Expressive Power of Temporal Logics

Alex Rabinovich
Department of Computer Science
Tel-Aviv University
www.math.tau.ac.il/∼rabino

WOLLIC
July 19-22, 2004, Fontainebleau, France

Motivation

- **Temporal Logics over Linear Time:**
  Major result (Kamp 68): The logic with the pair of modalities **U** ("p until q") and **S** ("p since q") is ***expressively complete*** for FOMLO over linear time models ($\langle \mathbb{N}, < \rangle$, $\langle \mathbb{R}^{+}, < \rangle$).
- **Temporal Logics over Branching Time:**
  - Many logics defined and examined.
  - Unlike the linear case, no canonical temporal logic emerged.
  - ***No Yardstick***
    " . . . While less is known about comparisons of Branching Time Logics against external "yardsticks", a great deal is known about comparisons of BTLs against each other. This contrasts with the reversed situation for Linear-Time Logics." (Emerson 90, 96)
- **Our Contribution:** We offer an explanation for the multiplicity of temporal logics of branching time and provide an ***objective quantified 'yardstick'*** to measure these logics.

Results

Question: Is there a temporal logic with a finite set of modalities which is expressive equivalent to a given fragment $\mathbb{L}$ of predicate logic.

Results: For natural fragments of predicate logics there is no expressive equivalent finite base temporal logic.

Plan

I. Background

- Systems evolving in time.
- Monadic Logic of Order.
- Temporal Logics.
- Expressive Completeness.

II. Expressive completeness for TL over linear time

III. Expressive completeness for TL over branching time

IV. Complexity and Succinctness

The Models - Linear Time

Discrete Time: $T = N$

Continuous Time: $T = R^+$

A System Evolving in Time (a run of a system):

$$M =< T; 0, <, P_1(t), \cdots, P_n(t) >$$

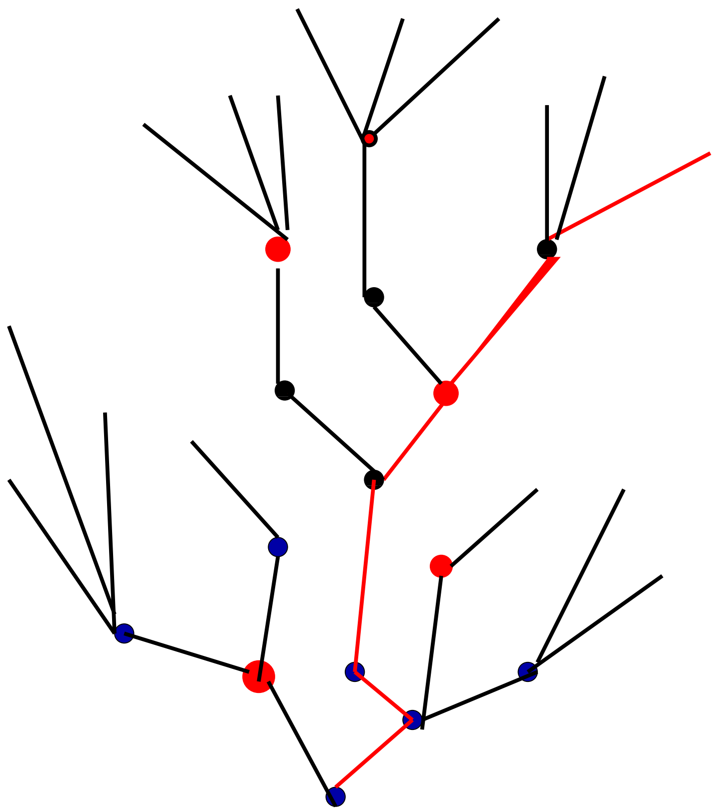
where $P_1, \cdots, P_n$ are all the interesting properties of the systems.

Variation: Include the binary function $+$ or the unary function $+1$ as we are interested in metric properties.

