Modal Logic

Propositional logic may be defined in a Hilbert style fashion

Propositional logic is a set H defined as smallest set X of formulas verifying the following properties:

1. if A, B, C are formulas then X contains the formulas (called axioms)

P1 $A \to (B \to A)$

P2 $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$

P3 $((\neg B \to \neg A) \to ((\neg B \to A) \to B))$

L is closed w.r.t. the following operation

MP if $A \in X$ and $A \to B \in X$ then $B \in X$(modus ponens)

We write $\vdash_H A$ to denote that $A \in H$

If Ω is a finite set of formulas we write $\Omega \vdash_H A$ to denote that $\vdash_H \bigwedge \Omega \to A$

If Ω is an infinite set of formulas we write $\Omega \vdash_H A$ to denote that there is a finite subset Ω_0 of Ω s.t. $\Omega_0 \vdash_H A$.

language of modal logic

alphabet:

(i) proposition symbols : $p_0, p_1, p_2, \ldots,$

(ii) connectives : $\rightarrow, \perp$

(iii) modal operator $\Box$

(iv) auxiliary symbols : (,).

$AT = \{p_0, p_1, p_2, \ldots,\} \cup \{\perp\}$

The set WFF of (modal) formulas is the smallest set X with the properties

(i) $p_i \in X$ $(i \in N)$, $\perp \in X$,

(ii) $A, B \in X \Rightarrow (A \rightarrow B) \in X$,

(iii) $A \in X \Rightarrow (\neg A) \in X$

(iv) $A \in X \Rightarrow (\Box A) \in X$

Let **Z** be a set o formula.

The normal modal logic **L**[**Z**] is defined as smallest set X of formulas verifying the following properties:

1. **Z**$\subseteq$ **X**
2. if A, B, C are formulas then X contains the formulas (called axioms)
   P1 $A\to(B\to A)$
   P2 $(A\to(B\to C))\to((A\to B)\to(A\to C))$
   P3 $((\neg B\to\neg A)\to((\neg B\to A)\to B))$
   P4 $\Box(A\to B)\to(\Box A\to\Box B)$
3. L is closed w.r.t. the following operation
   MP if $A\in X$ and $A\to B\in X$ then $B\in X$(modus ponens)
   NEC if $A\in X$ then $\Box A\in X$ (necessitation)

We write $\vdash_{\mathbf{L[Z]}} A$ to denote that $A\in$**L**[**Z**]

If Ω is a finite set of formulas we write $\Omega \vdash_{\mathbf{L[Z]}} A$ to denote that $\vdash_{\mathbf{L[Z]}} \bigwedge\Omega \to A$

If Ω is an infinite set of formulas we write $\Omega \vdash_{\mathbf{L[Z]}} A$ to denote that there is a finite subset Ω_0 of Ω s.t. $\Omega_0 \vdash_{\mathbf{L[Z]}} A$.

$L[\varnothing]$ is called minimal normal modal logic and $L[\varnothing]$ is denoted simply by **K**

Abbreviations

The usual abbreviations of classical logic plus

$\Diamond A := \neg\Box\neg A$

If $N_1,..,N_k$ are names of schemas of formula the sequence $N_1..N_k$ is the set $N_1^*\cup\ldots\cup N_1^*$, where

$N_i^* =\{A: A \text{ is an instance of the schema } N_i\}$

some schema

D. $\Box A\rightarrow\Diamond A$

T. $\Box A\rightarrow A$

4. $\Box A\rightarrow\Box\Box A$

B. $A\rightarrow\Box\Diamond A$

some modal logic

$T := L[T]$

$S4 := L[T4]$

$S5 := L[T4B]$

$KT := L[T]$

$K4 := L[4]$

Possible world semantics
or
Kripke semantics

Let Prop be the set of propositional symbols.

A **structure** $F = \langle U,R \rangle$, where U is a nonempty set and $R \subseteq U x U$ is called **frame** ($\mathscr{F}$ is a graph).

A **valuation** on a frame $F=\langle U,R \rangle$ is a function $V : U \rightarrow 2^{Prop}$.

A **(Kripke) model** M is a frame plus a valuation V, $M = \langle U,R,V \rangle$

Let $M = \langle U, R, V \rangle$ a model,

the satisfiability relation $M \vDash \subseteq$ UxWFF

is defined as

1. $M, w \vDash A \wedge B \Leftrightarrow M, w \vDash A$ AND $M, w \vDash B$

2. $M, w \vDash A \vee B \Leftrightarrow M, w \vDash A$ OR $M, w \vDash B$

3. $M, w \vDash \neg A \Leftrightarrow M, w \nvDash A$,

4. $M, w \vDash A \rightarrow B \Leftrightarrow (M, w \vDash A \Rightarrow M, w \vDash B)$,

5. $M, w \vDash \Box A \Leftrightarrow \forall u\ (wRu \Rightarrow M, u \vDash A)$

6. $M, w \vDash \Diamond A \Leftrightarrow \exists u\ (wRu$ AND $M, u \vDash A)$

7. $M, w \nvDash \bot$

8. $M, w \vDash p$ iff $p \in V(w)$

$let\ M\ be\ a\ model,\ M \models A\ iff\ for\ each\ u \in U\ we\ have\ M, u \models A$

$let\ M\ be\ a\ model\ and\ let\ \Sigma\ be\ a\ set\ of\ formulas,\ M \models \Sigma\ iff\ for\ each\ A \in \Sigma\ M \models A$

