STŘEDOŠKOLSKÁ ODBORNÁ ČINNOST

Obor č. 1: matematika a statistika

Intuicionistická logika a její modely

Jan Engler

Jihomoravský kraj

Brno 2021

STŘEDOŠKOLSKÁ ODBORNÁ ČINNOST

Obor č. 1: matematika a statistika

Intuicionistická logika a její modely

Intuicionistic logic and it's models

Autor: Jan Engler

Škola: Gymnázium Hodonín, obchodní akademie a jazyková škola s právem státní jazykové zkoušky, příspěvková organizace, Legionářů 1, 695 11 Hodonín

Kraj: Jihomoravský kraj

Konzultant: Mgr. Dominik Trnka

Brno 2022

Prohlášení

Prohlašuji, že jsem svou práci SOČ vypracoval samostatně a použil jsem pouze prameny a literaturu uvedené v seznamu bibliografických záznamů. Prohlašuji, že tištěná verze a elektronická verze soutěžní práce SOČ jsou shodné. Nemám závažný důvod proti zpřístupňování této práce v souladu se zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších předpisů.

V Brně dne: . . . . . Podpis: . . . . . .

Poděkování

Děkuji především Mgr. Dominiku Trnkovi, který mě seznámil se spoustou fascinující matematiky a vedl mě celým procesem SOČ. Dále děkuji své škole a okolí za velkou podporu při psaní.

Anotace

Cílem práce je představit intuicionistickou logiku s důrazem na konstrukci modelů, konkrétně Heytingových algeber. Heytingovy algebry zkonstruujeme z kolekcí subobjektů v toposu. Zaměříme se na toposy funktorů, jejichž hodnoty jsou množiny - takto lze popsat např. Kripkeho modely, kategorii akcí monoidů a kategorii funkcí.

Klíčová slova

intuicionistická logika, kategorie, topos, Heytingova algebra

Annotation

This thesis aims to introduce intuitionistic logic with emphasis on construction of models, specifically Heyting algebras. We construct Heyting algebras from collections of subobjects in a topos. We focus on topoi of set-valued functors - in this way we can describe Kripke models, the category of monoid actions and the category of functions.

Keywords

intuitionistic logic, categories, topos, heyting algebras

Obsah

Úvod

Hlavní motivací pro vznik této práce je pochopení logiky, tj. lidského uvažování, na konkrétních příkladech a v konkrétních situacích. To je ovšem složitější, než pouhé rozlišování absolutní pravdy a nepravdy: pravdivost může záviset na místě, čase, podmínkách, či jiných vstupních datech. Tudíž v reálném světě objevíme celé spektrum pravdivosti. Polopravdy správně odvozené z neověřených předpokladů (sekce **4.4**), pravdivé jen na některých místech (příklady 1.2.12, 2.3.3, 4.2.1 a 4.2.5), jen v určitém čase (příklady 2.4.2, 4.3.2 a 4.2.3), nebo jen po některých rozhodnutích (příklady 4.2.2, 4.3.3 a 4.3.4), se vyskytují ve všech oblastech lidského vědění, a proto by bylo vhodné je umět popsat.

V klasické logice jsme nuceni prohlásit, že tvrzení s nejasnou pravdivostí nejsou výroky a výroky s neúplnou pravdivostí jsou nepravdivé. Logika, která vnímá neúplnou pravdivost jako nepravdivost, je ovšem příliš idealizovaná a nedostačující. Ačkoliv lidské myšlení nikdy nepopíšeme úplně věrohodně, můžeme pro každou situaci zkonstruovat *model*, analyzovat všechny možné míry pravdivosti (tj. pravdivostní hodnoty), a jak spolu pravdivostní hodnoty interagují pomocí logických spojek. V takovém modelu se vždy vyskytují alespoň dvě pravdivostní hodnoty: pravda $\top$ (znamenající pravdu ve všech možných stavech daného modelu) a nepravda $\bot$ (znamenající nepravdu ve všech možných stavech). Všechny ostatní pravdivostní hodnoty jsou slabější verze $\top$: měří, do jaké míry je výrok pravdivý.

Toto obohacení logice nepřidá jen na expresivitě, ale také značně změní její charakter. Existence více pravdivostních hodnot mění chování i samotné pravdy $\top$ a nepravdy $\bot$. Najednou musíme rozlišovat mezi pojmy „není pravda" (znamená $\neq \top$) a „je nepravda" (znamená $= \bot$.) Výrokové formule, které v klasické logice se dvěma pravdivostními hodnotami platí nezávisle na pravdivosti jejich částí (tzv. tautologie), v našich modelech platit nemusí. Práce v těchto modelech vyžaduje přehodnotit základní principy logiky, a tím vytvořit novou, neklasickou logiku.

Výsledkem je *intuicionistická* logika - logika, jejíž principy jsou platné ve *všech* výše popsaných modelech. V kapitole **1** popíšeme klasickou logiku a v kapitole **2** intuicionistickou logiku. Popíšeme, jak tyto logiky přistupují k dedukci a sémantice a jak je popsat axiomaticky. *Dedukce* studuje odvozování nových poznatků z již známých. Pravidla dedukce říkají, jak lze výroky odvodit a co z nich lze odvodit. Kombinací těchto pravidel vzniká ono *odvození*. *Sémantika* studuje význam výroků a jejich ohodnocování pravdivostními hodnotami. Hlavní výsledek sémantiky pro nás bude, že pravdivostní hodnoty v intuicionistické logice vždy tvoří *Heytingovu algebru* - toto musí mít společné všechny chtěné modely.

Kapitoly **3** a **4** se zabývají konstrukcí modelů. Definujeme *topos,* což je „vesmír zobecněných množin". V toposu lze definovat analog podmnožiny a zeptat se, „jak moc" konkrétní prvek patří do ony zobecněné podmnožiny. Možné odpovědi na tuto otázku tvoří právě Heytingovu algebru, a tedy modelují intuicionistickou logiku. V kapitole **3** tuto myšlenku formalizujeme za použití teorie kategorií a v kapitole **4** popíšeme konkrétní modely. Příklady 4.2.1, 4.2.2, 4.2.4, 4.3.3, všechny příklady v sekci **4.4** a interpretace všech příkladů jsou au-

torské.

V práci budu, na první pohled paradoxně, využívat klasickou logiku a naivní teorii množin. Symboly $\wedge, \vee, \sim, ...$ zanechávám pro formální zápis; neformální logika využívaná v důkazech bude používat pouze česká slova „a, nebo, ne, kdykoliv" atd. Formálně se v práci kvantifikátory nevyskytují, neformálně ano, ve formě „pro každé" a „pro nějaké". Cíl intuicionistické logiky není zavrhnout všechny principy klasické logiky a matematiku z ní vybudovanou, ale upřesnit ji v případech, kdy není vhodná. Níže popsané modely, ačkoliv vybudované klasickou a naivní logikou, jsou přirozeně intuicionistické.

Kapitola 1

Klasická logika

V této kapitole představíme klasickou výrokovou logiku **CPL** a popíšeme pro ni sémantiku a axiomatické systémy. Pak sémantiku zobecníme z pravdivostních hodnot $\bot, \top$ na libovolnou Booleovu algebru.

1.1 Sémantika a axiomy

Úsudek je metalogické prohlášení, na základě kterého rozsuzujeme vlastnosti logiky.

Výroky jsou základní stavební blok logiky, prostřednictvím nich můžeme ohodnocovat a odvozovat. V klasické logice je výrok tvrzení, které platí, nebo neplatí. To nám dává tři úsudky:

$$\begin{aligned}&\alpha \text{ je výrok,}\\ &\alpha \text{ platí,}\\ &\alpha \text{ neplatí.}\end{aligned}$$

Základní tvrzení jako

„Dnes prší." „Mám červenou čepici."

se nazývají *atomické výroky.* Množinu všech atomických výroků označujeme $\Phi_0 = \{\pi_0; \pi_1; ...\}$. Výroky v Φ_0 můžeme kombinovat pomocí *logických spojek* $\wedge$ (konjunkce), $\vee$ (disjunkce), $\sim$ (negace) a $\to$ (implikace) s významem

$$\begin{aligned}&\sim \alpha \text{ znamená „ne } \alpha\text{"},\\ &\alpha \wedge \beta \text{ znamená „}\alpha \text{ a současně } \beta\text{"},\\ &\alpha \vee \beta \text{ znamená „}\alpha \text{ nebo } \beta\text{" (nebo ve slučovacím významu)},\\ &\alpha \to \beta \text{ znamená „z } \alpha \text{ vyplývá } \beta\text{"},\\ &\alpha \leftrightarrow \beta \text{ znamená „}\alpha \text{ právě tehdy, když } \beta\text{"}\end{aligned}$$

($\alpha \leftrightarrow \beta$ používáme také jako zkratku pro $(\alpha \to \beta) \wedge (\beta \to \alpha)$. „Zkombinované výroky" jako

$$\alpha \vee (\sim \beta \to \gamma)$$

se nazývají *výrokové formule* (všechny spojky mají přednost před $\sim$, jinak se využívají závorky). Množinu všech výrokových formulí označme Φ.

Formační pravidla udávají, jak se pomocí atomických výroků a logických spojek tvoří výroky. Tím nám pomáhají rozsoudit úsudek „α je výrok".

Jazyk $\mathcal{L}_{PL}$ pro **CPL** obsahuje abecedu
1) atomických výroků π_n pro $n \in \mathbb{N}$,
2) logických spojek $\wedge$, $\vee$, $\sim$ a $\rightarrow$,
3) závorek (pro upřesnění pořadí)

a formační pravidla
1) každé $\pi_n \in \Phi_0$ je výrok,
2) pokud α, β jsou výroky, pak $\sim \alpha$; $\alpha \wedge \beta$; $\alpha \vee \beta$; $\alpha \rightarrow \beta$ jsou výroky.

Sémantika pro $\mathcal{L}_{PL}$: *Valuace* (ohodnocení) je funkce, která každému výroku z Φ přiřadí pravdivostní hodnotu $\top$ nebo $\bot$. To probíhá ve dvou krocích. Prvně ohodnotíme atomické výroky pravidlem:

„Každému $\pi_n \in \Phi_0$ přiřadíme $\top$, pokud ho usuzujeme za platný a $\bot$, pokud ho usuzujeme za neplatný."

Dále popíšeme, jak ohodnocovat složené výroky z ohodnocení jejich částí. Na to potřebujeme sémantické analogy logických spojek: *logické funkce* $\cap, \cup, \neg$ a $\Rightarrow$. Spojka $\neg$ je unární (tj. typu $\{\top, \bot\} \rightarrow \{\top, \bot\}$), všechny ostatní jsou binární (tj. typu $\{\top, \bot\} \times \{\top, \bot\} \rightarrow \{\top, \bot\}$). Předpisy logických funkcí jsou určeny následujícími tabulkami. Pro úplnost uvádím i $\Leftrightarrow$, což je analog ke spojce $\leftrightarrow$.

$\cap$	$\bot$	$\top$
$\bot$	$\bot$	$\bot$
$\top$	$\bot$	$\top$

$\cup$	$\bot$	$\top$
$\bot$	$\bot$	$\top$
$\top$	$\top$	$\top$

$\neg$	
$\bot$	$\top$
$\top$	$\bot$

$\Rightarrow$	$\bot$	$\top$
$\bot$	$\top$	$\top$
$\top$	$\bot$	$\top$

$\Leftrightarrow$	$\bot$	$\top$
$\bot$	$\top$	$\bot$
$\top$	$\bot$	$\top$

Pomocí logických funkcí rozšíříme valuaci $V\colon \Phi_0 \rightarrow \{\bot; \top\}$ na funkci $V'\colon \Phi \rightarrow \{\bot; \top\}$ induktivně:

$$\begin{aligned} V'(\sim \alpha) &= \neg V'(\alpha), \\ V'(\alpha \vee \beta) &= V'(\alpha) \cup V'(\beta), \\ V'(\alpha \wedge \beta) &= V'(\alpha) \cap V'(\beta), \\ V'(\alpha \rightarrow \beta) &= V'(\alpha) \Rightarrow V'(\beta). \end{aligned}$$

Pro jednoduchost dále nerozlišujme mezi V a V'.

Výrok α je *tautologie* (psáno $\models_{\mathbf{CPL}} \alpha$), pokud $V(\alpha) = \top$ pro jakékoliv $V\colon \Phi \rightarrow \{\bot; \top\}$.

Příklad 1.1.1. Následující výroky jsou v klasické logice tautologie.

1) $(\sim \alpha \wedge \sim \beta) \leftrightarrow (\sim (\alpha \vee \beta))$
2) $(\sim \alpha \vee \sim \beta) \leftrightarrow (\sim (\alpha \wedge \beta))$
3) $(\alpha \to \beta) \leftrightarrow (\sim \alpha \vee \beta)$
4) $(\sim\sim \alpha) \leftrightarrow \alpha$
5) $\alpha \vee \sim \alpha$
6) $(\alpha \to \beta) \vee (\beta \to \alpha)$
7) $((\alpha \wedge \beta) \to \gamma) \leftrightarrow ((\alpha \to \gamma) \vee (\beta \to \gamma))$
8) $((\alpha \vee \beta) \to \gamma) \leftrightarrow ((\alpha \to \gamma) \wedge (\beta \to \gamma))$

Výroky **1)**, **2)** se nazývají *de Morganovy zákony.* Výrok **5)** se nazývá *zákon o vyloučení třetího* neboli **LEM** (law of excluded middle). ■

Alternativně můžeme logiku studovat *jen* prostřednictvím tautologií. To nás vede k
Axiomatickým systémům pro CPL:

Vybereme si výrokové formule, tzv. *axiomy,* které považujeme za základní a platné nezávisle na jejich částech. Z axiomů odvozujeme další formule pomocí *pravidel odvozování.* Axiomatický systém je pak soubor
1) axiomů a
2) pravidel odvozování.

Důkaz v systému **A** je konečná posloupnost výrokových formulí $\alpha_0,\ \alpha_1,\ \ldots,\ \alpha_n$ taková, že každé α_i je
1) axiom v **A**, nebo
2) pravidlo odvození v **A** použito na axiomy v **A** a formule α_j pro $j < i$.

Věta α v systému **A** je formule, pro níž existuje důkaz v **A** končící formulí α. Píšeme:

$$\vdash_{\mathbf{A}} \alpha.$$

Příklad 1.1.2. systém L_3 ([Wal17]).
Axiomy:

$$\begin{aligned} \text{I} &: \alpha \to (\beta \to \alpha) \\ \text{II} &: (\alpha \to (\beta \to \gamma)) \to ((\alpha \to \beta) \to (\alpha \to \gamma)) \\ \text{III} &: (\sim \alpha \to \sim \beta) \to (\beta \to \alpha) \end{aligned}$$

Pravidla odvozování:

Modus ponens (MP): Pokud $\vdash_{L_3} \alpha$ a $\vdash_{L_3} \alpha \to \beta$, pak $\vdash_{L_3} \beta$.
Substituce (Sub): Pokud $\vdash_{L_3} \phi(\alpha)$ pro každé $\alpha \in \Phi$, pak $\vdash_{L_3} \phi(\beta)$.

Zde $\phi(\alpha)$ je konečná výroková formule obsahující výrok α. Větu $\alpha \to \alpha$ v L_3 odvodíme následovně.

i) $\alpha \to ((\beta \to \alpha) \to \alpha)$ (Sub do I)
ii) $(\alpha \to ((\beta \to \alpha) \to \alpha)) \to ((\alpha \to (\beta \to \alpha)) \to (\alpha \to \alpha))$
iii) $(\alpha \to (\beta \to \alpha)) \to (\alpha \to \alpha)$ (MP na $i), ii)$)
iv) $\alpha \to (\beta \to \alpha)$ (I)
v) $\alpha \to (\beta \to \alpha)$ (I)
vi) $\alpha \to \alpha$ (MP na iv), ii))

Sémantický a axiomatický přístup jsou na první pohled velmi odlišné. Určují dvě různé koncepce důsledku:
1) α je *sémantický* důsledek **CPL**, pokud $\models_{\mathbf{CPL}} \alpha$ a
2) α je *syntaktický* důsledek **A**, pokud $\vdash_{\mathbf{A}} \alpha$.

Axiomatický systém **A** logiku popisuje věrohodně, pokud jeho věty (syntaktické důsledky) jsou právě tautologie (sémantické důsledky) ony logiky. Jinak řečeno, **A** musí být
1) *bezesporný:* $\models_{\mathbf{PCL}} \alpha$ kdykoliv $\vdash_{\mathbf{A}} \alpha$
2) *úplný:* $\vdash_{\mathbf{A}} \alpha$ kdykoliv $\models_{\mathbf{PCL}} \alpha$.

1.2 Modely klasické logiky & Booleovy algebry

Doteď jsme uvažovali sémantický přístup jako základní a axiomatický jsme k němu přidali jako alternativu. V následující sekci tento proces obrátíme: začneme s axiomy a přidáme jim význam pomocí modelů.

Jazyk $\mathcal{L}$ je soubor *slov* skládajících se z *písmen* podle *formačních pravidel.*
Teorie $\mathcal{T}$ jazyka $\mathcal{L}$ je soubor formulí $\alpha \in \Phi$ zvaných *axiomy. Interpretace* jazyka $\mathcal{L}$ je dvojice $\mathcal{U} = (U, \mathcal{I})$, kde:
1) U je množina pravdivostních hodnot obsahující $\bot, \top$ a
2) $\mathcal{I}$ je *interpretační funkce*, která každému $\alpha \in \Phi$ přiřadí $\mathcal{I}(\alpha) \in U$ a každé logické spojce $f\colon \Phi^n \to \Phi$ přiřadí logickou funkci $\mathcal{I}(f) : U^n \to U$. Říkáme, že α je *validní* v $\mathcal{U}$ (psáno $\mathcal{U} \models \alpha$), kdykoliv $\mathcal{I}(\alpha) = \top$.
Interpretace $\mathcal{U} = (U, \mathcal{I})$ je *modelem* teorie $\mathcal{T}$, psáno $\mathcal{U} \models \mathcal{T}$, pokud $\mathcal{U} \models \alpha$ pro všechny axiomy $\alpha \in \mathcal{T}$.

Příklad 1.2.1. $\mathcal{L}_{\mathbf{PL}}$ je jazyk, jehož písmeny jsou atomické výroky $\pi_n \in \Phi_0$ a jehož slova jsou výroky, které se z písmen skládají spojkami $\sim, \wedge, \vee, \to$. Axiomy L_3 tvoří teorii v jazyce $\mathcal{L}_{\mathbf{PL}}$. Pro libovolnou valuaci V je dvojice $(\{\bot; \top\}, V)$ model teorie L_3, kde $V(\sim) := \neg$, $V(\wedge) := \cap$, $V(\vee) := \cup$ a $V(\to) := \Rightarrow$.
Podle této terminologie tedy chápeme logické funkce jako interpretace logických spojek.

Poznámka. Výše uvedená definice jazyka a modelu je velmi zjednodušená. Pro přesnější popis viz. [WD15].

Najít model pro logiku specifikovanou axiomaticky pak znamená najít interpretaci výroků (tj. množinu pravdivostních hodnot) a logických spojek (tj. logických funkcí), které splňují axiomy této logiky. V tomto duchu jsou syntaktické důsledky ty věty, které lze odvodit z axiomů v $\mathcal{T}$ a odvozovacích pravidel. Sémantické důsledky jsou věty, které platí ve všech modelech $\mathcal{T}$. Vztah mezi teorií a modelem je určen bezesporností a úplností.

V následující posloupnosti definic zavedeme **Booleovy algebry,** které budou sloužit jako „univerzální modely" klasické logiky.