Models - Branching Time

A ***computation tree*** is a structure $(|T|, \leq, P_1, P_2, \ldots)$, where

- $(|T|, \leq)$ is a p.o. set with a minimal element such that for each $s \in |T|$: $\{s' : s' < s\}$ is a finite total order.
- $P_1, P_2, \ldots$ are subsets of $|T|$.



A ***path*** π through T, starting at an element $s_1 \in |T|$, is a maximal linearly ordered sequence of successive nodes $\pi = \langle s_1, s_2, s_3, \ldots \rangle$.

Monadic Logic of Order (MLO)

MLO *Monadic Second-Order Logic of Order*

- 1st-order variables $x, y, z, \ldots$ ranging over ***nodes***
- 2nd-order variables $X, Y, Z, \ldots$ ranging over ***sets of nodes***
- ***formulas***:

$$x = y \qquad x < y \qquad x \in X \qquad x \in P_a$$

$$\varphi \wedge \varphi' \qquad \neg\varphi \qquad \exists x \varphi \qquad \exists X \varphi$$

FOMLO *First-Order Monadic Logic*

- The subset of first order formulas.

MPL *Monadic Path Logic*

- MLO with 2nd-order variables ranging over ***paths***.

$\boxed{(T, s_1, \ldots, s_m, S_1, \ldots, S_n) \models \varphi(x_1, \ldots, x_m, X_1, \ldots, X_n)}$ iff

$\varphi(x_1, \ldots, x_m, X_1, \ldots, X_n)$ is satisfied in the computation tree T with x_i (X_i) interpreted by s_i (S_i).

Modalities

”People do not think variables and quantifiers. To express complex notions they name intermediate notions and compose them with each other”.

$\Diamond P$ - Sometime in the future P will be true.
is defined by the Truth Table

$$\Psi(t_0, P) = \exists t > t_0 . t \in P$$

$P \mathit{until} Q$ - is defined by the Truth Table

$$\Psi(t_0, P, Q) = \exists t > t_0 (t \in Q \wedge \forall s (t_0 < s < t \longrightarrow s \in P))$$

Similarly the dual modalities are defined:

$\diamondminus P$ - Sometimes in the past P was true.

$P \mathit{since} Q$ - P holds since a point in the past when Q held.

Temporal Logics - Syntax

- ***Vocabulary:***
  - A set of ***variables*** $Q = \{q_1, q_2, \ldots\}$.
  - A set of ***modality names*** with prescribed arity $M = \{m_1^{(k_1)}, m_2^{(k_2)}, \ldots\}$.

- **Formulas:**

$$\varphi \;::=\; q_i \;\mid\; \varphi_1 \wedge \varphi_2 \;\mid\; \neg\varphi_1 \;\mid\; m_i^{(k)}(\varphi_1, \varphi_2, \ldots, \varphi_k)$$

- A temporal logic based on M is denoted $TL(M)$;
  - The set of modalities M is called the ***basis*** of $TL(M)$.
  - M might be infinite.

Temporal Logics - Semantics

- **Interpretation of variables.** The interpretation of a variable q_i is the subset Q_i of $\mid T \mid$.

- **Interpretation of modalities.** Every k-place modality $m^{(k)}$ is interpreted in every tree T as an operator $m_T^{(k)} : [P(T)]^k \to P(T)$ which assigns "the set of points where $m^{(k)}[P_1, \ldots, P_k]$ holds" to the $k-$tuple $\langle P_1, \ldots, P_k \rangle$.

The **semantics.** $T, s \models \varphi$ "φ holds at point s in a tree $T = (\mid T \mid, \leq, Q_1, Q_2, \ldots)$" is defined inductively :

- For atomic formulas $T, s \models q_i$ iff $s \in Q_i$;

- For Boolean connectives - as usual;

- For modalities : $T, s \models m^{(k)}(\varphi_1, \varphi_2, \ldots, \varphi_k)$ iff $s \in m_T^{(k)}(R_{\varphi_1}, R_{\varphi_2}, \ldots, R_{\varphi_k})$ where $R_{\varphi_i} = \{a : T, a \models \varphi_i\}$ for all i, $1 \leq i \leq k$.