$\models A\ iff\ for\ each\ model\ M\ we\ have\ M \models A.$

$let\ F\ be\ a\ frame,\ F \models A\ iff\ for\ each\ valuation\ V,\ \langle F, V \rangle \models A$

$let\ F\ be\ a\ frame,\ F, w \models A\ iff\ for\ each\ valuation\ V,\ \langle F, V \rangle, w \models A$

$let\ M\ be\ a\ model,\ Th(M) = \{A : M \models A\}$

$let\ F\ be\ a\ ,\ Th(F) = \{A : F \models A\}$

$Md(A) = \{M : M is\ a\ model, M \models A\}$

$Md(\Sigma) = \{M : M is\ a\ model, M \models \Sigma\}$

$Fr(A) = \{F : F is\ a\ frame, F \models A\}$

$Fr(\Sigma) = \{F : F is\ a\ model, F \models \Sigma\}$

Theorem 1.2.2 (soundness) *Let* Σ *be a set of formulas and let* $M \in Md(\Sigma)$ *(*$F \in Fr(\Sigma)$*) then for each theorem* $A \in \mathbf{L}[\Sigma]$ *we have that* $M \models A$ *(*$F \models A$*).*

Modal definability

First order translation

Let us assume a modal language with a denumerable set Prop of propositional symbols.
Let us consider a first order language *L*, with a denumerable set Π of unary predicate symbols, and a binary predicate symbol R.
Let τ:Prop$\rightarrow\Pi$ a bijective map
Let Form be the set of first order formula formulas in the language *L.*
Given a fixed variable x, we define an injective mapping
ST: WFF→Form

1. ST(p) = P(x) for p $\in$Prop and P = τ(p);
2. ST(¬A)=¬ST(A)
3. ST(A→B)=ST(A)→ST(B)
4. ST($\Box$A) = $\forall$y(xRy→ST (A)[x/y]) where y does no occur in ST(A).

definability

Let A (Σ) be a formula (a set of formulas), we say that A (Σ) defines a first/second order property Φ in the language with (R, =), if for each F ($F \in Fr(A)$ ($F \in Fr(\Sigma)$) $\Longleftrightarrow F \models \Phi$)

If the set Σ defines the condition Φ then we say also that the logic L[Σ] defines Φ.

formula name	formula	first order property
D	$\Box A \to \Diamond A$	$\forall x \exists y. xRy$
T	$\Box A \to A$	$\forall x. xRx$
4	$\Box A \to \Box\Box A$	$\forall xyz.(xRy \wedge yRz \to xRz)$
B	$\Diamond\Box A \to A$	$\forall x \forall y.(xRy \to yRx)$
G	$\Diamond\Box A \to \Box\Diamond A$	$\forall xyz.((xRy \wedge xRz) \to \exists w(yRw \wedge zRw))$

Proposition 1.3.7 $\Box\alpha \to \Box\Box\alpha$ *defines transitivity* $\forall xyz.(xRy \wedge yRz \to xRz)$

PROOF

Proposition 1.3.7 $\Box\alpha \to \Box\Box\alpha$ *defines transitivity* $\forall xyz.(xRy \wedge yRz \to xRz)$

Proof.

1. $F \models \forall xyz.(xRy \wedge yRz \to xRz) \Rightarrow F \models \Box\alpha \to \Box\Box\alpha$. Let $F, w \models \Box\alpha$, and w', w'' s.t. $wRw', w'Rw''$ then by transitivity we have that wRw'' and therefore $F, w'' \models \alpha$; namely $F, w' \models \Box\alpha$ and $F, w \models \Box\Box\alpha$.

2. $F \models \Box\alpha \to \Box\Box\alpha \Rightarrow F \models \forall xyz.(xRy \wedge yRz \to xRz)$. Let us suppose that $F, w \models \Box\alpha \to \Box\Box\alpha$; we fix the following assignment $V(\alpha) = \{v | wRv\}$. We have that $F, V, w \models \Box\alpha$ and by hypothesis $F, V, w \models \Box\Box\alpha$. Now for a generic $v \in V(\alpha)$ let w'' s.t. vRw''. As $F, V, w'' \models \alpha$, we must have that R is transitive.

■

Proposition 1.3.8 $\Diamond\Box\alpha \to \Box\Diamond\alpha$ *defines directness:*
$dir = \forall xyz((xRy \wedge xRz) \to \exists u(yRu \wedge zRu))$

Proposition 1.3.8 $\Diamond\Box\alpha \rightarrow \Box\Diamond\alpha$ *defines directness:*
$dir = \forall xyz((xRy \wedge xRz) \rightarrow \exists u(yRu \wedge zRu))$

Proof

1. $F \models \forall xyz((xRy \wedge xRz) \rightarrow \exists u(yRu \wedge zRu)) \Rightarrow F \models \Diamond\Box\alpha \rightarrow \Box\Diamond\alpha$
   Let $w \in W$ and $F, w \models \Diamond\Box\alpha$ then $\exists w', wRw' s.t. \forall w'' w'Rw'' \Rightarrow w'' \models \alpha$.