Definice 1.2.2. Částečně uspořádaná množina (angl. *partially ordered set* neboli *poset*) $\mathbb{P}$ je dvojice $(P, \sqsubseteq)$, kde
1) P je množina,

2) $\sqsubseteq$ je reflexivní, antisymetrická a tranzitivní binární relace (částečné uspořádání) na P. Explicitně, pro každé $x, y, z \in P$ platí

1) $x \sqsubseteq x$ (reflexivita),
2) pokud $x \sqsubseteq y$ a $y \sqsubseteq x$, pak $x = y$ (antisymetrie),
3) pokud $x \sqsubseteq y$ a $y \sqsubseteq z$, pak $x \sqsubseteq z$ (tranzitivita).

Pro jednoduchost budeme psát $x \in \mathbb{P}$ místo $x \in P$.

Definice 1.2.3. Poset je *ohraničený,* pokud existuje *nejmenší prvek* $\bot_{\mathbb{P}}$ a *největší prvek* $\top_{\mathbb{P}}$ splňující

$$\bot_{\mathbb{P}} \sqsubseteq x \sqsubseteq \top_{\mathbb{P}}$$

pro každé $x \in \mathbb{P}$.

Definice 1.2.4. Buď $\mathbb{P} = (P, \sqsubseteq), \mathbb{Q} = (Q, \preceq)$ posety. Monotónní zobrazení $f\colon \mathbb{P} \to \mathbb{Q}$ je funkce $f\colon P \to Q$ taková, že $f(x) \preceq f(y)$ kdykoliv $x \sqsubseteq y$ pro libovolná $x, y \in \mathbb{P}$.

Definice 1.2.5. Buď $\mathbb{P}$ poset, $x, y \in \mathbb{P}$. Infimum $x \sqcap y$, pokud existuje, je prvek $\mathbb{P}$, jenž je jednoznačně definován vztahy

1) $x \sqcap y \sqsubseteq x, \quad x \sqcap y \sqsubseteq y$,
2) pokud $z \sqsubseteq x$ a $z \sqsubseteq y$ pro nějaké $z \in \mathbb{P}$, je $z \sqsubseteq x \sqcap y$.

Supremum $x \sqcup y$, pokud existuje, je definováno analogicky vztahy

1) $x \sqsubseteq x \sqcup y, \quad y \sqsubseteq x \sqcup y$,
2) pokud $x \sqsubseteq z$ a $y \sqsubseteq z$ pro nějaké $z \in \mathbb{P}$, je $x \sqcup y \sqsubseteq z$.

Definice 1.2.6. $\mathbb{P}$ je *svaz,* pokud pro každé $x, y \in \mathbb{P}$, $x \sqcap y$ a $x \sqcup y$ existují. Pak píšeme $\mathbb{P} = (P, \sqsubseteq, \sqcup, \sqcap)$. Svaz $\mathbb{P}$ je *distributivní*, pokud platí

$$x \sqcup (y \sqcap z) = (x \sqcup y) \sqcap (x \sqcup z),$$
$$x \sqcap (y \sqcup z) = (x \sqcap y) \sqcup (x \sqcap z),$$

pro každé $x, y, z \in \mathbb{P}$.

Lemma 1.2.7. Buď $\mathbb{P}$ svaz. Zobrazení $(-) \sqcap a : \mathbb{P} \to \mathbb{P}$ s předpisem $x \mapsto x \sqcap a$ je monotónní zobrazení.
Důkaz. Předpokládejme $x \sqsubseteq y$. Pak

$$x \sqcap a \sqsubseteq x \sqsubseteq y,$$
$$x \sqcap a \sqsubseteq a.$$

Z definice infima je pak $x \sqcap a \sqsubseteq y \sqcap a$.

Definice 1.2.8. Buď $\mathbb{P} = (P, \sqsubseteq, \sqcup, \sqcap)$ ohraničený svaz a $x \in \mathbb{P}$. *Komplement* x (psáno $\neg x$), pokud existuje, je prvek $\mathbb{P}$ splňující

$$x \sqcap \neg x = \bot_{\mathbb{P}} \quad \text{a} \quad x \sqcup \neg x = \top_{\mathbb{P}}.$$

Definice 1.2.9. *Booleova algebra* $\mathbb{B}$ je pětice $(B, \sqsubseteq, \sqcup, \sqcap, \neg)$, kde
1) $(B, \sqsubseteq, \sqcup, \sqcap)$ je ohraničený distributivní svaz,
2) komplement $\neg x$ existuje pro každé $x \in B$.
Označme $x \Rightarrow y := \neg x \sqcap y$, tzv. „relativní komplement."

Sémantika v CPL: Výroky jazyka $\mathcal{L}_{\mathbf{PL}}$ můžeme ohodnocovat $\mathbb{B}$-valuací $V\colon \Phi_0 \to B$, kterou rozšíříme na funkci $V'\colon \Phi \to B$ induktivně pravidly

$$\begin{aligned} V'(\sim \alpha) &= \neg V'(\alpha), \\ V'(\alpha \vee \beta) &= V'(\alpha) \sqcup V'(\beta), \\ V'(\alpha \wedge \beta) &= V'(\alpha) \sqcap V'(\beta), \\ V'(\alpha \to \beta) &= V'(\alpha) \Rightarrow V'(\beta). \end{aligned}$$

Věta 1.2.10. Nechť $\mathbb{B}$ je Booleova algebra a $V\colon \Phi_0 \to \mathbb{B}$ je $\mathbb{B}$-valuace. Pak $(\mathbb{B}, V')$ je interpretace klasické logiky, kde

$$\begin{aligned} \text{komplement } \neg &= V'(\sim) \text{ interpretuje negaci,} \\ \text{supremum } \sqcup &= V'(\vee) \text{ interpretuje disjunkci,} \\ \text{infimum } \sqcap &= V'(\wedge) \text{ interpretuje konjunkci,} \\ \text{relativní komplement } \Rightarrow &= V'(\to) \text{ interpretuje implikaci.} \end{aligned}$$

Značení $\mathbb{B} \models \alpha$ (čteme „α je validní v $\mathbb{B}$") je zkratka pro $(\mathbb{B}, V') \models \alpha$, tj. „$\alpha$ je validní ve všech $\mathbb{B}$-valuacích".

Poznámka. Intuitivně $x \sqsubseteq y$ znamená, že výrok α s pravdivostní hodnotou $V'(\alpha) = x$ je *silnější* než výrok β s hodnotou $V'(\beta) = y$. Tím je myšleno, že kdykoliv platí α, musí platit β. Skutečně máme

$$x \sqsubseteq y \text{ právě tehdy, když } (x \Rightarrow y) = \top.$$

Příklad 1.2.11. Množina $\mathbf{2} = \{0; 1\}$ s uspořádáním $0 \sqsubseteq 0,\ 0 \sqsubseteq 1,\ 1 \sqsubseteq 1$ tvoří Booleovu algebru. Hraniční prvky jsou $0 = \bot_{\mathbf{2}}$ a $1 = \top_{\mathbf{2}}$, dále $x \sqcap y = x \cap y$ (konjunkce), $x \sqcup y = x \cup y$ (disjunkce), $x \Rightarrow y$ (implikace) a $\neg x$ (negace) jsou logické funkce definované tabulkou na str. 10. Booleova algebra $\mathbf{2}$ je „standartní" model **CPL,** který interpretuje výroky jako absolutně nepravdivé ($V(\alpha) = 0$) a absolutně pravdivé ($V(\alpha) = 1$). ■

Příklad 1.2.12. Buď X množina. Pak $(\mathcal{P}(X), \subseteq, \cup, \cap, -)$ je Booleova algebra, kde $\emptyset = \bot_{\mathcal{P}(X)}$, $X = \top_{\mathcal{P}(X)}$, supremum $\cup$ je sjednocení, infimum $\cap$ je průnik, komplement $-A := X \setminus A$ je doplněk a $A \rightarrowtriangle B := -A \cup B$ je relativní komplement.

Interpretace: Pokud si X představíme jako množinu míst (prostor), $V(\alpha) = A$ znamená, že α platí v bodech A. Místa v X mohou být např. hlavní města v Evropě a α může být výrok „Počet obyvatel je větší než 10 milionů."- pak $V(\alpha)$ obsahuje města s více než 10 miliony obyvateli. Hlavní města jsou od sebe daleko a nijak si počet obyvatel navzájem neovlivňují, na $V(\alpha)$ tedy nejsou kladeny žádné topologické požadavky. ■

Věta 1.2.13. Buď $\mathbb{B}$ Booleova algebra. Pak pro $x, y \in \mathbb{B}$ platí:

1) $\neg\neg x = x$,
2) $\neg(x \sqcap y) = (\neg x) \sqcup (\neg y)$,
3) $\neg(x \sqcup y) = (\neg x) \sqcap (\neg y)$.

Důkaz:
1) Platí

$$(\neg\neg x) \sqcap \neg x = \neg(\neg x) \sqcap (\neg x) = 0,$$
$$(\neg\neg x) \sqcup \neg x = \neg(\neg x) \sqcup (\neg x) = 1.$$

Z jedinečnosti komplementu je $\neg\neg x = x$.
2) Platí

$$(x \sqcap y) \sqcap (\neg x \sqcup \neg y) = x \sqcap ((y \sqcap \neg x) \sqcup \underbrace{(y \sqcup \neg y)}_{=0}) = \underbrace{x \sqcap \neg x}_{=0} \sqcap y = 0,$$
$$(x \sqcap y) \sqcup (\neg x \sqcup \neg y) = (\underbrace{(x \sqcup \neg x)}_{=1} \sqcap (y \sqcup \neg x)) \sqcup \neg y = \underbrace{(y \sqcup \neg y)}_{=1} \sqcup \neg x = 1.$$

Z jedinečnosti komplementu je $\neg x \sqcup \neg y = \neg(x \sqcap y)$. Analogicky lze dokázat **3)**.

Pravidlo **1)** je sémantický analog tautologie $\sim\sim \alpha \leftrightarrow \alpha$. Pravidla **2)**, **3)** jsou sémantické analogy de Morganových zákonů (tautologie **1)**, **2)** v příkladu 1.1.1). □

Vyberme si nějaký axiomatický systém **A** pro **CPL** (např. L_3) a chápejme $\vdash_{\mathbf{CPL}} \alpha$ jako „α je syntaktický důsledek **A**". Dále $\mathbf{BA} \models \alpha$ (čteme „α je **BA**-validní") znamená, že $\mathbb{B} \models \alpha$ pro každou Booleovu algebru $\mathbb{B}$. Máme následující charakterizaci **CPL** (viz. [CKA]):

Věta 1.2.14. Syntaktické důsledky **A** jsou právě sémantické důsledky **BA**.

$$\text{bezespornost: } \mathbf{BA} \models \alpha \text{ kdykoliv } \vdash_{\mathbf{CPL}} \alpha,$$
$$\text{úplnost: } \vdash_{\mathbf{CPL}} \alpha \text{ kdykoliv } \mathbf{BA} \models \alpha.$$

Kapitola 2

Intuicionistická logika

2.1 Brouwerův program

Na konci 19. století začala matematikou proudit myšlenka *formalizace*: všechny matematické zákonitosti lze redukovat na pár axiomů, pomocí kterých je vybudována celá matematika ([Gol84]). Dosud nejvíc používaný „základ matematiky" je *teorie množin*, zejména *Zermelo-Fraenkelova axiomatická teorie množin* **ZFC**. Ordinály $\emptyset, \{\emptyset\}, \{\emptyset; \{\emptyset\}\}$, ... formalizují přirozená čísla, která lze různými množinově-teoretickými konstrukcemi rozšířit až na reálná a komplexní čísla. Mnoho matematických objektů (monoid, vektorový prostor, topologický prostor, okruh, ...) lze chápat jako *množinu s přidanou strukturou*.

Zdaleka nejkontroverznější axiom teorie množin byl axiom výběru: „Pro libovolnou množinu neprázdných množin existuje funkce, která každé dané množině náhodně přiřadí právě jeden její prvek." Na jednu stranu je tento axiom potřeba, aby platila velmi intuitivní tvrzení (každá surjektivní funkce má pravou inverzi, každý vektorový prostor má bázi, kartézský součin neprázdných množin je neprázdný), ale na druhou stranu má za důsledek *větu o dobrém uspořádání*:

Prvky každé množiny X lze uspořádat tak, aby každá podmnožina $A \subseteq X$ obsahovala nejmenší prvek.

Tato věta, ač velmi neintuitivní, není v rozporu s žádným jiným tvrzením, tj. *není nepravdivá.* Problém je, že se zatím nikomu nepodařilo (a jistě ani nepodaří) explicitně zapsat žádné takové uspořádání na reálných číslech.

Podobné výsledky o nekonečných množinách a dalších „neintuitivních" objektech přimělo některé matematiky přehodnotit jisté ontologické otázky ([Zal]). Vznikl *konstruktivismus:* filozofický směr popírající existenci nezkonstruovatelných objektů, jako například dobrého uspořádání na $\mathbb{R}$. Odnož konstruktivismu, tzv. *intuicionismus*, je právě studiem této práce. Byl založen L.E.J. Brouwerem a jeho základní principy jsou:

1) Čistá matematika se skládá pouze z vědomých konstrukcí a ne z abstraktní manipulace symbolů. Matematika je jazykem popsatelná, ale nezávisí na něm.

2) Logika je součást matematiky. Matematika na logice není závislá.

Princip **1)** vyjadřuje onen konstruktivismus: podle něj musí být každý objekt matematické diskuze vědomě zkonstruován. Koncept nezkonstruovatelný, jako dobré uspořádání na $\mathbb{R}$, není matematický objekt. Aby abstraktní koncepty měly význam a mohly se stát objektem matematické diskuze, nestačí, aby teorie je popisující byla logicky bezesporná. Zejména

důkaz, že neexistence objektu vede ke sporu, není důkaz existence. Konstruktivně je tedy tvrzení o existenci α silnější, než tvrzení o nepravdivosti neexistence $\sim\sim \alpha$: pokud jsme nějaký objekt zkonstruovali, pak nemůže neexistovat, ale pokud dokážeme, že jeho neexistence vede ke sporu, nezkonstruovali jsme ho a tedy (prozatím) neexistuje. Implikace $\sim\sim \alpha \to \alpha$ není intuicionisticky validní. To je v rozporu s klasickou logikou, ve které je $\sim\sim \alpha$ vždy ekvivalentní s α (příklad 1.1.1). Podle principu **2)** se tato analýza vztahuje nejen na existenční tvrzení, ale na celou logiku. Konkrétně pak „důkaz sporem" $\sim\sim \alpha \to \alpha$ nemůžeme považovat za validní princip logiky. Logické principy akceptovatelné v intuicionistické filozofii tvoří *intuicionistickou logiku.* Z principu **1)** dále plyne, že žádný formální jazyk není úplně věrohodný intuici a že jakýkoliv pokus o formalizaci intuicionismu, a tedy i intuicionistické logiky, bychom měli brát s nadsázkou. Formalizace popsané v sekcích **2.2-2.4** jsou ovšem v jistém slova smyslu „nejlepší možné", a proto právě je budeme studovat.

První krok k hlubšímu pochopení intuicionistické logiky je přesnější vymezení pojmu „zkonstruovat". To můžeme například prostřednictvím

Brouwer-Heyting-Kolmogorovy (BHK) interpretace intuicionistické logiky:

1) Důkaz výroku $\alpha \wedge \beta$ se skládá z důkazu α a důkazu β.

2) Důkaz výroku $\alpha \vee \beta$ se skládá z důkazu α nebo důkazu β a prohlášení, že daný důkaz chceme považovat za svědectví o $\alpha \vee \beta$.

3) Důkaz výroku $\alpha \to \beta$ je konstrukce, která důkaz α přemění na důkaz β.

4) Důkaz výroku $\bot$ je spor a nemůže být zkonstruován. Důkaz výroku $\sim \alpha := \alpha \to \bot$ je konstrukce, která důkaz α přemění na spor.

Hlavní neshoda s klasickou logikou je v bodě **2),** podle kterého k platnosti $\alpha \vee \beta$ nestačí, aby „alespoň jeden z α, β vždy platil", ale abychom si byli *vědomi*, který platí. Důkaz výroku $\alpha \vee \sim \alpha$ je v intuicionistické logice vědomá konstrukce výroku α, nebo konstrukce, která důkaz α změní na spor. Výrok $\alpha \vee \sim \alpha$ neplyne z nutnosti a v každé své instanci musí být dokázán. Jeho důkaz je rozhodnutí o platnosti α. Pro nerozhodnuté výroky α, jako Riemannova hypotéza nebo „vesmír je nekonečný", tudíž nemůžeme **LEM** $(\alpha \vee \sim \alpha)$ prohlásit za pravdivý.

Příklad 2.1.1. Klasická reálná analýza využívá *trichotomie reálných čísel:* Pro každá reálná x, y platí

$$(x < y) \ \vee \ (x = y) \ \vee \ (x > y).$$

Toto můžeme chápat jako instanci **LEM** ve tvaru $(x = y) \vee (x \neq y)$ (zde jsme „sloučili" $x < y$ a $x > y$ do $x \neq y$, což je zkratka pro $\sim (x = y)$). Pro racionální x skutečně platí $(x = y) \vee (x \neq y)$, neboť to můžeme rozhodnout algoritmem pro porovnávání čísel, který kvůli racionalitě x, y musí skončit, a tím dát výsledek onoho porovnávání. Pro iracionální x, y ale algoritmus musí začít od největší číslice a vždy se dívat jen na zaokrouhlení čísel x, y. Pokud je skutečně $(x > y) \vee (x < y)$, algoritmus porovnání ukončí za konečně mnoho kroků. Dokud ale neskončí, nemůžeme si být jisti, jestli je $x = y$, nebo jsou x, y jen neskutečně blízko, a tedy $(x = y) \vee (x \neq y)$ do konce porovnávání nelze prohlásit za pravdivé.

Porovnávání je ovšem limitováno systémem, na němž běží. Reálný systém bude mít nejmenší rozpoznatelnou hodnotu $\epsilon > 0$, takže kdykoliv $x - y < \epsilon$, systém nerozpozná x od y. Platí $\epsilon-$trichotomie:

$$(x < y) \ \vee \ (|x - y| < \epsilon) \ \vee \ (x > y).$$

Algoritmus buď rozhodne, že je jedno z čísel větší, nebo je od sebe nerozezná. $\epsilon-$trichotomie je slabší než klasická trichotomie: například z ní nelze dokázat $(x^2 = 0) \to (x = 0)$. 64-bitový systém má $\epsilon = 10^{-308}$, takže pro $x = 10^{-200}$ by systém považoval x^2 za nulu, ale x by od nuly rozeznal.

Buď α nějaký zatím nerozhodnutý výrok ($\alpha \vee \sim \alpha$ jsme nedokázali). Definujme posloupnost (a_n) předpisem

$$a_n = \begin{cases} (-2)^{-n} & \text{pokud } \alpha \text{ není rozhodnut v čase } n \\ (-2)^{-k} & \text{pokud } \alpha \text{ byl rozhodnut v čase } k \end{cases}$$

Pak (a_n) konverguje k reálnému a, pro které nemůžeme rozhodnout $(a < 0) \vee (a = 0) \vee (a > 0)$. ■

V příkladu 2.1.1 jsme „vyvrátili" **LEM** předložením výroku tvaru $\alpha \vee \sim \alpha$, který konstruktivně nelze dokázat. Tomuto argumentu se říká *slabý protipříklad.* Slabým protipříkladem se nesnažíme dokázat, že nějaká instance **LEM** neplatí: neudáváme žádné *protipříklady* **LEM.** Dokonce lze intuicionisticky dokázat, že ačkoliv **LEM** neplatí, nikdy žádný protipříklad nenajdeme: $\sim\sim (\alpha \vee \sim \alpha)$ je intuicionisticky validní (viz. 2.2.5). Díky tomu, ač není intuicionisticky validní, lze **LEM** v intuicionistické logice *konzistentně* předpokládat jako axiom - tím vznikne klasická logika.

