Tomorrow and Always, Locally and globally, knowledge and common knowledge... and EXPTIME!

François Schwarzentruber

Chapter 1

Introduction

In this course we will define important modal logics where we consider both a relation and its transitive and reflexive closure.

For instance with CTL, we can express things happening tomorrow ($\exists X$, $\forall X$) and what is happening in the future ($\exists F, \forall F, \exists G, \forall G$).

We will define several logics that have the same behaviour and speak about many domains: program verification, logical reasoning, economy, philosophy... We will prove EXPTIME-hardness of those logics (by introducing alternating Turing machine). We finally prove EXPTIME-ness by considering an axiomation of those logics, filter the canonical model and see that we can construct a filtrated version of the canonical model deterministically in exponential time! Waouh!

Chapter 2

A museum of logic with a relation and its transitive closure

We will see three applications of logics with a relation and its transitive closure:

- a general notion in modal logic: global consequence (modal logic in general)
- Propositional Dynamic Logic (program verification)
- Common knowledge (economy, philosophy)

2.1 Global consequence in K

We have seen:

$\Sigma \models \varphi$ is by definition for all pointed model $\mathcal{M}, w$ of $\mathcal{C}$, we have $\mathcal{M}, w \models \Sigma$ implies $\mathcal{M}, w \models \varphi$.

[p. 32, Blackburn] We define $\mathcal{M}, \varphi$ iff for all $w \in W$, $\mathcal{M}, w \models \varphi$.

We define also $\Sigma \models_{\mathcal{C}}^{global} \varphi$ is by definition for all models $\mathcal{M}$ of $\mathcal{C}$, we have $(\mathcal{M} \models \Sigma)$ implies $(\mathcal{M}, \models \Sigma)$.

Example 1 *We do not have* $p \models \Box p$

We have $p \models^{global} \Box p$

Remark 1 *We have those following facts:*

- $\Sigma \models^{global} \varphi$ *iff* $\{\Box^n \psi, n \in \mathbb{N}, \psi \in \Sigma\} \models \varphi$*;*
- $\Sigma \models_{S4}^{global} \varphi$ *iff* $\{\Box \psi, \psi \in \Sigma\} \models \varphi$

2.2 Propositional Dynamic logic

2.2.1 History

- Pratt's idea: associer à chaque programme π une modalité $[\pi]$ et $[\pi]\varphi$ signifie 'une fois le programme π terminé, φ est vrai'.
- PDL defined by Fischer and Ladner (1979)

2.2.2 Application: abstraction of Dynamic logic

$$[\pi]\varphi$$

prover Key

2.2.3 Syntax

Definition 1 ()

$$\varphi ::= p \mid \neg\varphi \mid \varphi \vee \varphi[\pi]\varphi$$

$$\pi ::= a \mid \pi \cup \pi \mid \pi^* \mid \varphi? \mid \pi;\pi$$

2.2.4 Standard models

Definition 2 ()
A Kripke model $\mathcal{M} = (W, (R_\pi)_{\pi \in PROG}, V)$ is said to be a standard model of PDL iff:

- $R_{\psi?} = \{(w, w) \mid \mathcal{M}, w \models \psi\}$;
- $R_{\pi_1;\pi_2} = R_{\pi_1} \circ R_{\pi_2}$;
- $R_{\pi_1 \cup \pi_2} = R_{\pi_1} \cup R_{\pi_2}$;
- $R_{\pi *} = (R_\pi)*$.

Definition 3 ()
$\mathcal{M}, w \models [\pi]\varphi$ iff for all $u \in R_\pi(w)$ we have $\mathcal{M}, u \models \varphi$

Branching Contrary to K and S4, in PDL we can enforce a branch of the model to be exponential.

Example 2 $(x = k)[x := x + 1](x = k + 1)...$

- $[a*] \bigvee_{i=1}^{n} \Big(\neg p_i \wedge \bigwedge_{j=i+1}^{n} p_j \rightarrow [a](\bigwedge_{j=i+1}^{n} \neg p_j) \wedge p_i \wedge (\bigwedge_{j=1}^{i-1} (p_j \rightarrow [a]p_j) \wedge (\neg p_j \rightarrow [a]\neg p_j) \Big)$
- $\bigwedge_{j=1}^{n} \neg p_j$
- $[a*]\langle a \rangle \top$

enforces to have a branch of exponential length.

2.3 Common knowledge

2.3.1 Syntax

Let AGT a set of agents.

$$\varphi ::= p \mid \neg\varphi \mid \varphi \vee \varphi \mid K_j\varphi \mid CK_J\varphi$$

where $j \in AGT$ and $J \in 2^{AGT}$.