   As dir holds we have that $\forall v wRv \exists s w'Rs, vRs$ as $F, s \models \alpha$ and therefore $F, w \models \Box\Diamond\alpha$

2. $F \models \Diamond\Box\alpha \supset \Box\Diamond\alpha \Rightarrow F \models \forall xyz((xRy \wedge xRz) \rightarrow \exists u(yRu \wedge zRu))$
   Let w, w', w'' s.t. wRw', wRw'' and let V the assignment s.t. $V(\alpha) = \{s : w'Rs\}$

   We have that $F, w' \models \Box\alpha$ and that $F, w' \models \Diamond\Box\alpha$. As $F \models G$ we have that $F, w \models \Box\Diamond\alpha$ and therefore $\forall v wRv \Rightarrow \exists t F, t \models \alpha \Rightarrow t \in V(\alpha) \Rightarrow F \models dir$

∎

$$Fr(\mathbf{K}) = \{\langle U, R\rangle : R \text{ is a generic relation}\}$$
$$Fr(\mathbf{KD}) = \{\langle U, R\rangle : R \text{ is total}\}$$
$$Fr(\mathbf{KT}) = \{\langle U, R\rangle : R \text{ is reflexive}\}$$
$$Fr(\mathbf{S4}) = \{\langle U, R\rangle : R \text{ is a preorder}\}$$
$$Fr(\mathbf{S5}) = \{\langle U, R\rangle : R \text{ is an equivalence}\}$$

COMPLETENESS

L[Z] is defined as smallest set X of formulas verifying the following properties:

1. Z⊆ X

2. if A, B, C are formulas then X contains the formulas (called axioms)

P1 $A\to(B\to A)$

P2 $(A\to(B\to C))\to((A\to B)\to(A\to C))$

P3 $((\neg B\to\neg A)\to((\neg B\to A)\to B))$

P4 $\square(A\to B)\to(\square A\to\square B)$

3. L is closed w.r.t. the following operation

MP if $A\in X$ and $A\to B\in X$ then $B\in X$(modus ponens)

NEC if $A\in X$ then $\square A\in X$ (necessitation)

Given a set Z of modal fomulas the modal logic L[Z] is defined by means of the following axioms and inference rules plus a notion of derivation.

axioms

1. if A, B, C are formulas then the following are axioms

P1 $A\to(B\to A)$

P2 $(A\to(B\to C))\to((A\to B)\to(A\to C))$

P3 $((\neg B\to\neg A)\to((\neg B\to A)\to B))$

P4 $\square(A\to B)\to(\square A\to\square B)$

2. if $A\in$**Z** then A is an axiom

Inference rules

$$\frac{A \quad A\to B}{B}$$ **MP**

$$\frac{A}{\square A}$$ **NEC**

Derivations

A derivation is a finite sequence $A_1, \ldots, A_n$ of formulas s.t. for each $i \in [1, n]$

A_i is an axiom; or

$A_i \equiv B$ and $\exists j, k < i$ s.t. $A_j \equiv A$, $A_k \equiv A \to B$;

$A_i \equiv \square A$ and $\exists k < i$ s.t. $A_k \equiv A$;

We write $\vdash_{L[Z]} A$ to denote that there is a derivation $A_1,\ldots,A_n$ with $A_n \equiv A$

The construction of the canonical model

Maximal Consistent Sets

A set Γ of WFF is **consistent** if
$\Gamma \nvdash \perp$.
A set Γ of WFF is **inconsistent** if
$\Gamma \vdash \perp$.

A set Γ is maximally consistent iff
(a) Γ is consistent,
(b) $\Gamma \subseteq \Gamma'$ and Γ' consistent $\Rightarrow \Gamma = \Gamma'$.

If Γ is maximally consistent, then Γ is closed under derivability (i.e. $\Gamma \vdash \phi \Rightarrow \phi \in \Gamma$).

Theorem:
Each consistent set Γ is contained in a maximally consistent set Γ^*

1) enumerate all the formulas

$\varphi_0, \varphi_1, \varphi_2, \ldots\ldots$

2) define the non decreasing sequence:

$\Gamma_0 = \Gamma$

$$\Gamma_{n+1} = \begin{cases} \Gamma_n \cup \{\phi_n\} \text{ if } \Gamma_n \cup \{\phi_n\} \text{ is consistent,} \\ \Gamma_n \text{ otherwise} \end{cases}$$

3) define

$$\Gamma^* = \bigcup_{n \geq 0} \Gamma_n \,.$$

Propositional logic:

If Γ is consistent, then there exists a CANONICAL valuation such that $[\psi] = 1$ for all $\psi \in \Gamma$.

Let L be a normal modal logic, a model $M = \langle U,R,V \rangle$ is called canonical iff

1. $U = \{w : w \text{ is maximal consistent}\}$
2. $R = \{(u,v) : \{A : \Box A \in u\} \subseteq v$
3. $u \in V(p) \Leftrightarrow p \in u$

A logic L is called **canonical** if, taken the canonical model $\langle U,R,V\rangle$, we have $\langle U,R\rangle \in Fr(L)$.

Theorem CM

Let $\langle U,R,V\rangle$ the canonical model of L

$\vdash_L \alpha \Leftrightarrow \langle U,R,V\rangle \vDash \alpha$

A normal modal logic L is said to be **model complete** if for each formula A:

$$\vdash_L A \Leftrightarrow \forall M \in Md(L)\ M \models A$$

Theorem

Each normal modal logic is model complete

Proof

$$(\Rightarrow)$$

$\vdash_L A \Rightarrow \forall M \in Md(L) M \models A$ by soundness

$$(\Leftarrow)$$

In order to prove
$\forall M \in Md(L) M \models A \Rightarrow \vdash_L A$ we use the canonical model.

If $\forall M \in Md(L)\ M \models A$ we have in particular that taken the canonical model $\langle U, R, V\rangle$ we have that $\langle U, R, V\rangle \models A$, and applying theorem CM we conclude.

