SAPIENZA
UNIVERSITÀ DI ROMA

"Sapienza" University of Rome
Faculty of Information Engineering,
Informatics and Statistics
Department of Computer Science

Mathematical Logic for Computer Science

Lecture notes integrated with the book TODO

Author
Alessio Bandiera

June 11, 2025

Contents

Information and Contacts

Personal notes and summaries collected as part of the *Mathematical Logic for Computer Science* course offered by the degree in Computer Science of the University of Rome "La Sapienza".

Further information and notes can be found at the following link:
https://github.com/aflaag-notes. Anyone can feel free to report inaccuracies, improvements or requests through the Issue system provided by GitHub itself or by contacting the author privately:

- Email: **alessio.bandiera02@gmail.com**
- LinkedIn: **Alessio Bandiera**

The notes are constantly being updated, so please check if the changes have already been made in the most recent version.

Suggested prerequisites:

TODO

Licence:

1 Homeworks

1.1 Homework 1

Exercise 1.4 Let $\mathcal{L} = \{E(x, y)\}$ be the language of graphs.

1. For each fixed $n \in \mathbb{N}$, write a sentence C_n such that for any graph $\mathcal{G}$, $\mathcal{G} \models C_n$ if and only if $\mathcal{G}$ contains a cycle of length n.
2. Prove using Compactness that the property of being *a cycle* is not expressible by a theory in $\mathcal{L}$ over the class of graphs.

Solution. Let $\mathcal{L} = \{E(x, y)\}$ be the language of graphs.

1. The property "$\mathcal{G}$ contains a cycle of length n" can be written as follows

$$C_n := \exists x_1 \dots \exists x_n \quad \left(\bigwedge_{\substack{1 \le i,j \le n \\ i \neq j}} \neg(x_i = x_j) \right) \wedge \left(\bigwedge_{1 \le i \le n-1} E(x_i, x_{i+1}) \wedge E(x_n, x_1) \right)$$

   In fact, the first conjunction implies that $x_1, \dots, x_n$ are *distinct*, and the second conjunction describes the existence of the n-long *cycle* itself.

2. Consider the property $P_n :=$ "$\mathcal{G}$ is *a cycle* of length n". This property can be expressed by *extending* C_n as follows:

$$\begin{aligned} V_n &:= \forall y \quad \bigvee_{1 \le j \le n} (y = x_j) \\ E_n &:= \bigwedge_{1 \le i \le n-1} \bigwedge_{\substack{1 \le j \le n: \\ j \neq i+1}} \neg E(x_i, x_j) \wedge \bigwedge_{2 \le j \le n} \neg E(x_n, x_j) \\ C'_n &:= \exists x_1 \dots \exists x_n \quad C_n \wedge V_n \wedge E_n \end{aligned}$$

   where we have that

   - V_n ensures that $\mathcal{G}$ has *exactly* n vertices
   - E_n ensures that the only edges present in $\mathcal{G}$ are the ones that describe the cycle graph of n vertices
   - C'_n describes our property P_n

   Now, consider the property $P :=$ "$\mathcal{G}$ is *a cycle*", and in particular $\neg P :=$ "$\mathcal{G}$ is not *a cycle*". We observe that we can build the following infinte theory

$$T^{\neg P} := \{\neg C'_n \mid n \in \mathbb{N}_{\ge 3}\}$$

   for which it is easy to see that

$$\mathcal{G} \models \neg P \iff \neg P(\mathcal{G}) \text{ holds}$$

   meaning that $\neg P$ is expressible through $T^{\neg P}$.

   Claim: $T^{\neg P} \in \mathsf{FINSAT}$.

   Proof of the Claim. Fix $T_0 \underset{fin}{\subseteq} T^{\neg P}$. We observe that $T_0 := \{\neg C'_{i_1}, \dots, \neg C'_{i_k}\}$

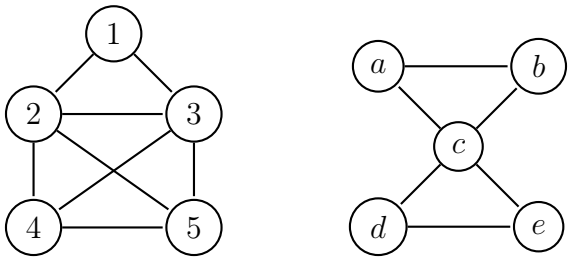
for some $i_1, \dots, i_k \in \mathbb{N}$. Now, if we consider $i^* := \max_{j \in [k]} i_j$, then the cycle graph that has $i^* + 1$ vertices is clearly a structure that satisfies T_0. □

Claim: P is not expressible by a theory in $\mathcal{L}$ over the class of graphs.

Proof of the Claim. By way of contradiction, suppose that P is expressible, i.e. there is a theory T^P for which P can be expressed. Then, consider the theory $T := T^P \cup T^{\neg P}$. By the previous claim, we have that $T \in \mathsf{FINSAT}$, and by Compactness this is true if and only if $T \in \mathsf{SAT}$. However, this is a contradiction, because a graph cannot be and not be a cycle at the same time. □

Finally, this last claim concludes the proof. □

Exercise 2.1 Consider the following two structures $\mathcal{G}_1$ and $\mathcal{G}_2$ for the languages of graphs:



Write at least two sentences distinguishing the two structures. Discuss the EF-game played on these structures: for what k can the Duplicator win the k-rounds game? For what k can the Spoiler win?

Solution. Some properties that can distinguish these two structures are the following:

1. "$\mathcal{G}$ contains a vertex of degree 3", which is represented by the following sentence of rank 5

$$\exists x_1 \exists x_2 \exists x_3 \exists x_4 \quad \left(\bigwedge_{\substack{1 \le i,j \le 4 \\ i \neq j}} \neg(x_i = x_j) \right) \wedge \left(\bigwedge_{2 \le i \le 4} E(x_1, x_i) \right) \wedge \left(\forall y \quad \neg E(x_1, y) \vee \bigvee_{2 \le j \le 4} (y = x_j) \right)$$

2. "$\mathcal{G}$ contains edges as $\mathcal{G}_1$", which is represented by the following sentence of rank 5

$$\begin{aligned} \exists x_1 \exists x_2 \exists x_3 \exists x_4 \exists x_5 \quad & E(x_1, x_2) \wedge E(x_1, x_3) \wedge \\ & E(x_2, x_3) \wedge E(x_2, x_4) \wedge E(x_2, x_5) \wedge \\ & E(x_3, x_4) \wedge E(x_4, x_5) \wedge \\ & E(x_4, x_5) \end{aligned}$$

   we observe that the edges of $\mathcal{G}_2$ are not sufficient to distinguish the two sentences, because $\mathcal{G}_2$ is a subgraph of $\mathcal{G}_1$

3. "$\mathcal{G}$ contains a cycle of length 5", which is represented by C_5 of the previous exercise, and has rank 5
4. "$\mathcal{G}$ contains a cycle of length 4", which is represented by C_4 of the previous exercise, and has rank 4
5. "$\mathcal{G}$ contains K_4 as subgraph", which is represented by the following sentence having rank 4

$$\exists x_1 \exists x_2 \exists x_3 \exists x_4 \quad \left(\bigwedge_{\substack{1 \leq i,j \leq 4 \\ i \neq j}} \neg(x_i = x_j) \right) \wedge \left(\bigwedge_{\substack{1 \leq i,j \leq 4 \\ i \neq j}} E(x_i, x_j) \right)$$

These sentences *may seem* to suggest that the two structures are 3-equivalent, meaning that there is no sentence of rank 3 that can distinguish $\mathcal{G}_1$ from $\mathcal{G}_2$. For now, let's focus on proving that they are *at least* 2-equivalent.

Claim: The Duplicator wins $G_2(\mathcal{G}_1, \mathcal{G}_2)$.

Proof of the Claim. Let s_i and d_i be the i-th nodes chosen by the Spoiler and the Duplicator, respectively. Then, we can define the following strategy for the Duplicator:

- if $s_1 \in \{1, 4, 5\}$, then the Duplicator chooses $d_1 \in \{a, b, d, e\}$, otherwise if $s_1 \in \{2, 3\}$ then $d_1 = c$
- similarly, if $s_1 \in \{a, b, d, e\}$, then the Duplicator chooses $d_1 \in \{1, 4, 5\}$, otherwise if $s_1 = c$ then $d_1 \in \{2, 3\}$

Then, no matter the choice of s_2, the Duplicator can always answer with a node d_2 that preserves the partial isomorphism, in fact:

- if $s_2 \sim s_1$, it is guaranteed that there is a vertex d_2 in the other structure such that $d_2 \sim d_1$ because $\delta(\mathcal{G}_1) = \delta(\mathcal{G}_2) = 2$ — and the same argument applies if $s_2 \sim d_1$ for finding a vertex $d_2 \sim s_1$
- if $s_2 \nsim s_1$, the strategy that we provided for the Duplicator guarantees that there exists at least one vertex d_2 in the other structure such that $d_2 \nsim d_1$ — and the same argument applies if $s_2 \nsim d_1$ for finding a vertex $d_2 \nsim s_1$

Thus, the Duplicator has a strategy to always win at least 2 rounds, therefore the Duplicator wins $G_2(\mathcal{G}_1, \mathcal{G}_2)$ by Ehrenfeucht's theorem. □

Now that we proved that $\mathcal{G}_1 \equiv_2 \mathcal{G}_2$, is it true that they are also 3-equivalent? Unfortunately, the following claim proves that this is indeed false.

Claim: The Spoiler wins $G_3(\mathcal{G}_1, \mathcal{G}_2)$.

Proof of the Claim. The following is a strategy that guarantees the Spoiler to win in 3 rounds:

- let $s_1 \in \{4, 5\}$

- by the previous claim, we know that the strategy for the Duplicator to win at least 2 rounds is to choose $d_1 \in \{a, b, d, e\}$, thus we may assume that $d_1 \neq c$
- now, let $s_2 = 1$
- to preserve the partial isomorphism, we observe that
  - if $d_1 \in \{a, b\}$, then $d_2 \in \{d, e\}$
  - if $d_1 \in \{d, e\}$, then $d_2 \in \{a, b\}$
- now, it suffices for the Spoiler to choose s_3 in $\mathcal{G}_2$ such that $s_3 \sim d_2$ and $s_3 \neq c$: by construction of $\mathcal{G}_2$, we see that $s_3 \nsim d_1$, but all the vertices in $\{2, 3, 5\}$ are adjacent to s_1, which would violate the partial isomorphism

□

In fact, we can actually find a property that distinguishes $\mathcal{G}_1$ from $\mathcal{G}_2$ which can be written through a sentence of rank 3: "there are two vertices x_1 and x_2 of $\mathcal{G}$ such that for each third vertex x_3 there is a K_3 as subgraph of $\mathcal{G}$ such that $V(K_3) = \{x_1, x_2, x_3\}$"

$$\exists x_1 \exists x_2 \forall x_3 \quad \left(\bigwedge_{\substack{1 \leq i,j \leq 3 \\ i \neq j}} \neg(x_i = x_j) \right) \wedge E(x_1, x_2) \wedge E(x_2, x_3) \wedge E(x_3, x_1)$$

Let x_1, x_2 and x_3 be the three choosen vertices — and we may assume that $x_1 \sim x_2$ otherwise the sentence is trivially unsatisfied. Then, we observe that

- in $\mathcal{G}_1$ if $\{x_1, x_2\} = \{2, 3\}$, then for any other vertex $x_3 \in \{1, 4, 5\}$ we can always find a K_3 having x_1, x_2 and x_3 as its vertices
- in $\mathcal{G}_2$ we have two cases
  - if $\{x_1, x_2\} \subseteq \{a, b, c\}$, the property is unsatisfied for $x_3 \in \{d, e\}$
  - if $\{x_1, x_2\} \subseteq \{c, d, e\}$, the property is unsatisfied for $x_3 \in \{a, b\}$

In conclusion, we have that $\mathcal{G}_1 \equiv_2 \mathcal{G}_2$, and that $\mathcal{G}_1 \not\equiv_3 \mathcal{G}_2$. □

1.2 Homework 2

Exercise 1.1 Let (W, R) be a *quasi-order*; that is, assume that R is transitive and reflexive. Define the binary relation $\sim$ on W by putting $s \sim t \iff R(s,t) \wedge R(t,s)$.

(a) Show that $\sim$ is an equivalence relation.

Let $[s]$ denote the equivalence class of s under this relation, and define the following relation on the collection of equivalence classes: $[s] \leq [t] \iff R(s,t)$.

(b) Show that this relation is well-defined.

(c) Show that $\leq$ is a partial order.

Solution. We prove the statements as follows.