2.3.2 Semantics

Definition 4 ()
Let $\mathcal{M} = (W, R, V)$ a Kripke model.

- $\mathcal{M}, w \models K_j\varphi$ iff for all $u \in R_j(w)$, we have $\mathcal{M}, u \models \varphi$;
- $\mathcal{M}, w \models CK_J\varphi$ iff for all $u \in (\cup_{j \in J} R_j))*$, we have $\mathcal{M}, u \models \varphi$.

Chapter 3

EXPTIME-hard

3.1 Alternating Turing machine

3.1.1 Definitions

[Papadimitriou for non-deterministic machine, p.45] [Alternation p. 100]

Definition 5 ()
An alternating Turing machine is a triple $M = (Q, U, \delta, s)$ where:

- Q is a finite set of states;
- $U \subseteq Q$ the set of universal states (other states are existential);
- $\delta \subseteq (Q \times \Sigma) \times ((Q \cup \{no, yes\}) \times \Sigma \times \{-1, 0, 1\}$ is a transition relation;
- $s \in Q$ is the initial state;

[la déf de Papadimitriou est trop lourde je trouve]

Definition 6 ()
A configuration is a triple (q, k, w) where q is a state, k a positive integer and w a finite word.

Definition 7 ()
$(q, k, w) \rightarrow (q', k', w')$ iff there exists $((q, \sigma), (q', \rho, dir)) \in \delta$ such that:

- $w[k] = \sigma$;
- $w' = w$ except $w'[k] = \rho$;
- $k' = k + dir$;
- $k' \geq 0$.

We note $\mathcal{C}$ the set of configurations of TM M.

3.1.2 Computation

Definition 8 ()
The computation (tree) of an alternating machine M on input x is (possibly infinite tree) where the nodes correspond to TM configurations and children of a node c are the configuration c' such that $c \to c'$. Formally, we can see a computation T as a map from $\{0 \dots\}*$ in $\mathcal{C}$.

Definition 9 ()
A labeling $L : \{0 \dots\}* \to \{0, 1\}$ of T is said to be acceptable if:

- $L(i) = 1$ if $T(i)$ is an accepting configuration;
- $L(i) = \bigvee_{i.n} L(i.n)$ if $T(i)$ is a non accepting existential configuration;
- $L(i) = \bigwedge_{i.n} L(i.n)$ if $T(i)$ is a non accepting universal configuration.

Remark 2 *There is a unique acceptable labelings on finite computation trees.*

[alternation, p. 100]

Definition 10 ()
M accepts x iff $L(\epsilon) = 1$ for all labeling L that labels the computation tree where the root is the initial configuration with x on the tape.

Definition 11 ()
M accepts L iff M accepts x for all $x \in L$.

[Alternation p. 100-101]

Definition 12 ()
M accepts L in time f iff M accepts L and for all $x \in \Sigma*$, the computation tree of M on input x is of depth at most $f(|x|)$.

Remark 3 *We may remove the condition that for rejecting worlds x the computation tree is of depth at most $f(|x|)$ for good functions f.*

Definition 13 ()
M accepts L in space f iff M accepts L and for all $x \in \Sigma*$, the computation tree of M on input x only contains configurations where the size of the tape is bounded by $f(|x|)$.

Definition 14 ()
AP = the class of langages L such that there exists a polynomial f such that L can be accepted by a ATM in time f.

Definition 15 ()
APSPACE = the class of langages L such that there exists a polynomial f such that L can be accepted by a ATM in space f.

3.2 Comparison of complexity classes

Theorem 1 *AP = PSPACE*

PROOF.

$\boxed{\subseteq}$ Let $L \in AP$. There exists an ATM M and a polynomial f such that M accepts L in time f. Let $x \in \Sigma*$. We simulate the execution of the ATM by performing a first-depth search in the computation tree of M, x in PSPACE. As the length of a branch is polynomial we only use a polynomial amount of memory for the backtrack process.

$\boxed{\supseteq}$ Let $L \in PSPACE$. Thus, as QBF is PSPACE-hard, there is a reduction f from L to QBF such that $x \in L$ iff $f(x) \in L$.

We design an alternating algorithm running in polynomial time that solves the QBF-SAT problem.

■

[Alternation, p. 102]

[Finite model theory and descriptive complexity, Grädel]

Theorem 2 $APSPACE = EXPTIME$

PROOF.

$\boxed{\subseteq}$

Let $L \in APSPACE$. It is accepted by an alternating Turing machine M using a polynomial amount of memory. Let f be this polynomial.