Příklad 2.1.2. V klasické reálné analýze je funkce

$$f(x) = \begin{cases} x + 1 & x \leq 3, \\ x^2 & x > 3, \end{cases}$$

nespojitá v $x = 3$. Definice f ovšem předpokládá trichotomii reálných čísel a f tedy intuicionisticky není dobře definovaná. Z podobného důvodu se ukazuje, že každá intuicionisticky definovatelná funkce je spojitá, ačkoliv toto nelze intuicionisticky dokázat. Stejně jako v případě **LEM** můžeme tento princip konzistentně předpokládat jako axiom. Pak už ale nemůžeme předpokládat **LEM**, neboť ten dovoluje konstrukci nespojitých funkcí.
Více o konstruktivní analýze najdete v [Bri19]. ■

Příklad 2.1.3.

Dirichletův princip není intuicionisticky validní: dokazuje existenci sporem.

Bézoutovo lemma je intuicionisticky validní: jeho důkaz je algoritmus, které řešení zkonstruuje.

Euklidův důkaz existence nekonečně mnoha prvočísel je intuicionisticky validní. V dnešní době se sice prezentuje jako důkaz sporem, ale toto je zbytečné, neboť algoritmus nová prvočísla opravdu zkonstruovat umí (ačkoliv velmi neefektivně).

Axiom úplnosti není intuicionisticky validní: nepopisuje způsob, jak supremum množiny najít. Důsledky axiomu úplnosti také nejsou validní: např. za splnění podmínek Bolzanovy věty sice „existuje" řešení rovnice $f(x) = y$, ale nevíme, jak ho zkonstruovat. ■

Věta 2.1.4. Existují irracionální čísla a, b taková, že a^b je racionální.

Klasický (nekonstruktivní) důkaz: Pokud $\sqrt{2}^{\sqrt{2}}$ je racionální, pak $a = b = \sqrt{2}$ funguje. V opačném případě (zde využíváme **LEM**) $(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = 2$, takže $a = \sqrt{2}^{\sqrt{2}},\ b = \sqrt{2}$ funguje.

Konstruktivní důkaz: $\sqrt{2}^{\log_2 9} = 8$, takže $a = \sqrt{2},\ b = \log_2 9$ funguje. □

2.2 Přirozená dedukce pro IPL

Po zbytek kapitoly budeme formalizovat myšlenky minulé sekce. Začneme s přístupem *deduktivním*. Neformálně řečeno, výroky jsou chápány jako nositelé informace, logické spojky jako způsoby skládání informací a dedukce jako manipulace informací.

Výroky jsou tvrzení, pro něž lze jasně určit, z čeho se skládá jejich důkaz. Výrok je *pravdivý,* pokud jsme jeho důkaz zkonstruovali. To nám dává dva úsudky:

1) α je výrok,
2) α platí.

Oproti klasické logice „α není pravdivá" (tj. nezkonstruovali jsme důkaz α) nepovažujeme za úsudek. K této problematice se vrátíme v sekci **2.4.**

Dedukce se skládá z konečně mnoha použití nějaké instance jednoho z *pravidel dedukce* a *již dokázaných tvrzení.* Pravidla dedukce dělíme na pravidla
1) *formační,* která pro každou spojku určují, že formule jí vytvořená je výrok,
2) *introdukční,* která pro každou spojku určují, jak výroky vytvořenou danou spojkou dokázat (ty jsme už neformálně popsali v **BHK** interpretaci),
3) *eliminační,* která pro každou spojku určují, co lze z výroků danou spojkou vytvořených dokázat.

Každý krok dedukce (použití jednoho z výše uvedených pravidel) zapisujeme podle vzoru

$$\frac{P_1 \quad \ldots \quad P_n}{\mathrm{Z}}\,\Box X.$$

V zápisu P_i pro $1 \leq i \leq n$ (premisy, předpoklady) a Z (závěr) mohou být úsudky tvaru „α je výrok" nebo „α platí", $\Box$ je spojka, jejíž pravidlo používáme a X je forma pravidla: F pro formační, I pro introdukční a E pro eliminační (pokud je nějakých pravidel víc, rozlišují se přirozeným indexováním). Formační pravidla jsou

$$\frac{\alpha \text{ je výrok}}{\sim\alpha \text{ je výrok}}\sim F, \quad \frac{}{\top \text{ je výrok}}\top F, \quad \frac{}{\bot \text{ je výrok}}\bot F, \quad \frac{\alpha \text{ je výrok} \qquad \beta \text{ je výrok}}{\alpha\wedge\beta \text{ je výrok}}\wedge F,$$

$$\frac{\alpha \text{ je výrok} \qquad \beta \text{ je výrok}}{\alpha\vee\beta \text{ je výrok}}\vee F, \qquad \frac{\alpha \text{ je výrok} \qquad \beta \text{ je výrok}}{\alpha\to\beta \text{ je výrok}}\to F.$$

Pravda ($\top$) platí vždy a *nepravda* ($\bot$) neplatí nikdy. Introdukční pravidlo $\top$ je volné (pravdu lze odvodit z čehokoliv) a eliminační pravidlo pro $\top$ není (z toho, že pravda platí, nic neodvodíme). Introdukční pravidlo pro $\bot$ neexistuje (nepravda nelze odvodit) a eliminační pravidlo pro $\bot$ je volné (z nepravdy lze odvodit cokoliv):

$$\frac{\alpha \text{ platí}}{\top \text{ platí}}\top I, \qquad\qquad \frac{\bot \text{ platí}}{\alpha \text{ platí}}\bot E.$$

Výrok $\alpha\wedge\beta$ dokážeme, pokud dokážeme α a β. Naopak z $\alpha\wedge\beta$ můžeme odvodit α i β:

$$\frac{\alpha \text{ platí} \qquad \beta \text{ platí}}{\alpha\wedge\beta \text{ platí}}\wedge I, \qquad \frac{\alpha\wedge\beta \text{ platí}}{\alpha \text{ platí}}\wedge E_1, \qquad \frac{\alpha\wedge\beta \text{ platí}}{\beta \text{ platí}}\wedge E_2.$$

Konjunkci $\alpha\to\beta$ dokážeme, pokud dokážeme β za předpokladu platnosti α. Předpoklady značíme písmeny u, v, w, ... vedle horizontální čáry. Pokud otevřeme předpoklad, odvození se stává *hypotetické*. Pokud v hypotetickém odvození odvodíme α, neznamená to, že α platí: platí jen hypoteticky. Při použití pravidla $\to I^u$ předpoklad $\overline{\alpha}^u$ *uzavřeme* a nemůžeme ho již použít. Po otevření předpokladu je odvození hypotetické, dokud předpoklad neuzavřeme.

Naopak z $\alpha \to \beta$ a α můžeme odvodit β. Pravidlo $\to E$ s názvem *modus ponens* často slouží jako odvozovací pravidlo axiomatických systémů.

$$\dfrac{\dfrac{\dfrac{}{\alpha \text{ platí}}\,u}{\begin{array}{c}\vdots\\ \beta \text{ platí}\end{array}}}{\alpha \to \beta \text{ platí}} \to I^u \qquad\qquad \dfrac{\alpha \text{ platí} \qquad \alpha \to \beta \text{ platí}}{\beta \text{ platí}} \to E$$

Negaci $\sim$ definujeme jako $\sim \alpha := \alpha \to \bot$, z čehož vyplývají následující pravidla.

$$\dfrac{\dfrac{\dfrac{}{\alpha \text{ platí}}\,u}{\begin{array}{c}\vdots\\ \bot \text{ platí}\end{array}}}{\sim \alpha \text{ platí}} \sim I^u \qquad\qquad \dfrac{\alpha \text{ platí} \qquad \sim \alpha \text{ platí}}{\bot \text{ platí}} \sim E$$

Disjunkci $\alpha \vee \beta$ můžeme dokázat z α nebo z β. Výrok $(\alpha \vee \beta) \to \gamma$ dokážeme, pokud dokážeme $\alpha \to \gamma$ a $\beta \to \gamma$. To je rozdělování na případy: může platit α, nebo β, a pokud γ dokážeme v obou případech, pak z $\alpha \vee \beta$ vyplývá γ.

$$\dfrac{\alpha \text{ platí}}{\alpha \vee \beta \text{ platí}} \vee I_1 \quad \dfrac{\beta \text{ platí}}{\alpha \vee \beta \text{ platí}} \vee I_2 \quad \dfrac{\alpha \to \gamma \text{ platí} \qquad \beta \to \gamma \text{ platí} \qquad \alpha \vee \beta \text{ platí}}{\gamma \text{ platí}} \vee E$$

Výše popsaný systém nazývejme **ND**. Píšeme $\vdash_{\mathbf{ND}} \alpha$, pokud existuje dedukce výroku α v **ND**. Kdykoliv $\vdash_{\mathbf{ND}} \alpha$, můžeme v dedukci použít α bez použití premis či otevírání předpokladů:

$$\dfrac{}{\alpha.}$$

Pokud $\vdash_{\mathbf{ND}} \alpha \to \beta$, říkáme, že α je *silnější* než β. Pokud $\vdash_{\mathbf{ND}} \alpha \leftrightarrow \beta$, říkáme, že α je *stejně silná* jako β.

Příklad 2.2.1. Ukážeme $\vdash_{\mathbf{ND}} (\alpha \wedge \beta) \to (\beta \wedge \alpha)$:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\alpha \wedge \beta \text{ platí}}\,u}{\beta \text{ platí}} \wedge E_2 \quad \dfrac{\dfrac{}{\alpha \wedge \beta \text{ platí}}\,u}{\alpha \text{ platí}} \wedge E_1}{\beta \wedge \alpha \text{ platí}} \wedge I}{(\alpha \wedge \beta) \to (\beta \wedge \alpha) \text{ platí}}$$

Substitucí dostáváme analogický důkaz $(\beta \wedge \alpha) \to (\alpha \wedge \beta)$, z čehož vidíme, že $\vdash_{\mathbf{ND}} (\alpha \wedge \beta) \leftrightarrow (\beta \wedge \alpha)$. ■

Příklad 2.2.2. Výrok $\alpha \in \Phi$ je obecně silnější, než jeho negace: $\vdash_{\mathbf{ND}} \alpha \to (\sim\sim \alpha)$.

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\alpha \text{ platí}}\,u \qquad \dfrac{}{\sim \alpha \text{ platí}}\,v}{\bot \text{ platí}} \sim E}{\sim\sim \alpha \text{ platí}} \sim I^v}{\alpha \to (\sim\sim \alpha) \text{ platí}} \to \mathrm{I}^u$$

.. ■

Příklad 2.2.3. Ukážeme $\vdash_{\mathbf{ND}} \sim\sim\sim \alpha \to \sim \alpha$

$$\dfrac{\dfrac{\dfrac{}{\sim\sim\sim \alpha \text{ platí}}\, u \quad \dfrac{\dfrac{}{\alpha \text{ platí}}\, v \quad \dfrac{}{\alpha \to (\sim\sim \alpha) \text{ platí}}}{\sim\sim \alpha \text{ platí}} \to E}{\sim \alpha \text{ platí}} \sim E}{\dfrac{\bot \text{ platí}}{\sim \alpha \text{ platí}} \sim \mathrm{I}^{v}}{(\sim\sim\sim \alpha) \to (\sim \alpha) \text{ platí}} \to \mathrm{I}^{u}$$

■

Z příkladů 2.2.2 a 2.2.3 pak dostáváme $\vdash_{\mathbf{ND}} \sim \alpha \leftrightarrow \sim\sim\sim \alpha$. Pokud je výrok $\alpha \in \Phi$ negace nějakého jiného výroku (tj. platí $\alpha \leftrightarrow \sim \beta$ pro nějaké $\beta \in \Phi$,) pak je stejně silný jako svoje dvojitá negace:

$$\alpha \leftrightarrow \sim \beta \leftrightarrow \sim\sim\sim \beta \leftrightarrow \sim\sim \alpha.$$

Příklad 2.2.4. Ukážeme $\vdash_{\mathbf{ND}} ((\alpha \vee \beta) \to z) \leftrightarrow ((\alpha \to \gamma) \wedge (\beta \to z))$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\alpha \text{ platí}}\, u}{\alpha \vee \beta \text{ platí}} \vee \mathrm{I} \quad \dfrac{}{(\alpha \vee \beta) \to \gamma \text{ platí}}\, v}{\gamma \text{ platí}} \mathrm{T}}{\alpha \to \gamma \text{ platí}} \to \mathrm{I}^{u} \quad \dfrac{\dfrac{\dfrac{\dfrac{}{\beta \text{ platí}}\, w}{\alpha \vee \beta \text{ platí}} \vee \mathrm{I} \quad \dfrac{}{(\alpha \vee \beta) \to \gamma \text{ platí}}\, v}{\gamma \text{ platí}} \mathrm{T}}{\beta \to \gamma \text{ platí}} \to \mathrm{I}^{w}}{(\alpha \to \gamma) \wedge (\beta \to \gamma)} \wedge \mathrm{I}}{((\alpha \vee \beta) \to \gamma) \to ((\alpha \to \gamma) \wedge (\beta \to \gamma)) \text{ platí}} \to \mathrm{I}^{v}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{(\alpha \to \gamma) \wedge (\beta \to \gamma) \text{ platí}}\, u}{(\alpha \to \gamma) \text{ platí}} \wedge \mathrm{E} \quad \dfrac{\dfrac{}{(\alpha \to \gamma) \wedge (\beta \to \gamma) \text{ platí}}\, u}{(\beta \to \gamma) \text{ platí}} \wedge \mathrm{E} \quad \dfrac{}{\alpha \vee \beta \text{ platí}}\, v}{\gamma \text{ platí}} \vee \mathrm{E}}{(\alpha \vee \beta) \to \gamma \text{ platí}} \to \mathrm{I}^{v}}{((\alpha \to \gamma) \wedge (\beta \to \gamma)) \to ((\alpha \vee \beta) \to \gamma) \text{ platí}} \to \mathrm{I}^{u}$$

■

Příklad 2.2.5. Zvláštní případ předchozího příkladu je $\vdash_{\mathbf{ND}} \sim (\alpha \vee \sim \alpha) \leftrightarrow ((\sim \alpha) \wedge (\sim\sim \alpha))$, pomocí něhož ukážeme, že **LEM** nemá žádné protipříklady: $\vdash_{\mathbf{ND}} \sim\sim (\alpha \vee \sim \alpha)$.

$$\dfrac{\dfrac{\dfrac{}{\sim (\alpha \vee \sim \alpha)}\, u \quad \dfrac{}{\sim (\alpha \vee \sim \alpha) \leftrightarrow ((\sim \alpha) \wedge (\sim\sim \alpha))}}{\sim \alpha \wedge \sim\sim \alpha} \to E}{\bot} \sim E}{\sim\sim (\alpha \vee \sim \alpha)} \sim I^{u}$$

Alternativně můžeme v důkazu $\vdash_{\mathbf{ND}} \alpha \to \beta$ předpoklad $\overline{\alpha}^{u}$ neuzavírat, čímž dostaneme důkaz „z α odvoď β”:

$$\dfrac{\dfrac{\alpha \text{ platí}}{\vdots}}{\beta \text{ platí}}$$

Píšeme $\alpha \vdash_{\mathbf{ND}} \beta$. Pomocí implikace $\to$ popisuje **ND** relaci $\vdash_{\mathbf{ND}}$: úsudek „$\alpha \to \beta$ platí” je „vnitřní” verze úsudku „$\alpha \vdash_{\mathbf{ND}} \beta$”.

2.3 Heytingovy algebry

Pro sémantický a axiomatický přístup k **IPL** se obrátíme k Arendu Heytingovy. Jeho přínos k intuicionistické logice je, navzdory Brouwerova anti-formalistického přesvědčení, formalizace intuicionistické logiky.

Výroky v **IPL** budeme ohodnocovat valuací $V' \colon \Phi \to H$, kde Φ je množina výrokových formulí a H množina pravdivostních hodnot. V analogii s klasickým případem (poznámka pod větou 1.2.10) budou rovněž pravdivostní hodnoty výroků $\alpha, \beta \in \Phi$ přirozeně uspořádány principem „silnější výroky jsou níž":

$$V'(\alpha) \sqsubseteq V'(\beta), \text{ pokud z } \alpha \text{ lze } \textit{intuicionisticky} \text{ odvodit } \beta.$$

V **ND** místo „α lze *intuicionisticky* odvodit β" píšeme $\alpha \vdash_{\mathbf{ND}} \beta$. Pravidla $\wedge E_1, \wedge E_2, \wedge I$ pak představují vlastnosti infima a $\vee I_1, \vee I_2, \vee E$ vlastnosti suprema (1.2.5). Interpretace pravidel $\to I, \to E$ jazykem teorie uspořádání nás vede k podmínce

$$x \sqsubseteq a \Rightarrow b \;\text{ právě tehdy, když }\; x \sqcap a \sqsubseteq b,$$

kde $\Rightarrow$, tzv. „relativní pseudokomplement", je ona interpretace spojky $\to$. Jednoduše řečeno, $a \Rightarrow b$ definujeme jako *nejslabší* možnou pravdivostní hodnotu splňující modus ponens $\to E$. Dále po vzoru **ND** definujeme „pseudokomplement" $\neg x := x \Rightarrow \bot$ podmínkou

$$x \sqsubseteq \neg a \;\text{ právě tehdy, když }\; x \sqcap a = 0$$

tj. negace je nejslabší možná splňující $\sim E$.

Definice 2.3.1. *Heytingova algebra* $\mathbb{H}$ je pětice $(H, \sqsubseteq, \sqcup, \sqcap, \Rightarrow)$, kde
1) $(H, \sqsubseteq, \sqcup, \sqcap)$ je distributivní ohraničený svaz
2) *relativní pseudokomplement* $a \Rightarrow b$ je jednoznačně definován podmínkou

$$x \sqsubseteq a \Rightarrow b \;\text{ právě tehdy, když }\; x \sqcap a \sqsubseteq b$$

Označme $\neg x := x \Rightarrow \bot_{\mathbb{H}}$, tzv. *pseudokomplement*.

Sémantika v IPL: V analogii s klasickým případem definujeme $\mathbb{H}$-valuaci $V \colon \Phi_0 \to H$, kterou indukcí na logických spojkách pravidly

$$\begin{aligned} V'(\sim \alpha) &= \neg V'(\alpha) \\ V'(\alpha \vee \beta) &= V'(\alpha) \sqcup V'(\beta) \\ V'(\alpha \wedge \beta) &= V'(\alpha) \sqcap V'(\beta) \\ V'(\alpha \to \beta) &= V'(\alpha) \Rightarrow V'(\beta) \end{aligned}$$

rozšíříme na $V' \colon \Phi \to H$. Píšeme $\mathbb{H} \models \alpha$, pokud $V(\alpha) = \top_{\mathbb{H}}$ pro každou $\mathbb{H}-$valuaci $V \colon {}_0\Phi \to H$ a $\mathbf{HA} \models \alpha$, pokud $\mathbb{H} \models \alpha$ pro každou Heytingovu algebru $\mathbb{H}$.