$\mathcal{MLO}$ Truth Tables

Definition: A ***truth table*** is a formula $\varphi(x_0, X_1, X_2, \ldots, X_k)$ of $\mathcal{MLO}$ with one free first-order variable x_0 and k set variables.

Definition: The ***operator*** OP_φ definable by a truth table $\varphi(x_0, X_1, X_2, \ldots, X_k)$ over a tree T:
For subsets $P_i \subseteq \mid T \mid$

$$OP_\varphi(P_1, P_2, \ldots, P_k) =$$

$$\{s \ : \ \mid T \mid, \leq, s, P_1, P_2, \ldots, P_k \models \varphi(x_0, X_1, X_2, \ldots, X_k)\}$$

Example: Some modalities and their truth tables:

- The one place modality **F**X ("eventually X"); $\varphi(x_0, X) \equiv \exists y(y > x_0 \wedge y \in X)$.
- The two place modality **U**(X, Y) ("X until Y"); $\exists y(y > x_0 \wedge y \in X \wedge \forall z(x_0 < z < y) \rightarrow z \in Y)$.

Empirical Fact: All the modalities which were suggested in the literature are definable by $\mathcal{MLO}$ truth tables.

The choice of the particular modalities with their truth tables determines the different TLs.

Interpreting Temporal Logic in Predicate Logic

Proposition: If ***every modality*** of a temporal logic TL has a truth table in a given predicate logic PL then ***every formula*** φ of TL corresponds to a formula $\tilde{\varphi}$ in PL such that

$$M, a \models \varphi \quad \text{iff} \quad M, a \models \tilde{\varphi}(t_0)$$

Hence if the modalities of a temporal logic are defined within some predicate logic then it represents a fragment of that predicate logic.

Expressive Completeness

Definition. A temporal logic TL defined in a predicate logic PL is Expressively Complete with respect to a class of models C if every formula of PL with single variable is equivalent to some formula of TL.

Theorem (Kamp 68): The temporal logic $TL(Until, Since)$ is expressively complete for $FOMLO$ with respect to the class of discrete and real time models.

1. Given $q \in TL(Until, Since)$ there is $\varphi_q \in FOMLO$ such that
$$Nat, n \models q \quad \text{iff} \quad Nat, n \models \varphi_q.$$
2. Given $\varphi \in FOMLO$ there is $q_\varphi \in TL(Until, Since)$ such that
$$Nat, n \models \varphi \quad \text{iff} \quad Nat, n \models q_\varphi.$$