In order to see if $x \in L$. We compute the graph $G = (V, E)$ where:

- V is the set of all configurations of the machine M where the length of the tape $f(|x|)$.
- E is the set of edges (c, c') such that $c \rightarrow c'$.

We then decide for each configuration $c \in G$ whether c is accepting or refusing by the following algorithm:

```
ACC := the set of all configurations in state yes
pendantQue ACC changes
|     for c ∈ G
|     |     if c is existential and there exists c' such that c → c' and c' ∈ ACC
|     |     |     ACC.add(c')
|     |     endIf
|     |     if c is universal and for all c' such that c → c' we have c' ∈ ACC
|     |     |     ACC.add(c')
|     |     endIf
|     endFor
finPendantQue
```

The algorithm is a deterministic algorithm running in exponential time. The initial configuration where x is written in the tape is in ACC iff $x \in L$.

$\boxed{\supseteq}$

Let L be accepted by a Turing machine M in exponential time. Let f be the polynomial such that the computation of x on M is of length $2^{f(|x|)}$.

By abuse of notation, we suppose that the tape also contains the information of the state and the position of the cursor (as usual). For instance the tape at the initial configuration is:

(s, x_0)	x_1	x_2	...
$x[0]$	$x[1]$	$x[2]$	...

From δ we can create a function μ that takes 3 characters (α, β, γ) and returns what is written at the place of b.

α	β	γ	
	$\Downarrow$		...
	$\mu(\alpha, \beta, \gamma)$		

Here is an alternating algorithm running in polynomial space accepting L:

//returns 'yes' iff the k^{th}-cell of the tape contains c at time t of the execution of M on x.
function tape(t, k, c)
  if $t = 0$
    if $x[k] = c$ **accept else reject**
  else
    choose $(\exists) c'_{k-1}, c'_k, c'_{k+1}$
    if $\mu(c'_{k-1}, c'_k, c'_{k+1}) \neq c$ **reject**
    choose $(\forall) j \in \{k-1, k, k+1\}$
    tape$(t-1, j, c'_j)$
  endIf
endFunction

function acceptL(x)
  choose $(\exists) t \in \{1 \dots 2^{f(|x|)}\}$
  choose $(\exists) k \in \{1 \dots 2^{f(|x|)}\}$
  choose a character (c, ok).
  tape$(t, k, (c, ok))$
endFunction

We have to prove by induction that tape(t, k, c) succeeds iff the execution of M on the input x is such that at time t, the k^{th} cell of the tape contains c.

■

3.2.1 An EXPTIME-hard problem

[Blackburn, p. 395] utilise la preuve avec le TWO PERSON CORRIDOR PROBLEM... mais je n'ai pas la preuve que c'est EXPTIME-hard... l'encodage du début du cours ne marche pas

[Dynamic logic, p. 217] : ils font un encodage direct depuis la machine de Turing non déterministe

Theorem 3 *The satisfiability problem of PDL is EXPTIME-hard.*

Proof.

Let L be a APSPACE problem. Let M be an alternating Turing machine accepting L running in space f. We can suppose that the machine stops running after $2^{O(f(|x|))}$ steps.

We introduce the following propositions:

- c_i^a: the cell of the tape in the column i contains a a;
- s_i^q: the machine is currently scanning the column i and is in the state q
- s_i^ℓ means that the scanning cursor is at $j < i$;
- s_i^r means that the scanning cursor is at $j > i$;
- *accept* means that the current state is accepting.

We note $\delta(q, \sigma) = \{(q', \rho, dir) \mid ((q, \sigma), (q', \rho, dir)) \in \delta\}$.
Let us consider an input x for M. Let $n = f(|x|)$.
The machine M accepts x iff the following conjunction is satisfiable in PDL:

- $s_0^s \wedge \bigwedge_i c_i^{x_i}$
- $[\alpha^*] \bigwedge_{0 \leq i \leq n+1} \bigvee c_i^a$: a symbol everywhere
- $[\alpha^*] \bigwedge_{0 \leq i \leq n+1} \bigvee_{a \in \Sigma} (c_i^a \rightarrow \bigwedge_{b \in \Sigma, b \neq a} c_i^b)$: unicity of the symbol written on the tape
- the machine is always in a state (and the state is unique)
- $[\alpha^*] \bigwedge_i \bigwedge_{q \in Q \cup \{\ell\}} s_i^q \rightarrow s_{i+1}^\ell$;
- $[\alpha^*] \bigwedge_i \bigwedge_{q \in Q \cup \{\ell\}} s_i^q \rightarrow s_{i-1}^r$;
- $[\alpha^*](\bigwedge_i (s_i^\ell \vee s_i^r \rightarrow (\bigwedge_a c_i^a \rightarrow [\alpha] c_i^a)$;