(a) To prove that $\sim$ is an equivalence relation, it suffices to show that $\sim$ has the following properties:

- *reflexivity*: $\forall s \in W \quad R(s,s)$ by reflexivity of R, therefore $s \sim s$
- *symmetry*: $\forall s,t \in W \quad s \sim t \iff R(s,t) \wedge R(t,s) \iff t \sim s$
- *transitivity*: $\forall s,t,u \in W \quad \begin{cases} s \sim t \iff R(s,t) \wedge R(t,s) \\ t \sim u \iff R(t,u) \wedge R(u,t) \end{cases}$ and by transitivity of R we have that
  - $R(s,t) \wedge R(t,u) \implies R(s,u)$
  - $R(u,t) \wedge R(t,s) \implies R(u,s)$

  and by definition $R(s,u) \wedge R(u,s) \iff s \sim u$

(b) To prove that $\leq$ is well-defined, we need to show that

$$\forall s,t,s',t' \quad s \sim s' \wedge t \sim t' \implies ([s] \leq [t] \iff [s'] \leq [t'])$$

We observe that

- $s \sim s' \iff R(s,s') \wedge R(s',s)$
- $t \sim t' \iff R(t,t') \wedge R(t',t)$

therefore, we have that

- $[s] \leq [t] \iff R(s,t)$, and by transitivity of R it holds that $R(s',s) \wedge R(s,t) \implies R(s',t)$; therefore, by transitivity of R again we have that $R(s',t) \wedge R(t,t') \implies R(s',t') \iff [s'] \leq [t']$
- $[s'] \leq [t'] \iff R(s',t')$, and by transitivity of R it holds that $R(s',t') \wedge R(t',t) \implies R(s',t)$; therefore, by transitivity of R again we have that $R(s,s') \wedge R(s',t) \implies R(s,t) \iff [s] \leq [t]$

(c) To prove that $\leq$ is a partial order, it suffices to show that $\leq$ has the following properties:

- *reflexivity*: $\forall s \in W \quad R(s,s)$ by reflexivity of R, and $R(s,s) \iff [s] \leq [s]$

- *antisymmetry*: $\forall s,t \in W \quad \begin{cases} [s] \leq [t] \iff R(s,t) \\ [t] \leq [s] \iff R(t,s) \end{cases} \implies R(s,t) \wedge R(t,s) \iff s \sim t \iff [s] = [t]$
- *transitivity*: $\forall s,t,u \in W \quad \begin{cases} [s] \leq [t] \iff R(s,t) \\ [t] \leq [u] \iff R(t,u) \end{cases} \implies R(s,t) \wedge R(t,u) \implies R(s,u)$ by transitivity of R, and $R(s,u) \iff [s] \leq [u]$

□

Exercise 2.2 Let $\mathcal{N} = (\mathbb{N}, S_1, S_2)$ and $\mathcal{B} = (\mathbb{B}, R_1, R_2)$ be the following frames for a modal similarity type with two diamonds $\Diamond_1$, $\Diamond_2$. Here, $\mathbb{N}$ is the set of natural numbers and $\mathbb{B}$ is the set of strings of 0's and 1's, and the relations are defined by

$$\begin{aligned} S_1(m,n) &\iff n = m+1 \\ S_2(m,n) &\iff m > n \\ R_1(s,t) &\iff t = s0 \vee t = s1 \\ R_2(s,t) &\iff t \sqsubset s \end{aligned}$$

where $t \sqsubset s$ if and only if t is a *proper prefix* of s — i.e. t is a prefix of s such that $t \neq s$ (thus t can be ε). Which of the following formulas are valid on $\mathcal{N}$ and $\mathcal{B}$, respectively?

(a) $(\Diamond_1 p \wedge \Diamond_2 q) \to \Diamond_1(p \wedge q)$

(b) $(\Diamond_2 p \wedge \Diamond_2 q) \to \Diamond_2(p \wedge q)$

(c) $(\Diamond_1 p \wedge \Diamond_1 q \wedge \Diamond_1 r) \to (\Diamond_1(p \wedge q) \vee \Diamond_1(p \wedge r) \vee \Diamond_1(q \wedge r))$

(d) $p \to \Diamond_1 \Box_1 p$

(e) $p \to \Diamond_2 \Box_1 p$

(f) $p \to \Box_1 \Diamond_2 p$

(g) $p \to \Box_2 \Diamond_1 p$

Solution. First, consider the following extension to the $\wedge$ operator on the inductive definition of satisfiability of formulas.

Claim: Given a model $\mathfrak{M} = (W, R, V)$, and a state $w \in W$, it holds that $\mathfrak{M}, w \models \phi \wedge \psi \iff \mathfrak{M}, w \models \phi \wedge \mathfrak{M}, w \models \psi$.

Proof of the Claim. By using De Morgan's law, we have that

$$\begin{aligned} \mathfrak{M}, w \models \phi \wedge \psi = \neg(\neg\phi \vee \neg\psi) &\iff \neg\mathfrak{M}, w \models \neg\phi \vee \neg\psi \\ &\iff \neg(\mathfrak{M}, w \models \neg\phi \vee \mathfrak{M}, w \models \neg\psi) \\ &\iff \neg(\neg\mathfrak{M}, w \models \phi \vee \neg\mathfrak{M}, w \models \psi) \\ &\iff \mathfrak{M}, w \models \phi \wedge \mathfrak{M}, w \models \psi \end{aligned}$$

□

For all the following propositions, we will assume that $\mathfrak{M} = (\mathbb{N}, S_1, S_2, V)$ and $\mathfrak{M}' = (\mathbb{B}, R_1, R_2, V)$ are two models over $\mathcal{N}$ and $\mathcal{B}$ respectively.

(a) $(\Diamond_1 p \wedge \Diamond_1 q) \to \Diamond_1 (p \wedge q)$

- By the claim, for any $m \in \mathbb{N}$ it holds that

$$\begin{aligned}
\mathfrak{M}, m \models \Diamond_1 p \wedge \Diamond_1 q &\iff \mathfrak{M}, m \models \Diamond_1 p \wedge \mathfrak{M}, m \models \Diamond_1 q \\
&\iff \begin{cases} \exists n_p \in \mathbb{N} & S_1(m, n_p) \wedge \mathfrak{M}, n_p \models p \\ \exists n_q \in \mathbb{N} & S_1(m, n_q) \wedge \mathfrak{M}, n_q \models q \end{cases} \\
&\iff \begin{cases} \exists n_p \in \mathbb{N} & n_p = m + 1 \wedge n_p \in V(p) \\ \exists n_q \in \mathbb{N} & n_q = m + 1 \wedge n_q \in V(p) \end{cases} \\
&\iff m + 1 \in V(p) \wedge m + 1 \in V(q) \\
&\iff m + 1 \in V(p) \cap V(q)
\end{aligned}$$

  and again, by the claim we have that

$$\begin{aligned}
\mathfrak{M}, m \models \Diamond_1 (p \wedge q) &\iff \exists n \in \mathbb{N} \quad S_1(m, n) \wedge \mathfrak{M}, n \models p \wedge q \\
&\iff \exists n \in \mathbb{N} \quad n = m + 1 \wedge (\mathfrak{M}, n \models p \wedge \mathfrak{M}, n \models q) \\
&\iff \exists n \in \mathbb{N} \quad n = m + 1 \wedge (n \in V(p) \wedge n \in V(q)) \\
&\iff \exists n \in \mathbb{N} \quad n = m + 1 \wedge n \in V(p) \cap V(q) \\
&\iff m + 1 \in V(p) \cap V(q)
\end{aligned}$$

  from which we conclude that

$$\mathfrak{M}, m \models \Diamond_1 p \wedge \Diamond_1 q \iff m + 1 \in V(p) \cap V(q) \iff \mathfrak{M}, m \models \Diamond_1 (p \wedge q)$$

  implying that the formula is valid on $\mathcal{N}$.

- By the claim, for any $s \in \mathbb{B}$ it holds that

$$\begin{aligned}
\mathfrak{M}', s \models \Diamond_1 p \wedge \Diamond_1 q &\iff \mathfrak{M}', s \models \Diamond_1 p \wedge \mathfrak{M}', s \models \Diamond_1 q \\
&\iff \begin{cases} \exists t_p \in \mathbb{B} & R_1(s, t_p) \wedge \mathfrak{M}', t_p \models p \\ \exists t_q \in \mathbb{B} & R_1(s, t_q) \wedge \mathfrak{M}', t_q \models q \end{cases} \\
&\iff \begin{cases} \exists t_p \in \mathbb{B} & (t_p = s0 \vee t_p = s1) \wedge t_p \in V(p) \\ \exists t_q \in \mathbb{B} & (t_q = s0 \vee t_q = s1) \wedge t_q \in V(q) \end{cases} \\
&\iff \begin{cases} s0 \in V(p) \vee s1 \in V(p) \\ s0 \in V(q) \vee s1 \in V(q) \end{cases} \\
&\iff \{s0, s1\} \cap V(p) \neq \varnothing \wedge \{s0, s1\} \cap V(q) \neq \varnothing
\end{aligned}$$

  and again, by the claim we have that

$$\begin{aligned}
\mathfrak{M}', s \models \Diamond_1 (p \wedge q) \models &\iff \exists t \in \mathbb{B} \quad R_1(s, t) \wedge \mathfrak{M}', t \models p \wedge q \\
&\iff \exists t \in \mathbb{B} \quad (t = s0 \vee t = s1) \wedge (\mathfrak{M}', t \models p \wedge \mathfrak{M}', t \models q) \\
&\iff \exists t \in \mathbb{B} \quad (t = s0 \vee t = s1) \wedge (t \in V(p) \wedge t \in V(q)) \\
&\iff \exists t \in \mathbb{B} \quad (t = s0 \vee t = s1) \wedge t \in V(p) \cap V(q) \\
&\iff s0 \in V(p) \cap V(q) \vee s1 \in V(p) \cap V(q) \\
&\iff \{s0, s1\} \cap V(p) \cap V(q) \neq \varnothing
\end{aligned}$$

Now suppose $V(p) = \{s0\}$ and $V(q) = \{s1\}$; then we have that $\{s0, s1\} \cap V(p) = \{s0\} \neq \varnothing \wedge \{s0, s1\} \cap V(q) = \{s1\} \neq \varnothing \iff \mathfrak{M}', s \models \Diamond_1 p \wedge \Diamond_1 q$ although $\{s0, s1\} \cap V(p) \cap V(q) = \{s0, s1\} \cap \varnothing = \varnothing \iff \mathfrak{M}', s \not\models \Diamond_1(p \wedge q)$, implying that the formula is not valid on $\mathcal{B}$.

(b) $(\Diamond_2 p \wedge \Diamond_2 q) \to \Diamond_2(p \wedge q)$

- By definition, for any $m \in \mathbb{N}$ it holds that

$$\begin{aligned}
\mathfrak{M}, m \models \Diamond_2 p \wedge \Diamond_2 q &\iff \mathfrak{M}, m \models \Diamond_2 p \wedge \mathfrak{M}, m \models \Diamond_2 q \\
&\iff \begin{cases} \exists n_p \in \mathbb{N} & S_2(m, n_p) \wedge \mathfrak{M}, n_p \models p \\ \exists n_q \in \mathbb{N} & S_2(m, n_q) \wedge \mathfrak{M}, n_q \models q \end{cases} \\
&\iff \begin{cases} \exists n_p \in \mathbb{N} & m > n_p \wedge n_p \in V(p) \\ \exists n_q \in \mathbb{N} & m > n_q \wedge n_q \in V(q) \end{cases}
\end{aligned}$$

and again, by the claim we have that

$$\begin{aligned}
\mathfrak{M}, m \models \Diamond_2(p \wedge q) &\iff \exists n \in \mathbb{N} \quad S_2(m, n) \wedge \mathfrak{M}, n \models p \wedge q \\
&\iff \exists n \in \mathbb{N} \quad m > n \wedge (\mathfrak{M}, n \models P \wedge \mathfrak{M}, n \models q) \\
&\iff \exists n \in \mathbb{N} \quad m > n \wedge (n \in V(p) \wedge n \in V(q)) \\
&\iff \exists n \in \mathbb{N} \quad m > n \wedge n \in V(p) \cap n \in V(q)
\end{aligned}$$

Now take an $n \geq 2$, and consider $n_p, n_q \in \mathbb{N}$ such that $n_p \neq n_q \wedge n > n_p, n_q$, and suppose that $V(p) = \{n_p\}$ and $V(q) = \{n_q\}$; then we have that $\begin{cases} \exists n_p \in \mathbb{N} & n > n_p \wedge n_p \in V(p) \\ \exists n_q \in \mathbb{N} & n > n_q \wedge n_q \in V(q) \end{cases} \iff \mathfrak{M}, m \models \Diamond_2 p \wedge \Diamond_2 q$ although $n_p \neq n_q \implies V(p) \cap V(q) = \varnothing \implies \nexists n \in \mathbb{N} \quad m > n \wedge n \in V(p) \cap V(q) \iff \mathfrak{M}, m \not\models \Diamond_2(p \wedge q)$, implying that the formula is not valid on $\mathcal{N}$.

- By the claim, for any $s \in \mathbb{B}$ it holds that

$$\begin{aligned}
\mathfrak{M}', s \models \Diamond_2 p \wedge \Diamond_2 q &\iff \mathfrak{M}', s \models \Diamond_2 p \wedge \mathfrak{M}', s \models \Diamond_2 q \\
&\iff \begin{cases} \exists t_p \in \mathbb{B} & R_2(s, t_p) \wedge \mathfrak{M}', t_p \models p \\ \exists t_q \in \mathbb{B} & R_2(s, t_q) \wedge \mathfrak{M}', t_q \models q \end{cases} \\
&\iff \begin{cases} \exists t_p \in \mathbb{B} & t_p \sqsubset s \wedge t_p \in V(p) \\ \exists t_q \in \mathbb{B} & t_q \sqsubset s \wedge t_q \in V(p) \end{cases}
\end{aligned}$$

and again, by the claim we have that

$$\begin{aligned}
\mathfrak{M}' s \models \Diamond_2(p \wedge q) &\iff \exists t \in \mathbb{B} \quad t \sqsubset s \wedge (\mathfrak{M}', t \models p \wedge \mathfrak{M}', t \models q) \\
&\iff \exists t \in \mathbb{B} \quad t \sqsubset s \wedge (t \in V(p) \wedge t \in V(q)) \\
&\iff \exists t \in \mathbb{B} \quad t \sqsubset s \wedge t \in V(p) \cap V(q)
\end{aligned}$$

Now take $s = 000$, consider $t_p = 0$ and $t_q = 0$, and suppose that $V(p) = \{t_p\} = \{0\}$ and $V(q) = \{t_q\} = \{00\}$; we observe that $t_p = 0 \sqsubset 000 = s$ and $t_q = 00 \sqsubset 000 = s$, therefore $\begin{cases} \exists t_p \in \mathbb{B} & t_p \sqsubset s \wedge t_p \in V(p) \\ \exists t_q \in \mathbb{B} & t_q \sqsubset s \wedge t_q \in V(q) \end{cases} \iff \mathfrak{M}', s \models \Diamond_2 p \wedge \Diamond_2 q$

although $V(p) \cap V(q) = \{t_p\} \cap \{t_q\} = \{0\} \cap \{00\} = \varnothing \implies \nexists t \in \mathbb{B} \quad t \sqsubset s \wedge t \in V(p) \cap V(q) \iff \mathfrak{M}', s \not\models \Diamond_2(p \wedge q)$, implying that the formula is not valid on $\mathcal{B}$.