Věta 2.3.2. Každá Booleova algebra $\mathbb{B}$ je Heytingova algebra s $a \Rightarrow b := \neg a \sqcup b$, kde $\neg$ je komplement v dané $\mathbb{B}$.
Důkaz: Potřebujeme ukázat

$$x \sqsubseteq \neg a \sqcup b \;\text{ právě tehdy, když }\; x \sqcap a \sqsubseteq b.$$

„⇒": Předpokládejme $x \sqsubseteq \neg a \sqcup b$. Pak

$$x \sqcap a \sqsubseteq (\neg a \sqcup b) \sqcap a = (\neg a \sqcap a) \sqcup (b \sqcap a) \sqsubseteq b \sqcap a \sqsubseteq b$$

„⇐": Předpokládejme $x \sqcap a \sqsubseteq b$. Pak

$$\begin{aligned} x &\sqsubseteq \neg a \sqcup x = (a \sqcup \neg a) \sqcap (\neg a \sqcup x) \\ &= (a \sqcap \neg a) \sqcup (a \sqcap x) \sqcup (\neg a \sqcap \neg a) \sqcup (\neg a \sqcap x) \\ &\sqsubseteq \neg a \sqcup (a \sqcap x) \sqsubseteq \neg a \sqcap b \end{aligned}$$

□

Příklad 2.3.3. (Zobecnění příkladu 1.2.12) Buď (X, τ) topologický prostor. Pak $(\tau,\ \subseteq\ ,\ \cup,\ \cap,\ \Rightarrow,\ -)$ je Heytingova algebra, kde $\emptyset = \bot_\tau,\ X = \top_\tau$, supremum $\sqcup$ je sjednocení $\cup$, infimum $\sqcap$ je průnik $\cap$ a

$$A \Rightarrow B := (X \setminus A)^{\text{int}} \cup B$$

je relativní pseudokomplement. Pseudokomplement $\neg A := (X \setminus A)^{\text{int}}$ je vnitřek doplňku. Vnitřek C^{int} je z definice sjednocení všech otevřených podmnožin C a používáme ho, protože doplněk otevřené množiny nemusí být otevřený. Skutečně máme

$$U \subseteq (X \setminus V)^{\text{int}} \cup W \ \text{ právě tehdy, když } \ U \cap V \subseteq W.$$

„⇒": Předpokládejme $U \subset (X \setminus V)^{\text{int}} \cup W$ a $x \in U \cap V$. Pak $x \in U \subseteq (X \setminus V)^{\text{int}} \cup W$, jenže z $x \in V$ máme $x \notin X \setminus V \supseteq (X \setminus V)^{\text{int}}$, a tedy nutně musí být $x \in W$.
„⇐": Předpokládejme $U \cap V \subseteq W$ a $x \in U$. Pak $x \in V \Rightarrow_{\mathcal{P}(X)} W = (X \setminus V) \cup W$, kde $\Rightarrow_{\mathcal{P}(X)}$ je relativní komplement v $\mathcal{P}(X)$. V případě $x \in X \setminus V$ ovšem x leží v otevřené množině (U), takže můžeme BÚNO $x \in X \setminus V$ zesílit na $x \in (X \setminus V)^{int}$.
V případě $\tau = \mathcal{P}(X)$ (diskrétní topologie) zpětně dostáváme příklad 1.2.12.

Interpretace je podobná jako v příkladu 1.2.12, jen místa v X jsou opravdu body prostoru, takže pravdivost výroku se může spojitě měnit. $V(\alpha) = A$ znamená, že α platí v bodech A. Když pak přecházíme do $V(\sim \alpha) = (X \setminus A)^{int}$, kde α neplatí, přejdeme přes okraj ∂A, kde nemusí α platit, ani neplatit:

$$V(\alpha \vee \sim \alpha) = A \cup \neg A = A \cup (X \setminus \overline{A}) = X \setminus (\partial A \setminus A),$$

což není X kdykoliv A není uzavřená.

Uvažujme například výrok $\alpha =$ „Teplota v prostoru X je mezi $20°C$ a $25°C$." Teplota T $(°C)$ je spojité zobrazení $T\colon X \to \mathbb{R}$, takže $V(\alpha) = T^{-1}((20, 25))$ je (z definice spojitého zobrazení) otevřená množina. Obdobně se můžeme ptát na rozpětí tlaku, vlhkosti vzduchu, atd. Také $\beta =$ „V prostoru X prší.", ačkoliv má na otevřených množinách $V(\beta)$ a $\neg V(\beta)$ konstantní hodnoty, na okraji může mít jinou hodnotu. ■

Buď Φ množina výroků v $\mathcal{L}_{PL}$. Definujme relaci $\sim_{\mathbf{ND}}$ na Φ

$$\alpha \sim_{ND} \beta \ \text{ , pokud } \ \vdash_{ND} \alpha \leftrightarrow \beta.$$

Pak $\sim_{\mathbf{ND}}$ je relace ekvivalence a množina tříd ekvivalence $L := \Phi/\ \sim_{\mathbf{ND}}$ je částečně uspořádaná principem „silnější výroky jsou níž":

$$[\alpha] \sqsubseteq [\beta] \quad \text{ pokud } \quad \vdash_{ND} \alpha \to \beta.$$

Věta 2.3.4. $\mathbb{L} = (\Phi/\sim_{\mathbf{ND}}, \sqsubseteq, \cup, \cap, \Rightarrow)$ je Heytingova algebra, kde

$$\begin{aligned} \mathbf{1)}\ & [\alpha] \sqcup [\beta] := [\alpha \vee \beta], \\ \mathbf{2)}\ & [\alpha] \sqcap [\beta] := [\alpha \wedge \beta], \\ \mathbf{3)}\ & [\alpha] \Rightarrow [\beta] := [\alpha \to \beta], \\ \mathbf{4)}\ & \neg[\alpha] := [\sim \alpha]. \end{aligned}$$

Důkaz:

1) Ukážeme, že $\sqcup$ je infimum. Máme $\vdash_{ND} \alpha \to (\alpha \vee \beta)$, $\vdash_{ND} \beta \to (\alpha \vee \beta)$, a pokud $\vdash_{ND} \alpha \to \gamma$ a $\vdash_{ND} \beta \to \gamma$, pak $\vdash_{ND} (\alpha \vee \beta) \to \gamma$:

$$\dfrac{\dfrac{\overline{\alpha \vee \beta}^{\,u} \quad \overline{\alpha \to \gamma} \quad \overline{\beta \to \gamma}}{\gamma} \vee E}{(\alpha \vee \beta) \to \gamma} \to I^u$$

2) $\sqcap$ je supremum: analogické s **1)**.

3) Chceme

$$\vdash_{ND} x \to (\alpha \to \beta) \text{ právě tehdy, když } \vdash_{ND} (x \wedge \alpha) \to \beta.$$

„$\Rightarrow$ " : Předpokládejme $\vdash_{ND} x \to (\alpha \to \beta)$. Pak $\vdash_{ND} (x \wedge \alpha) \to \beta$:

$$\dfrac{\dfrac{\dfrac{\overline{x \to (\alpha \to \beta)} \quad \dfrac{\overline{x \wedge \alpha \text{ platí}}^{\,u}}{\text{x}} \wedge E_1}{\alpha \to \beta} \to E \quad \dfrac{\overline{x \wedge \alpha \text{ platí}}^{\,u}}{\alpha} \wedge E_2}{\beta} \to E}{(x \wedge \alpha) \to \beta} \to I^u$$

„$\Leftarrow$ " : Předpokládejme $\vdash_{ND} x \wedge \alpha \to \beta$. Pak $\vdash_{ND} x \to (\alpha \to \beta)$:

$$\dfrac{\dfrac{\dfrac{\overline{x}^{\,\text{u}} \quad \overline{\alpha}^{\,v}}{x \wedge \alpha} \wedge I \quad x \wedge \alpha \to \beta}{\beta} \to E}{\alpha \to \beta} \to I^v}{x \to (\alpha \to \beta)} \to I^u$$

4) $[\sim \alpha] = [\alpha \to \bot] = [\alpha] \Rightarrow \bot_{\mathbb{L}} = \neg[\alpha]$. □

Pomocí $\mathbb{L}$ ukážeme úplnost Heytingových algeber: pokud $\mathbf{HA} \models \alpha$, máme $\mathbb{L} \models \alpha$, a tedy $V(\alpha) = \top_{\mathbb{L}}$ pro $V\colon \alpha \mapsto [\alpha]$. Z toho $\vdash_{ND} \alpha \leftrightarrow \top$, takže $\vdash_{ND} \alpha$. Spolu s bezesporností, jenž vyplývá z rutinních výpočtů z definice Heytingových algeber, dostáváme charakterizaci Heytingových algeber:

Věta 2.3.5. Syntaktické důsledky **IPL** jsou právě sémantické důsledky **HA**.

$$\begin{aligned} \text{bezespornost pro } \mathbf{ND}\text{: } & \mathbf{HA} \models \alpha, \text{ kdykoliv } \vdash_{\mathbf{ND}} \alpha \\ \text{úplnost pro } \mathbf{ND}\text{: } & \vdash_{\mathbf{ND}} \alpha, \text{ kdykoliv } \mathbf{HA} \models \alpha \end{aligned}$$

Inspirován hilbertovskými systémy Heyting také navrhl následující
Axiomatický systém pro IPL:

Jazyk: $\mathcal{L}_{PL}$ (stejný jako pro **CPL**)
Axiomy:

$$\begin{aligned}
\text{I} &: \alpha \to (\alpha \wedge \alpha) \\
\text{II} &: \alpha \wedge \beta \to \beta \wedge \alpha \\
\text{III} &: (\alpha \to \beta) \to ((\alpha \wedge \gamma) \to (\beta \wedge \gamma)) \\
\text{IV} &: ((\alpha \to \beta) \wedge (\beta \to \gamma)) \to (\alpha \to \gamma) \\
\text{V} &: \alpha \to (\beta \to \alpha) \\
\text{VI} &: \alpha \wedge (\alpha \to \beta) \to \beta \\
\text{VII} &: \alpha \to (\alpha \vee \beta) \\
\text{VIII} &: (\alpha \vee \beta) \to (\beta \vee \alpha) \\
\text{IX} &: ((\alpha \to \gamma) \wedge (\beta \to \gamma)) \to ((\alpha \vee \beta) \to \gamma) \\
\text{X} &: \sim \alpha \to (\alpha \to \beta) \\
\text{XI} &: ((\alpha \to \beta) \wedge (\alpha \to \sim \beta)) \to \sim \alpha
\end{aligned}$$

Pravidla odvozování:

$$\begin{aligned}
\text{Modus ponens (MP): Pokud } &\vdash_{IPL} \alpha \text{ a } \vdash_{IPL} \alpha \to \beta, \text{ pak } \vdash_{IPL} \beta. \\
\text{Substituce (Sub): Pokud } &\vdash_{IPL} \phi(\alpha) \text{ pro každé } \alpha \in \Phi, \text{ pak } \vdash_{IPL} \phi(\beta).
\end{aligned}$$

Podobným způsobem, jako v příkladu **2.3.5**, lze ukázat ([Gol84]):

Věta 2.3.6.

$$\begin{aligned}
\text{bezespornost pro } \mathbf{IPL}\text{: } \mathbf{HA} &\models \alpha, \text{ kdykoliv } \vdash_{\mathbf{IPL}} \alpha \\
\text{úplnost pro } \mathbf{IPL}\text{: } &\vdash_{\mathbf{IPL}} \alpha, \text{ kdykoliv } \mathbf{HA} \models \alpha
\end{aligned}$$

Toto určuje ekvivalenci mezi deduktivním, sémantickým a axiomatickým přístupem k intuicionistické logice.

2.4 Kripkeho sémantika

V intuicionistické logice výrok není pravdivý, pokud jsme ho nedokázali. To ovšem neznamená, že ho nedokážeme nikdy - možná ho dokážeme později, nebo za určitého předpokladu. Jeho pravdivost není absolutní, ale závisí na času a podmínkách, tj. na momentálním *stavu.* Čas a podmínky dávají stavům uspořádání: pokud jsem výrok dokázal dnes, bude od dneška platit navždy. Pokud jsem ukázal, že výrok je důsledek Riemannovy hypotézy a někdo tuto hypotézu dokáže, můj výrok bude od daného momentu platit navždy.

Množina všech stavů P je uspořádána kauzalitou $\sqsubseteq$, a tedy $\mathbb{P} = (P, \sqsubseteq)$ je poset. Pokud jsou dva stavy $p, q \in \mathbb{P}$ uspořádané jako $p \sqsubseteq q$ a výrok $\pi_i \in \Phi_0$ platí ve stavu p, pak musí platit i ve stavu q. Pravdivostní hodnota výroku by měla vyjadřovat, ve kterých stavech platí. Toho můžeme jednoduše docílit zabalením těchto stavů do množiny. Pravdivostní hodnoty

$A \subseteq P$ pak budou *kauzálně uzavřené*, tj. pokud $p \sqsubseteq q$ a $p \in A$, pak $q \in A$. Množinu všech kauzálních podmnožin $\mathbb{P}$ (pravdivostních hodnot) nazveme $\mathbb{P}^+$. Výroky budeme ohodnocovat $\mathbb{P}-$valuací $V\colon \Phi_0 \to \mathbb{P}^+$ s předpisem

$$V(\pi_i) = \{p \in P : \pi_i \text{ je pravdivý v } p\}.$$

Toto lze indukcí rozšířit na $V'\colon \Phi \to \mathbb{P}^+$ následujícími pravidly.

1) $V'(\pi) = V(\pi)$ pro $\pi \in \Phi_0$
2) $V'(\alpha \wedge \beta) = V'(\alpha) \cap V'(\beta)$
3) $V'(\alpha \vee \beta) = V'(\alpha) \cup V'(\beta)$
4) $V'(\sim \alpha) = -V'(\alpha) = \{p \in P;$ pro každé $p \sqsubseteq q$ platí $q \notin V'(\alpha)\}$
5) $V'(\alpha \to \beta) = V'(\alpha) \Rightarrow V'(\beta) =$
$= \{p \in P;$ pro každé $p \sqsubseteq q$ platí $q \in V'(\beta)$ kdykoliv $q \in V'(\alpha)\}$

Pokud podle **4)** v p dokážeme, že α je nepravdivý, v žádném z následujících stavů $p \sqsubseteq q$ výrok α nebude pravdivý. Pravidlo **5)** říká, že pokud ve stavu p dokážeme $\alpha \to \beta$, pak ve všech následujících stavech bude β platit v jakémkoliv stavu, ve kterém platí α.

Výrok α je *pravdivý ve valuaci* V, pokud platí ve všech stavech, tj. $V'(\alpha) = P$. Výrok α je validní v $\mathbb{P}$ (psáno $\mathbb{P} \models \alpha$), pokud je pravdivý ve všech valuacích, tj. $V'(\alpha) = P$ pro libovolné $V\colon \Phi_0 \to \mathbb{P}^+$.

Dvojice $(\mathbb{P}, V'\colon \Phi \to \mathbb{P}^+)$ se nazývají *Kripkeho modely.* V tomto kontextu se danému posetu říká *rámec* (angl. *frame*). Pro alternativní popis kripkeho modelů viz. [Sha].

Příklad 2.4.1. $\mathbb{P} = (\{0;1;2;...;n\}, \Delta_P)$, kde $\Delta_P = \{\langle 0;0\rangle; \langle 1;1\rangle; ...; \langle n;n\rangle\}$ je triviální uspořádání. V tomto posetu je $V'(\sim \alpha) = \{1;2;...;n\} \setminus V'(\alpha)$.

$$V(\alpha \vee \sim \alpha) = V(\alpha) \cup (\{1;2;...;n\} \setminus V(\alpha)) = \{1;2;...;n\} = P,$$

takže $\mathbb{P} \models \alpha \vee \sim \alpha$. Dále

$$V(\sim\sim \alpha) = \{1;2;...;n\} \setminus (\{1;2;...;n\} \setminus V(\alpha)) = V(\alpha),$$

takže $V(\sim\sim \alpha \to \alpha) = P$, a tedy $\mathbb{P} \models \sim\sim \alpha \to \alpha$. Všechny klasické formule jsou validní v $\mathbb{P}$, pravdivostní hodnoty jsou jednoprvkové podmnožiny $\mathbb{P}$ a tvoří Booleovu algebru. Pro $n = 1$ dostaneme klasickou logiku, kde pravdivost v $\{0\}$ znamená absolutní pravdivost a v $\emptyset$ absolutní nepravdivost. ■

Příklad 2.4.2. $\mathbb{P} = (\mathbb{N}, \leq)$, kde $0 \leq 1 \leq 2 \leq ...$ je měkká nerovnost. Pravdivostní hodnoty jsou tzv. *principální množiny*

$$[k) := \{n \in \mathbb{N} : k \leq n\},$$

kde $k \in \mathbb{N}$. Uspořádání $\leq$ představuje *plynutí času*: $V'(\alpha) = [k)$ znamená, že α začne platit za k jednotek času (např. k dnů) od daného počátku. Pokud α začne platit za n jednotek času a β za m jednotek času, jejich disjunkce začne platit, až začne platit alespoň jeden z nich:

$$V(\alpha \vee \beta) = [n) \cup [m) = [\min(n,m))$$

a konjunkce, až začnou platit oba:

$$V(\alpha \wedge \beta) = [n) \cap [m) = [\max(n,m)).$$

Implikace $\alpha \to \beta$ je složitější. Pokud $V(\alpha) \subseteq V(\beta)$, vždy platí β kdykoliv platí α, a tedy $V(\alpha \to \beta) = \top_{\mathbb{N}}$. Pokud $V(\beta) \subseteq V(\alpha)$, v některých stavech může platit α, ale β ne. Jakmile ale začne platit α, platí i β, a tedy $V(\alpha \to \beta) = V(\alpha)$. Z toho dostáváme předpis pro $\mapsto$:

$$[n) \mapsto [m) = \begin{cases} \top_{\mathbb{N}} & \text{pokud } m \leq n, \\ [m) & \text{pokud } n \leq m. \end{cases}$$

Pokud α začne platit za 5 dnů ($V(\alpha) = [5)$), dnes nejde říct ani že platí, ale ani, že neplatí.

$$V(\alpha \vee \sim \alpha) = [5) \cup \emptyset = [5) \neq \top_{\mathbb{N}},$$

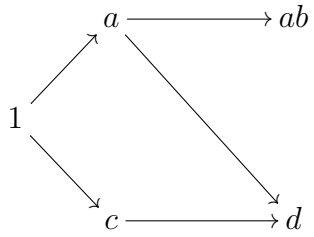
a tedy $\mathbb{P} \not\models \alpha \vee \sim \alpha$. ■

Věta 2.4.3. $(\mathbb{P}^+, \subseteq, \cup, \cap, \mapsto, \neg)$ je Heytingova algebra.
Důkaz. $\bot_{\mathbb{P}^+} = \emptyset$ a $\top_{\mathbb{P}^+} = P$. Dále musíme dokázat

$$A \subseteq B \Rightarrow C \quad \text{právě tehdy, když} \quad A \cap B \subseteq C$$

„⇒": Předpokládejme $A \subseteq B \Rightarrow C$. Pokud $p \in A \cap B$, musí být $p \in B$ a $p \in B \Rightarrow C$, takže pro každé $p \sqsubseteq q$ je $q \in C$. Jenže $p \sqsubseteq p$, takže $p \in C$.
„⇐": Předpokládejme $A \cap B \subseteq C$. Pak pokud $p \in A$ a $q \in B$ pro nějaké $p \sqsubseteq q$, musí být $q \in A$ (plyne z kauzální uzavřenosti A) a tedy $q \in A \cap B$, takže $q \in C$. Zpětným zabalením do definice máme $p \in B \Rightarrow C$. □

Příklad 2.4.4. Uvažujme následující poset $\mathbb{P}$ reprezentovaný následujícím diagramem.