- $[\alpha^*] \bigwedge_i \bigwedge_{a \in \Sigma, q \in Q} s_i^q \wedge c_i^a \rightarrow (\bigwedge_{(q',\rho,dir) \in \delta(q,\sigma)} \langle \alpha \rangle (c_i^\rho \wedge s_{i+dir}^{q'})$
  $[\alpha](\bigvee_{(q',\rho,dir) \in \delta(q,\sigma)} (c_i^\rho \wedge s_{i+dir}^{q'})$
  All transitions are represented... and only transitions!
- $accept$
- $[\alpha^*] \bigwedge_i \bigwedge_{q \text{ existential}} s_i^q \rightarrow (accept \leftrightarrow \langle \alpha \rangle accept)$
- $[\alpha^*] \bigwedge_i \bigwedge_{q \text{ universal}} s_i^q \rightarrow (accept \leftrightarrow [\alpha] accept)$
- $count = 0$
- $[\alpha^*](count = i) \rightarrow (count = i + 1)$
- $[\alpha^*](count = c^n - 1) \rightarrow [\alpha] \neg accept$

where c is big enough.

■

Chapter 4

Axiomatization

4.1 Compacity

Proposition 1 *Logic K is compact, that is for all set of formulas Σ, Σ is satisfiable iff for all finite $\Sigma' \subseteq \Sigma$, we have Σ' is satisfiable.*

Or Σ is unsatisfiable iff there exists $\Sigma' \subseteq \Sigma$ such that Σ' is unsatisfiable.

Proof.

Comes from the strong completness.

Σ unsat implies $\Sigma \models \bot$ implies $\Sigma \vdash \bot$ implies there exists $\Sigma' \subseteq \Sigma$ such that $\Sigma' \vdash \bot$ implies there exists $\Sigma' \subseteq \Sigma$ such that $\Sigma' \models \bot$ implies there exists $\Sigma' \subseteq \Sigma$ such that Σ' unsatisfiable. ■

Proposition 2 *PDL is not compact. That is we can find Σ unsatisfiable but every finite subset $\Sigma' \subseteq \Sigma$ is satisfiable.*

Proof.

$\Sigma = \{[a^n]p, n \in \mathbb{N}\} \cup \{\langle a^* \rangle \neg p\}$

■

4.2 Nonstandard models

[Dynamic logic, p. 199]

Definition 16 ()
A Kripke model $\mathcal{M} = (W, (R_\pi)_{\pi \in PROG}, V)$ is said to be a non-standard model of PDL iff:

- $R_{\psi?} = \{(w, w) \mid \mathcal{M}, w \models \psi\}$;

- $R_{\pi_1;\pi_2} = R_{\pi_1} \circ R_{\pi_2}$;
- $R_{\pi_1 \cup \pi_2} = R_{\pi_1} \cup R_{\pi_2}$;
- $R_{\pi *}$ is a reflexive, transitive relation containing $(R_\pi)*$;
- for all $w \in W$, for all φ, for all π, $\mathcal{M}, w \models (\varphi \wedge [\pi][\pi*]\varphi) \leftrightarrow [\pi*]\varphi$;
- for all $w \in W$, for all φ, for all π, $\mathcal{M}, w \models \varphi \wedge [\pi*](\varphi \rightarrow [\pi]\varphi) \rightarrow [\pi*]\varphi$.

Example 3 $\mathbb{N} \cup \{+\infty\}$ *where* a *is interpreted as the successor function* S *and* $a*$ *as* $\leq$ *and* p *is true everwhere is a nonstandard model.*

Example 4 $\mathbb{N} \cup \{+\infty\}$ *where* a *is interpreted as the successor function* S *and* $a*$ *as* $\leq$ *and* p *is true over* $\mathbb{N}$ *and not over* $+\infty$ *is NOT a nonstandard model.*

4.3 Filtration

4.3.1 Fischer-Ladner closure

To prove decidability, we can proceed by filtration. But filter by the set of subformulas does not work.