A normal modal logic $L(\Sigma)$ is said to be **frame complete** if for each formula A:

$\vdash_L A \Leftrightarrow \forall F \in Fr(\Sigma)\ F \vDash A$

Theorem The logics K, KD, KT, S4, S5, are frame complete.

Proof

Let $L \in \{K, KD, KT, S4, S5\}$, it is sufficient to show that if $\langle U,R,V \rangle$ is the canonical model of L then the frame $\langle U,R \rangle \in Fr(L)$.

Let Σ be a set of formulas, and let $\mathscr{C} \subseteq Fr(\Sigma)$ a set of frames; the modal logic $L[\Sigma]$ is said to be **$\mathscr{C}$-complete** (complete w.r.t. the class $\mathscr{C}$ of frames) if

$A \in L(\Sigma) \Leftrightarrow \forall F \in C, F \vDash A$

Theorem

1. The logics K (KD) is complete with respect to the class of denumerable frames with irreflexive, asymmetric and intransitive (total) accessibility relation.
2. The logic S4 is complete w.r.t. the set of denumerable partial order.

Modal logic and intuitionism

Let us consider the following translation function []* from propositional formulas to modal ones.

$p^* = \Box p$ (p is a propositional symbol)

$[A \wedge B]^* = [A]^* \wedge [B]^*$

$[A \vee B]^* = [A]^* \vee [B]^*$

$[A \rightarrow B]^* = \Box([A]^* \rightarrow [B]^*)$

$[\neg A]^* = \Box(\neg [A]^*)$

Lemma

Let $\langle W,R,V_i\rangle$ be an intuitionistic model and $\langle W,R,V_{S4}\rangle$ be a partial order model of S4 s.t. for each propositional symbol p,

$w \Vdash_i p$ iff $w \vDash_{S4} \Box p$,

then for each propositional formula A, $w \Vdash_i A$ iff $w \vDash_{s4} A^*$

Lemma

Let $M_i=\langle W,R,V_i\rangle$ be an intuitionistic model and $M_{S4}=\langle W,R,V_{S4}\rangle$ be a partial order model of S4 s.t. for each propositional symbol p,

$w \Vdash_i p$ iff $w \vDash_{S4} \Box p$,

then for each propositional formula A, $M_i \Vdash_i A$ iff $M_{S4} \vDash_{s4} A^*$

Theorem

$\vdash_i A \Leftrightarrow \vdash_{S4} A^*$

natural deduction?

There is no general way of giving a proof theory for modal logics.

The case of S4

$$
\dfrac{\begin{array}{c} \Box\Gamma, \neg\Diamond\Gamma' \\ \mathcal{D} \\ A \end{array}}{\Box A}\,\Box I
\qquad\qquad
\dfrac{\begin{array}{c} \mathcal{D} \\ \Box A \end{array}}{A}\,\Box E
$$

$$
\dfrac{\begin{array}{c} \mathcal{D} \\ A \end{array}}{\Diamond A}\,\Diamond I
\qquad\qquad
\dfrac{\begin{array}{c} \mathcal{D}_1 \\ \Diamond B \end{array} \qquad \begin{array}{c} \Box\Gamma, \neg\Diamond\Gamma', [\![B]\!] \\ \mathcal{D}_2 \\ C \end{array}}{C}\,\Diamond E
$$

$$\dfrac{\begin{array}{c}\mathcal{D}\\ A\end{array}}{\Box A}\ \Box I$$

$C \in hp\,\mathcal{D} \Leftrightarrow$ *C has the shape either* $\Box B$ *or* $\neg\Diamond B$

failure of normalisation

$$
\cfrac{\cfrac{\Box A\land\Box B}{\Box A}\,\land E \qquad \cfrac{\cfrac{\cfrac{\cfrac{\cfrac{[\Box A]^1}{A}\,\Box E \quad \cfrac{[\Box B\,]}{B}\,\Box E}{A\land B}\,\land I}{\Box(A\land B)}\,\Box I}{\Box B\supset\Box(A\land B)}\,\supset I}{\Box A\supset(\Box B\supset\Box(A\land B))}\,\supset I\ (1)}{\Box B\supset\Box(A\land B)}\,\supset E
$$

failure of normalisation

$$
\dfrac{\dfrac{\Box A \wedge \Box B}{\Box A}\,\wedge E \qquad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[\Box A]^1}{A}\,\Box E \quad \dfrac{[\Box B]}{B}\,\Box E}{A \wedge B}\,\wedge I}{\Box(A \wedge B)}\,\Box I}{\Box B \supset \Box(A \wedge B)}\,\supset I}{\Box A \supset (\Box B \supset \Box(A \wedge B))}\,\supset I\ (1)}{\Box B \supset \Box(A \wedge B)}\,\supset E
\quad \rhd \quad
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Box A \wedge \Box B}{\Box A}\,\wedge E}{A}\,\Box E \quad \dfrac{[\Box B]}{B}\,\Box E}{A \wedge B}\,\wedge I}{\Box(A \wedge B)}\,\Box I}{\Box B \supset \Box(A \wedge B)}\,\supset I
$$

The solution proposed by Prawitz

$$
\dfrac{\begin{array}{ccc} \mathcal{D}_1 & & \mathcal{D}_n \\ [\Box\tau_1 & \ldots & \Box\tau_n] \\ & \mathcal{D} & \\ & \sigma & \end{array}}{\Box\sigma}\ \Box I
$$