V tomto orientovaném grafu jsou vrcholy prvky $\mathbb{P}$ a šipka $x \to y$ značí $x \sqsubseteq y$. Nechť výroky $\alpha, \beta, \gamma, \delta$ mají pravdivostní hodnoty

$$V(\alpha) = [ab), \quad V(\beta) = [a), \quad V(\gamma) = [d), \quad V(\delta) = [c).$$

Jakmile se dostaneme do stavu v množině

$$V(\alpha \vee \sim \alpha) = [ab) \cup [c) = \{ab, c, d, \emptyset\},$$

máme pravdivost α rozhodnutou. Dále

$$V(\sim \alpha \vee \sim \gamma) = [c) \cup [ab), \quad \text{ale} \quad V'(\sim (\alpha \wedge \gamma)) = \neg(\emptyset) = [1),$$

protože ve stavu a neplatí $\sim \gamma$, ale $\sim (\alpha \wedge \gamma)$ platí vždy. Ve stavu 1 nelze rozhodnout, zda-li platí β nebo $\sim \alpha$, ale $\alpha \to \beta$ lze rozhodnout, protože to platí vždy. Pak tedy

$$V(\alpha \to \beta) = [1), \text{ ale } V(\sim \alpha \vee \beta) = [a) \cup [c),$$

Dále $V(\sim\sim \gamma) = \neg[ab) = [d)$, takže

$$V(\sim\sim \gamma \to \gamma) = [d) \Rightarrow [c) = [a) \neq [1).$$

Stavy a, c jsou neporovnatelné, takže

$$V((\beta \to \delta) \vee (\delta \to \beta)) = [d) \cup ([d) \cap [ab)) = \{d, ab\} \neq [1)$$

Z $\alpha \wedge \delta$ vyplývá γ, ale ve stavu 1 ještě nevíme, jestli platí $\alpha \to \gamma$ nebo $\delta \to \gamma$. Až se přesuneme do stavu a nebo c, jedno z β, δ začne platit, takže z toho druhého začne vyplývat γ (protože $\alpha \wedge \delta \to \gamma$ platí v celém $\mathbb{P}$). Máme

$V((\beta \wedge \delta) \to \gamma) = [d) \Rightarrow [d) = [1)$, ale $V((\beta \to \gamma) \vee (\delta \to \gamma)) = ([ab) \cup [d)) \cup [d) = [d) \cup [ab) \neq [1)$.

Ve výše popsaném framu neplatí tautologie **2)-7)** z příkladu 1.1.1.

$$\mathbb{P} \not\models (\sim \alpha \vee \sim \beta) \leftrightarrow (\sim (\alpha \wedge \beta))$$
$$\mathbb{P} \not\models (\alpha \to \beta) \leftrightarrow (\sim \alpha \vee \beta)$$
$$\mathbb{P} \not\models (\sim\sim \alpha) \leftrightarrow \alpha$$
$$\mathbb{P} \not\models \alpha \vee \sim \alpha$$
$$\mathbb{P} \not\models (\alpha \to \beta) \vee (\beta \to \alpha)$$
$$\mathbb{P} \not\models ((\beta \wedge \delta) \to \gamma) \leftrightarrow ((\beta \to \gamma) \vee (\delta \to \gamma))$$

■

Po zbytek práce se budeme věnovat zobecněním posetů, tzv. *kategoriím*. V kategoriích může mezi dvěma vrcholy být více než jedna šipka. To vyjadřuje existenci více způsobů, jak se dostat z jednoho stavu do druhého.

Kapitola 3

Toposy

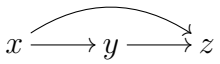
Následující kapitola představuje *teorii kategorií* a její velmi expresivní jazyk, kterým později definujeme nástroje užitečné při konstrukci modelů intuicionistické logiky.

3.1 Motivace

Reprezentace posetu v příkladu 2.4.4 nám umožňuje chápat některé jeho vlastnosti prostřednictvím „přirozených operacích na šipkách". V případě, kdy je uvažovaný poset Heytingova algebra, můžeme existenci šipky $x \to y$ chápat doslova jako „z x lze odvodit y".

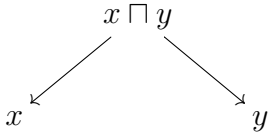
• *reflexivita:* Každý prvek x má „triviální šipku" $x \to x$. Toto logicky koresponduje faktu, že každý výrok plyne sám ze sebe.

• *tranzitivita:* Šipky $x \to y$ a $y \to z$ můžeme „složit" do šipky $x \to z$, diagramaticky zapsáno

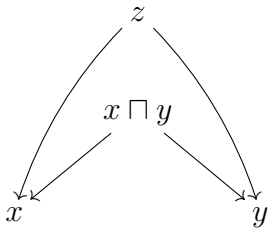


Logicky to koresponduje faktu, že pokud z x plyne y a z y plyne z, pak z x plyne z.

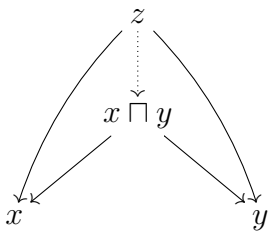
• *infimum:* Z $x \sqcap y$ vede šipka do x a y.



Logicky toto koresponduje k pravidlům $\wedge E_1, \wedge E_2$ v **ND**. Dále pokud ze z vedou šipky $z \to x$ a $z \to y$,

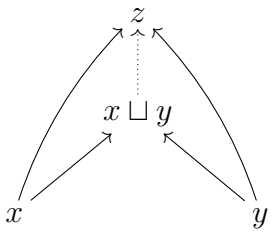


musí existovat šipka $z \to x \sqcap y$. Šipky existující „z nutnosti" zapisujeme přerušovaně:



Ze všech objektů, ze kterých vede šipka do x a y, je $x \sqcup y$ „univerzální" ve smyslu, že ze všech ostatních takových objektů musí vést šipka do $x \sqcup y$. Logicky toto koresponduje k pravidlu $\wedge E$.

• *supremum:* Situace je analogická jako pro infima, akorát jsou všechny šipky „naopak":

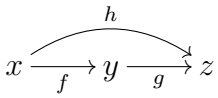


šipky $x \to x \sqcup y$ a $y \to x \sqcup y$ logicky vyjadřují $\vee I_1, \vee I_2$ a univerzalita $x \sqcup y$ vyjadřuje $\vee E$.

Stejnou „analýzu šipek" můžeme provést pro množiny: vrcholy (dále jen *objekty*) budou značit množiny a šipky funkce. Mezi dvěma množinami může být více než jedna funkce a obecně je nebudeme kreslit všechny.

• *„reflexivita":* Pro každou množinu A lze definovat funkci $id_A : A \to A$ s předpisem „nic nedělej": $x \mapsto x$

• *„tranzitivita":* Pokud $f : A \to B$ a $g : B \to C$ jsou funkce, můžeme sestrojit funkci $h : A \to C$ pravidlem $h(x) = g(f(x))$. Pak pro každé $x \in A$ platí, že ať v diagramu

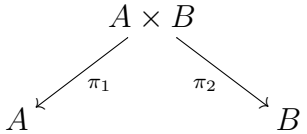


půjdeme z A do C „po šipkách" jakoukoliv cestou (buď si vybereme f a g, nebo h), dostaneme stejný výsledek. Říkáme, že tento diagram *komutuje.* Nad rovností

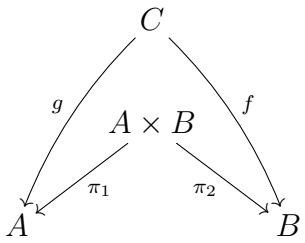
$$h(x) = g(f(x)) \quad \text{pro každé } x \in A,$$

je jednodušší uvažovat jako nad rovností funkcí $h = g \circ f$.

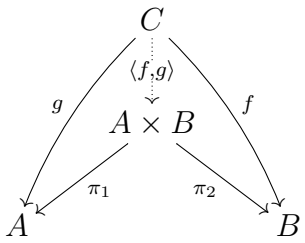
• *„infimum":* Z kartézského součinu $A \times B$ vede funkce $\pi_1 \colon A \times B \to A$ s předpisem „zapomeň druhou komponentu". $[x; y] \mapsto x$ a $\pi_2 \colon A \times B \to B$ s předpisem „zapomeň první komponentu": $[x; y] \mapsto y$.



Pokud máme funkce $f : C \to A$ a $g : C \to B$,



můžeme sestrojit funkci $\langle f, g\rangle \colon C \to A \times B$ s předpisem $\langle f, g\rangle(x) = [f(x); g(x)]$. Ta je jedinečná taková, že diagram

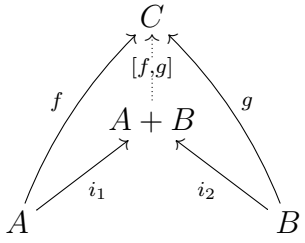


komutuje (což v tomto případě znamená $\pi_1 \circ \langle f, g\rangle = f$ a $\pi_2 \circ \langle f, g\rangle = g$). Zde přerušovaná čára neznamená jen „existuje z nutnosti" jako v případě posetů, ale „existuje z nutnosti a je jedinečná taková, že diagram komutuje."

• *„supremum":* D disjunktního sjednocení $A + B := A \times \{0\} \cup B \times \{1\}$ vede $i_1 \colon A \to A + B$ s předpisem $x \mapsto [x; 0]$ a $i_2 \colon B \to A + B$ s předpisem $x \mapsto [x; 1]$. Funkce $f \colon A \to C$ a $g \colon B \to C$ nám určují právě jednu funkci $[f; g] : A + B \to C$ s předpisem

$$[f; g]([x; i]) = \begin{cases} f(x) & \text{pokud } \ i = 0, \\ g(x) & \text{pokud } \ i = 1, \end{cases}$$

takovou, že



komutuje.

Hlavní myšlenka teorie kategorií je, že výše popsanou „analýzu šipek" lze provádět v mnoha rozmanitých situacích. Tyto situace tím objasňuje, zjednodušuje a dává do souvislosti s jinými, na první pohled odlišně vypadajícími situacemi. Šipce $a \to a$ zobecňující reflexivitu říkáme *identita,* zobecnění tranzitivity je *skládání šipek* (operace $\circ$), zobecnění infima je *produkt* a suprema *koprodukt.*

Obecněji mohou *objekty* představovat různé matematické objekty a šipky zobrazení mezi nimi. Soubor objektů a šipek, tzv. *kategorie*, tvoří prostředí pro matematickou teorii. První

příklad je poset $\mathbb{P}$, jehož objekty jsou prvky a šipky značí ono uspořádání. Druhý příklad je kategorie **Set**, jejíž objekty jsou množiny a šipky funkce. Teorie grup hovoří o kategorii **Grp**, jejíž objekty jsou grupy a šipky grupové homomorfismy; lineární algebra hovoří o kategorii **k-Vect**, jejíž objekty jsou vektorové prostory nad tělesem k a šipky lineární transformace; topologie hovoří o kategorii **Top**, jejíž objekty jsou topologické prostory a šipky spojitá zobrazení. Mnoho konstrukcí používané v těchto teoriích jsou kategoriální: objekty lze popsat tím, jaké z nich a do nich vedou šipky. Například výše popsaná konstrukce pro produkty (zobecnění infima) v **Grp**, **k-Vect** a **Top** určuje přesně objekt, který je v dané teorii známý jako „součin": pro **Grp** je to přímý součin grup s násobením „po komponentách", v **k-Vect** je to součin vektorových prostorů se sčítáním „po komponentách" a v **Top** je to součin topologických prostorů, jehož topologii generují kartézské součiny prvků bází jednotlivých prostorů.

„Pěkně se chovající" vztahy mezi matematickými objekty různého druhu (z množiny uděláme volnou grupu, z grupy lineární reprezentaci, z topologického prostoru fundamentální grupu), tzv. *funktory*, jsou zobrazení mezi danými kategoriemi zachovávající kategoriální strukturu. Toto nám umožňuje vytvářet vztahy mezi různými matematickými disciplínami.

Další přínos teorie kategorií je velmi sugestivní diagramatické znázornění vztahů pomocí komutativních diagramů. Diagram označujeme jako $\mathcal{C}-$diagram, pokud jeho vrcholy jsou objekty z kategorie $\mathcal{C}$. Například pravidlo

$$V(\sim \alpha) = \neg V(\alpha) \qquad \text{pro každé } \alpha \in \Phi$$

pro $\mathbb{H}-$valuaci $V\colon \Phi \to H$ lze přepsat jako rovnost funkcí $V \circ \sim \; = \neg \circ V$, a tedy znázornit komutativním **Set**-diagramem

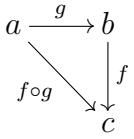
$$\begin{array}{ccc} \Phi & \xrightarrow{\sim} & \Phi \\ {\scriptstyle V}\downarrow & & \downarrow{\scriptstyle V} \\ H & \xrightarrow{\neg} & H. \end{array}$$

Úloha V je zde „přetáhnout" Φ na $\mathbb{H}$ takovým způsobem, aby se $\sim$ změnilo na $\neg$. Tím jsme kategoriálně vyjádřili, že $\neg$ je interpretace $\sim$.

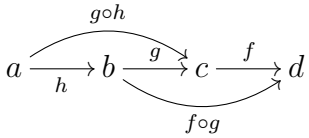
3.2 Základní pojmy

V následující sekci výše popsané myšlenky formalizujeme.

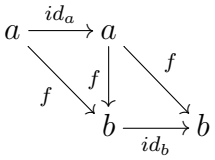
Definice 3.2.1. Kategorie $\mathcal{C}$ obsahuje
1) soubor $\mathbf{Ob}(\mathcal{C})$ $\mathcal{C}-$objektů,
2) „hom-set" $\mathrm{Hom}_{\mathcal{C}}(a,b)$ pro každé $\mathcal{C}-$objekty a, b. Prvky hom-setů se nazývají $\mathcal{C}-$šipky a píše se $f\colon a \to b$ jako zkratka pro $f \in \mathrm{Hom}_{\mathcal{C}}(a,b)$,
3) operace dom, cod, které každé $\mathcal{C}-$šipce $f\colon a \to b$ přiřadí $\mathrm{dom}\, f = a$ a $\mathrm{cod}\, f = b$,
4) operaci $\circ$, která každým dvěma šipkám s $\mathrm{cod}\, g = \mathrm{dom}\, f$ přiřadí kompozici $f \circ g$ tak, aby diagram



komutoval. Dále musí platit $f \circ (g \circ h) = (f \circ g) \circ h$, kdykoliv jsou $f \circ g$ a $g \circ h$ definovány. Jinak řečeno, diagram



komutuje.
5) operaci $id_{(-)}$, která každému $\mathcal{C}-$objektu a přiřadí $\mathcal{C}-$šipku $id_a \colon a \to a$ takovou, že $f \circ id_a = f = id_b \circ f$ pro každou $\mathcal{C}-$šipku $f \colon a \to b$. Jinak řečeno, diagram



komutuje.

Příklad 3.2.2. Kategorie $\mathbb{P}$, **Set**, **Grp**, **k-Vect**, **Top**, popsané v sekci **3.1**. ■

Příklad 3.2.3. Jakoukoliv množinu X lze chápat jako „diskrétní" kategorii: objekty jsou prvky X a jediné šipky jsou identity. ■

Příklad 3.2.4. Monoid $\mathbb{M} = (M, \cdot, e)$ lze chápat jako kategorii s jedním objektem $*$. Prvky monoidu $m \in \mathbb{M}$ jsou jednoduše šipky $m \colon * \to *$. Skládání šipek je násobení v $\mathbb{M}$: $m \circ n \colon * \to *$ je prvek $m \cdot n \in \mathbb{M}$. Identita v $\mathbb{M}$ je $e_{\mathbb{M}} = id_* \colon * \to *$. Naopak pro každou kategorii $\mathcal{C}$ a $\mathcal{C}-$objekt a je $\mathrm{Hom}_{\mathcal{C}}(a, a)$ monoid. ■

Příklad 3.2.5. Homomorfismus Heytingových algeber $\phi \colon \mathbb{H} \to \mathbb{K}$ je monotónní zobrazení $\phi \colon H \to K$ takové, že pro každé $a, b \in H$ platí

1) $\phi(a \sqcup b) = \phi(a) \sqcup \phi(b)$
2) $\phi(a \sqcap b) = \phi(a) \sqcap \phi(b)$
3) $\phi(a \Rightarrow b) = \phi(a) \Rightarrow \phi(b)$

Heytingovy algebry jsou objekty kategorie **HeytAlg**, jejíž šipky jsou právě homomorfismy Heytingových algeber. ■

Definice 3.2.6. Buď $\mathcal{C}$ kategorie. Definujeme *opačnou* kategorii $\mathcal{C}^{op}$, jejíž objekty jsou $\mathcal{C}-$objekty a šipky jsou $f^{op} \colon b \to a$ pro každou $\mathcal{C}-$šipku $f \colon a \to b$.

Výše popsaná konstrukce je teoreticky velmi důležitá: pokud S je věta v jazyce teorie kategorií, pak existuje *duální* věta S^{op}, kterou z S dostaneme změnou

$$\begin{aligned} dom\ f &\mapsto cod\ f, \\ cod\ f &\mapsto dom\ f, \\ (f = g \circ h) &\mapsto (f = h \circ g). \end{aligned}$$

Pokud S vyplývá z axiomů teorie kategorií, pak platí ve všech kategoriích $\mathcal{C}$. Každá kategorie je ale opačná k nějaké kategorii, takže S^{op} musí platit ve všech kategoriích. Tento poznatek se nazývá *princip duality.* Každou kategoriální konstrukci lze dualizovat „obrácením" šipek, čímž se zachová její validita.

Příklad 3.2.7. Buď $\mathbb{P} = (P, \sqsubseteq)$ poset, který chápeme jako kategorii. $\mathbb{P}^{op} = (P, \sqsupseteq)$ je duální poset s uspořádáním

$$x \sqsupseteq y \quad \text{právě tehdy, když} \quad y \sqsubseteq x.$$

Infima v $\mathbb{P}$ jsou suprema v $\mathbb{P}^{op}$ a suprema v $\mathbb{P}$ jsou infima v $\mathbb{P}^{op}$. Explicitně zapsáno,

$$\begin{aligned} x \sqcup_{\mathbb{P}} y &= x \sqcap_{\mathbb{P}^{op}} y \\ x \sqcap_{\mathbb{P}} y &= x \sqcup_{\mathbb{P}^{op}} y. \end{aligned}$$

Říkáme, že supremum a infimum jsou *duální operace.* ■

Definice 3.2.8. Buď $\mathcal{C}$ kategorie. Šipka $f\colon a \to b$ je *isomorfismus* (zkráceně iso), pokud existuje šipka $g\colon b \to a$ taková, že $f \circ g = id_b$ a $g \circ f = id_a$. Pokud mezi a, b existuje isomorfismus, píšeme $a \cong b$ a říkáme, že a, b jsou isomorfní.

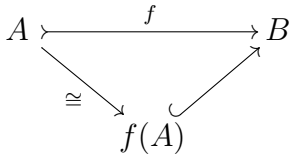
Poznámka. Šipka g je jednoznačně definována a nazývá se *inverze k* f. Píšeme $g = f^{-1}$. Isomorfismus je jako koncept duální sám sobě: pokud $f\colon a \to b$ je iso v $\mathcal{C}$, pak $f^{op}\colon b \to a$ je iso v $\mathcal{C}^{op}$. Všechny kategoriální konstrukce pro objekt a lze aplikovat na objekt $b \cong a$ „přetáhnutím" přes iso šipku $f\colon a \to b$. Naopak, pokud objekt a definujeme kategoriální konstrukcí, není definovaný jednoznačně v normálním slova smyslu, neboť každý objekt s a isomorfní bude splňovat stejné „kategoriální" vlastnosti. Jedinečnost v teorii kategorií tedy neznamená jedinečnost až na rovnost, ale jedinečnost *až na isomorfismus.*

Příklad 3.2.9. V **Set** jsou isomorfismy bijekce. V **Grp** jsou to isomorfismy grup, v **Top** homeomorfismy a v **HeytAlg** bijektivní homomorfismus Heytingových algeber. Jednoobjektová kategorie, jejíž všechny šipky jsou iso, je kategoriální grupa (analogicky s příkladem **3.1.6**) a naopak soubor všech iso šipek $a \to a$ v jakékoliv kategorii je grupa. ■

Definice 3.2.10. Buď $\mathcal{C}$ kategorie. Šipka $f : b \rightarrowtail c$ je *monomorfismus* (zkratka monic), pokud pro každé dvě šipky $g, h\colon a \to b$ platí $g = h$, kdykoliv $f \circ g = f \circ h$. Šipka $f\colon a \twoheadrightarrow b$ je *epimorfismus* (zkratka epic), pokud pro každé dvě šipky $g, h\colon a \to b$ platí $g = h$, kdykoliv $g \circ f = h \circ f$ (duální koncept k monomorfismu). V diagramech se monické šipky značí symbolem $\rightarrowtail$ a epické symbolem $\twoheadrightarrow$.