Example 5 *If we filter*

$$\bullet([a^2]\neg p, p) \rightarrow^a \bullet([a^2]\neg p, p)$$

by the set of subformulas of $[a^2]\neg p$ *we obtain:*

$$\bullet([a^2]\neg p, p) loop^a$$

[Dynamic logic, Harel, Kozen, Tiuryn]

Definition 17 ()
We define FL and $FL^\Box$ by induction:

- $FL(p) = \{p\}$;
- $FL(\varphi \vee \psi) = \{\varphi \vee \psi\} \cup FL(\varphi) \cup FL(\psi)$;
- $FL(\neg\varphi) = \{\neg\varphi\} \cup FL(\varphi)$;
- $FL([\pi]\varphi) = FL^\Box([\pi]\varphi) \cup FL(\varphi)$.
- $FL^\Box([a]\varphi) = \{[a]\varphi\}$;

- $FL^{\Box}([\pi_1 \cup \pi_2]\varphi) = \{[\pi_1 \cup \pi_2\varphi\} \cup FL^{\Box}([\pi_1]\varphi) \cup FL^{\Box}([\pi_2]\varphi)$;
- $FL^{\Box}([\pi_1; \pi_2]\varphi) = \{[\pi_1; \pi_2]\varphi\} \cup FL^{\Box}([\pi_1][\pi_2]\varphi) \cup FL^{\Box}([\pi_2]\varphi)$;
- $FL^{\Box}([\pi*]\varphi) = \{[\pi*]\varphi\} \cup FL^{\Box}([\pi][\pi*]\varphi)$
- $FL^{\Box}([\psi?]\varphi) = \{[\psi?]\varphi\} \cup FL(\psi)$.

Proposition 3 • *For any formula* φ, $\mathrm{card}(FL(\varphi)) \leq |\varphi|$;

- *For any formula* $[\pi]\varphi$, $\mathrm{card}(FL^{\Box}([\pi]\varphi)) \leq |\pi|$.

PROOF.
Double induction. [Dynamic logic, p.194] ■

4.3.2 Filtered model

[p. 196]
Given a nonstandard model $\mathcal{M} = (W, R, V)$ we define the filtrated standard model $\mathcal{M}_{/FL(\varphi)} = (W_{/FL(\varphi)}, R_{/FL(\varphi)}, V_{/FL(\varphi)})$ where:

- $W_{/FL(\varphi)} = \{[w] \mid w \in W\}$ where $[w]$ denotes the class of w according to the equivalence relation $w \equiv u$ iff for all $\psi \in FL(\varphi)$, $(\mathcal{M}, w \models \varphi$ iff $\mathcal{M}, u \models \varphi)$;
- $R_{/FL(\varphi)_a} = \{([w], [u]) \mid (w, u) \in R_a\}$ for all atomic program a;
- for all complex programs π, $R_{/FL(\varphi)_\pi}$ is defined as in a standard model;
- $V_{/FL(\varphi)}(p) = \{[u], u \in V(p)\}$.

[p. 196 and p. 200]

Proposition 4 *Let* $\mathcal{M}$ *be a nonstandard Kripke model and* w, u *two worlds.*

1. *For all* $\psi \in FL(\varphi)$, $\mathcal{M}, w \models \psi$ *iff* $\mathcal{M}_{/FL(\varphi)}, [w] \models \psi$;
2. *For all* $[\pi]\varphi \in FL(\varphi)$,
   (a) *if* $wR_\pi u$ *then* $[w]R_{/FL(\varphi)_\pi}[u]$;
   (b) *if* $[w]R_{/FL(\varphi)_\pi}[u]$ *and* $\mathcal{M}, w \models [\pi]\psi$ *then* $\mathcal{M}, u \models \psi$.

PROOF.
Induction on the well-founded subexpression relation.
1.
$\boxed{[\pi]\psi}$

$\mathcal{M}, w \models [\pi]\psi$ implies for all $[u] \in R_\pi([w])$, $\mathcal{M}, u \models \psi$ by 2. (b)
implies for all $[u] \in R_\pi([w])$, $\mathcal{M}_{/FL(\varphi)}, [u] \models \psi$ by 1.
equivalent to $\mathcal{M}_{/FL(\varphi)}, [w] \models [\pi]\psi$

$\mathcal{M}_{/FL(\varphi)}, [w] \models [\pi]\psi$ equivalent to for all $[u] \in R_\pi([w])$, $\mathcal{M}_{/FL(\varphi)}, [u] \models \psi$
for all $u \in R_\pi(w)$, $\mathcal{M}_{/FL(\varphi)}, [u] \models \psi$ by 2. (a)
for all $u \in R_\pi(w)$, $\mathcal{M}, u \models \psi$ by 1.
$\mathcal{M}, w \models [\pi]\psi$.