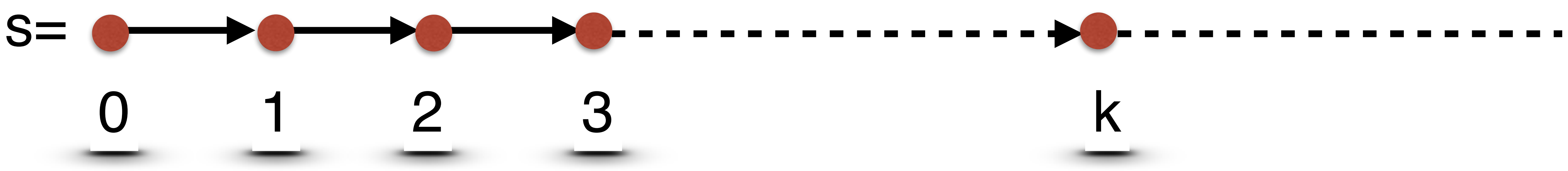
TEMPORAL LOGIC

LTL: Linear Temporal Logic

timeline/computation/fullpath

Kripke frame is **Nat**=$\langle \mathbb{N}, \sigma, \leq \rangle$

(as usual $\sigma(n)$ will be written as $n+1$)



each natural number identifies an temporal instant

A Linear Time Kripke model **M** (or, simply, a model) is a frame plus a valuation of propositional symbols, namely **M**= $\langle$**Nat**, $V:\mathbb{N}\rightarrow 2^{Prop}\rangle$

σ induces the accessibility relation

$\mathcal{N} \subseteq \mathbb{N} \times \mathbb{N}$

$n \mathcal{N} m \Longleftrightarrow m=n+1$

language of linear temporal logic

alphabet:

(i) proposition symbols : p_0, p_1, p_2, . . . ,

(ii) connectives : $\to, \perp$

(iii) modal operator $\bigcirc$, $\mathcal{U}$,

(iv) auxiliary symbols : (,).

$AT = \{p_0, p_1, p_2, \ldots,\} \cup \{\perp\}$

The set WFF of (modal) formulas is the smallest set X with the properties

(i) $p_i \in X$ ($i \in N$), $\perp \in X$,

(ii) $A, B \in X \Rightarrow (A \to B) \in X$,

(iii) $A \in X \Rightarrow (\neg A) \in X$

(iv) $A \in X \Rightarrow (\bigcirc A) \in X$

(v) $A, B \in X \Rightarrow (A \,\mathcal{U}\, B) \in X$,

abbreviations:

$\Diamond A := (\neg\perp)\,\mathcal{U}\,A$

$\Box A := \neg\Diamond\neg A$

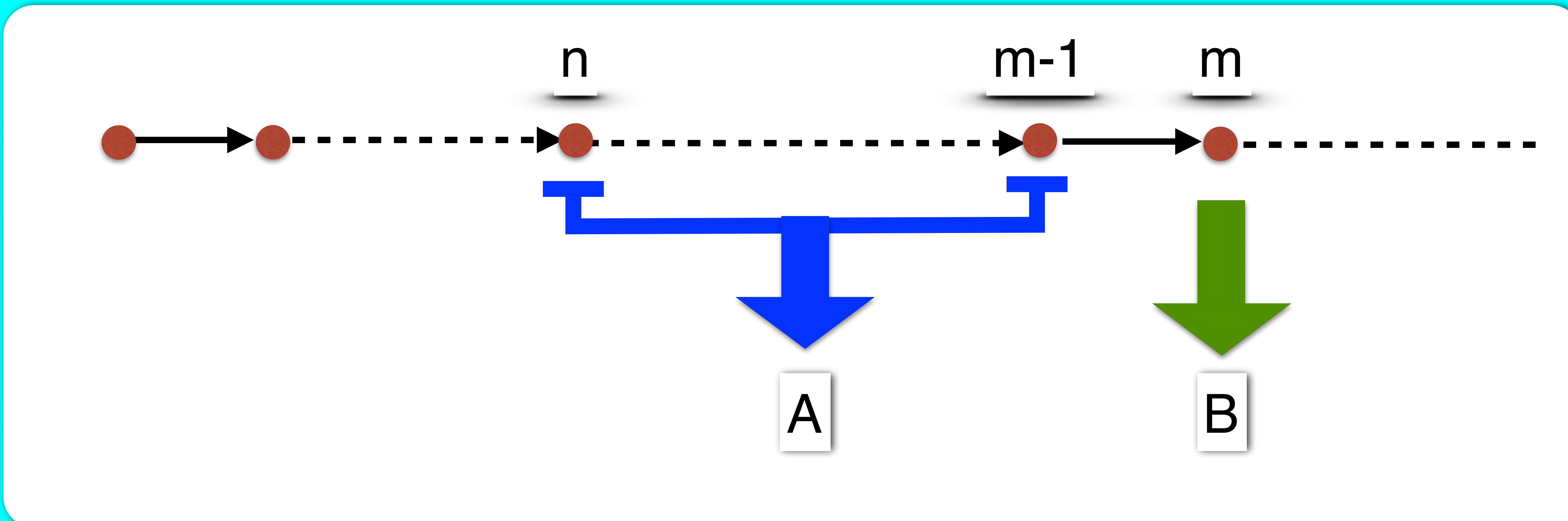
Let **M**= $\langle$**Nat**, V$\rangle$ a model,