Příklad 3.2.11. V **Set** jsou monomorfismy prosté funkce, epimorfismy surjektivní funkce. Triviální případ prostých funkcí jsou *inkluze* $A \hookrightarrow B$ s předpisem $x \mapsto x$, které jen „vloží"prvky A do B. Naopak pokud máme v **Set** prostou funkci $f\colon A \rightarrowtail B$, můžeme ji „přetáhnout" na

inkluzi $f(A) \hookrightarrow B$, kde $f(A) = \{f(x);\ x \in A\}$ tak, že diagram



komutuje.
Každá bijekce je prostá a surjektivní a obecněji každá iso šipka je monic i epic. Naopak to ale neplatí: např. v **Top** je zobrazení $[0;1] \to S^1$ s předpisem $x \mapsto e^{2\pi ix}$ epic a monic, ale ne iso. ■

Definice 3.2.12. Buď $\mathcal{C}, \mathcal{D}$ kategorie. Funktor $F\colon \mathcal{C} \to \mathcal{D}$ je soubor $\mathcal{D}-$objektů $F(a)$ pro každý $\mathcal{C}-$objekt a a $\mathcal{D}$-šipek $Ff\colon F(a) \to F(b)$ pro každou $\mathcal{C}-$šipku $f : a \to b$ takový, že
1) $F(f \circ g) = Ff \circ Fg$, kdykoliv $f \circ g$ je definována,
2) $F(id_a) = id_{F(a)}$.
Tyto vlastnosti se nazývají *funktorialita.*

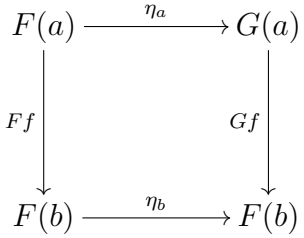
Příklad 3.2.13. Nechť $F\colon \mathbb{P} \to \mathbb{Q}$, kde $\mathbb{P}$ a $\mathbb{Q}$ jsou posety. Pokud $p \subseteq q$, pak v $\mathbb{P}$ jakožto v kategorii bude právě jedna šipka $pq\colon p \to q$. Pak v $\mathbb{Q}$ budeme mít šipku $Fpq\colon F(p) \to F(q)$, takže $F(p) \subseteq F(q)$ v $\mathbb{Q}$. F je tedy monotónní zobrazení (šipka v **Pos**). ■

Příklad 3.2.14. Nechť $F\colon \mathbb{M} \to \mathbb{N}$ jsou monoidy. Z funktoriality platí pro každé dvě $\mathbb{M}-$šipky $x, y\colon M \to M$

$$F(x \circ y) = Fx \circ Fy,$$

tedy F je homomorfismus (šipka v **Mon**). Pokud bychom volili $\mathbb{M}, \mathbb{N}$ grupy, F by byl homomorfismus grup. ■

Definice 3.2.15. Buď $F, G\colon \mathcal{C} \rightrightarrows \mathcal{D}$ funktory. *Přirozená* transformace $\eta\colon F \to G$ je soubor $\mathcal{D}-$šipek $\eta_a\colon F(a) \to G(a)$ pro každý $\mathcal{C}-$objekt a, jenž splňuje tzv. *axiom přirozenosti:*



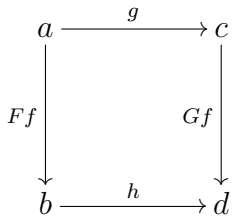
komutuje pro jakékoliv $\mathcal{C}-$objekty a, b a $\mathcal{C}-$šipku $f\colon a \to b$. Šipky η_a, η_b se nazývají *komponenty* η.

Definice 3.2.16. Buď $\mathcal{D}, \mathcal{C}$ kategorie. *Funktorová kategorie* $\mathcal{D}^{\mathcal{C}}$ má objekty funktory $F\colon \mathcal{C} \to \mathcal{D}$ a šipky přirozené transformace $\eta\colon F \to G$. Skládání přirozených transformací je asociativní a pro každý funktor F lze definovat přirozenou transformaci $id_F\colon F \to F$ s $id_F(a) = a$ pro každý $\mathcal{D}-$objekt a.

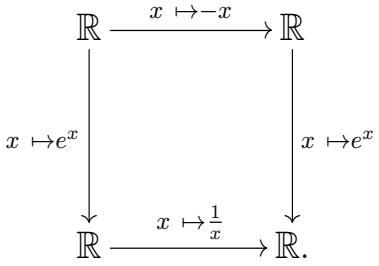
Příklad 3.2.17. Buď $\mathcal{C}$ libovolná kategorie a $\longrightarrow$ kategorie s objekty $0, 1$ a jedinou netriviální šipkou $f\colon 0 \to 1$.

$$0 \xrightarrow{f} 1$$

Objekt $\mathcal{C}^{\to}$ je funktor F z $\longrightarrow$ do $\mathcal{C}$, tj. soubor $\mathcal{C}$-objektů $a = F(0), b = F(1)$ a $\mathcal{C}-$šipky $Ff\colon a \to b$ ($F(id_0), F(id_1)$ pro jednoduchost ignorujeme). Ještě jednodušeji můžeme F chápat jen jako $\mathcal{C}$-šipku Ff (a, b dostaneme operacemi dom, cod). $\mathcal{C}^{\to}$-šipka (přirozená transformace) $\eta\colon F \to G$ mezi $\mathcal{C}-$šipkami $Ff\colon a \to b$ a $Gf\colon c \to d$ je dvojice $[g, h]$ $\mathcal{C}-$šipek $g = \eta_0\colon a \to c$ a $h = \eta_1\colon b \to d$ takových, že



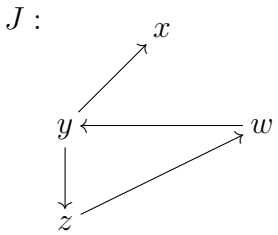
komutuje. Pokud například funkce $k, l\colon \mathbb{R} \rightrightarrows \mathbb{R}$ mají předpis $k(x) = -x, l(x) = \frac{1}{x}$, pak $[r; r]\colon k \to l$, kde $r\colon \mathbb{R} \to \mathbb{R}$ má předpis $r(x) = e^x$, je $\mathbf{Set}^{\to}-$šipka:

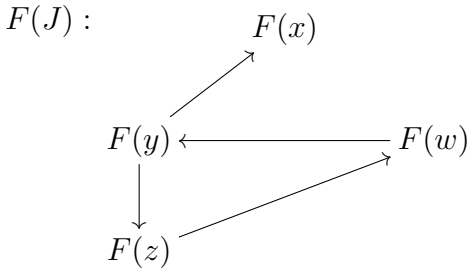


Exponenciální funkce takto doslova mění additivní inverze $(-x)$ na multiplikativní inverze $(\frac{1}{x}.)$ ■

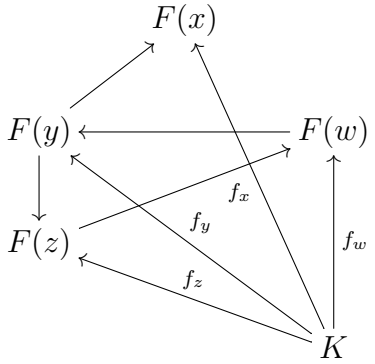
V následující definici formalizujeme diagramy a zavedeme pojmy *limita* a *kolimita* diagramu. Pak rozebereme různé instance těchto konstrukcí.

Definice 3.2.18. *Malá* kategorie je taková, jejíž objekty a Hom-sety nejsou vlastní třídy. Buď $\mathcal{C}$ libovolná kategorie a buď J malá kategorie. $\mathcal{C}-$diagram je funktor $F\colon J \to \mathcal{C}$. *Kužel* diagramu F je $\mathcal{C}-$objekt K a soubor $\mathcal{C}-$šipek $f_a\colon K \to F(a)$ pro každý $J-$objekt a takový, že $Ff \circ f_a = f_b$ pro každou $J-$šipku $f\colon a \to b$. *Limita* diagramu F je kužel $(\lim F, \{f_a\colon a \text{ je } J-\text{objekt}\})$ takový, že pokud $(N, \{g_a : a \text{ je } J-\text{objekt}\})$ je kužel, pak existuje právě jedna $\mathcal{C}-$šipka $f\colon N \to \lim F$ taková, že $f_a \circ f = g_a$ pro každý $J-$objekt a.

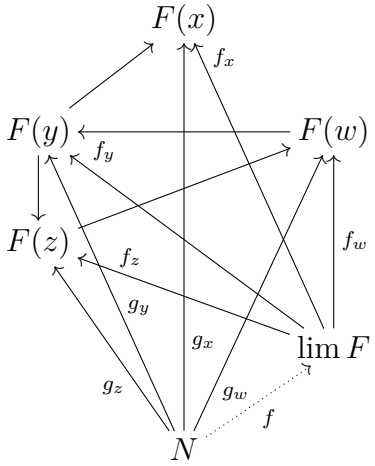




Definice pro kužel $(K, \{f_a\colon a \text{ je } J-\text{objekt}\})$ říká, že $\mathcal{C}-$diagram

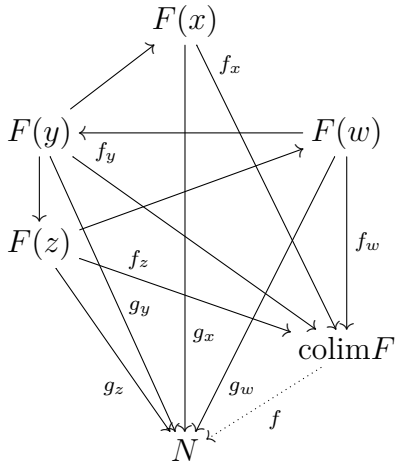


komutuje. Šipky mezi $J-$objekty komutovat nemusí, ale pro každé $\mathcal{C}-$objekty a, b a $\mathcal{C}-$šipku f platí $Ff \circ f_a = f_b$.



Existenci a jedinečnosti šipky f říkáme *univerzální vlastnost.* Z definice vyplývá, že objekt $\lim F$ je definován až na jedinečný isomorfismus.

Definice 3.2.19. Kolimita diagramu $F : J \to \mathcal{C}$ (colim F) je definována duálně k limitě.



Existenci a jedinečnosti $f\colon$ colim $F \to N$ říkáme *kouniverzální vlastnost.* Objekt colim F je opět definován až na jedinečný isomorfismus.

V dalších pár příkladech si ukážeme limity jednoduchých diagramů, které budeme po zbytek práce využívat. Každá z limit existuje jen v některých kategoriích. Pokud má $\mathcal{C}$ limitu každého konečného diagramu (J má konečně mnoho objektů), říkáme, že $\mathcal{C}$ je konečně úplná. Duální koncept ($\mathcal{C}$ má kolimitu každého konečného diagramu) je konečná koúplnost.

Příklad 3.2.20. Terminální objekt $1_\mathcal{C}$ kategorie $\mathcal{C}$ je limita prázdného diagramu (J nemá objekty). Je to tedy $\mathcal{C}-$objekt $1_\mathcal{C}$ takový, že pro každý $\mathcal{C}-$objekt a existuje právě jedna šipka $a \to 1$:

$$a \dashrightarrow 1_\mathcal{C}.$$

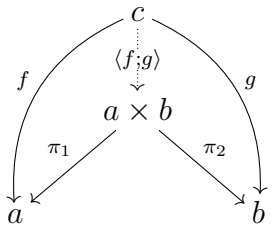
V **Set** je terminální objekt každá jednoprvková množina $\{*\}$. BÚNO volíme $1 := \{0\}$ (zapisujeme terminální objekt doslova jako ordinál 1). V **Grp** je terminální objekt triviální grupa. V $\mathbb{P}$ je terminální objekt největší prvek $\top_\mathbb{P}$. ■

Příklad 3.2.21. *Iniciální* objekt je definován duálně k terminálnímu objektu jako *kolimita* prázdného diagramu: objekt $0_\mathcal{C}$ takový, že pro každý $\mathcal{C}-$objekt a existuje právě jedna šipka $0 \to a$. V **Set** je iniciální objekt prázdná množina $\emptyset$: na definování funkce $\emptyset \to A$ z prázdné množiny nepotřebujeme předpis. ■

Příklad 3.2.22. Produkt $a \times b$ je limita následujícího diagramu:

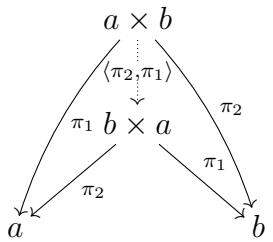
$$a \bullet \qquad \bullet\, b.$$

Šipky z $a \times b$, tzv. *projekce*, jsou $\pi_1 \colon a \times b \to a$ a $\pi_2 \colon a \times b \to b$. Pokud z nějakého objektu c vedou šipky $f \colon c \to a$ a $g \colon c \to b$, pak existuje právě jedna šipka $\langle f ; g \rangle \colon c \to a \times b$ taková, že

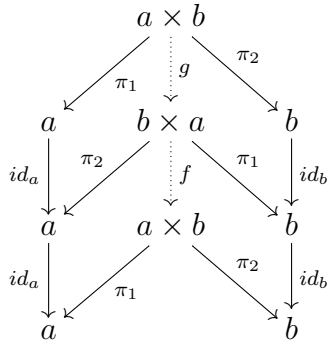


komutuje. ■

Poznámka. Nechť $\mathcal{C}$ má produkty. Pak $a \times b \cong b \times a$ pro libovolné $\mathcal{C}-$objekty a, b. Máme totiž jedinečné $f = \langle \pi_2, \pi_1 \rangle \colon a \times b \to b \times a$ tak, že

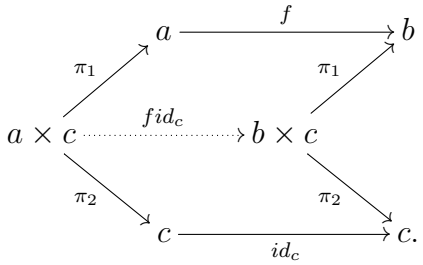


komutuje a analogicky $g \colon b \times a \to a \times b$. Pak $f \circ g \colon a \times b \to a \times b$ je jedinečná taková, že



komutuje, a tedy $\pi_1 \circ (f \circ g) = id_a \circ id_a \circ \pi_1$. Jenže $id_{a\times b}$ toto splňuje, takže $f \circ g = id_{a\times b}$ a tedy f je iso, z čehož $a \times b \cong b \times a$.

Poznámka. Nechť $\mathcal{C}$ má produkty. Pak $F\colon \mathcal{C} \to \mathcal{C}$ s předpisem $a \mapsto a \times c$ je funktor, který šipce $f\colon a \to b$ přiřadí jedinečnou šipku $Ff = f \times id_c = \langle f \circ \pi_1, g \circ \pi_2 \rangle\colon a \times c \to b \times c$ existující z univerzální vlastnosti produktu $b \times c$:

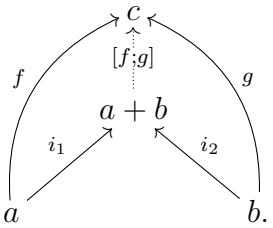


V případě $\mathcal{C} = \mathbb{P}$ (poset) nám výsledek této poznámky dává alternativní důkaz lemmatu **1.2.5** (monotónní zobrazení $\mathbb{P} \to \mathbb{P}$ je funktor $\mathbb{P} \to \mathbb{P}$, infima v $\mathbb{P}$ jsou produkty).

Příklad 3.2.23. Koprodukt $a + b$ je colimita diagramu

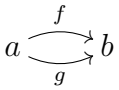
$$a \bullet \qquad \bullet\ b.$$

Šipky do $a+b$, tzv. *injekce*, značíme i_1, i_2. Pokud do c vedou šipky $f\colon a \to c$ a $g\colon b \to c$, pak existuje právě jedna šipka $[f; g]\colon a + b \to c$ taková, že

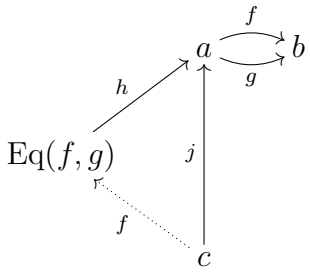


komutuje. ■

Příklad 3.2.24. Equalizer $\mathrm{Eq}(f, g)$ šipek $f, g : a \rightrightarrows b$ je limita diagramu



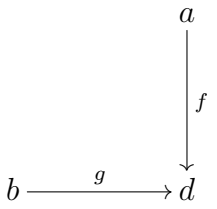
Šipka $h\colon\ \mathrm{Eq}(f,g) \to a$ splňuje $f \circ h = g \circ h$, a pokud $f \circ j = g \circ j$ pro jakýkoliv $j\colon c \to a$, pak existuje právě jedna šipka $f\colon c \to \mathrm{Eq}(f,g)$ taková, že diagram



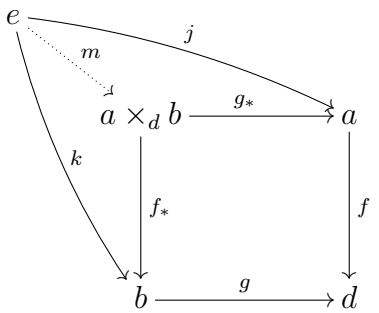
komutuje.

V **Set** je $\mathrm{Eq}(f,g) = \{x : f(x) = g(x)\}$; $h\colon\ \mathrm{Eq}(f,g) \hookrightarrow a$ inkluze. V **Grp** lze pro každé grupy G, H sestrojit homomorfismus triv: $G \to H$ s předpisem triv: $x \mapsto e_H$ (e_H je identita v H). Pak Eq(f, triv)= ker f. Obecněji equalizer $\mathrm{Eq}(f,g)$ nese informaci o „řešeních rovnice $f(x) = g(x)$". ■

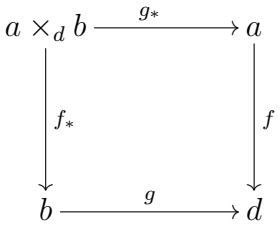
Příklad 3.2.25. Pullback $a \times_d b$ je limita diagramu



Šipky $f_*\colon a \times_d b \to b$ a $g_*\colon a \times_d b \to a$ splňují $g \circ f_* = f \circ g_*$. Pokud existuje objekt e a šipky $j\colon e \to a,\ k\colon e \to b$ splňující $f \circ j = g \circ k$, pak existuje právě jedna šipka $m\colon e \to a \times_d b$ taková, že



komutuje. Říkáme, že diagram



je pullback v $\mathcal{C}$.

V **Set** je $A \times_D B = \{[x;y] \in A \times B; f(x) = g(y)\}$, f_* má předpis $[x;y] \mapsto x$ a g_* má předpis $[x;y] \mapsto y$. ■

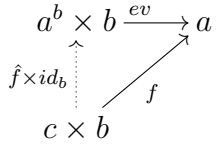
Definice 3.2.26. Buď $\mathcal{C}$ kategorie s terminálním objektem. *Globální prvek* $\mathcal{C}$-objektu a je šipka $x : 1 \to a$.