(c) $(\Diamond_1 p \wedge \Diamond_1 q \wedge \Diamond_1 r) \to (\Diamond_1(p \wedge q) \vee \Diamond_1(p \wedge r) \vee \Diamond_1(q \wedge r))$

- By the claim, for any $m \in \mathbb{N}$ it holds that

$$\begin{aligned}
\mathfrak{M}, m \models \Diamond_1 p \wedge \Diamond_1 q \wedge \Diamond_1 r &\iff \mathfrak{M}, m \models \Diamond_1 p \wedge \mathfrak{M}, m \models \Diamond_1 q \wedge \mathfrak{M}, m \models \Diamond_1 r \\
&\iff \begin{cases} \exists n_p \in \mathbb{N} & S_1(m, n_p) \wedge \mathfrak{M}, n_p \models \Diamond_1 p \\ \exists n_q \in \mathbb{N} & S_1(m, n_q) \wedge \mathfrak{M}, n_q \models \Diamond_1 q \\ \exists n_r \in \mathbb{N} & S_1(m, n_r) \wedge \mathfrak{M}, n_r \models \Diamond_1 r \end{cases} \\
&\iff \begin{cases} \exists n_p \in \mathbb{N} & n_p = m + 1 \wedge n_p \in V(p) \\ \exists n_q \in \mathbb{N} & n_q = m + 1 \wedge n_q \in V(q) \\ \exists n_r \in \mathbb{N} & n_r = m + 1 \wedge n_r \in V(r) \end{cases} \\
&\iff \begin{cases} m + 1 \in V(p) \\ m + 1 \in V(q) \\ m + 1 \in V(r) \end{cases} \\
&\iff m + 1 \in V(p) \cap V(q) \cap V(r)
\end{aligned}$$

and again, by the claim we have that

$$\begin{aligned}
\mathfrak{M}, m \models \Diamond_1(p \wedge q) \vee \Diamond_1(p \wedge r) \vee \Diamond_1(q \wedge r) &\iff (\mathfrak{M}, m \models \Diamond_1(p \wedge q)) \\
&\qquad \vee (\mathfrak{M}, m \models \Diamond_1(p \wedge r)) \\
&\qquad \vee (\mathfrak{M}, m \models \Diamond_1(q \wedge r)) \\
&\iff (\exists n_1 \in \mathbb{N} \quad S_1(m, n_1) \wedge \mathfrak{M}, n_1 \models p \wedge q) \\
&\qquad \vee (\exists n_2 \in \mathbb{N} \quad S_1(m, n_2) \wedge \mathfrak{M}, n_2 \models p \wedge r) \\
&\qquad \vee (\exists n_3 \in \mathbb{N} \quad S_1(m, n_3) \wedge \mathfrak{M}, n_3 \models q \wedge r) \\
&\iff (\exists n_1 \in \mathbb{N} \quad n_1 = m + 1 \wedge n_1 \in V(p) \cap V(q)) \\
&\qquad \vee (\exists n_2 \in \mathbb{N} \quad n_2 = m + 1 \wedge n_2 \in V(p) \cap V(r)) \\
&\qquad \vee (\exists n_3 \in \mathbb{N} \quad n_3 = m + 1 \wedge n_3 \in V(q) \cap V(r)) \\
&\iff (m + 1 \in V(p) \cap V(q)) \\
&\qquad \vee (m + 1 \in V(p) \cap V(r)) \\
&\qquad \vee (m + 1 \in V(q) \cap V(r))
\end{aligned}$$

Hence, we see that

$$\begin{aligned}
\mathfrak{M}, m \models \Diamond_1 p \wedge \Diamond_1 q \wedge \Diamond_1 r &\iff m + 1 \in V(p) \cap V(q) \cap V(r) \\
&\implies \begin{cases} m + 1 \in V(p) \cap V(q) \\ m + 1 \in V(p) \cap V(r) \\ m + 1 \in V(q) \cap V(r) \end{cases} \\
&\iff \mathfrak{M}, m \models \Diamond_1(p \wedge q) \vee \Diamond_1(p \wedge r) \vee \Diamond_1(q \wedge r)
\end{aligned}$$

implying that the formula is valid in $\mathcal{N}$.

- By the claim, for any $s \in \mathbb{B}$ it holds that

$$\begin{aligned}
\mathfrak{M}', s \models \Diamond_1 p \wedge \Diamond_1 q \wedge \Diamond_1 r &\iff \mathfrak{M}', s \models \Diamond_1 p \wedge \mathfrak{M}', s \models \Diamond_1 q \wedge \mathfrak{M}', s \models \Diamond_1 r \\
&\iff \begin{cases} \exists t_p \in \mathbb{B} & R_1(s, t_p) \wedge \mathfrak{M}', t_p \models p \\ \exists t_q \in \mathbb{B} & R_1(s, t_q) \wedge \mathfrak{M}', t_q \models q \\ \exists t_r \in \mathbb{B} & R_1(s, t_r) \wedge \mathfrak{M}', t_r \models r \end{cases} \\
&\iff \begin{cases} \exists t_p \in \mathbb{B} & (t_p = s0 \vee t_p = s1) \wedge t_p \in V(p) \\ \exists t_p \in \mathbb{B} & (t_q = s0 \vee t_q = s1) \wedge t_q \in V(q) \\ \exists t_r \in \mathbb{B} & (t_r = s0 \vee t_r = s1) \wedge t_r \in V(r) \end{cases} \\
&\iff \begin{cases} \{s0, s1\} \cap V(p) \neq \varnothing \\ \{s0, s1\} \cap V(q) \neq \varnothing \\ \{s0, s1\} \cap V(r) \neq \varnothing \end{cases}
\end{aligned}$$

  and again, by the claim we have that

$$\begin{aligned}
\mathfrak{M}', s \models \Diamond_1(p \wedge q) \vee \Diamond_1(p \wedge r) \vee \Diamond_1(q \wedge r) &\iff (\mathfrak{M}', s \models \Diamond_1(p \wedge q)) \\
&\quad \vee (\mathfrak{M}', s \models \Diamond_1(p \wedge r)) \\
&\quad \vee (\mathfrak{M}', s \models \Diamond_1(q \wedge r)) \\
&\iff (\exists t_1 \in \mathbb{B} \quad R_1(s, t_1) \wedge \mathfrak{M}', t_1 \models p \wedge q) \\
&\quad \vee (\exists t_2 \in \mathbb{B} \quad R_1(s, t_2) \wedge \mathfrak{M}', t_2 \models p \wedge r) \\
&\quad \vee (\exists t_3 \in \mathbb{B} \quad R_1(s, t_3) \wedge \mathfrak{M}', t_3 \models q \wedge r) \\
&\iff (\exists t_1 \in \mathbb{B} \quad (t_1 = s0 \vee t_1 = s1) \wedge t_1 \in V(p) \cap V(q)) \\
&\quad \vee (\exists t_2 \in \mathbb{B} \quad (t_2 = s0 \vee t_2 = s1) \wedge t_2 \in V(p) \cap V(r)) \\
&\quad \vee (\exists t_3 \in \mathbb{B} \quad (t_3 = s0 \vee t_3 = s1) \wedge t_3 \in V(q) \cap V(r)) \\
&\iff \{s0, s1\} \cap V(p) \cap V(q) \neq \varnothing \\
&\quad \vee \{s0, s1\} \cap V(p) \cap V(q) \neq \varnothing \\
&\quad \vee \{s0, s1\} \cap V(q) \cap V(r) \neq \varnothing
\end{aligned}$$

  Now suppose that $\mathfrak{M}', s \models \Diamond_1 p \wedge \Diamond_1 q \wedge \Diamond_1 r$, which happens if and only if $\begin{cases} \{s0, s1\} \cap V(p) \neq \varnothing \\ \{s0, s1\} \cap V(q) \neq \varnothing \\ \{s0, s1\} \cap V(r) \neq \varnothing \end{cases}$ as proved previously; by the pigeonhole principle, since there are 2 strings in $\{s0, s1\}$ and we have 3 sets $V(p)$, $V(q)$ and $V(r)$, there must be at least one string $x \in \{s0, s1\}$ such that $x \in V(a) \cap V(b)$, where $a, b \in \{p, q, r\}$ distinct. Without loss of generality, suppose that $x = s0$ and $a = p$ and $b = q$; then we have that

$$\begin{aligned}
x = s0 \in V(p) \cap V(q) &\implies x \in \{s0, s1\} \cap V(p) \cap V(q) \\
&\implies \{s0, s1\} \cap V(p) \cap V(q) \neq \varnothing \\
&\implies \mathfrak{M}', s \models \Diamond_1(p \wedge q) \vee \Diamond_1(p \wedge r) \vee \Diamond_1(q \wedge r)
\end{aligned}$$

  implying that the formula is valid on $\mathcal{B}$.

(d) $p \to \Diamond_1 \Box_2 p$

- By definition, for any $m \in \mathbb{N}$ it holds that

$$\begin{aligned}
\mathfrak{M}, m \models \Diamond_1 \Box_2 p &\iff \exists n \in \mathbb{N} \quad S_1(m,n) \wedge \mathfrak{M}, n \models \Box_2 p \\
&\iff \exists n \in \mathbb{N} \quad n = m+1 \wedge (\forall k \in \mathbb{N} \quad S_2(n,k) \implies \mathfrak{M}, k \models p) \\
&\iff \exists n \in \mathbb{N} \quad n = m+1 \wedge (\forall k \in \mathbb{N} \quad n > k \implies k \in V(p)) \\
&\iff \forall k \in \mathbb{N} \quad m+1 > k \implies k \in V(p) \\
&\iff V(p) = \{k \in \mathbb{N} \mid m+1 > k\}
\end{aligned}$$

  Now take $m = 1 \in \mathbb{N}$, and suppose $V(p) = \{m\} = \{1\}$; then $m \in V(p) \iff \mathfrak{M}, m \models p$, however for instance $k = 0 \in \mathbb{N}$ is such that $m + 1 = 1 + 1 = 2 > 0 = k$ although $k = 0 \notin V(p)$, therefore $\exists k \in \mathbb{N} \quad m + 1 > k \wedge k \notin V(p) \implies V(p) \neq \{k \in \mathbb{N} \mid m + 1 > k\} \iff \mathfrak{M}, m \not\models \Diamond_1 \Box_2 p$ which implies that the formula is not valid on $\mathcal{N}$.

- By definition, for any $s \in \mathbb{B}$ it holds that

$$\begin{aligned}
\mathfrak{M}', s \models \Diamond_1 \Box_2 p &\iff \exists t \in \mathbb{B} \quad R_1(s,t) \wedge \mathfrak{M}', t \models \Box_2 p \\
&\iff \exists t \in \mathbb{B} \quad (t = s0 \vee t = s1) \wedge (\forall u \in \mathbb{B} \quad R_2(t,u) \implies \mathfrak{M}', u \models p) \\
&\iff \exists t \in \mathbb{B} \quad (t = s0 \vee t = s1) \wedge (\forall u \in \mathbb{B} \quad u \sqsubset t \implies u \in V(p))
\end{aligned}$$

  Now take $s = 00 \in \mathbb{B}$, and suppose $V(p) = \{s\} = \{00\}$; then $s \in V(p) \iff \mathfrak{M}', s \models p$, however if $t = s0$ or $t = s1$, there still is $u = 0$ such that $u = 0 \sqsubset 00 = t$ although $u = 0 \notin V(p)$, therefore $(t = s0 \vee t = s1) \implies (\exists u \in \mathbb{B} \quad u \sqsubset t \wedge u \notin V(p)) \iff \mathfrak{M}', s \not\models \Diamond_1 \Box_2 p$ which implies that the formula is not valid on $\mathcal{B}$.

(e) $p \to \Diamond_2 \Box_1 p$

- By definition, for any $m \in \mathbb{N}$ it holds that

$$\begin{aligned}
\mathfrak{M}, m \models \Diamond_2 \Box_1 p &\iff \exists n \in \mathbb{N} \quad S_2(m,n) \wedge \mathfrak{M}, n \models \Box_1 p \\
&\iff \exists n \in \mathbb{N} \quad m > n \wedge (\forall k \in \mathbb{N} \quad S_1(n,k) \implies \mathfrak{M}, k \models p) \\
&\iff \exists n \in \mathbb{N} \quad m > n \wedge (\forall k \in \mathbb{N} \quad k = n+1 \implies k \in V(p)) \\
&\iff \exists n \in \mathbb{N} \quad m > n \wedge n + 1 \in V(p)
\end{aligned}$$

  Now take $m = 0 \in \mathbb{N}$, and suppose $V(p) = \{m\} = \{0\}$; then $m \in V(p) \iff \mathfrak{M}, m \models p$, however there is no $n \in \mathbb{N}$ such that $m = 0 > n$, therefore $\nexists n \in \mathbb{N} \quad m > n \wedge n + 1 \in V(p) \iff \mathfrak{M}, m \not\models \Diamond_2 \Box_1 p$ which implies that the formula is not valid on $\mathcal{N}$.