the satisfiability relation **M** $\models \subseteq \mathbb{N}$xWFF

is defined as

1. **M** ,n $\models A \wedge B \Leftrightarrow$ M,n $\models$A & M,n $\models$B
2. M ,n $\models A \vee B \Leftrightarrow$ M,n $\models$A OR M,n$\models$B
3. M,n $\models \neg A \Leftrightarrow$ M,n $\not\models$ A,
4. M,n $\models A \rightarrow B \Leftrightarrow$ (M,n $\models A \Rightarrow$ M,n $\models$B),
5. M,n $\models A \mathcal{U} B \Leftrightarrow \exists$ m(n$\leq$m & (M,m $\models$ B & $\forall$j(j$\in$[n,m-1]$\Rightarrow$M,j $\models$A)))
6. M,n $\models \Box A \Leftrightarrow$ $\forall$ m (n$\leq$m $\Rightarrow$M,m $\models$ A)
7. M,n $\models \Diamond A \Leftrightarrow$ $\exists$ m (n$\leq$m & M,m $\models$ A)
8. M,n $\models \bigcirc A \Leftrightarrow$ M,n+1 $\models$ A)
9. M ,n $\not\models \bot$
10. M ,n $\models$ p iff p$\in$V(n)

$M,n \models A\,\mathcal{U}\,B \Leftrightarrow \exists\ m \geq n\ M,m \models B\ \&\ \forall j \in [n,m-1]\ M,j \models A$



Sometimes in literature a model is given by

K=$\langle T, s:\mathbb{N}\rightarrow T, V\rangle$

where

T is a denumerable set of temporal instants

s is a bijection and

$V:T\rightarrow 2^{Prop}$ is a valuation

these models are completely equivalent to the models previously introduced.

Let $\mathbf{K}=\langle T, s:\mathbb{N}\rightarrow T, V\rangle$,
the satisfiability relation $\mathbf{K} \models \subseteq T \mathrm{x} WFF$
is defined as

$M,s_k \models A\rightarrow B \Leftrightarrow (M,s_k \models A \Rightarrow M,s_k \models B)$,

$M,s_n \models A\mathcal{U}B \Leftrightarrow \exists\, m(n\leq m\ \&\ (M,s_m \models B\ \&\ \forall j(j\in[n,m-1] \Rightarrow M,s_j \models A)))$

$M,s_n \models \bigcirc A \Leftrightarrow M,s_{n+1} \models A)$

$M ,s_n \not\models \perp$

$M ,s_n \models p$ iff $p\in V(s_n)$

$$M \models A \iff \forall n\ M,n \models A$$

$$\models A \iff \forall M.\ M \models A$$

A0 All temporal instances of propositional classical tautologies.

A1 $\circ(A\rightarrow B)\rightarrow(\circ A\rightarrow\circ B)$

A2 $\neg\circ A\rightarrow\circ\neg A$

A3 $\Box(A\rightarrow B)\rightarrow(\Box A\rightarrow\Box B)$

A4 $\Box A \rightarrow A$

A5 $\Box A \rightarrow \Box\Box A$

A6 $\Box A\rightarrow\circ A$

A7 $\Box A \rightarrow \circ\Box A$

A8 $A\wedge\Box(A\rightarrow\circ A)\rightarrow\Box A$

MP $\dfrac{A \quad A\rightarrow B}{B}$

Gen$\Box$ $\dfrac{A}{\Box A}$

Gen$\circ$ $\dfrac{A}{\circ A}$

temporal induction

$$A \wedge \Box(A \rightarrow \circ A) \rightarrow \Box A$$

$$0 \models A \wedge \Box(A \rightarrow \circ A) \rightarrow \Box A$$

$$\Longleftrightarrow$$

$$(0 \models A \ \& \ \forall n (n \models A \Rightarrow n+1 \models A)) \Rightarrow \forall n \ (n \models A)$$

Let $\alpha(x)$ be the property $x \models A$

$$0 \models A \wedge \Box(A \rightarrow \circ A) \rightarrow \Box A$$

$$\Longleftrightarrow$$

$$(\alpha(0) \ \& \ \forall n (\alpha(n) \Rightarrow \alpha(n+1))) \Rightarrow \forall n \ (\alpha(n))$$

$$k \models A \wedge \Box(A \rightarrow \circ A) \rightarrow \Box A$$

$$\Longleftrightarrow$$

$$(\alpha(k) \ \& \ \forall n \geq k (\alpha(n) \Rightarrow \alpha(n+1))) \Rightarrow \forall n \geq k \ (\alpha(n))$$

SOUNDNESS

$$\vdash A \;\Rightarrow\; \models A$$

(A simple induction on derivations: exercise)