Příklad 3.2.27. V **Set** jsou globální prvky funkce $\hat{x}\colon \{0\} \to A$ s předpisem $\hat{x}(0) = x \in A$. Předpis

$$\begin{aligned}(x \in A) &\mapsto (\hat{x}\colon \{0\} \to A,\ \hat{x}(0) = x)\\ (\hat{x}\colon \{0\} \to A) &\mapsto (\hat{x}(0) \in A)\end{aligned}$$

určuje bijekci $A \cong \mathrm{Hom}_{\mathbf{Set}}(1, A)$. V **Set** jsou tedy globální prvky „totéž", co prvky. ■

Definice 3.2.28. Buď $\mathcal{C}$ kategorie a a, b $\mathcal{C}-$objekty. *Exponent* a, b, pokud existuje, je $\mathcal{C}-$objekt a^b spolu s $\mathcal{C}-$šipkou *„evaluace"* $ev\colon a^b \times b \to a$, splňující následující univerzální vlastnost: pro každou šipku $f : c \times b \to a$ existuje právě jedna šipka $\hat{f}\colon c \to a^b$ taková, že



komutuje, kde $\hat{f} \times id_b = \langle f \circ \pi_1, id_b \circ \pi_2 \rangle$.

Poznámka. Předpis

$$\begin{aligned}(f\colon c \times b \to a) &\mapsto (\hat{f}\colon c \to a^b)\\ (\hat{f}\colon c \to a^b) &\mapsto (f = ev \circ \hat{f} \times_b\colon c \times b \to a)\end{aligned}$$

určuje bijekci $\mathrm{Hom}_{\mathcal{C}}(c \times b, a) \cong \mathrm{Hom}_{\mathcal{C}}(c, a^b)$. Pokud má $\mathcal{C}$ terminální objekt, vždy platí $a \times 1 \cong a$, a tedy $\mathrm{Hom}_{\mathcal{C}}(b, a) \cong \mathrm{Hom}_{\mathcal{C}}(1, a^b)$ - globální prvky a^b „jsou" šipky $b \to a$.

Příklad 3.2.29. V **Set** je $A^B = \{f\colon B \to A\}$ množina funkcí z $B \to A$ (globální prvky $1 \to A^B$ jsou tedy skutečně šipky $B \to A$) a evaluace $ev\colon A^B \times B$ má předpis „dosaď do funkce" $[f;x] \mapsto f(x)$. ■

Příklad 3.2.30. V $\mathbb{P}$ je q^p, pokud existuje, roven relativnímu pseudokomplementu $p \Rightarrow q$: z isomorfismu

$$\mathrm{Hom}_{\mathcal{C}}(c \times b, a) \cong \mathrm{Hom}_{\mathcal{C}}(c, a^b)$$

máme $c \sqcap b = c \times b \sqsubseteq a$ právě tehdy, když $c \sqsubseteq a^b$. Šipka $ev\colon q^p \times p = (p \Rightarrow q) \sqcap p \to q$ vyjadřuje modus ponens $(p \Rightarrow q) \sqcap p \sqsubseteq q$. Konkrétněji

$$\mathrm{Hom}_{\mathcal{C}}(x, y) \cong \mathrm{Hom}_{\mathcal{C}}(1, x \Rightarrow y).$$

Z toho vidíme, že $x \sqsubseteq y$ právě tehdy, když $x \Rightarrow y = 1 = \top$ (poznámka pod větou 1.2.10).

Pokud je $\mathbb{P}$ úplně uspořádaná (platí $x \sqsubseteq y \vee y \sqsubseteq x$), exponenty jsou dány předpisem

$$q^p = \begin{cases} 1_{\mathbb{P}} & p \sqsubseteq q, \\ q & \text{jindy}, \end{cases}$$

nám známým z příkladu 2.4.4.

V analogií s interpretací exponentů v **Set** můžeme modus ponens chápat jako „dosazování" důkazu p do důkazu $p \to q$, stejně jako v **BHK** interpretaci.

Na základě charakterizace relativního pseudokomplementu jako exponentu v posetové kategorii můžeme Heytingovy algebry definovat jako *konečně úplné, koúplné (kategoriální) posety s exponenty.* ■

3.3 Elementární topos

V následujících dvou sekcích zavedeme pojem *topos:* speciální kategorie, která umožňuje jazykem teorie kategorií popsat analogy množinově-teoretických konstrukcí jako doplněk, průnik a sjednocení. Tím nám umožní zkonstruovat složitější modely **IPL** než v kapitole **2** a přidá nový pohled na již popsané modely. Tento postup je velmi výhodný, neboť umí zkonstruovat rozmanité modely a ve všech modelech určit sémantiku sjednoceným postupem.

Začneme jedním z nejdůležitějších pojmů teorie množin - *podmnožina.*

Buď B množina. Axiom separace říká, že pokud $\varphi\colon B \to \Phi$ je formule s volnou proměnnou, můžeme sestrojit podmnožinu $A \subseteq B$ pravidlem

$$A = \{x \in B; \phi(x) \text{ platí}\}.$$

„$\phi(x)$ platí" znamená $V(\phi(x)) = 1$, kde V je momentálně používaná valuace. Pokud definujeme funkci $\top\colon 1 = \{0\} \to 2 = \{0; 1\}$, podmnožinu A lze zapsat ve tvaru

$$A = \{x \in B; V \circ \phi(x) = 1\} \cong \{[x; 0] \in B \times 1; V \circ \phi(x) = \top(0)\} = B \times_2 1.$$

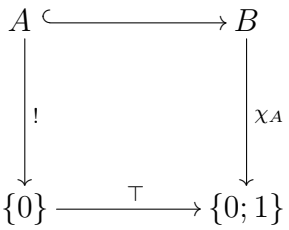
Jinak řečeno,

$$\begin{array}{ccc} A & \hookrightarrow & B \\ \downarrow{\scriptstyle !} & & \downarrow{\scriptstyle V\circ\phi} \\ \{0\} & \xrightarrow{\top} & \{0; 1\} \end{array}$$

je pullback v **Set**, kde $!\colon A \to \{0\}$ je jedinečná šipka s předpisem $!(x) = 0$ (připomeňmě, že $\{0\}$ je terminální v **Set**) a bezejmenná šipka $A \hookrightarrow B$ je inkluze $x \mapsto x$. Obecněji pro jakoukoliv podmnožinu $A \subseteq B$ můžeme definovat *charakteristickou funkci* $\chi_A\colon B \to 2$ s předpisem

$$\chi_A(x) = \begin{cases} 1 & x \in A, \\ 0 & x \notin A. \end{cases}$$

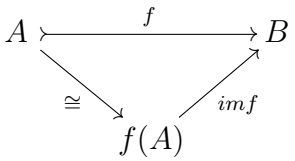
Pak je



pullback v **Set**. Ještě obecněji můžeme jakoukoliv prostou funkci $f\colon A \to B$ „přetáhnout" na inkluzi $imf\colon f(A) \hookrightarrow B$, kde

$$f(A) = \{f(x); x \in A\},$$

tak, že diagram



komutuje. Sestrojíme charakter množiny $f(A)$ a konstrukci přetáhneme zpátky. Výsledek je $\chi_A\colon B \to 2$ s předpisem

$$\chi_A(x) = \begin{cases} 1 & x = f(a) \text{ pro nějaké } a \in A \\ 0 & \text{jinak.} \end{cases}$$

Naopak z jakékoliv funkce $g : B \to 2$ můžeme sestrojit podmnožinu $g^{-1}(1) \subseteq B$. Přiřazení

$$A \subseteq B \mapsto (\chi_A\colon B \to 2),$$
$$(f\colon B \to 2) \mapsto f^{-1}(1) \subseteq B,$$

určuje bijekci

$$\mathcal{P}(B) = \{A;\ A \subseteq B\} \cong 2^B = \{f : B \to 2\},$$

tj. korespondenci mezi podmnožinami B (prvky „potenční množiny" z teorie množin) a funkcemi $B \to 2$ (prvky 2^B). Tuto myšlenku zobecníme pro jakoukoliv kategorii, pokud prosté funkce výměníme za monické šipky, $\{0\}$ za terminální objekt a 2 za Subobject classifier (definován níže):

Definice 3.3.1. Buď $\mathcal{C}$ kategorie a $d\,\mathcal{C}-$objekt. *Subobjekt* objektu d je monická šipka $f\colon a \rightarrowtail d$. Na těchto šipkách definujme ekvivalenci danou předpisem

$$f \sim g \text{ právě tehdy, když } (\text{dom } f) \cong (\text{dom } g).$$

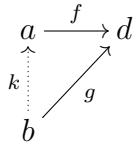
Pak Sub(d) je množina tříd ekvivalencí subobjektů:

$$\text{Sub}(d) := \{[f];\ f = d \text{ a } f \text{ je monická}\}.$$

Sub(d) je částečně uspořádána relací $\sqsubseteq$ s předpisem

$f \sqsubseteq g$ právě tehdy, když existuje právě jedno $k\colon\ \text{dom}f \to \text{dom } g$ takové, že $k \circ g = f$.

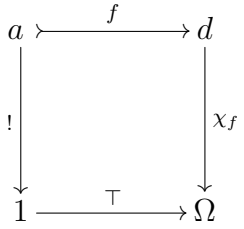
Jinak řečeno, pro suobjekty $f\colon a \to d$ a $g\colon b \to d$ platí $f \sqsubseteq g$ právě tehdy, když existuje jedinečné k takové, že diagram



komutuje.

Příklad 3.3.2. V **Set** jsou subobjekty „totéž", co podmnožiny: $\mathrm{Sub}(A) \cong \mathcal{P}(A)$. ■

Definice 3.3.3. Buď $\mathcal{C}$ kategorie s terminálním objektem. *Subobject classifier* v $\mathcal{C}$ je $\mathcal{C}-$objekt Ω a $\mathcal{C}-$šipka $\top\colon 1 \to \Omega$ splňující **Ω-axiom:** pro každou monickou šipku $f\colon a \to d$ existuje právě jeden charakter $\chi_f\colon B \to \Omega$ takový, že



je pullback v $\mathcal{C}$.

Poznámka. Předpis

$$(f\colon a \to d) \mapsto (\chi_f\colon d \to \Omega)$$
$$(g\colon d \to \Omega) \mapsto (g*\colon d \times_\Omega 1 \to d)$$

určuje bijekci $\mathrm{Sub}(d) \cong \mathrm{Hom}_{\mathcal{C}}(d, \Omega)$.

Příklad 3.3.4. Set má classifier $\Omega = 2 = \{0; 1\}$ a $\top\colon 1 \to 2$ má předpis $\top(0) = 1$. ■

Příklad 3.3.5. Top je kategorie topologických prostorů, kde šipky jsou spojitá zobrazení. Terminální objekt je jednobodový prostor $1 = \{0\}$. Classifier v **Top** je $\Omega = (X, \tau)$, kde $X = \{0; 1\}$ a $\tau = \{\emptyset; \{1\}; \{0; 1\}\}$. Charakter funguje stejně jako v **Set**, jen místo libovolných podmnožin pracuje s otevřenými podmnožinami: z definice spojitých zobrazení musí být $\chi_A^{-1}(1) = A$ otevřená v B. ■

Příklad 3.3.6. Set $\times$ **Set** je kategorie dvojic množin $[A; B]$. Šipky jsou dvojice funkcí $[f; g]\colon [A; B] \to [C; D]$, kde $f\colon A \to C$ a $g\colon B \to D$. Terminální objekt je $1 = [\{0\}; \{0\}]$. Classifier je $\Omega = [2; 2]$. Pokud je $f\colon [A; B] \rightarrowtail [C; D]$ monická, charakter χ_f je $[\chi_A; \chi_B]\colon [C; D] \to [2; 2]$, kde χ_a, χ_B jsou classifiery v **Set**. ■

Definice 3.3.7. *Elementární topos* je kategorie $\mathcal{C}$ taková, že
1.) $\mathcal{C}$ je konečně úplná a koúplná,
2.) $\mathcal{C}$ má exponenty a
3.) $\mathcal{C}$ má subobject classifier.

Příklad 3.3.8. Set a **Set** $\times$ **Set** jsou toposy. **Top** není topos, neboť nemá exponenty. ■

3.4 Vnitřní logika toposu

Logické funkce $\cap, \cup, \Rightarrow$ typu $\{\top;\bot\}\times\{\top;\bot\}\to\{\top;\bot\}$ a $\neg$ typu $\{\top;\bot\}\to\{\top;\bot\}$ mají analog v každém toposu, když vyměníme $2\cong\{\top;\bot\}$ za Ω.

Nepravda: stejně jako $\top\colon 1\to 2$ má hodnotu $\top(0)=1$, což je $\top$ v Booleově algebře 2, definujme $\bot\colon 1\to 2$ s hodnotou $\bot(0)=0$, což je $\bot$ v Booleově algebře 2. Pullback $\bot$ (limita diagramu $1\xrightarrow{\bot}2\xleftarrow{\top}1$) je $\emptyset$:

$$\begin{array}{ccc} \emptyset & \hookrightarrow & 1 \\ {\scriptstyle !}\downarrow & & \downarrow{\scriptstyle \bot} \\ 1 & \xrightarrow{\top} & 2. \end{array}$$

Z $\Omega-$axiomu je $\bot=\chi_\emptyset=\chi_0$. Obecně v toposu $\mathcal{C}$ definujeme $\bot:=\chi_{0_1}\colon 1\to\Omega$, kde $0_1\colon 0\to 1$ je jedinečná šipka z iniciálního do terminálního objektu v $\mathcal{C}$.

Negace: V **Set** je

$$\begin{array}{ccc} \{0\} & \hookrightarrow & 2 \\ {\scriptstyle !}\downarrow & & \downarrow{\scriptstyle \neg} \\ 1 & \xrightarrow{\top} & 2 \end{array}$$

pullback, takže z $\Omega-$axiomu je $\neg=\chi_\bot$. Obecně tedy definujeme $\neg:=\chi_\bot:\Omega\to\Omega$ v libovolném toposu.

Konjunkce: V **Set** je

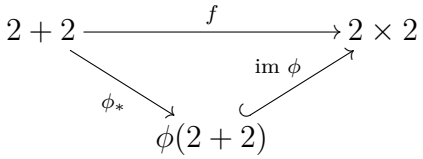
$$\begin{array}{ccc} \{[1;1]\} & \hookrightarrow & 2\times 2 \\ {\scriptstyle !}\downarrow & & \downarrow{\scriptstyle \sqcap} \\ 1 & \xrightarrow{\top} & 2 \end{array}$$

pullback, a tedy $\sqcap=\chi_{\{[1;1]\}}$. Kategoriálně můžeme $\{[1;1]\}$ popsat jako $\langle\top,\top\rangle(\{0\})$, kde $\langle\top,\top\rangle\colon 1\to 2\times 2$ (tato funkce do obou složek dá $1=\top(0)$ - toto značí, že aby konjunkce byla pravdivá, musí být pravdivé obě „složky"). Obecně tedy definujeme $\sqcap:=\chi_{\langle\top,\top\rangle}\colon\Omega\times\Omega\to\Omega$.

Disjunkce: V **Set** je

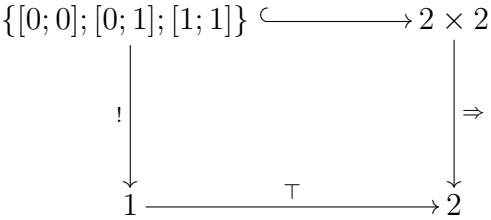
$$\begin{array}{ccc} \{[0;1];[1;0];[1;1]\} & \hookrightarrow & 2\times 2 \\ {\scriptstyle !}\downarrow & & \downarrow{\scriptstyle \cup} \\ 1 & \xrightarrow{\top} & 2 \end{array}$$

pullback, a tedy $\sqcup = \chi_{\{[0;1];[1;0];[1;1]\}}$. Kategoriálně je $\{[0;1];[1;0];[1;1]\} = \phi(2+2)$, kde $\phi = [\langle \top, id_2\rangle, \langle id_2, \top\rangle] \colon 2+2 \to 2\times 2$ (tato funkce buď pošle vstup do druhé složky a do první dá $1 = \top(0)$, nebo naopak: toto značí, že aby disjunkce byla pravdivá, musí být pravdivá alespoň jedna „složka"). Obraz im $\phi \circ \phi_*$ dostaneme z tzv. *epi-mono faktorizace* ϕ (ty jsou možné v každém toposu, viz. [Tri19]; v práci je budeme počítat jen pro množiny, takže si bez kategoriální konstrukce vystačíme).



Obecně tedy definujeme $\sqcup := \chi_{\mathrm{im}\phi} \colon \Omega\times\Omega \to \Omega$, kde $\phi = [\langle \top, id_\Omega\rangle, \langle id_\Omega, \top\rangle] \colon \Omega+\Omega \to \Omega\times\Omega$.

Implikace: V **Set** je



pullback, a tedy $\Rightarrow = \chi_{\{[0;0];[0;1];[1;1]\}}$. Zde znovu vidíme vztah mezi $\sqsubseteq$ a $\Rightarrow$ v Booleově algebře $2 \cong \{\bot;\top\}$: pullback $\Rightarrow$, tj. množina všech $[x;y]$ s $x \Rightarrow y = 1 = \top(0)$, je přesně uspořádání $\sqsubseteq$ na množině 2. Uspořádání můžeme také dostat „zpět z infima": ve svazu platí $x \sqsubseteq y$ právě tehdy, když $x \sqcap y = x$, tj. kdykoliv $\cap(x,y) = \pi_1(x,y)$. Pak můžeme $\{[0;0];[0;1];[1;1]\}$ popsat kategoriálně jako equalizer $\mathrm{Eq}(\cap, \pi_1)$:

$$\mathrm{Eq}(\cap,\pi_1) \xrightarrow{e} \Omega\times\Omega \underset{\pi_1}{\overset{\cap}{\rightrightarrows}} \Omega.$$

Obecně tedy definujeme $\Rightarrow := \chi_e \colon \Omega\times\Omega \to \Omega$, kde $e \colon\ \mathrm{Eq}(\cap,\pi_1) \to \Omega\times\Omega$.

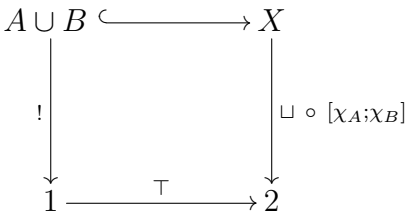
Operace na Sub(d): V Booleově algebře $(\mathcal{P}(X),\ \subseteq,\ \cup,\ \cap,\ \Rightarrow,\ -)$ jsou množinové operace interpretace logických spojek (viz. **Sémantika v CPL**) a v teorii množin se definují $\cup, \cap, -$ pomocí $\vee, \wedge, \neg$:

$$\begin{aligned} A \cup B &:= \{x;\ (x\in A)\vee(x\in B)\},\\ A \cap B &:= \{x;\ (x\in A)\wedge(x\in B)\},\\ A \Rightarrow B &:= \{x;\ (x\in A)\to(x\in B)\},\\ -A &:= \{x;\ \neg(x\in A)\}. \end{aligned}$$

Abychom množinové operace chápali jako operace v $\mathcal{P}(X)$, budeme uvažovat $A, B \subseteq X$.

$$\begin{aligned} A\cup B &= \{x\in X;\ (x\in A)\vee(x\in B)\} = \{x\in X; \chi_A(x)\sqcup\chi_B(x) = 1\}\\ &= \{[x;0]\in X\times 1; \sqcup\circ[\chi_A;\chi_B](x) = \top(0)\} \end{aligned}$$

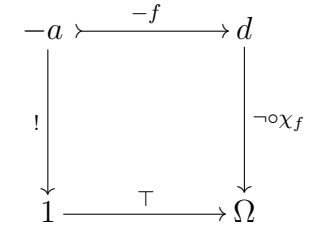
Vidíme, že

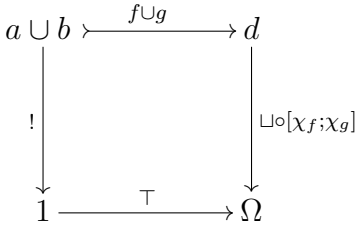


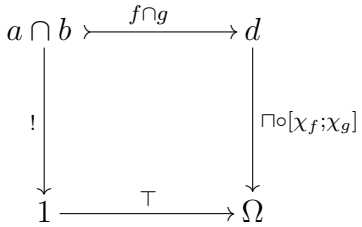
je pullback v **Set.** Obecně v toposu $\mathcal{C}$ pro $f, g \in \mathrm{Sub}(d)$ s dom $f = a$ a dom $g = b$ definujeme $-, \cup, \cap, \Rightarrow$ tak, aby

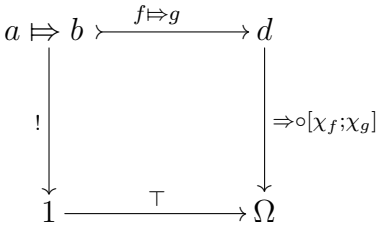
$$\begin{aligned} \chi_{-f} &= \neg \circ \chi_f, \\ \chi_{f \cup g} &= \sqcup \circ [\chi_f; \chi_g], \\ \chi_{f \cap g} &= \sqcap \circ [\chi_f; \chi_g], \\ \chi_{f \Rightarrow g} &= \Rightarrow \circ [\chi_f; \chi_g]. \end{aligned}$$

Ekvivalentně,









jsou pullbacky v $\mathcal{C}$.