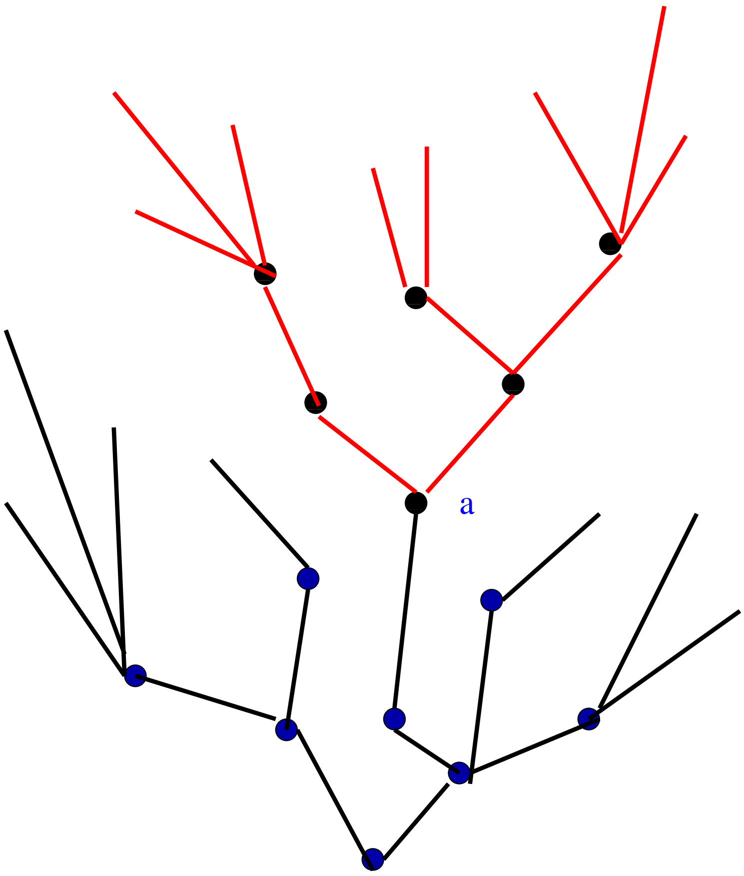
Theorem (Gabbay 198?): The temporal logic $TL(Until)$ is expressively complete for the future fragment of $FOMLO$ with respect to the class discrete time models.

Theorem (Stavi 198?): The temporal logic $TL(Until, Since, Until^s, Since^s)$ is expressively complete for $FOMLO$ with respect to the class of all linear orders.

Future formulas

Definition: ***Future formulas*** **of** MLO**:**
A formula $\varphi(x_0, X_1, X_2, \ldots, X_k)$ of MLO with one free first-order variable x_0, is a ***future formula***, iff its truth values at a node a in a tree T is defined by its truth values at the root of $T_{\geq a}$

($T_{\geq a}$ - the subtree of T rooted at a)



$T, a \models \varphi(x_0)$ iff $\quad T_{\geq a}, a \models \varphi(x_0)$

TL over Linear Models

Theorem (Hirshfeld & R. 99) The future fragment of FOMLO has no finite base over the reals.

Basis for Second-order logics

Theorem (Beauquier & R. 00) MLO has no finite base over the natural numbers.

Corollary (Beauquier & R. 00) Let A be an infinite set. MLO has no finite base over A.

TL over Computation Trees

$TL(U)$ and $TL(U, S)$ have very limited expressive power over trees.

Example. Inevitability

p is inevitable: "for all paths that start at t_0 eventually p holds" is not expressible in $TL(\mathbf{U})$.

Many TL logics were suggested.

The basic modalities of these logics have the form

1. **E** "there exists a linear run" followed by a formula in $TL(U)$ or

2. **A** "for every linear run" followed by a formula in $TL(U)$.

Example. Inevitability: $\mathbf{A}(True U P)$

Summary of Results

- We define an ***infinite hierarchy*** of temporal logics over branching time: QTL_k.
- We use this hierarchy to
  - Show: CTL^* has no finite base
  - Show: Bisimulation invariant fragment of FOMLO has no finite base
  - Examine the expressive power of commonly used temporal logics of branching time.
- Hierarchies based on Alternation Depth and Arity
- **Model Checking Problem** - for ***finite base*** TL is easy.

CTL^* **Modalities**

Definition: (CTL^* ***Modalities***) For every $\mathrm{TL}(\mathrm{Until})$ formula $\varphi(X_1, X_2, \ldots, X_k)$, we define a modality $\mathbf{E}\varphi$ as follows: $T, a \models \mathbf{E}\varphi$ iff there is a path π from a in T,

such that $T_\pi, a \models \varphi(X_1, X_2, \ldots, X_k)$.

Note. (1) CTL^* is based on ***infinite set*** of modalities.
(2)Their truth tables can be defined by MPL formulas with only one path quantifier.
(3) However, formulas of CTL^* (as formulas of every temporal logic) permit arbitrary deep nesting of modalities and can express "branching" properties which require many path quantifiers.