- By definition, for any $s \in \mathbb{B}$ it holds that

$$\begin{aligned}
\mathfrak{M}', s \models \Diamond_2 \Box_1 p &\iff \exists t \in \mathbb{B} \quad R_2(s,t) \wedge \mathfrak{M}', t \models \Box_1 p \\
&\iff \exists t \in \mathbb{B} \quad t \sqsubset s \wedge (\forall u \in \mathbb{B} \quad R_1(t,u) \implies \mathfrak{M}', u \models p) \\
&\iff \exists t \in \mathbb{B} \quad t \sqsubset s \wedge (\forall u \in \mathbb{B} \quad (u = t0 \vee u = t1) \implies u \in V(p)) \\
&\iff \exists t \in \mathbb{B} \quad t \sqsubset s \wedge (t0 \in V(p) \vee t1 \in V(p))
\end{aligned}$$

  Now take $s = \varepsilon \in \mathbb{B}$, and suppose $V(p) = \{s\} = \{\varepsilon\}$; then $s \in V(p) \iff \mathfrak{M}', s \models p$, however there is no $t \in \mathbb{B}$ such that $t \sqsubset s$, therefore $\nexists t \in \mathbb{B} \quad t \sqsubset s \wedge (t0 \in V(p) \vee t1 \in V(p)) \iff \mathfrak{M}', s \not\models \Diamond_2 \Box_1 p$ which implies that the formula is not valid on $\mathcal{B}$.

(f) $p \to \Box_1 \Diamond_2 p$

- By definition, for any $m \in \mathbb{N}$ it holds that

$$\begin{aligned}
\mathfrak{M}, m \models \Box_1 \Diamond_2 p &\iff \forall n \in \mathbb{N} \quad S_1(m,n) \implies \mathfrak{M}, n \models \Diamond_2 p \\
&\iff \forall n \in \mathbb{N} \quad n = m+1 \implies (\exists k \in \mathbb{N} \quad S_2(n,k) \wedge \mathfrak{M}, k \models p) \\
&\iff \forall n \in \mathbb{N} \quad n = m+1 \implies (\exists k \in \mathbb{N} \quad n > k \wedge k \in V(p)) \\
&\iff \exists k \in \mathbb{N} \quad m+1 > k \wedge k \in V(p)
\end{aligned}$$

  Now suppose $m \in V(p) \iff \mathfrak{M}, m \models p$; we observe that for every $m \in \mathbb{N}$ it holds that $m+1 > m$, therefore $m+1 > m \wedge m \in V(p) \iff \exists k \in \mathbb{N} \quad m+1 > k \wedge k \in V(p) \iff \mathfrak{M}, m \models \Box_1 \Diamond_2 p$, which implies that the formula is valid on $\mathcal{N}$.

- By definition, for any $s \in \mathbb{B}$ it holds that

$$\begin{aligned}
\mathfrak{M}', s \models \Box_1 \Diamond_2 p &\iff \forall t \in \mathbb{B} \quad R_1(s,t) \implies \mathfrak{M}', t \models \Diamond_2 p \\
&\iff \forall t \in \mathbb{B} \quad (t = s0 \vee t = s1) \implies (\exists u \in \mathbb{B} \quad R_2(t,u) \wedge \mathfrak{M}', u \models p) \\
&\iff \forall t \in \mathbb{B} \quad (t = s0 \vee t = s1) \implies (\exists u \in \mathbb{B} \quad u \sqsubset t \wedge u \in V(p))
\end{aligned}$$

  Now suppose $s \in V(p) \iff \mathfrak{M}', s \models p$; we observe that for every $s \in \mathbb{B}$ it holds that $s \sqsubset s0, s1$, therefore $\exists u \in \mathbb{B} \quad (u \sqsubset s0 \vee u \sqsubset s1) \wedge u \in V(p) \iff \mathfrak{M}', s \models \Box_1 \Diamond_2 p$, which implies that the formula is valid on $\mathcal{B}$.

(g) $p \to \Box_2 \Diamond_1 p$

- By definition, for any $m \in \mathbb{N}$ it holds that

$$\begin{aligned}
\mathfrak{M}, m \models \Box_2 \Diamond_1 p &\iff \forall n \in \mathbb{N} \quad S_2(m,n) \implies \mathfrak{M}, n \models \Diamond_2 p \\
&\iff \forall n \in \mathbb{N} \quad m > n \implies (\exists k \in \mathbb{N} \quad S_1(n,k) \wedge \mathfrak{M}, k \models p) \\
&\iff \forall n \in \mathbb{N} \quad m > n \implies (\exists k \in \mathbb{N} \quad k = n+1 \wedge k \in V(p)) \\
&\iff \forall n \in \mathbb{N} \quad m > n \implies n+1 \in V(p)
\end{aligned}$$

  Now take $m = 2 \in \mathbb{N}$, and suppose $V(p) = \{m\} = \{2\}$; then $m \in V(p) \iff \mathfrak{M}, m \models p$, however for instance $n = 0 \in \mathbb{N}$ is such that $m = 2 > 0 = n$ and $n+1 = 0+1 = 1 \notin V(p)$, therefore $\exists n \in \mathbb{N} \quad m > n \wedge n+1 \notin V(p) \iff \mathfrak{M}, m \not\models \Box_2 \Diamond_1 p$, which implies that the formula is not valid on $\mathcal{N}$.

- By definition, for any $s \in \mathbb{B}$ it holds that

$$\begin{aligned}
\mathfrak{M}', s \models \Box_2 \Diamond_1 p &\iff \forall t \in \mathbb{B} \quad R_2(s,t) \implies \mathfrak{M}', t \models \Diamond_2 p \\
&\iff \forall s \in \mathbb{B} \quad t \sqsubset s \implies (\exists u \in \mathbb{B} \quad R_1(t,u) \wedge \mathfrak{M}', u \models p) \\
&\iff \forall s \in \mathbb{B} \quad t \sqsubset s \implies (\exists u \in \mathbb{B} \quad (u = t0 \vee u = t1) \implies u \in V(p))
\end{aligned}$$

  Now take $s = 000 \in \mathbb{B}$, and suppose $V(p) = \{s\} = \{000\}$; then $s \in V(p) \iff \mathfrak{M}', s \models p$, however for instance $t = 0 \in \mathbb{B}$ is such that $t = 0 \sqsubset 000 = s$ although there is no $u = t0 = 00$ or $u = t1 = 01$ such that $u \in V(p)$, therefore $\exists t \in \mathbb{B} \quad t \sqsubset u \wedge (\nexists u \in \quad (u = t0 \vee u = t1) \wedge u \in V(p)) \iff \mathfrak{M}', s \not\models \Box_2 \Diamond_1 p$ which implies that the formula is not valid on $\mathcal{B}$.

□

Exercise 3.2 Consider the basic modal language, and the tuple $\mathfrak{f} = (\mathbb{N}, <, A)$ where A is the collection of finite and co-finite subsets of $\mathbb{N}$. Show that $\mathfrak{f}$ is a general frame.

Solution. First, consider the follwing two claims.

Claim 1: If $X \subseteq \mathbb{N}$ is finite, and $Y \subseteq \mathbb{N}$ is co-finite, then $X \cup Y$ is co-finite.

Proof of the Claim. Since X is finite, $\mathbb{N} - X$ is finite, and since Y is co-finite, $\mathbb{N} - Y$ is finite; this implies that

$$\mathbb{N} - (X \cup Y) = (\mathbb{N} - X) \cap (\mathbb{N} - Y)$$

is the intersection of a co-finite and a finite set. In particular, we observe that

- such intersection will be a subset of $\mathbb{N} - Y$ by definition of intersection
- $\mathbb{N} - Y$ is finite
- a subset of a finite set is always finite

concluding that such intersection must be finite as well. Lastly, by definition we have that $\mathbb{N} - (X \cup Y)$ is finite if and only if $X \cup Y$ is co-finite. □

Claim 2: If $X, Y \subseteq \mathbb{N}$ are co-finite, then $X \cup Y$ is co-finite.

Proof of the Claim. By repeating the same argument of the previous claim, we have that $\mathbb{N} - (X \cup Y) = (\mathbb{N} - X) \cap (\mathbb{N} - Y)$ except that in this case both $\mathbb{N} - X$ and $\mathbb{N} - Y$ are finite, which implies that their intersection must be finite, hence $\mathbb{N} - (X \cup Y)$ is co-finite by definition. □

To prove that $\mathfrak{f}$ is a general frame, it suffices to prove that the set A is closed under the following operations

- *union*: fix two sets $X, Y \in A$; then, by definition of A, we have that
  - if both X and Y are finite, then $X \cup Y$ is finite, hence $X \cup Y \in A$
  - without loss of generality, if X is finite and Y is co-finite, by Claim 1 $X \cup Y$ is co-finite, therefore $X \cup Y \in A$
  - if both X and Y are finite, then $X \cup Y$ is co-finite by Claim 2, therefore $X \cup Y \in A$
- *relative complement*: fix a set $X \in A$; then, by definition of A we trivially have that
  - if X is finite, then $\mathbb{N} - X$ is co-finite, hence $\mathbb{N} - X \in A$
  - if X is co-finite, then $\mathbb{N} - X$ is finite, hence $\mathbb{N} - X \in A$
- *modal operations*: assume that "$<$" is the relation referring to a unary modal operator $\langle < \rangle$, and fix a set $X \in A$; by definition, we have that

$$m_{\langle < \rangle}(X) = \{n \in \mathbb{N} \mid \exists x \in X \quad n < x\}$$

therefore, we have that

- if X is finite, then

$$m_{\langle<\rangle}(X) = \{n \in \mathbb{N} \mid n < \max(X)\}$$

  therefore $m_{\langle<\rangle}(X)$ is an "initial segment of $\mathbb{N}$", implying that it is finite, hence $m_{\langle<\rangle}(X) \in A$

- if X is co-finite, then $\mathbb{N} - X$ is finite, implying that X is infinite; this implies that $\max(X)$ is not defined, therefore

$$m_{\langle<\rangle}(X) = \mathbb{N} \implies \mathbb{N} - m_{\langle<\rangle}(X) = \mathbb{N} - \mathbb{N} = \varnothing$$

  and since $\varnothing$ is finite, we conclude that $m_{\langle<\rangle}(X)$ is co-finite, thus $m_{\langle<\rangle}(X) \in A$

□

Exercise 4.3 Let Σ be a set of formulas in the basic modal language, and let M denote the class of all models. Show that $\Sigma \models^g_{\mathsf{M}} \phi$ if and only if $\{\Box^n\sigma \mid \sigma \in \Sigma, n \in \mathbb{N}\} \models_{\mathsf{M}} \phi$.

Solution. Let $\Pi := \{\Box^n\sigma \mid \sigma \in \Sigma, n \in \mathbb{N}\}$. We are going to split the two directions of the proof into two claims.

Claim: If $\Sigma \models^g_{\mathsf{M}} \phi$, then $\Pi \models_{\mathsf{M}} \phi$.

Proof of the Claim. Assume that $\Sigma \models^g_{\mathsf{M}} \phi$; fix a model $\mathfrak{M}$ defined over a domain W, and a world $w \in W$. Suppose that $\mathfrak{M}, w \models \Pi$; then, by the claim of Exercise 2.2 we know that

$$\begin{aligned} &\forall \sigma \in \Sigma, n \in \mathbb{N} \quad \mathfrak{M}, w \models \Box^n\sigma \\ \iff &\forall \sigma \in \Sigma, n \in \mathbb{N}, x_1, \dots, x_n \in W \quad w \xrightarrow{R} x_1 \xrightarrow{R} \dots \xrightarrow{R} x_n \implies \mathfrak{M}, x_n \models \sigma \end{aligned}$$

where $a \xrightarrow{R} b \iff R(a, b)$.