COMPLETENESS

$$\models A \;\Rightarrow\; \vdash A$$

Difficult: the canonical kripke model is not a temporal model

BRANCHING TIME

INTUITIVE IDEA: TREES/GRAPHS instead of COMPUTATIONS

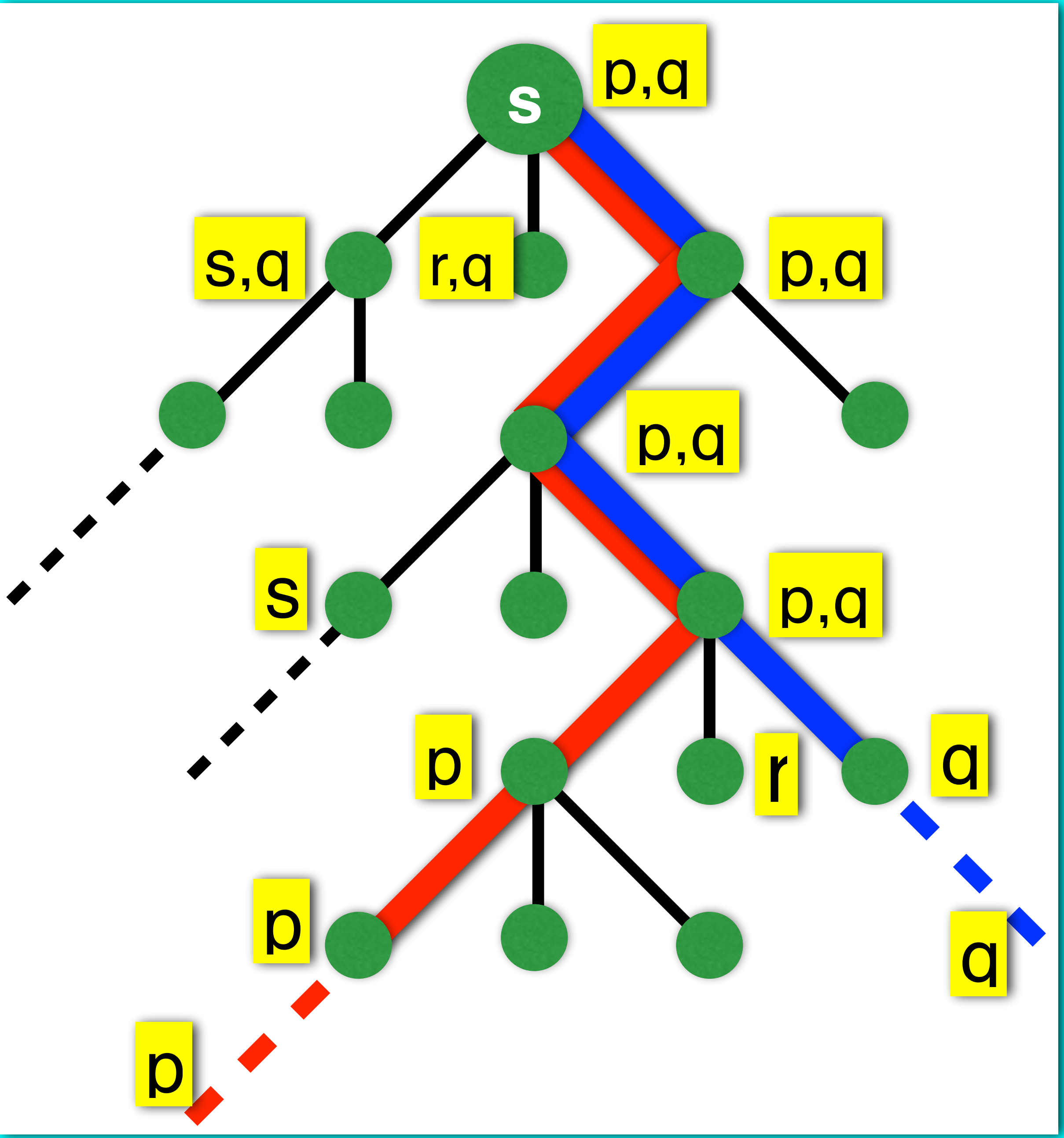
∀◯ =for each next time; ∃◯= there exists a next time such that

∀□= for each computation and for each state in it

∀◇= for each computation there exists a state in it such that

∃□= there exists a computation such that for each state in it

∃◇=there exists a computation and a state in it such that



$s \models \forall\bigcirc\, q$

$s \models \exists\bigcirc\, s \wedge \exists\bigcirc p$

$s \models \exists\Box\, p$

$s \models \exists\Box\, q$

$s \models \exists\Diamond\, r$

$s \models \exists\Diamond\, (s \wedge \neg q)$

language of UB

alphabet:

(i) proposition symbols : $p_0, p_1, p_2, \ldots,$

(ii) connectives : $\to, \perp$

(iii) modal operator $\forall\bigcirc, \forall\Box, \forall\Diamond$

(iv) auxiliary symbols : (,).

$AT = \{p_0, p_1, p_2, \ldots,\} \cup \{\perp\}$

The set WFF of (modal) formulas is the smallest set X with the properties

(i) $p_i \in X$ $(i \in N)$, $\perp \in X$,

(ii) $A, B \in X \Rightarrow (A \to B) \in X$,

(iii) $A \in X \Rightarrow (\neg A) \in X$

(iv) $A \in X \Rightarrow (\forall\Diamond A), (\forall\Box A), (\forall\bigcirc A) \in X$

abbreviations:

$\exists\Box A := \neg\forall\Diamond\neg A$

$\exists\Diamond A := \neg\forall\Box\neg A$

$\exists\bigcirc A := \neg\forall\bigcirc\neg A$

Semantics

an (UB-)frame is a graph

$$\langle S,N \rangle$$

where $N \subseteq S \mathrm{x} S$ is total ($\forall s \exists s' \; sNs'$)