Example: $\mathbf{E}((\mathbf{EF}p)\mathbf{U}q)$, where $\mathbf{F}p$ is $\mathrm{True}\mathbf{U}p)$

$$m_1(X_1, X_2) \stackrel{\text{def}}{=} \mathbf{E}(X_1 \mathbf{U} X_2)$$

$$m_2(X_1) \stackrel{\text{def}}{=} (\mathbf{EF}X_1)$$

$$m_1(m_2(p), q)$$

Questions about CTL^*

Question 1. What is the expressive power of CTL^*?

Question 2. Does CTL^* admits a finite base?

(Can we find a ***finite set*** M of modalities such that CTL^* is expressively equivalent to $\mathrm{TL}(\mathrm{M})$?)

CTL^* vs Monadic Path Logic

Theorem (Moller and R. 1999) CTL^* is expressive equivalent to the future fragment of $\mathrm{MPL}^\sim$.

($\mathrm{MPL}^\sim =$ the bisimulation invariant formulas of MPL.)

1. Given $q \in \mathrm{CTL}^*$ there is $\varphi_q \in \mathrm{MPL}^\sim$ such that
$$T, a \models q \quad \text{iff} \quad T, a \models \varphi_q.$$

2. Given $\varphi \in \mathrm{MPL}^\sim$ there is $q_\varphi \in \mathrm{CTL}^*$ such that
$$T, a \models \varphi \quad \text{iff} \quad T, a \models q_\varphi.$$

Def. The counting operator $D^n X$ with $n>0$ expresses: "at least $n>0$ different successors have property X".

Theorem (Moller and R. 2001) The extension of CTL^* by the counting operators $\{D^n\}_{n=1}^\infty$ is expressively equivalent (over trees) to the future fragment of MPL.

Theorem (R. 2001) The extension of CTL^* by the counting operators $\{D^n\}_{n=1}^\infty$ and by S ("since") is expressively equivalent (over trees) to MPL.

The Sequence QTL_k

- **Definition**:
  For every $k \geq 1$, let QTL_k be the temporal logic defined as $TL(M_k)$, where
  M_k =$\{$**E**$\varphi \ : \ qd(\varphi(x_0)) \leq k$ and $\varphi(x_0)$ is a FO future formula$\}$.

- **Note:**

  – For every $k \geq 1$, QTL_k is based on an infinite set of modalities.

  – Despite the fact that the basic modalities of QTL_k have quantifier depth $\leq k+1$, for every n and $k > 1$ there is a QTL_k formula which is equivalent to no MLO formula of quantifier depth $\leq n$.

$$\mathbf{EF}(p \wedge \mathbf{EF}(p \wedge \mathbf{EF}(p \wedge \ldots \mathbf{EF}p) \ldots))$$

The Quantifier Depth Hierarchy

Theorem (Maoz & R. 2000) For every k there exists $m > k$, such that QTL_m is ***strictly more expressive*** than QTL_k.

Note that $\bigcup_{k=1}^{\infty} QTL_k \equiv_{exp} CTL^*$.

Since QTL_k contains a ***true infinite hierarchy***, we obtain:

Theorem (Maoz & R. 2000) CTL^* has ***no finite*** base.

As a consequence of the proof we also obtain

Corollary (Maoz & R. 2000) The bisimulation invariant fragment of future $FOMLO$ has ***no finite*** base.

QTL_k vs. Commonly Used Branching Logics

Many TLs were suggested as branching time specification formalisms by **imposing syntactical restrictions on CTL^*.**

QTL_2 subsumes all sub-logics of CTL^* considered in the literature. Modalities examples: $\mathbf{EF}q$, $\mathbf{A}(\mathbf{G}q_1 \wedge \mathbf{F}q_2)$.

1. $\mathrm{B}(\mathbf{F})$ (Lamport 80) can be defined as $\mathrm{TL}(\{\mathbf{EG}, \mathbf{EF}, \mathbf{AG}, \mathbf{AF}\})$.