Now, consider the following restriction of W

$$W_w := \{v \in W_w \mid \exists n \in \mathbb{N}, x_1, \dots, x_{n-1} \in W \quad w \xrightarrow{R} x_1 \xrightarrow{R} \dots \xrightarrow{R} x_{n-1} \xrightarrow{R} v\}$$

where $v \in W_w$ if and only if v can be R-reached from w through a sequence of R-accessible elements. Moreover, consider the following restriction of R

$$R_w := (W_w \times W_w) \cap R$$

in which we consider the tuples of R that connect elements of W_w. Then, consider a model $\mathfrak{M}_w$ such that $\mathfrak{M}_w = (W_w, R_w, V_w)$ where

$$V_w = W_w \cap V$$

Consider some $x_1, \ldots, x_n \in W$ such that $w \xrightarrow{R} x_1 \xrightarrow{R} \ldots \xrightarrow{R} x_n$; by definition of W_w, this implies that all $x_1, \ldots, x_n$ are R-reachable from w, which implies that $x_1, \ldots, x_n \in W_w$; this means that

$$\begin{aligned} &\forall \sigma \in \Sigma, n \in \mathbb{N}, x_1, \ldots, x_n \in W \quad w \xrightarrow{R} x_1 \xrightarrow{R} \ldots \xrightarrow{R} x_n \implies \mathfrak{M}, x_n \models \sigma \\ \implies &\forall \sigma \in \Sigma, n \in \mathbb{N}, x_1 \ldots, x_n \in W_W \quad w \xrightarrow{R} x_1 \xrightarrow{R} \ldots \xrightarrow{R} x_n \implies \mathfrak{M}, x_n \models \sigma \end{aligned}$$

Moreover, since $x_1, \ldots, x_n$ are elements of W_w, by definition of R_w it holds that

$$\begin{aligned} &\forall \sigma \in \Sigma, n \in \mathbb{N}, x_1 \ldots, x_n \in W_W \quad w \xrightarrow{R} x_1 \xrightarrow{R} \ldots \xrightarrow{R} x_n \implies \mathfrak{M}, x_n \models \sigma \\ \implies &\forall \sigma \in \Sigma, n \in \mathbb{N}, x_1 \ldots, x_n \in W_W \quad w \xrightarrow{R_w} x_1 \xrightarrow{R_w} \ldots \xrightarrow{R_w} x_n \implies \mathfrak{M}, x_n \models \sigma \end{aligned}$$

Furthermore, since $W_w \subseteq W$ and $R_w \subseteq R$, by definition of $\mathfrak{M}_w$ we get that

$$\begin{aligned} &\forall \sigma \in \Sigma, n \in \mathbb{N}, x_1 \ldots, x_n \in W_W \quad w \xrightarrow{R_w} x_1 \xrightarrow{R_w} \ldots \xrightarrow{R_w} x_n \implies \mathfrak{M}, x_n \models \sigma \\ \implies &\forall \sigma \in \Sigma, n \in \mathbb{N}, x_1 \ldots, x_n \in W_W \quad w \xrightarrow{R_w} x_1 \xrightarrow{R_w} \ldots \xrightarrow{R_w} x_n \implies \mathfrak{M}_w, x_n \models \sigma \end{aligned}$$

This observation concludes that

$$\begin{aligned} &\forall \sigma \in \Sigma, n \in \mathbb{N}, x_1, \ldots, x_n \in W \quad w \xrightarrow{R} x_1 \xrightarrow{R} \ldots \xrightarrow{R} x_n \implies \mathfrak{M}, x_n \models \sigma \\ \implies &\forall \sigma \in \Sigma, n \in \mathbb{N}, x_1 \ldots, x_n \in W_W \quad w \xrightarrow{R_w} x_1 \xrightarrow{R_w} \ldots \xrightarrow{R_w} x_n \implies \mathfrak{M}_w, x_n \models \sigma \end{aligned}$$

Now, since for any $v \in W_w$ there are $y_1, \ldots, y_k \in W$ such that $w \xrightarrow{R_w} y_1 \xrightarrow{R_w} \ldots \xrightarrow{R_w} y_k \xrightarrow{R} v$ by definition of W_w, the previous observation implies that

$$\begin{aligned} &\forall \sigma \in \Sigma \in \mathbb{N} \quad \mathfrak{M}, w \models \Box^n \sigma \\ \iff &\forall \sigma \in \Sigma, n \in \mathbb{N}, x_1, \ldots, x_n \in W \quad w \xrightarrow{R} x_1 \xrightarrow{R} \ldots \xrightarrow{R} x_n \implies \mathfrak{M}, x_n \models \sigma \\ \implies &\forall \sigma \in \Sigma, n \in \mathbb{N}, x_1 \ldots, x_n \in W_W \quad w \xrightarrow{R_w} x_1 \xrightarrow{R_w} \ldots \xrightarrow{R_w} x_n \implies \mathfrak{M}_w, x_n \models \sigma \\ \implies &\forall \sigma \in \Sigma, v \in W_w \quad \mathfrak{M}_w, v \models \sigma \\ \implies &\forall v \in W_w, \sigma \in \Sigma \quad \mathfrak{M}_w, v \models \sigma \\ \iff &\forall v \in W_w \quad \mathfrak{M}_w, v \models \Sigma \\ \implies &\forall v \in W_w \quad \mathfrak{M}_w, v \models \phi \qquad (\Sigma \models^g_{\mathsf{M}} \phi) \\ \iff &\forall v \in W_w \quad w \in V_w(\phi) \\ \implies &W_w \subseteq V_w(\phi) \subseteq V(\phi) \end{aligned}$$

Lastly, we observe that $w \in W_w$, and since $W_w \subseteq V(\phi)$ we have that $w \in V(\phi)$, which happens if and only if $\mathfrak{M}, w \models \phi$.

This proves that for any model $\mathfrak{M}$ defined over a domain W, and every world $w \in W$, it holds that

$$\mathfrak{M}, w \models \Pi \implies \mathfrak{M}, w \models \phi$$

which implies that $\Pi \models_{\mathsf{M}} \phi$ by definition. □

Claim: If $\Pi \models_{\mathsf{M}} \phi$, then $\Sigma \models^g_{\mathsf{M}} \phi$.

Proof of the Claim. Assume that $\Pi \models_{\mathsf{M}} \phi$; fix a model $\mathfrak{M}$ defined over a domain W, and suppose that $\forall w \in W \quad \mathfrak{M}, w \models \Sigma$; then, by the claim of Exercise 2.2 we obtain the following

$$\begin{aligned}
&\forall w \in W \quad \mathfrak{M}, w \models \Sigma \\
\iff &\forall w \in W, \sigma \in \Sigma \quad \mathfrak{M}, w \models \sigma \\
\implies &\forall n \in \mathbb{N}, w, x_1, \ldots, x_n \in W, \sigma \in \Sigma \quad w \overset{R}{\to} x_1 \overset{R}{\to} \ldots \overset{R}{\to} x_n \implies \mathfrak{M}, x_n \models \sigma \\
\implies &\forall n \in \mathbb{N}, w \in W, \sigma \in \Sigma \quad \mathfrak{M}, w \models \Box^n \sigma \\
\iff &\forall w \in W \quad \mathfrak{M}, w \models \Pi \\
\implies &\forall w \in W \quad \mathfrak{M}, w \models \phi \qquad (\Pi \models_{\mathsf{M}} \phi)
\end{aligned}$$

This proves that for any model $\mathfrak{M}$ defined over a domain W it holds that

$$\forall w \in W \quad \mathfrak{M}, w \models \Sigma \implies \forall w \in W \quad \mathfrak{M}, w \models \phi$$

which implies that $\Sigma \models^{g}_{\mathsf{M}} \phi$ by definition. □

Finally, the two claims conclude the exercise. □

Exercise 5.1 Give K-proofs of $(\Box p \wedge \Diamond q) \to \Diamond(p \wedge q)$ and $\Diamond(p \vee q) \leftrightarrow (\Diamond p \vee \Diamond q)$.

Solution. In the first section of the solution, we are going to prove some useful derivations that will be extensively used in the actual K-proof of the two propositions. The right side of each line will be one of the following:

- (K): the K axiom
- (D): the Dual axiom
- (T): a propositional Tautology
- (MP(i, j)): the Modus Ponens rule applied on lines i and j
- (S(i)): the Substitution rule applied on line i
- (G(i)): the Generalization rule applied on line i
- (C$_k$($i_1, \ldots i_n$)): the k-th Claim applied on lines $i_1, \ldots, i_n$ — $k \in [7]$ and n depends on the number of lines the Claim refers to

Claim 1: If $p \to q$ can be K-proved, and $q \to r$ can be K-proved, then $p \to r$ can be K-proved in 4 steps.

Proof of the Claim. Consider a K-proof in which $p \to q$ is proved at step i, and $q \to r$ is

proved at step j — without loss of generality suppose that $i < j$; then we have that

$$\begin{array}{rll}
 & \dots & \\
i. & \vdash p \to q & \\
 & \dots & \\
j. & \vdash q \to r & \\
j+1. & \vdash (a \to b) \to ((b \to c) \to (a \to c)) & (\mathrm{T}) \\
j+2. & \vdash (p \to q) \to ((q \to r) \to (p \to r)) & (\mathrm{S}(j+1)) \\
j+3. & \vdash (q \to r) \to (p \to r) & (\mathrm{MP}(i,\, j+2)) \\
j+4. & \vdash p \to r & (\mathrm{MP}(j,\, j+3))
\end{array}$$

□

Claim 2: If $p \to q$ can be K-proved, then $\Box p \to \Box q$ can be K-proved in 4 steps.

Proof of the Claim. Consider a K-proof in which $p \to q$ is proved at step i; then, we have that

$$\begin{array}{rll}
 & \dots & \\
i. & \vdash p \to q & \\
i+1. & \vdash \Box(p \to q) & (\mathrm{G}(i)) \\
i+2. & \vdash \Box(a \to b) \to (\Box a \to \Box b) & (\mathrm{K}) \\
i+3. & \vdash \Box(p \to q) \to (\Box p \to \Box q) & (\mathrm{S}(i+2)) \\
i+4. & \vdash \Box p \to \Box q & (\mathrm{MP}(i+1,\, i+3))
\end{array}$$

□

Claim 3: If $p \to q$ can be K-proved, and $p \to r$ can be K-proved, then $p \to q \wedge r$ can be K-proved in 4 steps.

Proof of the Claim. Consider a K-proof in which $p \to q$ is proved at step i, and $p \to r$ is proved at step j — without loss of generality suppose $i < j$; then, we have that

$$\begin{array}{rll}
 & \dots & \\
i. & \vdash p \to q & \\
 & \dots & \\
j. & \vdash p \to r & \\
j+1. & \vdash (a \to b) \to ((a \to c) \to (a \to b \wedge c)) & (\mathrm{T}) \\
j+2. & \vdash (p \to q) \to ((p \to r) \to (p \to q \wedge r)) & (\mathrm{S}(j+1)) \\
j+3. & \vdash (p \to r) \to (p \to q \wedge r) & (\mathrm{MP}(i,\, j+2)) \\
j+4. & \vdash p \to q \wedge r & (\mathrm{MP}(j,\, j+3))
\end{array}$$

□

Claim 4: If $p \to q$ can be K-proved, then $\neg q \to \neg p$ can be K-proved in 3 steps. Moreover, if $p \to \neg q$ can be K-proved, then $q \to \neg p$ can be K-proved in 3 steps.

Proof of the Claim. Consider a K-proof in which $p \to q$ is proved at step i; then, we have that

$$\begin{aligned} &\dots \\ i.&\vdash p \to q \\ i+1.&\vdash (a \to b) \to (\neg b \to \neg a) && \text{(T)} \\ i+2.&\vdash (p \to q) \to (\neg q \to \neg p) && \text{(S}(i+1)\text{)} \\ i+3.&\vdash \neg q \to \neg p && \text{(MP}(i,\, i+2)\text{)} \end{aligned}$$

The same K-proof can be used to prove the rest of the claim by using the propositional tautology $(a \to \neg b) \to (b \to \neg a)$. □

Claim 5: If $p \leftrightarrow q$ can be K-proved, then $p \to q$ and $q \to p$ can be K-proved in 3 steps.

Proof of the Claim. Consider a K-proof in which $p \leftrightarrow q$ is proved at step i; then, we have that

$$\begin{aligned} &\dots \\ i.&\vdash p \leftrightarrow q \\ i+1.&\vdash (a \leftrightarrow b) \to (a \to b) && \text{(T)} \\ i+2.&\vdash (p \leftrightarrow q) \to (p \to q) && \text{(S}(i+1)\text{)} \\ i+3.&\vdash p \to q && \text{(MP}(i,\, i+2)\text{)} \end{aligned}$$

The case for $q \to p$ can be proved analogously by using the propositional tautology $(a \leftrightarrow b) \to (b \to a)$. □

Claim 6: If $p \to (q \to r)$ can be K-proved, then $p \wedge q \to r$ can be K-proved in 3 steps.

Proof of the Claim. Consider a K-proof in which $p \to (q \to r)$ is proved at step i; then, we have that

$$\begin{aligned} &\dots \\ i.&\vdash p \to (q \to r) \\ i+1.&\vdash (a \to (b \to c)) \to (a \wedge b \to c) && \text{(T)} \\ i+2.&\vdash (p \to (q \to r)) \to (p \wedge q \to r) && \text{(S}(i+1)\text{)} \\ i+3.&\vdash p \wedge q \to r && \text{(MP}(i,\, i+2)\text{)} \end{aligned}$$

□

Claim 7: If $p \to q$ can be K-proved, and $q \to p$ can be K-proved, then $p \leftrightarrow q$ can be proved in 4 steps.

Proof of the Claim. Consider a K-proof in which $p \to q$ is proved at step i, and $q \to p$ can be proved at step j — without loss of generality suppose $i < j$; then, we have that

$$
\begin{array}{rll}
 & \dots & \\
i. & \vdash p \to q & \\
 & \dots & \\
j. & \vdash q \to p & \\
j+1. & \vdash (a \to b) \to ((b \to a) \to (a \leftrightarrow b)) & (\mathrm{T}) \\
j+2. & \vdash (p \to q) \to ((q \to p) \to (p \leftrightarrow q)) & (\mathrm{S}(j+1)) \\
j+3. & \vdash (q \to p) \to (p \leftrightarrow q) & (\mathrm{MP}(i,\, j+2)) \\
j+4. & \vdash p \leftrightarrow q & (\mathrm{MP}(j,\, j+3))
\end{array}
$$

□

Now that we proved some preliminary claims, we can K-prove the two given propositions.

Claim 8: $(\Box p \wedge \Diamond q) \to \Diamond(p \wedge q)$ is K-provable.

