal{C}_r}$

$$\frac{x \leq y \qquad y \leq z}{x \leq z}\ \langle t_r \rangle \qquad \frac{xy \leq xy}{x \leq x}\ \langle d_r \rangle \qquad \frac{ky \leq ky \qquad x \leq y}{kx \leq ky}\ \langle c_r \rangle$$

$$\frac{x \leq y}{x \leq x}\ \langle l_r \rangle \qquad \frac{x \leq y}{y \leq y}\ \langle r_r \rangle$$

A tableaux method for LTBI

State labels

Definition (State labels sequence)

1. A *sate labels sequence* $\mathcal{S}_s$ is a subset of L_s indexed by naturals.
2. Some labels are marked (technically, with a predicate) as direct successors.
3. We can create a new state labels sequence by inserting new labels at given places.
4. $l \in \mathcal{S}_s$ is *stuck* if l **is** a direct successor and **has** a direct successor.
5. We define $\mathcal{E}_s$, a set of state labels equalities (of form $l = l'$) and the closure of this set.

Practical representation : $\{l_1, l_2, l_3; l_4; l_5\}$
";" marks direct succession (we cannot insert here).
Here, l_4 is stuck.

A tableaux method for LTBI

Tableaux

- Labelled formulas : $(\mathbb{S}, \phi, x, u) \in \{\mathbb{T}, \mathbb{F}\} \times \mathcal{L} \times L_r \times L_s$, written $\mathbb{S}\phi : (x, u)$.

- Constraint set of statements (CSS) : $\langle \mathcal{F}, \mathcal{C}_r, \mathcal{S}_s, \mathcal{E}_s \rangle$.

- Rules : $\boxed{\dfrac{\mathbb{T}\phi \wedge \psi : (x, u) \in \mathcal{F}}{\langle \{\mathbb{T}\phi : (x, u), \mathbb{T}\psi : (x, u)\}, \emptyset, \mathcal{S}_s, \emptyset \rangle} \; \langle \mathbb{T}\wedge \rangle}$

- Tableaux : A LTBI-tableau for a formula ϕ is a tree constructed with the rules as nodes and the following root :

$$\langle \mathbb{F}\phi : (1, l_1), \{1 \leq 1\}, \{l_1\}, \emptyset \rangle$$

A tableaux method for LTBI

Rules (extracts)

$$\frac{\mathbb{T}\phi \wedge \psi : (x, u) \in \mathcal{F}}{\langle \{\mathbb{T}\phi : (x, u), \mathbb{T}\psi : (x, u)\}, \emptyset, \mathcal{S}_s, \emptyset\rangle}\ \langle \mathbb{T}\wedge\rangle \qquad \frac{\mathbb{F}\phi \wedge \psi : (x, u) \in \mathcal{F}}{\langle \{\mathbb{F}\phi : (x, u)\}, \emptyset, \mathcal{S}_s, \emptyset\rangle \ \mid\ \langle \{\mathbb{F}\psi : (x, u)\}, \emptyset, \mathcal{S}_s, \emptyset\rangle}\ \langle \mathbb{F}\wedge\rangle$$

$$\frac{\mathbb{T}\phi \to \psi : (x, u) \in \mathcal{F} \text{ et } x \leq y \in \overline{\mathcal{C}_r}}{\langle \{\mathbb{F}\phi : (y, u)\}, \emptyset, \mathcal{S}_s, \emptyset\rangle \ \mid\ \langle \{\mathbb{T}\psi : (y, u)\}, \emptyset, \mathcal{S}_s, \emptyset\rangle}\ \langle \mathbb{T} \to\rangle$$

$$\frac{\mathbb{F}\phi \to \psi : (x, u) \in \mathcal{F}}{\langle \{\mathbb{T}\phi : (c_i, u), \mathbb{F}\psi : (c_i, u)\}, \{x \leq c_i\}, \mathcal{S}_s, \emptyset\rangle}\ \langle \mathbb{F} \to\rangle$$