2. UB (Ben-Ari, Manna & Pnueli 81) can be defined as $\mathrm{TL}(\{\mathbf{EF}, \mathbf{EG}, \mathbf{EX}\})$.

3. CTL and CTL^+ (Clark & Emerson 81).

    - CTL can be defined as $\mathrm{TL}(\{\mathbf{EX}, \mathbf{AX}, \mathbf{EU}, \mathbf{AU}\})$
    - CTL^+ can be defined as $\mathrm{TL}(\{\mathbf{E}\varphi \; : \; \varphi \in \Phi_1\})$, where Φ_1 is the set of $\mathrm{TL}(\mathbf{U})$ formulas of nd ≤ 1.

QTL_k vs. Commonly Used Branching Time Logics

Shorthands: $\mathbf{F}^\infty p$ for $\mathbf{GF}p$ - "infinitely often p";
$\mathbf{G}^\infty p$ for $\neg\mathbf{F}^\infty\neg p$

ECTL and ECTL$^+$ (Emerson 90).

- ECTL can be defined as $\mathrm{TL}(\{\mathbf{EX}, \mathbf{AX}, \mathbf{EU}, \mathbf{AU}, \mathbf{EF}^\infty, \mathbf{EG}^\infty, \mathbf{AF}^\infty, \mathbf{AG}^\infty\})$.
- ECTL^+ can be defined as $\mathrm{TL}(\{\mathbf{E}\varphi \ : \ \varphi \in \Phi_2\})$, where Φ_2 is the set of $\mathrm{TL}(\{\mathbf{X}, \mathbf{U}, \mathbf{F}^\infty, \mathbf{G}^\infty\})$ formulas of nd ≤ 1.

The formula $\mathbf{AF}(p \wedge \mathbf{X}p)$ was provided as an example for a CTL^* formula which is not expressible in ECTL^+ (Emerson & Halpern).

- It is expressible in QTL_3.
- As far as we know, this is the only modality discussed in the literature which is not definable in QTL_2.

Theorem (R. & Schnoebelen 2000)
ECTL^+ is expressively equivalent to QTL_2.

The Alternation Depth Hierarchy

Definition. For every $k \geq 1$, let $TLAL_k$ be the temporal logic defined as $TL(M_k)$, where
M_k =$\{$**E**φ $:$ $alternation\ depth \varphi(x_0) \leq k$ and $\varphi(x_0)$ is a FO future formula$\}$.

Theorem (R. 2001) For every k there exists $m > k$, such that $TLAL_m$ is ***strictly more expressive*** than $TLAL_k$.

The Arity Hierarchy

Def. Modality $\mathbf{R}_k(X_1, \ldots, X_k)$ says "there is a path such that along it every X_i ($i = 1, \ldots, k$) occurs infinitely often and at every point $\bigvee_{i=1}^{k} X_i$ holds."

Theorem (R. 2001) $\mathbf{R}_k(X_1, \ldots, X_k)$ is not expressible in TL with modalities definable by $k-1$-ary MLO truth tables.

Theorem (R. 2001) For every k the TL based on MLO modalities of arity $k+1$ is strictly more expressive than the TL based on MLO modalities of arity k.

Complexity of Verification

- Decidability and complexity of validity problem.

- Succinctness.

- Model Checking.

Question: Can the complexity theory distinguish between finite base Temporal Logics?

Decidability

1. Validity and satisfiability are ***decidable*** for second order monadic logic over the Natural Numbers [Büchi 62].

2. Validity and satisfiability are ***undecidable*** for second order monadic logic over the reals [Shelah 75].

3. Validity and satisfiability are ***decidable*** for first order monadic logic over the reals [Burges, Gurevich 85].

4. Validity and satisfiability are ***decidable*** for second order monadic logic over the class of trees [Rabin 69].

Complexity and Succinctness

1. Satisfiability problem for Temporal logic is ***PSPACE*** complete over the Natural numbers [Clarke, Emerson, Sistla 85].