2. (a)
$\boxed{[\pi*]\psi}$
[Dynamic logic p. 201]

Remark 4 *$\mathcal{M}$ is nonstandard: $R_{\pi*}$ contains but is not the reflexive and transitive closure of R_π.*

$\mathcal{M}_{/FL(\varphi)}$ is standard by definition: $R_{/FL(\varphi)_{\pi*}}$ has been defined as the reflexive and transitive closure of $R_{/FL(\varphi)_\pi}$.

Suppose that $uR_{\pi*}v$. And let us prove that $[u]R_{/FL(\varphi)_{\pi*}}[v]$, or equivalently that $v \in E$ where

$$E = \{t \in W \mid [u]R_{/FL(\varphi)_{\pi*}}[t]\}.$$

There is a PDL formula ψ_E defining E in $\mathcal{M}$, i.e. $E = \{t \in W \mid \mathcal{M}, t \models \psi_E\}$. Indeed, E is the union of equivalence classes defined by truth assignments to the elements of $Fl(\varphi)$ and:

$$\psi_E = \bigvee_{[t]|t\in E} \bigwedge_{\psi\in FL(\varphi)|\mathcal{M},t\models\psi} \psi \wedge \bigwedge_{\psi\in FL(\varphi)|\mathcal{M},t\not\models\psi} \neg\psi.$$

Remark that $w \in E$ and $wR_\pi u$ implies $u \in E$ (hyp ind 2.a).
For all worlds $x \in W$, we have:
$\mathcal{M}, x \models \psi_E \rightarrow [\pi]\psi_E$.
Hence for all worlds $w \in W$, $\mathcal{M}, w \models [\pi*](\psi_E \rightarrow [\pi]\psi_E)$.
As $\mathcal{M}$ is a non-standard model, the last condition of the definition of a non-standard model gives $\mathcal{M}, w \models \psi_E \wedge [\pi*](\psi_E \rightarrow [\pi]\psi_E) \rightarrow [\pi*]\psi_E$. we then have $\mathcal{M}, w \models \psi_E \rightarrow [\pi*]\psi_E$ (*).
As $u \in E$ we have $\mathcal{M}, u \models \psi_E$. By (*) we have $\mathcal{M}, u \models [\pi*]\psi_E$. As $uR_{\pi*}v$ we have $\mathcal{M}, v \models \psi_E$. So $v \in E$.
2. (b)
easy.
■
The thing to keep in mind:

Corollary 1 *If a formula φ is satisfiable in a non standard model $\mathcal{M}, w$, then it is satisfiable in a standard one (for instance $\mathcal{M}_{/FL(\varphi)}, |w|$)*

4.4 Axiomatization

4.4.1 Axioms

[p. 203]

- axioms for propositional logic
- $K([\pi])$;
- $[\pi_1 \cup \pi_2]\varphi \leftrightarrow [\pi_1]\varphi \wedge [\pi_2]\varphi$;
- $[\pi_1; \pi_2]\varphi \leftrightarrow [\pi_1][\pi_2]\varphi$;
- $[\psi?]\varphi \leftrightarrow (\psi \rightarrow \varphi)$;
- $[\pi*]\varphi \leftrightarrow (\varphi \wedge [\pi][\pi*]\varphi)$;
- $\varphi \wedge [\pi*](\varphi \wedge [\pi]\varphi) \rightarrow [\pi*]\varphi$.

+ MP and necessitation

Question 1 *Why are the last axioms important? What is going on if we drop them?*

Theorem 4 (Soundness of PDL) $\vdash \varphi$ *implies* $\models \varphi$.

4.4.2 Completness of the axiomatization

[Dynamic logic, p. 205]

Lemma 1 (Lindenbaum's lemma) *For all Σ' consistent, there exists Σ maximal consistent such that $\Sigma' \subseteq \Sigma$.*

Definition 18 ()
The canonical model $\mathcal{M} = (W, R, V)$ is defined as follows:

- W is the set of maximal consistent sets of formulas of PDL;
- $wR_\pi v$ iff for all ψ, if $[\pi]\psi \in w$ then $\psi \in v$.
- $V(p) = \{w \in W \mid p \in w\}$.

Lemma 2 (Truth lemma) $\mathcal{M}, w \models \varphi$ *iff* $\varphi \in w$.

Theorem 5 *The canonical model is a nonstandard Kripke model.*

Theorem 6 (Completeness of PDL) $\vdash \varphi$ *iff* $\models \varphi$.

PROOF.

We are going to prove that $\nvdash \varphi$ implies $\not\models \varphi$.

Let φ such that $\nvdash \varphi$. Then $\{\neg\varphi\}$ is consistent. (Indeed, if not, we would have $\vdash \neg\varphi \rightarrow \bot$, hence $\vdash \varphi$.) According to the Lindenbaum's lemma, we can find a mcs w such that $\{\neg\varphi\} \subseteq w$. According to Truth lemma, we have $\mathcal{M}, w \models \neg\varphi$.