Proof of the Claim.

$$
\begin{array}{rll}
1. & \vdash \Box(p \to q) \to (\Box p \to \Box q) & (\mathrm{K}) \\
2. & \vdash (\neg a \vee \neg b) \to (a \to \neg b) & (\mathrm{T}) \\
3. & \vdash (\neg p \vee \neg q) \to (p \to \neg q) & (\mathrm{S}(2)) \\
 & \dots & \\
7. & \vdash \Box(\neg p \vee \neg q) \to \Box(p \to \neg q) & (\mathrm{C}_2(3)) \\
8. & \vdash \Box(p \to \neg q) \to (\Box p \to \Box\neg q) & (\mathrm{S}(1)) \\
 & \dots & \\
12. & \vdash \Box(\neg p \vee \neg q) \to (\Box p \to \Box\neg q) & (\mathrm{C}_1(7,8)) \\
13. & \vdash (a \to b) \to (\neg a \vee b) & (\mathrm{T}) \\
14. & \vdash (\Box p \to \Box\neg q) \to (\neg\Box p \vee \Box\neg q) & (\mathrm{S}(13)) \\
 & \dots & \\
18. & \vdash \Box(\neg p \vee \neg q) \to (\neg\Box p \vee \Box\neg q) & (\mathrm{C}_1(12,14)) \\
19. & \vdash (\neg a \vee b) \to \neg(a \wedge \neg b) & (\mathrm{T}) \\
20. & \vdash (\neg\Box p \vee \Box\neg q) \to \neg(\Box p \wedge \neg\Box\neg q) & (\mathrm{S}(19)) \\
 & \dots & \\
24. & \vdash \Box(\neg p \vee \neg q) \to \neg(\Box p \wedge \neg\Box\neg q) & (\mathrm{C}_1(18,20)) \\
 & \dots & \\
27. & \vdash (\Box p \wedge \neg\Box\neg q) \to \neg\Box(\neg p \vee \neg q) & (\mathrm{C}_4(24)) \\
28. & \vdash \neg(a \wedge b) \to (\neg a \vee \neg b) & (\mathrm{T}) \\
29. & \vdash \neg(p \wedge q) \to (\neg p \vee \neg q) & (\mathrm{S}(27)) \\
 & \dots &
\end{array}
$$

$\ldots$

33. $\vdash \Box\neg(p \wedge q) \rightarrow \Box(\neg p \vee \neg q)$ ($C_2(28)$)

$\ldots$

36. $\vdash \neg\Box(\neg p \vee \neg q) \rightarrow \neg\Box\neg(p \wedge q)$ ($C_4(32)$)

$\ldots$

40. $\vdash (\Box p \wedge \neg\Box\neg q) \rightarrow \neg\Box\neg(p \wedge q)$ ($C_1(27, 36)$)
41. $\vdash \Diamond a \leftrightarrow \neg\Box\neg a$ (D)
42. $\vdash \Diamond(p \wedge q) \leftrightarrow \neg\Box\neg(p \wedge q)$ (S(41))

$\ldots$

45. $\vdash \neg\Box\neg(p \wedge q) \rightarrow \Diamond(p \wedge q)$ ($C_5(42)$)

$\ldots$

49. $\vdash (\Box p \wedge \neg\Box\neg q) \rightarrow \Diamond(p \wedge q)$ ($C_1(40, 45)$)
50. $\vdash \Diamond q \leftrightarrow \neg\Box\neg q$ (S(41))

$\ldots$

53. $\vdash \Diamond q \rightarrow \neg\Box\neg q$ ($C_5(50)$)
54. $\vdash (b \rightarrow c) \rightarrow (a \wedge b \rightarrow a \wedge c)$ (T)
55. $\vdash (\Diamond q \rightarrow \neg\Box\neg q) \rightarrow (\Box p \wedge \Diamond q \rightarrow \Box p \wedge \neg\Box\neg q)$ (S(54))
56. $\vdash \Box p \wedge \Diamond q \rightarrow \Box p \wedge \neg\Box\neg q$ (MP(53, 55))

$\ldots$

60. $\vdash (\Box p \wedge \Diamond q) \rightarrow \Diamond(p \wedge q)$ ($C_1(56, 49)$)

□

This claim concludes the K-proof of the first proposition. To K-prove the second proposition, we are going to split the K-proof into 3 claims.

Claim 9: $(\Diamond p \vee \Diamond q) \rightarrow \Diamond(p \vee q)$ is K-provable.

Proof of the Claim.

1. $\vdash \neg p \wedge \neg q \rightarrow \neg p$ (T)

$\ldots$

5. $\vdash \Box(\neg p \wedge \neg q) \rightarrow \Box\neg p$ ($C_2(1)$)
6. $\vdash \neg p \wedge \neg q \rightarrow \neg q$ (T)

$\ldots$

10. $\vdash \Box(\neg p \wedge \neg q) \rightarrow \Box\neg q$ ($C_2(2)$)

$\ldots$

14. $\vdash \Box(\neg p \wedge \neg q) \rightarrow \Box\neg p \wedge \Box\neg q$ ($C_3(10)$)

$\ldots$

...

17. $\vdash \neg(\Box\neg p \wedge \Box\neg q) \to \neg\Box(\neg p \wedge \neg q)$ (C_4(14))

18. $\vdash \neg a \vee \neg b \to \neg(a \wedge b)$ (T)

19. $\vdash \neg\Box\neg p \vee \neg\Box\neg q \to \neg(\Box\neg p \wedge \Box\neg q)$ (S(18))

...

23. $\vdash \neg\Box\neg p \vee \neg\Box\neg q \to \neg\Box(\neg p \wedge \neg q)$ (C_1(22, 17))

24. $\vdash \neg(a \vee b) \to \neg a \wedge \neg b$ (T)

25. $\vdash \neg(p \vee q) \to \neg p \wedge \neg q$ (S(24))

...

29. $\vdash \Box\neg(p \vee q) \to \Box(\neg p \wedge \neg q)$ (C_2(25))

...

32. $\vdash \neg\Box(\neg p \wedge \neg q) \to \neg\Box\neg(p \vee q)$ (C_4(29))

...

36. $\vdash \neg\Box\neg p \vee \neg\Box\neg q \to \neg\Box\neg(p \vee q)$ (C_1(23, 32))

37. $\vdash \Diamond a \leftrightarrow \neg\Box\neg a$ (D)

...

40. $\vdash \neg\Box\neg a \to \Diamond a$ (C_5(37))

41. $\vdash \neg\Box\neg(p \vee q) \to \Diamond(p \vee q)$ (S(40))

...

45. $\vdash \neg\Box\neg p \vee \neg\Box\neg q \to \Diamond(p \vee q)$ (C_1(36, 41))

...

49. $\vdash \Diamond a \to \neg\Box\neg a$ (C_5(37))

50. $\vdash \Diamond p \to \neg\Box\neg p$ (S(49))

51. $\vdash \Diamond q \to \neg\Box\neg q$ (S(49))

52. $\vdash (a \to c) \to ((b \to d) \to (a \vee b \to c \vee d))$ (T)

53. $\vdash (\Diamond p \to \neg\Box\neg p) \to ((\Diamond q \to \neg\Box\neg q) \to (\Diamond p \vee \Diamond q \to \neg\Box\neg p \vee \neg\Box\neg q))$ (S(52))

54. $\vdash (\Diamond q \to \neg\Box\neg q) \to (\Diamond p \vee \Diamond q \to \neg\Box\neg p \vee \neg\Box\neg q)$ (MP(50, 53))

55. $\vdash \Diamond p \vee \Diamond q \to \neg\Box\neg p \vee \neg\Box\neg q$ (MP(51, 54))

...

59. $\vdash \Diamond p \vee \Diamond q \to \Diamond(p \vee q)$ (C_1(55, 48))

□

Claim 10: $\Diamond(p \vee q) \to (\Diamond p \vee \Diamond q)$ is K-provable.

Proof of the Claim.

1. $\vdash \neg p \to (\neg q \to \neg p \wedge \neg q)$ (T)

...

5. $\vdash \Box\neg p \to \Box(\neg q \to \neg p \vee \neg q)$ (C_2(1))

...

...

6. $\vdash \Box(a \to b) \to (\Box a \to \Box b)$ (K)
7. $\vdash \Box(\neg q \to \neg p \wedge \neg q) \to (\Box \neg q \to \Box(\neg p \wedge \neg q))$ (S(6))

...

11. $\vdash \Box \neg p \to (\Box \neg q \to \Box(\neg p \wedge \neg q))$ ($C_1(5, 7)$)

...

14. $\vdash \Box \neg p \wedge \Box \neg q \to \Box(\neg p \wedge \neg q)$ ($C_6(11)$)

...

17. $\vdash \neg\Box(\neg p \wedge \neg q) \to \neg(\Box \neg p \wedge \Box \neg q)$ ($C_4(14)$)
18. $\vdash \neg(a \wedge b) \to \neg a \vee \neg b$ (T)
19. $\vdash \neg(\Box \neg p \wedge \Box \neg q) \to \neg\Box \neg p \vee \neg\Box \neg q$ (S(18))

...

23. $\vdash \neg\Box(\neg p \wedge \neg q) \to \neg\Box \neg p \vee \neg\Box \neg q$ ($C_1(17, 19)$)
24. $\vdash (\neg a \wedge \neg b) \to \neg(a \vee b)$ (T)
25. $\vdash (\neg p \wedge \neg q) \to \neg(p \vee q)$ (S(24))

...

29. $\vdash \Box(\neg p \wedge \neg q) \to \Box \neg(p \vee q)$ ($C_2(25)$)

...

32. $\vdash \neg\Box \neg(p \vee q) \to \neg\Box(\neg p \wedge \neg q)$ ($C_4(29)$)

...

36. $\vdash \neg\Box \neg(p \vee q) \to \neg\Box \neg p \vee \neg\Box \neg q$ ($C_1(32, 23)$)
37. $\vdash \Diamond a \leftrightarrow \neg\Box \neg a$ (D)

...

41. $\vdash \neg\Box \neg a \to \Diamond a$ ($C_5(37)$)
42. $\vdash \neg\Box \neg p \to \Diamond p$ (S(41))
43. $\vdash \neg\Box \neg q \to \Diamond q$ (S(41))
44. $\vdash (a \to c) \to ((b \to d) \to (a \vee b \to c \vee d))$ (T)
45. $\vdash (\neg\Box \neg p \to \Diamond p) \to ((\neg\Box \neg q \to \Diamond q) \to (\neg\Box \neg p \vee \neg\Box \neg q \to \Diamond p \vee \Diamond q))$ (S(44))
46. $\vdash (\neg\Box \neg q \to \Diamond q) \to (\neg\Box \neg p \vee \neg\Box \neg q \to \Diamond p \vee \Diamond q)$ (MP(41, 45))
47. $\vdash \neg\Box \neg p \vee \neg\Box \neg q \to \Diamond p \vee \Diamond q$ (MP(42, 46))

...

51. $\vdash \Diamond a \to \neg\Box \neg a$ ($C_5(37)$)
52. $\vdash \Diamond(p \vee q) \to \neg\Box \neg(p \vee q)$ (S(51))

...

56. $\vdash \Diamond(p \vee q) \to (\neg\Box \neg p \vee \neg\Box \neg q)$ ($C_1(52, 36)$)

...

60. $\vdash \Diamond(p \vee q) \to \Diamond p \vee \Diamond q$ ($C_1(56, 47)$)

□

Claim 11: $\Diamond(p \vee q) \leftrightarrow \Diamond(p \vee \Diamond q)$ is K-provable.

Proof of the Claim.

$$
\begin{aligned}
&\dots \\
59.\ &\vdash \Diamond p \vee \Diamond q \rightarrow \Diamond(p \vee q) && (\mathrm{C}_9) \\
&\dots \\
119.\ &\vdash \Diamond(p \vee q) \rightarrow \Diamond p \vee \Diamond q && (\mathrm{C}_{10}) \\
&\dots \\
123.\ &\vdash \Diamond(p \vee q) \leftrightarrow \Diamond p \vee \Diamond q && (\mathrm{C}_7(59, 119))
\end{aligned}
$$

□

This last claim concludes that the second proposition is K-provable as well. □

2 Script

2.1 Introduction

Dynamic Logics are modal logics for representing the states and the events of dynamic systems. Their language is both an *assertion language* able to express properties of computation states, and a *programming language* able to express properties of system transitions between these states.

The first DL system was developed in 1976 by Vaughan Pratt, an early pioneer in the field of computer science who has made several contributions to foundational areas such as search algorithms, sorting algorithms, and primality testing. Pratt's original dynamic logic of programs was a *first-order* modal logic, and **Propositional Dynamic Logic** (PDL) is the propositional counterpart of it. Being propositional, it makes no use of terms, predicates or functions, and its only two syntactic categories are *propositions* and *programs*.

In particular, *possibility* and *necessity* are expressed through modal operators that also indicate the programs they are referring to. For instance, the formula $\langle\pi\rangle\,\phi$ indicates that, starting from the "current" state, there is a possible execution of the program π that ends in a state in which ϕ is true. Analogously, the formula $[\pi]\,\psi$ means that, starting from the "current" state, *all* the possible executions of the program π end in states in which ψ is true.

2.2 Syntax

The syntax of standard PDL is based upon two countably infinite sets of symbols, namely Φ_0 — the set of *atomic formulas* — and Π_0 — the set of *atomic programs*.