$$\frac{\mathbb{T}\phi * \psi : (x, u) \in \mathcal{F}}{\langle \{\mathbb{T}\phi : (c_i, u), \mathbb{T}\psi : (c_j, u)\}, \{c_i c_j \leq x\}, \mathcal{S}_s, \emptyset\rangle}\ \langle \mathbb{T}*\rangle$$

$$\frac{\mathbb{F}\phi * \psi : (x, u) \in \mathcal{F} \text{ et } yz \leq x \in \overline{\mathcal{C}_r}}{\langle \{\mathbb{F}\phi : (y, u)\}, \emptyset, \mathcal{S}_s, \emptyset\rangle \ \mid\ \langle \{\mathbb{F}\psi : (z, u)\}, \emptyset, \mathcal{S}_s, \emptyset\rangle}\ \langle \mathbb{F}*\rangle$$

A tableaux method for LTBI

Rules (extracts)

$$\frac{\mathbb{T}\Diamond\phi : (x, u) \in \mathcal{F}}{\underbrace{\langle\{\mathbb{T}\phi : (x, l)\}, \emptyset, \mathcal{S}_s, \emptyset\rangle}_{\substack{\text{for all } l \text{ stuck after } u,\\ \text{including } u \text{ if it has a direct successor.}}} \quad \mid \underbrace{\langle\{\mathbb{T}\phi : (x, l_i)\}, \emptyset, S, \emptyset\rangle}_{\substack{\text{for all } S \text{ obtained by,}\\ \text{inserting } l_i \text{ after } u \text{ in } \mathcal{S}_s.}}} \ \langle\mathbb{T}\Diamond\rangle^*$$

$$\frac{\mathbb{F}\Diamond\phi : (x, u) \in \mathcal{F} \text{ and } v \text{ is after } u}{\langle\{\mathbb{F}\phi : (x, v)\}, \emptyset, \mathcal{S}_s, \emptyset\rangle} \ \langle\mathbb{F}\Diamond\rangle$$

A tableaux method for LTBI

Rules (extracts)

$$\frac{\mathbb{S} \bigcirc \phi : (x,u) \in \mathcal{F} \text{ and } u \text{ already has a direct successor } v}{\langle \{\mathbb{S}\phi : (x,v)\}, \emptyset, \mathcal{S}_s, \emptyset \rangle} \langle \bigcirc_1 \rangle$$

$$\frac{\mathbb{S} \bigcirc \phi : (x,u) \in \mathcal{F} \text{ and } u \text{ has a non-direct successor } v}{\langle \{\mathbb{S}\phi : (x,l_i)\}, \emptyset, \mathcal{S}'_s \backslash \{v\}, \{u = v\} \rangle \mid \langle \{\mathbb{S}\phi : (x,l_i)\}, \emptyset, \mathcal{S}'_s, \emptyset \rangle} \langle \bigcirc_2 \rangle$$

$$\frac{\mathbb{S} \bigcirc \phi : (x,u) \in \mathcal{F} \text{ and } u \text{ has no successor}}{\langle \{\mathbb{S}\phi : (x,l_i)\}, \emptyset, \mathcal{S}'_s, \emptyset \rangle} \langle \bigcirc_3 \rangle$$

Where $\mathcal{S}'_s$ is $\mathcal{S}_s$ with l_i inserted as a direct successor of u.

A tableaux method for LTBI

Closure

Definition (Closure conditions)

A CSS $\langle \mathcal{F}, \mathcal{C}_r, \mathcal{S}_s, \mathcal{E}_s \rangle$ is *closed* if one of the following condition is verified :

1. $\mathbb{T}\phi : (x,u) \in \mathcal{F}$, $\mathbb{F}\phi : (y,v) \in \mathcal{F}$ and $x \leq y \in \overline{\mathcal{C}_r}$ and either $u = v$ or $u = v \in \overline{\mathcal{E}_s}$
2. $\mathbb{F}\mathrm{I} : (x,u) \in \mathcal{F}$ et $1 \leq x \in \overline{\mathcal{C}_r}$
3. $\mathbb{F}\top : (x,u) \in \mathcal{F}$
4. $\mathbb{F}\phi : (x,u) \in \mathcal{F}$ and x is inconsistant