Hence $\mathcal{M}_{/FL(\varphi)}, w \models \neg\varphi$.

Hence $\not\models \varphi$.

■

Chapter 5

Satisfiability problem in EXPTIME

Let $\neg FL(\varphi) = FL(\varphi) \cup \{\neg\psi \mid \psi \in FL(\varphi)\}$.

A Hintikka set $w \subseteq \neg FL(\varphi)$ is a set where for all $\psi \in FL(\varphi)$, exactly one of ψ or $\neg\psi$ is in w, and that is satisfying the following condition:

- if $[\pi_1;\pi_2]\varphi \in w$ then $[\pi_1][\pi_2]\varphi \in w$;
- if $[\pi_1 \cup \pi_2]\varphi \in w$ then $[\pi_1]\varphi \in w$ or $[\pi_2]\varphi \in w$;
- if $[\pi*]\varphi \in w$ then $\psi \in w$ and $[\pi][\pi*]\varphi \in w$;
- if $[\psi?]\varphi \in w$ then (if $\psi \in w$ then $\varphi \in w$);
- if $\varphi \wedge \psi \in w$ then $\varphi, \psi \in w$;
- if $\neg(\varphi \wedge \psi) \in w$ then $\neg\varphi \in w$ or $\neg\psi \in w$.

Let $\mathcal{M} = (W, R, V)$ the canonical model filtrated by $FL(\varphi)$. There is a one-to-one correspondance between an equivalence class $[s] \in W$ and the set $s \cap \neg FL(\varphi)$.

Proposition 5 *uR_av iff for all $[a]\psi \in FL(\varphi)$, we have $[a]\psi \in u$ implies $\psi \in v$.*

Proof.

Suppose that uR_av.

■

A world $w \in W_n$ is happy for $[\pi]\psi \in FL(\varphi)$ in $\mathcal{M}_n$ iff (for all $u \in R_{n\pi}(w)$ such that $\psi \in u$) implies $[\pi]\psi \in w$.

A world $w \in W_n$ is happy for Γ in $\mathcal{M}_n$ iff w is happy for all $[\pi]\psi \in \Gamma$ in $\mathcal{M}_n$. [Dynamic logic, p. 213]

function PDLsat(φ)
Construct $\mathcal{M}_0 = (W_0, R_{0a}, V_0)$:

- W_0 := the set of all Hintikka set over $FL(\varphi)$;
- $R_{0a} := \{(w,u) \in W_0^2 \mid$ for all $[a]\psi \in FL(\varphi)$, if $[a]\psi \in w$ then $\psi \in u\}$;
- $V_0(p) = \{w \in W_0 \mid p \in w\}$.

repeat
$w_{todelete} =?$
for $[\pi]\psi \in FL(\varphi)$, sorted by the length of $|\pi|$
for $w \in W_{i-1}$
if w is not happy with $[\pi]\psi$ in $\mathcal{M}_{i-1}$
$w_{todelete} = w$
break
endIf
endFor
Construct $\mathcal{M}_i = (W_i, R_{ia}, V_i)$:

- $W_i := W_{i-1} \setminus \{w_{todelete}\}$;
- $R_{ia} := \{(w,u) \in W^{i2} \mid$ for all $[a]\psi \in FL(\varphi)$, if $[a]\psi \in w$ then $\psi \in u\}$;
- $V_i(p) = \{w \in W_i \mid p \in w\}$.

until $w_{todelete} \neq?$
if there exists $w \in \mathcal{M}_{2|\varphi|}$ such that $\varphi \in w$
return yes
else
return no
endIf
endFunction

Proposition 6 $W \subseteq W_0$.

Proof.
A world of W is a Hintikka set. ■

Proposition 7 *Let $i > 0$ such that $W \subseteq W_i$. Let $\chi \in FL(\varphi)$ and $u \in W_i$ such that u is happy with $FL(\chi)$.*

1. *For all $\psi \in FL(\chi)$ and $u \in W_i$ we have $\psi \in u$ iff $\mathcal{M}_i, u \models \psi$;*
2. *For all $[\pi]\psi \in Fl(\chi)$ and $u, v \in W_i$,*

(a) if $uR_\pi v$ then $uR^i_\pi v$; (holds also if π is minimum)

(b) if $uR^i_\pi v$ and $[\pi]\psi \in u$ then $\psi \in v$.

PROOF.