Then, we define the set of *more complex formulas* $\mathrm{Form}(\Phi_0)$ inductively as follows

- $\forall\phi \in \Phi_0 \quad \phi \in \mathrm{Form}(\Phi_0)$
- $\bot \in \mathrm{Form}(\Phi_0)$

- $\forall \phi \in \text{Form}(\Phi_0) \quad \neg\phi \in \text{Form}(\Phi_0)$
- $\forall \phi, \psi \in \text{Form}(\Phi_0) \quad \phi \vee \psi \in \text{Form}(\Phi_0)$
- $\forall \alpha \in \text{Prog}(\Pi_0), \phi \in \text{Form}(\Phi_0) \quad [\alpha]\,\phi \in \text{Form}(\Phi_0)$

where $\text{Prog}(\Pi_0)$ is the set of *more complex programs*, which is inductively defined as follows

- $\forall \alpha \in \Pi_0 \quad \alpha \in \text{Prog}(\Pi_0)$
- $\forall \alpha, \beta \in \text{Prog}(\Pi_0) \quad (\alpha; \beta) \in \text{Prog}(\Pi_0)$
- $\forall \alpha, \beta \in \text{Prog}(\Pi_0) \quad (\alpha \cup \beta) \in \text{Prog}(\Pi_0)$
- $\forall \alpha \in \text{Prog}(\Pi_0) \quad \alpha^* \in \text{Prog}(\Pi_0)$
- $\forall \phi \in \text{Form}(\Phi_0) \quad \phi? \in \text{Prog}(\Pi_0)$

The meaning of the operators inside this definition is the following:

- *sequence*: $(\alpha; \beta)$ is interpreted as "do α followed by β"
- *non-deterministic choice*: $(\alpha \cup \beta)$ is interpreted as "do α or β, non-deterministically"
- *unbounded iteration*: α^* is interpreted as "repeat α a finite, but non-deterministically determined, number of times"
- *test*: $\phi?$ is interpreted as "proceed is ϕ is true, else fail"

The other boolean connectives $\wedge$, $\rightarrow$ and $\leftrightarrow$ are defined through $\neg$ and $\vee$, and $\langle\alpha\rangle$ is defined to be the dual of $[\alpha]$, i.e. $\langle\alpha\rangle\,\phi \leftrightarrow \neg\,[\alpha]\,\neg\phi$. Some examples of formulas in PDL are

- $[\alpha \cup \beta]\,\phi$ means that whenever prorgam α or β is successfully executed, a state is reached where ϕ holds
- $\langle(\alpha; \beta)^*\rangle\,\phi$ means that there is a sequence of alternating executions of α and β such that a state is reached where ϕ holds

2.2.1 LTSs

To give meaning to statements in PDL we typically work with an abstract semantics in terms of **Labeled Transition Systems** (LTS), in which we label the transitions between the *worlds* (i.e. the *states* of the LTS) by names of *atomic programs*. For instance, a transition labeled π from one state x to a state y indicates that starting in x there is a possible execution of the program π that finishes in y. Formally, consider an LTS $\mathfrak{M} = (W, R, V)$ where

- W is a non-empty set of states
- R is a mapping from Π_0 into binary relations on W
- V is a mapping from Φ_0 into subsets of W

More specifically, R assigns to each $\pi \in \Pi_0$ some binary relation $R(\pi)$ on W with the intended meaning that $(x, y) \in R(\pi)$ if and only if there exists an execution of π from x that leads to y. Analogously, V assigns to each atomic formula $p \in \Phi_0$ some subset $V(p) \subseteq W$ with the intended meaning that $x \in V(p)$ if and only if p is true in the state x. However, in order to define such meanings we need to extend inductively R and V as follows:

- $(x, y) \in R(\alpha; \beta) \iff \exists z \in W \quad (x, z) \in R(\alpha) \wedge (z, y) \in R(\beta)$
- $(x, y) \in R(\alpha \cup \beta) \iff (x, y) \in R(\alpha) \vee (x, y) \in R(\beta)$
- $(x, y) \in R(\alpha^*) \iff \exists z_0, \ldots, z_n \in W \quad z_0 = x \wedge z_n = y \wedge (\forall k \in [n] \quad (z_{k-1}, z_k) \in R(\alpha))$
- $(x, y) \in R(\phi?) \iff x = y \wedge y \in V(\phi)$
- $V(\bot) = \varnothing$
- $V(\neg\phi) = W - V(\phi)$
- $V(\phi \vee \psi) = V(\phi) \cup V(\psi)$
- $V([\alpha]\,\phi) = \{x \mid \forall y \in W \quad (x, y) \in R(\alpha) \implies y \in V(\phi)\}$

For instance, consider the following LTS $\mathfrak{M} = (W, R, V)$

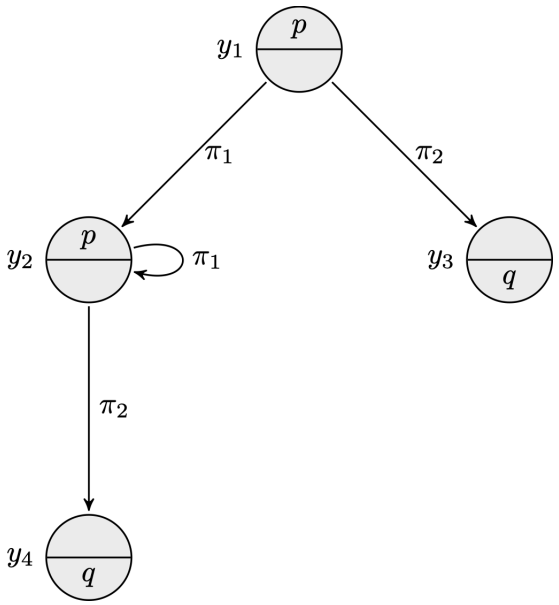


Figure 2.1: An LTS.

This LTS is formally defined as follows:

- $W = \{y_1, y_2, y_3, y_4\}$
- $R(\pi_1) = \{(y_1, y_2), (y_2, y_2)\}$
- $R(\pi_2) = \{(y_1, y_3), (y_2, y_4)\}$

- $V(p) = \{y_1, y_2\}$
- $V(q) = \{y_3, y_4\}$

These are some examples of formulas over $\mathfrak{M}$:

- $\mathfrak{M}, y_1 \models \langle \pi_1^*; \pi_2 \rangle\, q$
- $\mathfrak{M}, y_2 \models [\pi_1^*]\, p$
- $\mathfrak{M}, y_1 \models [\pi_1 \cup \pi_2]\, (p \vee q)$
- $\mathfrak{M}, y_3 \models [\pi_1 \cup \pi_2]\, \bot$

TODO bisimulation? idk

2.3 Axiomatization

Given a model $\mathfrak{M} = (W, R, V)$, and a formula ϕ, we write that $\mathfrak{M}, w \models \phi$ if and only if $w \in V(\phi)$. If this is true for all worlds $w \in W$, we say that ϕ is *valid in* $\mathfrak{M}$, denoted as $\mathfrak{M} \models \phi$

$$\mathfrak{M} \models \phi \iff \forall w \in W \quad \mathfrak{M}, w \models \phi$$

Lastly, we say that ϕ is **valid** if it is valid in any model, written as $\models \phi$

$$\models \phi \iff \forall \mathfrak{M} \quad \mathfrak{M} \models \phi$$

The purpose of the proof theory is to provide a *characterization of validity* in terms of axioms and rules of inference. To derive valid formulas, we are going to define a **deducibility predicate** $\vdash$ inductively, by operations on formulas that depend only on their syntactic structure. For the axioms, we assert that PDL contains every instance of the **distribution** axiom schema — namely (K) — and it is closed under the **necessitation** rule of inference — or *generalization* (N).

$$\text{(K)} \qquad [\alpha]\, (\phi \to \psi) \to ([\alpha]\, \phi \to [\alpha]\, \psi)$$

$$\text{(N)} \qquad \frac{\phi}{[\pi]\, \phi}$$

A modal logic is **normal** if it obeys (K) and (N). PDL can then be defined as the *least normal* modal logic containing every instance of the following axiom schemas

$$\begin{aligned}
&\text{(A1)} && [\alpha; \beta]\, \phi \leftrightarrow [\alpha]\, [\beta]\, \phi \\
&\text{(A2)} && [\alpha \cup \beta]\, \phi \leftrightarrow [\alpha]\, \phi \wedge [\beta]\, \phi \\
&\text{(A3)} && [\alpha^*]\, \phi \leftrightarrow \phi \wedge [\alpha]\, [\alpha^*]\, \phi \\
&\text{(A4)} && [\phi?]\, \psi \leftrightarrow (\phi \to \psi)
\end{aligned}$$

and closed under the *loop invariance* rule of inference:

$$\text{(I)} \qquad \frac{\phi \to [\alpha]\, \phi}{\phi \to [\alpha^*]\, \phi}$$

We also require PDL to satisfy the *Modus Ponens* inference rule

$$\text{(MP)} \qquad \frac{\phi \quad \phi \to \psi}{\psi}$$

and the usual **substitution** rule.

We are now ready to define $\vdash$: first, we have that

$$\vdash \phi \iff \varnothing \vdash \phi$$

in which case we say that ϕ is $\vdash$**-deducible**. Then, given a set of formulas Σ and a formula ϕ, we say that ϕ is $\vdash$*-deducible* from Σ — denoted as $\Sigma \vdash \phi$ — if there exists a sequence $\phi_0, \ldots, \phi_n$ of formulas such that $\phi_n = \phi$, and for all $i \in [n]$ it holds that ϕ_i satisfies one of the following

- ϕ_i is an instance of an axiom schema
- ϕ_i is an instance of a formula of Σ
- ϕ_i comes from earlier formulas of the sequence by a rule of inference

The objective is to obtain an axiomatization of PDL such that $\vdash$-deductions are both **sound** and **complete** in terms of validity, i.e. for any PDL formula ϕ it holds that

$$\vdash \phi \iff \models \phi$$

In fact, the direct implication is the *soundness* of $\vdash$ w.r.t $\models$, and the converse implication is the *completeness*. Do this set of axioms succeed in achieving this?

2.4 Completeness

In 1977 Segerberg [Seg82] proposed an axiomatization of PDL which replaces (I) with the following fifth axiom — the so called **induction** axiom schema

$$\text{(A5)} \qquad \phi \wedge [\alpha^*](\phi \to [\alpha]\phi) \to [\alpha^*]\phi$$

with the specific goal of proving that such axiomatization of PDL was indeed both *sound* and *complete*.

First, it is easy to prove that (I) can be $\vdash$-deduced from the other axioms:

1. $\vdash \phi \to [\alpha]\phi$	(premise)
2. $\vdash [\alpha^*](\phi \to [\alpha]\phi)$	(from 1 using (N) with $\pi = \alpha^*$)
3. $\vdash \phi \wedge [\alpha^*](\phi \to [\alpha]\phi) \to [\alpha^*]\phi$	(A5)
4. $\vdash [\alpha^*](\phi \to [\alpha]\phi) \to (\phi \to [\alpha^*]\phi)$	(from 3 through prop. reasoning)
5. $\vdash \phi \to [\alpha^*]\phi$	(from 2 and 4 using *Modus Ponens*)

Moreover, *soundness* of $\vdash$ w.r.t. $\models$ can be proved by induction on the length of ϕ's deduction in $\vdash$. So, what about completeness?

Completeness was pursued by several logicians. Segerberg's work was the first attempt to prove the completeness of $\vdash$, however in 1978 he found a flaw in his argument. Then, in the same year Parikh [Par78] published what is now considered the first proof of the completeness of $\vdash$, and since then various proofs have been published over the years, most notably the work by Kozen and Parikh [KP81] of 1981.

expand somehow on completeness

Different alternative proof theories of PDL have also been sought after, and various alternative formulations of deducibility predicates were defined even shortly after Parikh's work. For example, in 1992 Goldblatt [Gol87] proposed a deducibility predicate that exploits an *infinitary rule* of inference (i.e. a rule that takes an *infinite* number of premises). Let $\vdash'$ be the deducibility predicate corresponding in the language of PDL to the *least normal* modal logic containing every instance of the axiom schemas (A1), (A2), (A3) and (A4), and closed under the following *infinitary* rule of inference

$$(\mathrm{I}') \qquad \frac{\{[\beta]\,[\alpha^n]\,\phi \mid n \in \mathbb{N}\}}{[\beta]\,[\alpha^*]\,\phi}$$

Goldblatt was able to prove that $\vdash'$ is both sound and complete w.r.t. $\models$.

2.5 Complexity

Given a model $\mathfrak{M} = (W, R, V)$, a PDL formula ϕ is said to be *satisfiable in* $\mathfrak{M}$ if there exists a world $w \in W$ such that $\mathfrak{M}, w \models \phi$. Then, ϕ is said to be **satisfiable** if there exists a model $\mathfrak{M}$ such that ϕ is satisfiable in $\mathfrak{M}$.

Now, consider the following language

$$\text{PDL-SAT} := \{\langle\phi\rangle \mid \phi \text{ is a satisfiable PDL formula}\}$$

We observe that a formula ϕ is valid if and only if $\neg\phi$ is unsatisfiable. So, if a formula ϕ is not satisfiable, it suffices to prove that $\neg\phi$ is valid. Luckily, the recursive definition of the set of valid PDL formulas immediately provides a procedure P that consists in enumerating all the possible $\vdash$-deducible formulas, starting from the axioms and inferring other theorems through inference rules. Therefore, given enough time, if $\neg\phi$ is $\vdash$-deducible P will eventually find it and determine that ϕ is *not* satistiable.

However, if ϕ *is* satistiable, such procedure P would never terminate. Nonetheless, one of the earliest results on PDL was that PDL has the **finite model property**:

$$\forall\phi \in \mathrm{Form}(\Phi_0) \quad \langle\phi\rangle \in \text{PDL-SAT} \implies \exists\mathfrak{M}_{fin} \text{ finite} \quad \phi \text{ satisfiable in } \mathfrak{M}_{fin}$$

By contrapositive, such property directly provides an additional procedure P' that consists in enumerating all the possible finite models $\mathfrak{M}_{fin}$ of PDL and testing one by one if ϕ is satistiable in $\mathfrak{M}_{fin}$.

Thus, together P and P' offer a way of deciding whether a PDL formula ϕ is satisfiable or not, which implies that by running P and P' in parallel we can decide PDL-SAT. However, this algorithm is *very* inefficient. Can we do any better?

A result by Kozen and Parikh [KP81] proves that PDL has another useful property, namely the **small model property**:

$$\forall \phi \in \mathrm{Form}(\Phi_0) \quad \langle\phi\rangle \in \text{PDL-SAT} \implies \exists \mathfrak{M}_{fin} \text{ finite} \quad \begin{cases} |\mathfrak{M}_{fin}| < \exp(|\phi|) \\ \phi \text{ satisfiable in } \mathfrak{M}_{fin} \end{cases}$$

Hence again, by contrapositive this result implies that we can use P' to test whether a formula is satisfiable, but once we have exhausted all "small" models, we can conclude that the formula is not satisfiable. Such a procedure concludes that PDL-SAT $\in$ NEXP. Then, in 1980 Pratt [Pra80] proved that PDL-SAT is actually EXP-complete.

info about exp compl?