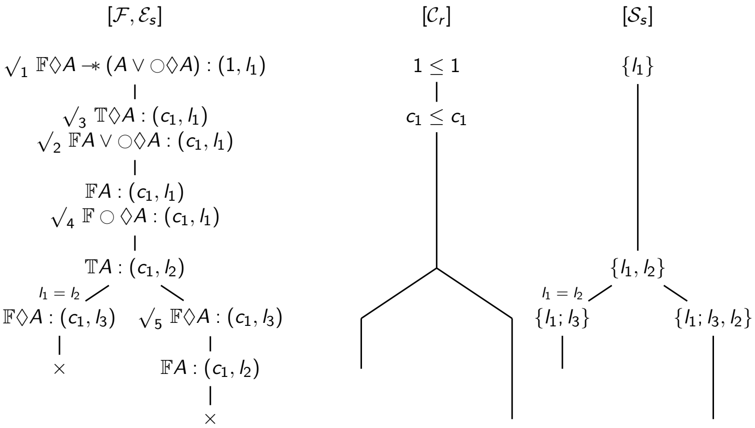
A CSS is *open* if it is not closed. A LTBI-tableau is closed if each of its branch is closed.

Definition (LTBI-proof)

An *LTBI-proof* for a formula ϕ is a closed LTBI-tableau for ϕ.

A tableaux method for LTBI

Example



$[\mathcal{F}, \mathcal{E}_s]$

$\surd_1\ \mathbb{F}\Diamond A \mathrel{-\!\!*} (A \vee \bigcirc\Diamond A) : (1, l_1)$

$\surd_3\ \mathbb{T}\Diamond A : (c_1, l_1)$

$\surd_2\ \mathbb{F}A \vee \bigcirc\Diamond A : (c_1, l_1)$

$\mathbb{F}A : (c_1, l_1)$

$\surd_4\ \mathbb{F}\bigcirc\Diamond A : (c_1, l_1)$

$\mathbb{T}A : (c_1, l_2)$

$l_1 = l_2$

$\mathbb{F}\Diamond A : (c_1, l_3)$

×

$\surd_5\ \mathbb{F}\Diamond A : (c_1, l_3)$

$\mathbb{F}A : (c_1, l_2)$

×

$[\mathcal{C}_r]$

$1 \le 1$

$c_1 \le c_1$

$[\mathcal{S}_s]$

$\{l_1\}$

$\{l_1, l_2\}$

$l_1 = l_2$

$\{l_1; l_3\}$

$\{l_1; l_3, l_2\}$

A tableaux method for LTBI

Correction and completeness

Theorem (Correction)

If a LTBI-proof for a formula ϕ exists, then it is valid.

With a notion of realization (as in the DBI proof)

Theorem (Completeness)

If a formula ϕ is valid, then there is an LTBI-proof of ϕ.

The completeness proof includes counter-model extraction model.

A tableaux method for LTBI

Problems with completeness

Adaptation of the completeness proof for DBI :

- Ab absurdo : we consider that ϕ has no proof and prove it is not valid
- Proof of the existence of an *oracle* containing all formulas that have no closed tableau.
- Creation of a sequence of formulas, according to the oracle : saturation of the tableau for ϕ
- The limit of the sequence is a counter-model for ϕ.

Problem the limit of sequences, by union, may not be a sequence.

Second tableaux method

Tableaux

Principle : $\Diamond\phi \equiv \phi \vee \circ\Diamond\phi$
$\Box\phi \equiv \phi \wedge \circ\Box\phi$

- Labelled formulas : $(\phi, x) \in \mathcal{L} \times L_r$ written $\phi : x$.
- Positive/Negative Triplets (PNT) : $\langle \mathcal{F}^+, \mathcal{F}^-, \mathcal{C}_r \rangle$.
- ■ is representing the *absurd PNT*.
- Rules : $$\boxed{\dfrac{\langle \{A \wedge B : x\} \cup \Gamma, \Delta, \mathcal{C}_r \rangle}{\langle \{A : x, B : x\} \cup \Gamma, \Delta, \mathcal{C}_r \rangle} \ \langle \wedge^+ \rangle}$$
- Tableaux : graphs. The rules translate the father/son link. If a node is obtained twice, it is not rewritten but linked accordingly.