1. By induction on ψ.

$\boxed{p}$

$p \in w$ iff $w \in V_i(p)$
iff $\mathcal{M}^i, w \models p$

$\boxed{[\pi]\psi}$

$[\pi]\psi \in w$ implies for all $v \in R^i_\pi(w)$, $\psi \in v$ (by inductive hypothesis 2.(b))
iff for all $v \in R^i_\pi(w)$, $\mathcal{M}^i, v \models \psi$ by inductive hypothesis 1.
iff $\mathcal{M}^i, w \models [\pi]\psi$ by truth condition.

$\mathcal{M}^i, w \models [\pi]\psi$ iff for all $v \in R^i_\pi(w)$, $\psi \in v$ (see above)
$[\pi]\psi \in w$ because $\mathcal{M}_i, w$ is happy for $[\pi]\psi \in w$

2. (a)
By induction on π.

$uR_a v$ iff for all $[a]\psi \in FL(\varphi)$, $[a]\psi \in u$ implies $\psi \in v$ (because $\mathcal{M}$ is the filtration of the canonical mod
$uR^i_a v$ (by definition of R^i_a)

Remark 5 *The case ψ? uses 1.*

2. (b) $\boxed{[a]\pi}$
$uR^i_a v$ and $[a]\psi \in u$ implies $\psi \in v$ by definition of $R^i_a v$.
$\boxed{[\pi*]\pi}$
Suppose that $uR^i_{\pi*} v$ and $[\pi*]\psi \in u$.
There exists $u = u_0 R^i \pi u_1 \ldots R^i \pi u_n = v$.
$[\pi*]\psi \in u_0$ hence $[\pi][\pi*]\psi \in u_0$. By induction hypothesis 2. (b), $[\pi*]\psi \in u_1$...
$[\pi*]\psi \in u_n$ hence $\psi \in u_n$.

Remark 6 *The case ψ? also uses 1.*

■

Proposition 8 *For all $i \geq 0$, $W \subseteq W_i$.*

PROOF.

By induction.

Basic case $i = 0$ is done.

Inductive case Suppose $W \subseteq W_i$ and let us prove that $W \subseteq W_{i+1}$.

Let $u \in W$. Suppose that u is deleted at step $i+1$.

It means that w is not happy with $[\pi]\psi$ in $\mathcal{M}_i$. I.e. the implication "(for all $u \in R^i{}_\pi(w)$ such that $\psi \in u$) implies $[\pi]\psi \in w$" is false. Let us prove that it is true.

The statement $(\forall v \in W_i\ (uR^i_\pi$ implies $\psi \in v))$ implies $(\forall v \in W, (uR_\pi v$ implies $\psi \in v)$ by Proposition 7.

It is equivalent to $(\forall v \in W, (uR_\pi v$ implies $\mathcal{M}, v \models \psi)$ because $\mathcal{M}$ is the filtrated model of the canonical model.

It is equivalent to $\mathcal{M}, u \models [\pi]\psi$ by truth conditions of $[\pi]$. It is equivalent to $[\pi]\psi \in u$.

So the implication "(for all $u \in R^i{}_\pi(w)$ such that $\psi \in u$) implies $[\pi]\psi \in w$" is true. Contradiction.

u is not deleted at step $i+1$ and thus $W \subseteq W_{i+1}$.

■

Proposition 9 *At the end, $\mathcal{M}^n = \mathcal{M}$.*

PROOF.

At the end, by Proposition 7, every $u \in W^n$ is satisfiable and is satisfied in the pointed model $\mathcal{M}^n, u$. Hence u can be extended as a mcs $\hat{u}$ in the canonical model. After filtration, $[\hat{u}] \in \mathcal{M}$. But $[\hat{u}] = u$. So $W_n \subseteq W$.

If $wR_a u$ then $wR^n_a u$. (2. (a) of Proposition 7.

If $uR^n_a v$ then for all $[a]\psi \in FL(\varphi)$, we have $[a]\psi \in u$ implies $\psi \in v$ (2. (b) of Proposition 7).

This is equivalent to $uR_a v$ because $\mathcal{M}$ is the filtration of the canonical model.

■

Theorem 7 *The algorithm succeeds on φ iff the formula φ is satisfiable.*

PROOF.

$\boxed{\Rightarrow}$ If it succeeds, the algorithm has constructed a model $\mathcal{M}^n$ satisfying φ. Hence φ is satisfiable.

$\boxed{\Leftarrow}$ If φ is satisfiable, it can be extended in a mcs u and hence is satisfiable in the canonical model. It is also satisfied in the filtrated model of the canonical model. The algorithm constructs the filtrated model of the canonical model hence it succeeds. ■