2. Satisfiability problem for First order monadic logic is ***non elementary*** over the Natural numbers [Meyer, Stockmeyer 72].

$$\exp_m(k) = 2^{2^{2^{\cdot^{\cdot^{\cdot^{k}}}}}} \Big\} m$$

   is the m-times iterated exponential function.

3. There is a succinctness gap between TL and FOMLO: any translation of the predicate logic to temporal logic is necessarily ***non elementary***.

4. Satisfiability problem for temporal logic is ***PSPACE*** complete over the Reals [Reinolds 99].

The Model Checking Problem

Model Checking

Input: A finite state Kripke structure K, $s \in K$ and a formula $\varphi(x_0)$.

Question: Decide whether $T_K, s \models \varphi(x_0)$

Logic	Basis	Complexity
CTL	finite	$O(\mid K \mid \times \mid \varphi \mid)$
CTL^+	infinite	P^{NP}
CTL^*	infinite	PSPACE

There is a tradeoff between expressive power, succinctness and complexity of model checking.

- CTL has the same expressive power as CTL^+ (Emerson & Halpern 1982).

- There is an exponential gap in succinctness of CTL and CTL^+ (Wilke 1999).

Model Checking for finite base TL

Theorem. Let $TL(M_1, M_2, \ldots, M_k)$ be a TL based on a finite set of modalities.

1. Assume that M_i $(i = 1, 2, \ldots, k)$ are of the form $E\varphi$, where φ is a future monadic second-order formula. Then, the model checking problem for $TL(M_1, M_2, \ldots, M_k)$ has time complexity $O(| K | \times | \varphi |)$.
2. Assume that M_i $(i = 1, 2, \ldots, k)$ are definable by future MLO-formulas. Then, the model checking problem for $TL(M_1, M_2, \ldots, M_k)$ is in PTIME.

Moral: The complexity theory does not provide a yardstick for choosing a finite base TL.

Further Results - three infinite base TL

QTL_2**:** modalities - $\mathbf{E}\varphi$, where φ is a $FOMLO$ formula of qd ≤ 2.

$ECTL^+$**:** modalities - $\mathbf{E}\varphi$, where φ is a $TL(\{\mathbf{X}, \mathbf{U}, \mathbf{F}^\infty, \mathbf{G}^\infty\})$ formula of nd ≤ 1.

$TL(U, R_1, \ldots R_k, \ldots)$**:** $\mathbf{R}_k(X_1, \ldots, X_k)$ says "there is a path such that along it every X_i ($i = 1, \ldots, k$) occurs infinitely often and at every point $\bigvee_{i=1}^k X_i$ holds"

$$\mathbf{R}_k(X_1, \ldots, X_k) \Leftrightarrow \mathbf{E}(\mathbf{G} \bigvee_{i=1}^{k} X_i \wedge \bigwedge_{i=1}^{k} \mathbf{F}^\infty X_i).$$

Theorem (R. & Schnoebelen 2000). All three formalisms are expressive equivalent and have no finite base.

Theorem (R. & Schnoebelen 2000). The model checking problems for QTL_2 and $ECTL^+$ are P^{NP} complete. The model-checking problem for $TL(U, R_1, \ldots R_k, \ldots)$ is in P

Theorem (R. & Schnoebelen 2000). There is an exponential succinctness gaps between QTL_2 and $ECTL^+$ and between $ECTL^+$ and $TL(U, R_1, \ldots R_k, \ldots)$

Further Results and Open Questions

- The results are valid not only for the class of all trees, but also for its interesting subclasses: the finite trees, trees obtained by unwinding finite Kripke structures, and trees with only infinite (ω) branches.

- Past modalities.

- Model Checking for infinite base TL

  Open Question. What is the complexity of the model checking problem for QTL_k.