Second tableaux method

Rules (extracts)

$$\frac{\langle \Gamma, \{\top : x\} \cup \Delta, \mathcal{C}_r \rangle}{\blacksquare} \; \langle \top \rangle$$

$$\frac{\langle \{A : x\} \cup \Gamma, \{A : y\} \cup \Delta, \mathcal{C}_r \rangle}{\blacksquare} \; \langle \bot \rangle \;\; \text{if } x \leq y \in \overline{\mathcal{C}_r}$$

$$\frac{\langle \{A \wedge B : x\} \cup \Gamma, \Delta, \mathcal{C}_r \rangle}{\langle \{A : x, B : x\} \cup \Gamma, \Delta, \mathcal{C}_r \rangle} \; \langle \wedge^{+} \rangle$$

$$\frac{\langle \Gamma, \{A \wedge B : x\} \cup \Delta, \mathcal{C}_r \rangle}{\langle \Gamma, \{A : x\} \cup \Delta, \mathcal{C}_r \rangle \mid \langle \Gamma, \{B : x\} \cup \Delta, \mathcal{C}_r \rangle} \; \langle \wedge^{-} \rangle$$

Second tableaux method

Rules (extracts)

$$\frac{\langle \{\Diamond A : x\} \cup \Gamma, \Delta, \mathcal{C}_r \rangle}{\langle \{A : x\} \cup \Gamma, \Delta, \mathcal{C}_r \rangle \mid \langle \{\bigcirc \Diamond A : x\} \cup \Gamma, \Delta, \mathcal{C}_r \rangle} \ \langle \Diamond^+ \rangle$$

$$\frac{\langle \Gamma, \{\Diamond A : x\} \cup \Delta, \mathcal{C}_r \rangle}{\langle \Gamma, \{A : x, \bigcirc \Diamond A : x\} \cup \Delta, \mathcal{C}_r \rangle} \ \langle \Diamond^- \rangle$$

$$\frac{\langle \{\bigcirc A_1 : x, \ldots, \bigcirc A_n : x\} \cup \Gamma, \{\bigcirc B_1 : x, \ldots, \bigcirc B_m : x\} \cup \Delta, \mathcal{C}_r \rangle}{\langle \{A_1 : x, \ldots, A_n : x\}, \{B_1 : x, \ldots, B_m : x\}, \mathcal{C}_r \rangle} \ \langle \bigcirc \rangle$$

if Δ and Γ only contains atomic formulas and no other rule can be applied

Second tableaux method

Clôture

Definition (Conditions de clôture)

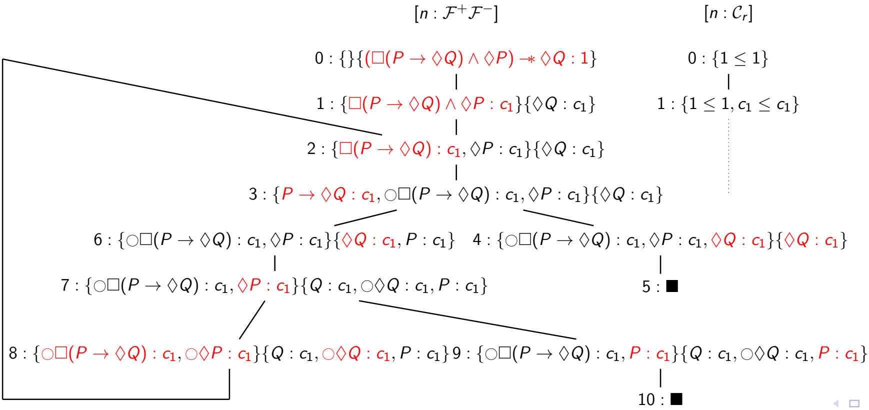
A PNT $C = \langle \mathcal{F}^+, \mathcal{F}^-, \mathcal{C}_r \rangle$ of a tableau $\mathcal{T} = (\mathcal{V}, \mathcal{E})$ is *closed* in the following cases :