An s-branch/s-computation is a sequence $b_s=(s_i)_{i<\omega}$ s.t. $s=s_0$ & $\forall\ i \in \mathbb{N}\ s_i N s_{i+1}$

if $b_s=(s_i)_{i<\omega}$ with $b_s[k]$ we denote s_k and with $s' \in b_s$ we mean that $\exists k$ s.t. $s'= b_s[k]$

an (UB-)model is a pair

$$\langle F,V \rangle$$

where F is a frame

and $V:S \rightarrow 2^{Prop}$

is a valuation

Let $M = \langle S,N,V \rangle$ a model,

the satisfiability relation $M \models \subseteq S \times WFF$

is defined as

1. $M, s \not\models \bot$
2. $M, s \models p$ iff $p \in V(s)$
3. $M, s \models A \wedge B \Leftrightarrow M,s \models A \;\&\; M,s \models B$
4. $M, s \models A \vee B \Leftrightarrow M,s \models A$ OR $M,s \models B$
5. $M,s \models \neg A \Leftrightarrow M,s \not\models A$,
6. $M,s \models A \rightarrow B \Leftrightarrow (M,s \models A \Rightarrow M,s \models B)$,
7. $M,s \models \forall\Box A \Leftrightarrow \forall b_s \forall s' \in b_s \; M,s' \models A$
8. $M,s \models \forall\Diamond A \Leftrightarrow \forall b_s \exists s' \in b_s \; M,s' \models A$
9. $M,s \models \exists\Box A \Leftrightarrow \exists b_s \forall s' \in b_s \; M,s' \models A$
10. $M,s \models \exists\Diamond A \Leftrightarrow \exists b_s \exists s' \in b_s \; M,s' \models A$
11. $M,s \models \forall\bigcirc A \Leftrightarrow \forall s' \,(sNs' \Rightarrow M,s' \models A)$
12. $M,s \models \exists\bigcirc A \Leftrightarrow \exists s' \,(sNs' \;\&\; M,s' \models A)$

AXIOMATIZATION ($\mathcal{U}$-free fragment)

A0 All temporal instances of propositional classical tautologies.

- (*A1*) $\forall\Box(A\to B)\supset(\forall\Box A\to\forall\Box B)$
- (*A2*) $\forall\bigcirc(A\to B)\supset(\forall\bigcirc A\to\forall\bigcirc B)$
- (*A3*) $\forall\Box A\to(\forall\Box A\wedge\forall\bigcirc\forall\Box A)$
- (*A4*) $A\wedge\forall\Box(A\to\forall\bigcirc A)\to\forall\Box A)$
- (*E1*) $\forall\Box(A\to B)\supset(\exists\Box A\to\exists\Box B)$
- (*E2*) $\exists\Box A\to(A\wedge\exists\bigcirc\exists\Box A)$
- (*E3*) $\forall\Box A\to\exists\Box A$
- (*E4*) $A\wedge\forall\Box(A\to\exists\bigcirc A)\to\exists\Box A$

$$\text{MP}\ \frac{A\quad A\to B}{B}$$

$$\text{Gen}\ \frac{A}{\forall\Box A}$$

SOUNDNESS

$$\vdash A \;\Rightarrow\; \models A$$

(A simple induction on derivations: exercise)

COMPLETENESS

$$\models A \;\Rightarrow\; \vdash A$$

Difficult: the canonical kripke model is not an UB-model

The Logic CTL

CTL= UB+$\mathcal{U}$*ntil*

language of CTL

alphabet:

(i) proposition symbols : $p_0, p_1, p_2, \ldots,$

(ii) connectives : $\rightarrow, \perp$

(iii) modal operator $\forall\bigcirc, \forall\mathcal{U}, \exists\mathcal{U}$

(iv) auxiliary symbols : (,).

$AT = \{p_0, p_1, p_2, \ldots,\} \cup \{\perp\}$

The set WFF of (modal) formulas is the smallest set X with the properties

(i) $p_i \in X$ $(i \in N)$, $\perp \in X$,

(ii) $A, B \in X \Rightarrow (A \rightarrow B) \in X$,

(iii) $A \in X \Rightarrow (\neg A) \in X$

(iv) $A, B \in X \Rightarrow (\forall\bigcirc A), (A \forall\mathcal{U} B) \in X$

abbreviations:

$\exists\bigcirc A = \neg\forall\bigcirc\neg A$

$\exists\Box A = \neg\forall\Diamond\neg A$ $\quad \forall\Box A = \neg\exists\Diamond\neg A$ $\quad \exists\Diamond\alpha \equiv true\ \exists\mathcal{U}\ A$ $\quad \forall\Diamond A \equiv true\ \forall\mathcal{U}\ A$

NOTATION: if $b_s=(s_i)_{i<\omega}$ with $b_s[k]$ we denote s_k

$M,s \models B\ \exists\mathcal{U}\ A$

$\Leftrightarrow$

$\exists b_s\ \exists k\ (\ M,b_s[k] \models A\ \&\ \forall j\in[0,k-1]\ b_s[j] \models B$

$M,s \models B\ \forall\mathcal{U}\ A$

$\Leftrightarrow$

$\forall b_s\ \exists k\ (\ M,b_s[k] \models A\ \&\ \forall j\in[0,k-1]\ b_s[j] \models B$

in order to axiomatize CTL we add to the axioms od UB the following

$$\forall\Box(C\rightarrow(\neg B\wedge(A\rightarrow\forall\bigcirc C))\rightarrow(C\rightarrow\neg(A\exists\mathcal{U}B))$$

$$\forall\Box(C\rightarrow(\neg B\wedge\exists\bigcirc C))\rightarrow(C\rightarrow\neg(A\forall\mathcal{U}B))$$

SOUNDNESS

$$\vdash A \;\Rightarrow\; \models A$$

(A simple induction on derivations: exercise)

COMPLETENESS

$$\models A \;\Rightarrow\; \vdash A$$

Difficult: the canonical kripke model is not CTL-model

Model Checking

Given a model M and a formula A

$M \models A$?

model checking is important for verification of properties of concurrent and distribute systems.
M represent the computational space and A the property to be verified

Theorem
The model checking problem for CTL is in deterministic polynomial time

Theorem
The model checking problem for LTL is PSPACE-complete