2.6 Variants

2.6.1 Test-free PDL

The "?" operator seems a bit *off* and rather different from the other operators: is it even needed in PDL? Let PDL_0 be the restriction of PDL to test-free programs, i.e. programs which do not contain tests. Is PDL_0 as expressive as PDL? In 1981 Berman and Paterson [BP81] proved that the following PDL formula

$$\langle (P?; A)^*; \neg P?; A; P? \rangle \top$$

has no PDL_0 equivalent formula, proving that test-free PDL has indeed *less expressive power*.

In the following section, we are going to present the most important details of their proof, but before going into the technical parts we will discuss the general idea. First, we observe that by removing tests, programs are restricted to *regular expressions*, therefore each program defines a regular language.

A set $S \subseteq \mathbb{N}$ is said to be **ultimately periodic** if there are integers $X \in \mathbb{N}$ and $Y > 0$ such that

$$\forall k \geq X \quad k \in S \iff k + Y \in S$$

In other words, after N values — starting from 0 — the membership in S repeats every p numbers. A well-known fact in the theory of context-free languages is that a *unary language* $L = \{1^n \mid n \in \mathbb{N}\}$ is regular if and only if the set $\{n \in \mathbb{N} \mid 1^n \in L\}$ is *ultimately periodic*. In other words, any regular unary language is represented by a regular expression of the form

$$1^X \left(1^Y\right)^*$$

This property is leveraged by Berman and Paterson as follows: the idea is to construct a family of models $\mathfrak{A}_m$ in which test-free PDL formulas *cannot* distinguish the worlds in which we are performing the evaluation. To achieve this, they construct models $\mathfrak{A}_m$ for each $m \geq 2$ in which the only program present is A, hence the languages defined from the programs over $\mathfrak{A}_m$ are both regular and unary, therefore the set of the lengths of their strings must be ultimately periodic, i.e. the languages can be rewritten as a regular expression $A^h(A^n)^*$.

Thus, they proceed to define each $\mathfrak{A}_m$ over a *cyclical structure* made of $2m+1$ worlds, where $2m+1$ is a *prime number*. This is a crucial detail, because it implies that the periodic part $(A^n)^*$ will generate *all* the possible residues modulo $2m+1$, meaning that each state is reachable starting from any possible state on the cycle, ensuring that no test-free PDL formula can distinguish the starting point of evaluation. This happens because ultimate periodicity forces the behaviour of formulas to eventually repeat regularly, hence test-free PDL formulas cannot "count" beyond a bounded region.

However, PDL with test *can* distinguish the worlds, because it possible to build programs which *depend on the truthness of propositions itself*. For instance, the program $(P?;A)^*;\neg P?$ proceeds through A-edges as long as P is true in the current state, and stops as soon as it becomes false. Thus, because test operators can observe the truth of propositions *mid-program*, it is possible to express properties that depend on non-periodic features of the model, something that test-free PDL cannot capture.

Now that we presented the general idea of their counterexample, we are going to provide some technical details of their proof. Let z be the formula $\langle (P?;A)^*;\neg P?;A;P?\rangle \top$. First, we need to introduce the definition of *equivalence*.

Definition. (Equivalence) Let $\mathfrak{M} = (W, R, V)$ be a model, and let p and q be two formulas. We say that p and q are *equivalent* in $\mathfrak{M}$ if for all $w \in W$ it holds that

$$\mathfrak{M}, w \models p \iff \mathfrak{M}, w \models q$$

In addition, p and q are *equivalent* if they are equivalent in all models.

Now, we are going to construct a *family of structures*: for any $m \geq 2$ let $\mathfrak{A}_m = (W_m, R_m, V_m)$ be a model such that

- $W_m = \{w_0, \ldots, w_{2m}\}$
- $R_m(A) = \{(w_i, w_{i+1}) \mid i \in [0, 2m-1]\} \cup \{(w_{2m}, w_0)\}$
- $R_m(B) = \varnothing$ for any other atomic program $B \in \Pi_0 - \{A\}$
- $V_m(P) = W_m - \{w_{m-1}, w_{2m-1}, w_{2m}\}$
- $V_m(Q) = W_m$ for any other atomic formula $Q \in \Phi_0 - \{P\}$

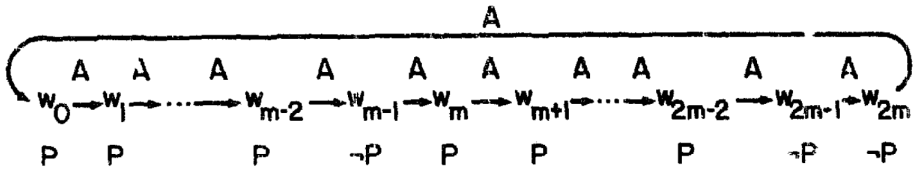


Figure 2.2: The structure $\mathfrak{A}_m$ as depicted in the original paper.

Definition. (α-unary formulas) Given an atomic program $\alpha \in \Pi_0$ and a formula ϕ, if the only subformulas $\langle\beta\rangle\,\psi$ occuring in ϕ have either $\beta = \alpha$ or $\beta = (\alpha^n)^*$ for some $n \geq 1$ we say that ϕ is **α-unary**.

Let L_A be the set of test-free A-unary formulas, and for each $p \in L_A$ let $n_A(p)$ be the number of occurrences of "$\langle A \rangle$" in p.

Lemma. For any test-free p formula, there is a $p' \in L_A$ equivalent to p in $\mathfrak{A}_m$ for all $m \geq 2$.

Theorem. There is no formula in PDL_0 equivalent to z.

Proof. First, consider the following claim.

Claim: For any $p \in L_A$, any $m \geq 2$ such that $2m+1 \in \mathbb{P}$, and any $0 \leq k \leq m - n_A(p) - 1$ it holds that $\mathfrak{A}_m, w_k \models p \iff \mathfrak{A}_m, w_{k+m} \models p$.

Proof of the Claim. We proceed by structural induction on p. If p is a propositional variable, or $\top$, or $\bot$, then $n_A(p) = 0$ therefore for any $0 \leq k \leq m$ it holds that

$$\mathfrak{A}_m, w_k \models p \iff \mathfrak{A}_m, w_{k+m} \models p$$

because $V_m(Q) = W_m$ for any $Q \in \Phi_0 - \{P\}$ by construction of $\mathfrak{A}_m$. Now, consider a formula p different from the base cases, and let $m, k \in \mathbb{N}$ two integers satisfying the claim.

If $p = \neg q$ then $n_A(p) = n_A(q)$, thus by induction on q we have that

$$\mathfrak{A}_m, w_k \models q \iff \mathfrak{A}_m, w_{k+m} \models q$$

therefore

$$\mathfrak{A}_m, w_k \models \neg q \iff \mathfrak{A}_m, w_{k+m} \models \neg q$$

If $p = q \vee r$ then $n_A(q), n_A(r) \leq n_A(p)$, hence by induction

$$\mathfrak{A}_m, w_k \models q \iff \mathfrak{A}_m, w_{k+m} \models r$$

$$\mathfrak{A}_m, w_k \models r \iff \mathfrak{A}_m, w_{k+m} \models r$$

from which it immediately follows that

$$\mathfrak{A}_m, w_k \models q \vee r \iff \mathfrak{A}_m, w_{k+m} \models q \vee r$$

If $p = \langle A \rangle\, q$ then $n_A(q) = n_A(p) - 1 < m - k - 1 = m - (k+1)$, hence by induction we get that

$$\mathfrak{A}_m, w_{k+1} \models q \iff \mathfrak{A}_m, w_{k+1+m} \models q$$

however, by construction of $\mathfrak{A}_m$ we observe that

$$\begin{aligned} \mathfrak{A}_m, w_k \models \langle A \rangle\, q &\iff \mathfrak{A}_m, w_{k+1} \models q \\ &\iff \mathfrak{A}_m, w_{k+1+m} \models q \\ &\iff \mathfrak{A}_m, w_{k+m} \models \langle A \rangle\, q \end{aligned}$$

Thus, since $p \in L_A$ the only case left to prove is if $p = \langle (A^n)^* \rangle\, q$, and we have only two options depending on n:

- if $(2m+1) \mid n$ then $(w_i, w_j) \in A^n \iff i = j$, therefore

$$\mathfrak{A}_m, w_i \models \langle (A^n)^* \rangle\, q \iff \mathfrak{A}_m w_i \models q$$

and by applying this observation to $i = k$ and $i = k + m$ we get that

$$\begin{aligned} \mathfrak{A}_m, w_k \models \langle (A^n)^* \rangle\, q &\iff \mathfrak{A}_m, w_k \models q \\ &\iff \mathfrak{A}_m, w_{k+m} \models q && \text{(by inductive hypothesis on } q) \\ &\iff \mathfrak{A}_m, w_{k+m} \models \langle (A^n)^* \rangle\, q \end{aligned}$$

- otherwise, if $(2m+1) \nmid n$, since $2m + 1 \in \mathbb{P}$ we get that

$$0n, 1n, 2n, \ldots, (2m-1)n, (2m)n$$

have all the $(2m+1)$ possible residues modulo $2m+1$. This implies that $(w_i, w_j) \in (A^n)^*$ for all $w_i, w_j \in W_m$, meaning that

$$\mathfrak{A}_m, w_i \models \langle (A^n)^* \rangle\, q \iff \exists w_j \in W \quad \mathfrak{A}_m, w_j \models q$$

and by applying this observation to $i = k$ and $j = k + m$ we get that

$$\mathfrak{A}_m, w_k \models \langle (A^n)^* \rangle\, q \iff \exists w_j \in W \quad \mathfrak{A}_m, w_j \models q \iff \mathfrak{A}_m, w_{k+m} \models \langle (A^n)^* \rangle\, q$$

□

By way of contradiction, suppose that there exists a test-free formula p equivalent to z. Let $p' \in L_A$ be a formula that satisfies the previous lemma and fix $m \geq 2$; then, by the claim it holds that

$$\mathfrak{A}_m, w_0 \models p' \iff \mathfrak{A}_m, w_m \models p'$$

by applying the claim on $k = 0$. However, by definition of V_m it holds that $\mathfrak{A}_m, w_0 \models z$ but $\mathfrak{A}_m, w_m \not\models z$, contradicting the fact that z and p were equivalent ↯. □

2.6.2 CPDL

CPDL is the extension of PDL with the addition of the **converse**. For all programs α, let α^{-1} stand for a new program such that

$$(x, y) \in R\left(\alpha^{-1}\right) \iff (y, x) \in R(\alpha)$$

For instance, $[\alpha^{-1}]\, \phi$ means that before executing α, ϕ had to hold. To obtain a sound and complete system, the addition of these two axioms schemas suffices

$$\begin{aligned} &\text{(A6)} \qquad \phi \to [\alpha] \left\langle \alpha^{-1} \right\rangle \phi \\ &\text{(A7)} \qquad \phi \to \left[\alpha^{-1}\right] \langle \alpha \rangle\, \phi \end{aligned}$$

As for PDL, it can be proven that CPDL has the **small model property** as well, and CPDL-SAT is also EXP-complete. So, what about the expressive power? Consider the two following models:

- $\mathfrak{M} = (W, R, V)$
  - $W = \{x, y\}$
  - $R(\pi) = \{(x, y)\}$
  - $V(x) = V(y) = \varnothing$
- $\mathfrak{M}' = (W', R', V')$
  - $W' = \{y'\}$
  - $R'(\pi) = \varnothing$
  - $V'(y') = \varnothing$

We observe that through the perspective of PDL $y \in W$ and $y' \in W'$ are completely *indistinguishable*, in fact for any formula ϕ it is the case that

$$\mathfrak{M}, y \models \phi \iff \mathfrak{M}', y' \models \phi$$

However, since $\top$ is true at all worlds by definition, we have that

$$\mathfrak{M}, y \models \langle \pi^{-1} \rangle \top$$

$$\mathfrak{M}', y' \not\models \langle \pi^{-1} \rangle \top$$

because there is a π-edge (x, y) in $\mathfrak{M}$ and no such edge in $\mathfrak{M}'$. This proves that, unsurprisingly, CPDL has more expressive power than standard PDL.

2.6.3 IPDL

The operators defined over programs on standard PDL do not include **intersection**, but what happens when we add such operator? We obtain IPDL, in which for all programs $\alpha, \beta \in \mathrm{Prog}(\Pi_0)$ the expression $\alpha \cap \beta$ stands for a new programs that has the following semantics

$$(x, y) \in R(\alpha \cap y) \iff (x, y) \in R(\alpha) \wedge (x, y) \in R(\beta)$$

For instance, the intended reading of $\langle \alpha \cap \beta \rangle \phi$ is that if we execute α and β in the "current" state, there exists a state reachable by both programs which satisfies ϕ. Thus, we have the following valid formula

$$\models \langle \alpha \cap \beta \rangle \phi \to \langle \alpha \rangle \phi \wedge \langle \beta \rangle \phi$$

even though, in general, the converse is *not* true.

Differntly from PDL and CPDL, the axiomatization of IDPL has been an open problem until 2003, when Balbiani and Vakarelov [BV03] presented a *complete* proof system of IPDL. In terms of complexity, Lange and Lutz [LL05] proved that IPDL-SAT is 2EXP-complete.

As a final note, the variant of the PDL satisfiability problem in which there are both the *intersection* and the *converse* operator ICPDL-SAT has been proven to be 2EXP-complete as well by Göller, Lohrey, and Lutz [GLL08] in 2008.