1. $C = \blacksquare$
2. $\phi : x \in \mathcal{F}^-$ and x is inconsistent
3. For all C_i such as $(C, C_i) \in \mathcal{E}$, C_i is closed (all the sons of C are closed)
4. If A is a formula $\Diamond A : x \in \mathcal{F}^+$ and for all node $C' = \langle \mathcal{F}^{+\prime}, \mathcal{F}^{-\prime}, \mathcal{C}_r' \rangle$ such as $A : x \in \mathcal{F}^{+\prime}$ the path (C, C') contain a closed PNT, then C is closed.
5. Similar rule $\Box$.

A LTBI-tableau is closed if its root is closed.

Second tableaux method

Example



$[n : \mathcal{F}^+\mathcal{F}^-]$

$0 : \{\}\{(\Box(P \to \Diamond Q) \wedge \Diamond P) -\!\!* \Diamond Q : 1\}$

$1 : \{\Box(P \to \Diamond Q) \wedge \Diamond P : c_1\}\{\Diamond Q : c_1\}$

$2 : \{\Box(P \to \Diamond Q) : c_1, \Diamond P : c_1\}\{\Diamond Q : c_1\}$

$3 : \{P \to \Diamond Q : c_1, \bigcirc\Box(P \to \Diamond Q) : c_1, \Diamond P : c_1\}\{\Diamond Q : c_1\}$

$6 : \{\bigcirc\Box(P \to \Diamond Q) : c_1, \Diamond P : c_1\}\{\Diamond Q : c_1, P : c_1\}$

$4 : \{\bigcirc\Box(P \to \Diamond Q) : c_1, \Diamond P : c_1, \Diamond Q : c_1\}\{\Diamond Q : c_1\}$

$7 : \{\bigcirc\Box(P \to \Diamond Q) : c_1, \Diamond P : c_1\}\{Q : c_1, \bigcirc\Diamond Q : c_1, P : c_1\}$

$5 : \blacksquare$

$8 : \{\bigcirc\Box(P \to \Diamond Q) : c_1, \bigcirc\Diamond P : c_1\}\{Q : c_1, \bigcirc\Diamond Q : c_1, P : c_1\}$

$9 : \{\bigcirc\Box(P \to \Diamond Q) : c_1, P : c_1\}\{Q : c_1, \bigcirc\Diamond Q : c_1, P : c_1\}$

$10 : \blacksquare$

$[n : \mathcal{C}_r]$

$0 : \{1 \leq 1\}$

$1 : \{1 \leq 1, c_1 \leq c_1\}$

Second tableaux method

Links between the methods

Theorem (Equivalence between the methods)

Let ϕ be a LTBI-formula. There is a proof for ϕ with the double-labelled tableaux method if and only if there is a proof for ϕ with the the single-labelled tableaux method.

Corollary

The single-labelled tableaux method is correct and complete.

(Those results are yet to be proved)

Second tableaux method

Comparison of the methods

Double-labelled	**Single-labelled**
Resource labels and constraints	Resource labels and constraints
State labels and sequences	No state labels
Complex rules (many special cases)	Simpler rules
Simple closure	More complex closure
Potentially a lot of branches	Shorter
On simple examples, take less space	On simple examples, may require a lot of space
Fitter to "handmade" proofs	Fitter to automatization
	Possible conversion of tableaux into automata

Conclusion

Work done :

- A new temporal separation logic, LTBI
- A double-labelled tableaux method (inspired by DBI)
- A single-labelled tableaux method (inspired by LTL)

Perspectives :

- LTBI as a new branching time logic
- Automata as models