V analogii s příkladem 1.2.12 máme následující charakterizaci ([Gol84]):

Věta 3.4.1. Nechť $\mathcal{C}$ je topos a d je $\mathcal{C}-$objekt. Pak $\mathrm{Sub}(d)$ je Heytingova algebra.
Důkaz je vynechán, poněvadž tvrzení nevyužijeme a v příští kapitole využijeme podobnou větu. □

Značení $\mathcal{C} \models \alpha$ je zkratka pro $\Omega_{\mathcal{C}} \models \alpha$, tj. „$\alpha$ je pravdivá ve všech valuacích $V' : \Phi \to \Omega_{\mathcal{C}}$."

Kapitola 4

Funktorové kategorie

V poslední kapitole popíšeme obecný postup, jak zkonstruovat modely **IPL** pomocí toposu $\mathbf{Set}^{\mathcal{C}}$, kde $\mathcal{C}$ je malá kategorie. Začneme s popisem jeho kategoriálních vlastností, pak rozebereme logické funkce v $\mathrm{Sub}(d)$ a v sekcích **4.2-4.4** rozebereme konkrétní modely.

$\mathbf{Set}^{\mathcal{C}}$-objekty jsou funktory $F\colon \mathcal{C} \to \mathbf{Set}$. Takovému funktoru budeme občas říkat „koncept množiny" (pojem je vysvětlen níže). Globální prvky $x : 1 \to F$ budeme nazývat „koncept množiny". Šipky jsou přirozené transformace, tj. „zobrazení mezi koncepty množiny" $\eta\colon F \to G$.

Limity (a analogicky kolimity) jsou definované „po komponentách". Pro každý $\mathcal{C}-$objekt a můžeme definovat diagram $D'\colon J \to \mathbf{Set}$, který každému $J-$objektu j přiřadí $D'(j) = D(j)(a)$. Pokud $D\colon J \to \mathbf{Set}^{\mathcal{C}}$ je $\mathbf{Set}^{\mathcal{C}}$-diagram, $\lim D\colon \mathcal{C} \to \mathbf{Set}$ je funktor, který každému $\mathcal{C}-$objektu a přiřadí limitu $\lim D'$ výše zkonstruovaného diagramu D'.

Konkrétněji pak terminální objekt 1 v $\mathbf{Set}^{\mathcal{C}}$ je funktor terminálních **Set**-objektů: 1 každému $\mathcal{C}-$objektu a přiřadí $1(a) = \{0\}$. Dále $F \times_H G(a) = F(a) \times_{H(a)} G(a)$ a diagram

$$\begin{array}{ccc} F \times_H G & \xrightarrow{\eta_*} & G \\ \downarrow{\scriptstyle \tau_*} & & \downarrow{\scriptstyle \tau} \\ F & \xrightarrow{\eta} & H \end{array}$$

je pullback v $\mathbf{Set}^{\mathcal{C}}$ právě tehdy, když je diagram

$$\begin{array}{ccc} F(a) \times_H (a)G(a) & \xrightarrow{(\eta_*)_a} & G(a) \\ \downarrow{\scriptstyle (\tau_*)_a} & & \downarrow{\scriptstyle \tau_a} \\ F(a) & \xrightarrow{\eta_a} & H(a) \end{array}$$

pullback v **Set** pro každý $\mathcal{C}-$objekt a.

Nechť a je $\mathcal{C}-$objekt. Definujeme *siev* na a (neboli $a-$siev) jako množinu X $\mathcal{C}-$šipek $\phi\colon a \to b$, která je zleva uzavřená nad skládáním. To znamená, že pokud $\phi \in X$, musí $f \circ \phi \in X$ pro libovolnou šipku f, kde $\mathrm{dom}\, f = b$:

$$X = \{\phi\colon a \to b;\ f \circ \phi \in X \text{ pro libovolné } f\}.$$

Classifier $\Omega\colon \mathcal{C} \to \mathbf{Set}$ každému $\mathcal{C}-$objektu a přiřadí množinu $a-$sievů

$$\Omega(a) = \{X;\ X \text{ je } a - siev\}$$

a $\mathcal{C}-$šipce $f\colon a \to b$ přiřadí funkci, která $a-$sievu X přiřadí

$$\Omega f(X) = \{\phi\colon b \to c;\ \phi \circ f \in X\}$$

Pro monickou $\eta\colon F \rightarrowtail G$ sestrojíme charakter χ_η s komponentami

$$(\chi_\eta)_a(x) = \{\phi\colon a \to b;\ G\phi(x) \in F(b)\}$$

(zde BÚNO η_a inkluze).

Jeden z hlavních výsledků teorie toposů činí ([Gol84]):

Věta 4.0.1. $\mathbf{Set}^{\mathcal{C}}$ je topos pro jakoukoliv malou kategorii $\mathcal{C}$.

Sémantika v $\mathbf{Set}^{\mathcal{C}}$: Valuace $V\colon \Phi \to \mathrm{Hom}_{\mathbf{Set}^{\mathcal{C}}}(1, \Omega)$ každému $\alpha \in \Phi$ přiřadí přirozenou transformaci $V(\alpha)\colon 1 \to \Omega$ s komponentami $V_a(\alpha)\colon \{0\} \to \Omega(a)$. $V_a(\alpha)(0)$ je množina $\mathcal{C}-$šipek f, po kterých když „půjdeme", začne α platit.

Interpretace: v analogií s Kripkeho sémantikou chápeme $\mathcal{C}-$objekty jako stavy vědění, ve kterých se můžeme nacházet. Stavy se mohou lišit časem, místem, či jinými podmínkami, a proto je vědění omezené stavem, ve kterém se nacházíme. $\mathcal{C}-$šipky jsou přechody mezi stavy a změny stavů: posun po šipce $f\colon a \to b$ vyjadřuje, že jsme se ze stavu vědění a přesunuli do stavu b „způsobem" f. Šipky $g\colon a \to a$ vyjadřují „způsob," jak změnit svůj momentální stav. Význam $\mathcal{C}-$šipek může být rozmanitý: mezi stavy můžeme přecházet postupem času (příklad 2.4.2, tvorbou rozhodnutí (sekce **4.3**), shromažďováním nových informací atd.

Množiny definované axiomem separace

$$A = \{x \in D;\ \phi(x) \text{ platí}\}$$

mohou v každém stavu a nabývat jiných prvků, neboť pravdivost výroku $\phi(x) \in \Phi$ závisí na stavu. Funktory $F\colon \mathcal{C} \to \mathbf{Set}$ jsou tzv. *koncepty množin*, které každému stavu a přiřadí množinu prvků patřících do „množiny" F ve stavu a. Pokud se ze stavu a do b můžeme přesunout „způsobem" f, funkce $Ff\colon F(a) \to F(b)$ každému $x \in F(a)$ přiřadí naši „představu" o prvku x ve stavu b. Představou myslíme formu, kterou prvek zapisujeme, a pomocí které nad prvkem uvažujeme. Pokud se naše představa o prvku nezmění, platí $Ff(x) = x$. Pokud se představa o prvcích přesunováním f nemění, je Ff inkluze a pokud každý prvek jen mění svou formu, je Ff prostá. Může se ovšem stát, že prvky x, y ve stavu a považujeme za různé, ale ve stavu b zjistíme, že jsou stejné: pak platí $Ff(x) = Ff(y)$ a Ff není ani prostá.

Ω je koncept množiny obsahující „nevratné změny". Siev na stavu a je množina „nevratných změn" stavu a (myslíme změny $a \to a$ i přechody $a \to b$). Přesněji řečeno, pokud se přechodem dostaneme do sievu $S \in \Omega(a)$, žádným přechodem už nemůžeme z S odejít. $V_a(\alpha)(0)$ je množina změn ze stavu a, po kterých začne α platit. Dokázání výroku je v intuicionistické logice nevratná změna, neboť vědění je kauzálně zachováno - proto musí $V_a(\alpha)(0)$ být $a-$siev. Pokud $V_a(\alpha)(0)$ obsahuje všechny šipky z a, znamená to, že ve stavu a výrok α platí a toto nelze žádným přechodem změnit. $\Omega f\colon \Omega(a) \to \Omega(b)$ každému $a-$sievu přiřadí množinu způsobů, jak se z b do tohoto $a-$sievu dostat. Zejména $\Omega f(V_a(\alpha)(0))$ je množina změn ze stavu b, po kterých začne α platit.

4.1 Operace na Sub(D) v $\mathbf{Set}^{\mathcal{C}}$

Popsat globální prvky $1 \to \Omega$ může být složité, a proto rozpočítáme operace v Sub(D). Zjistíme, že nejen $\mathrm{Hom}_{\mathbf{Set}^{\mathcal{C}}}(1, \Omega)$ je Heytingova algebra, ale $\Omega(n)$ je Heytingova algebra pro každý $\mathcal{C}-$objekt n.

• *Negace:* Nechť $A \in \mathrm{Sub(D)}$. Negace $\neg\colon \Omega \to \Omega$ definovaná tak, aby

$$\begin{array}{ccc} \{\emptyset\} & \xhookrightarrow{\ \bot_n\ } & \Omega(n) \\ \downarrow{\scriptstyle !_n} & & \downarrow{\scriptstyle \neg_n=(\chi_1)_n} \\ \{0\} & \xrightarrow[\ \top_n\ ]{} & \Omega(n) \end{array}$$

byl pullback, má komponenty $\neg_n(x) = \{\phi\colon n \to m; \Omega\phi(x) \in \{\emptyset\}\}$. $\neg A \in \mathrm{Sub(D)}$ má předpis

$$\begin{aligned} &\neg A(n) = \{x \in D(n);\ (\neg \circ \chi_A)_n(x) = \top_n(0)\} \\ &= \{x \in D(n);\ \neg_n(\{\phi\colon n \to m;\ D\phi(x) \in A(m)\}) = \top_n(0)\} \\ &= \{x \in D(n);\ \{\varphi\colon n \to b;\ \Omega\varphi(\{\phi\colon n \to m; D\phi(x) \in A(m)\} = \emptyset)\} = \top_n(0)\} \\ &= \{x \in D(n);\ \{\varphi\colon n \to b;\ \Omega\varphi(\{\phi\colon n \to m;\ D\phi(x) \in A(m)\})\} = \emptyset \text{ pro každé } \varphi\colon n \to b\} \\ &= \{x \in D(n);\ \{\varphi : n \to b;\ \{\omega : b \to c;\ \omega \circ \varphi \in \{\phi\colon n \to m;\ D\phi(x) \in A(m)\}\}\} = \emptyset \\ &\text{pro každé } \varphi\colon n \to b\} \\ &= \{x \in D(n);\ \omega \circ \varphi \notin \{\phi\colon n \to m;\ D\phi(x) \in A(m)\} \text{ pro každé } \omega \circ \varphi\colon n \to c\} \\ &= \{x \in D(n);\ D(\omega \circ \varphi)(x) \notin A(c) \text{ pro každé } \omega \circ \varphi\colon n \to c\} \\ &= \{x \in D(n);\ D\phi(x) \notin A(c) \text{ pro každé } \phi\colon n \to c\} \end{aligned}$$

Zajímavá je taktéž dvojitá negace:

$$\begin{aligned} \neg\neg A(n) &= \{x \in D(n);\ D\phi(x) \notin \neg A(l) \text{ pro každé } \phi\colon n \to l\} \\ &= \{x \in D(n);\ (D\phi(x) \notin \neg A(l) \text{ pro každé } \varphi\colon l \to k) \text{ nenastane pro žádné } \phi\colon n \to l\} \\ &= \{x \in D(n);\ \ \text{pro každé } \phi : n \to l \text{ existuje } \varphi\colon l \to c \text{ takové, že } D(\circ\phi)(x) \in A(c)\} \end{aligned}$$

Interpretace: $\neg A(n)$ obsahuje prvky, které se po žádném přechodu z n nemohou dostat do konceptu množiny A. $\neg\neg A(n)$ je množina prvků takových, že po jakémkoliv přechodu se vždy můžeme pořád dostat do konceptu A. V této interpretaci nad výrokem $\sim\!\sim \alpha$ můžeme uvažovat jako „α může vždy platit".

• *Konjunkce:* $\cap\colon \Omega \times \Omega \to \Omega$ je definovaná pullbackem

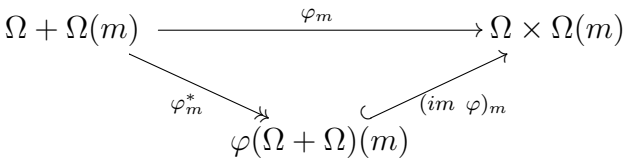
$$\begin{array}{ccc} \{[\top_n(0); \top_n(0)]\} & \xhookrightarrow{[\top_n;\top_n]} & \Omega \times \Omega(n) \\ \downarrow{\scriptstyle !_n} & & \downarrow{\scriptstyle \cap_n=(\chi_{[\top;\top]})_n} \\ \{0\} & \xrightarrow[\ \top_n\ ]{} & \Omega(n) \end{array}$$

a má komponenty $\cap_n(x,y) = \{\phi\colon n \to m;\ (\Omega\times\Omega)\phi(x,y) \in \{[\top_n(0);\top_n(0)]\}\}$. $A\cap B \in$ Sub(D) má komponenty

$$\begin{aligned}
A\cap B(n) &= \{x\in D(n);\ \cup\circ[\chi_A;\chi_B]_n(x) = \top_n(0)\}\\
&= \{x\in D(n);\ \{\phi : n\to m;\ \Omega\phi((\chi_A)_n(x)) = \top_n(0) \text{ a } \Omega\phi((\chi_B)_n(y)) = \top_n(0)\} = \top_n(0)\}\\
&= \{x\in D(n);\ \varphi\circ\phi \in (\chi_A)_n(x) \text{ pro každé } \varphi\circ\phi\colon n\to l\}\\
&\quad \cap\{y : \varphi\circ\phi \in (\chi_B)_n(x) \text{ pro každé } \varphi\circ\phi\colon n\to l\}\\
&= \{x\in D(n);\ D(\varphi\circ\phi)(x)\in A(l) \text{ pro každé } \varphi\circ\phi\colon n\to l\}\\
&\quad \cap\{y : D(\varphi\circ\phi)(y)\in A(l) \text{ pro každé } \varphi\circ\phi\colon n\to l\}\\
&= A(n)\cap B(n)
\end{aligned}$$

(v posledním kroku jsem položil $\varphi\circ\phi = id_n$, z čehož $D\ id_n(x) = x \in A(n)$ v první závorce a $D\ id_n(y) = y\in B(n)$ v druhé závorce).

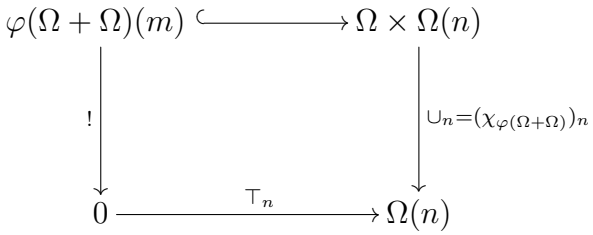
• *Disjunkce:* Epi-mono faktorizace šipky $\phi = ([id_\Omega;\top];[\top;id_\Omega])$ je znázorněna diagramem



Obraz φ je množina

$$\varphi(\Omega+\Omega)(m) = \{[x;\top_n(0)] : x\in\Omega(m)\}\cup\{[\top_n(0);y] : y\in\Omega(m)\},$$

$\cup\colon \Omega\times\Omega\to\Omega$



má komponenty

$$\begin{aligned}
\cup_n(x,y) &= \{\phi\colon n\to m;\ \Omega\times\Omega\phi(x,y)\in\varphi(\Omega+\Omega)(m)\}\\
&= \{\phi\colon n\to m;\ \Omega\phi(x) = \top_m(0) \text{ nebo } \Omega\phi(y) = \top_m(0)\}
\end{aligned}$$

$A\cup B\in$ Sub(D) má komponenty

$$\begin{aligned}
&A\cup B(n) = \{x\in D(n);\ (\cup\circ[\chi_A;\chi_B])_n(x) = \top_n(0)\}\\
&= \{x\in D(n);\ \{\phi\colon n\to m;\ \Omega\phi((\chi_A)_n(x))\} = \top_m(0)\} \text{ nebo } \{\Omega\phi((\chi_{Bn}(x)) = \top_m(0)\} = \top_n(0)\}\\
&= \{x\in D(n);\ \varphi\circ\phi\in(\chi_A)_n(x) \text{ nebo } \varphi\circ\phi\in(\chi_B)_n(x) \text{ pro každé } \varphi\circ\phi\colon n\to l\}\\
&= \{x\in D(n);\ D(\varphi\circ\phi)(x)\in A(l) \text{ pro každé } \varphi\circ\phi\colon n\to l\}\\
&\quad \cup\{x\in D(n);\ D(\varphi\circ\phi)(x)\in B(l) \text{ pro každé } \varphi\circ\phi\colon n\to l\} = A(n)\cup B(n)
\end{aligned}$$

• *Implikace:* Zkonstruujeme equalizer $\mathrm{Eq}(\cap, \pi_1)$ šipek $\cap, \pi_1 \colon \Omega \times \Omega \rightrightarrows \Omega$ znázorněný diagramem

$$\mathrm{Eq}(\cap, \pi_1)(n) \hookrightarrow \Omega \times \Omega(n) \underset{(\pi_1)_n}{\overset{\cap_n}{\rightrightarrows}} \Omega(n).$$

Explicitně můžeme $\mathrm{Eq}(\cap, \pi_1)(n)$ zapsat jako

$$\mathrm{Eq}(\cap, \pi_1)(n) = \{[x; y] \in \Omega \times \Omega(n); \cap_n(x, y) = x\}.$$

$\Rightarrow \colon \Omega \times \Omega \to \Omega$ má komponenty

$$\begin{array}{ccc} \mathrm{Eq}(\cap, \pi_1)(n) & \xrightarrow{\leq_n} & \Omega \times \Omega(n) \\ \Big\downarrow{\scriptstyle !} & & \Big\downarrow{\scriptstyle \Rightarrow_n} \\ \{0\} & \xrightarrow{\top_n} & \Omega(n) \end{array}$$

$$x \Rightarrow_n y = \{\phi \colon n \to m;\ (\Omega \times \Omega)\phi(x, y) \in \mathrm{Eq}(\cap, \pi_1)(m)\}$$

$A \rightarrowtriangle B(n) = \{x \in D(n); \Rightarrow \circ [\chi_A; \chi_B](x) = \top_n(0)\}$
$= \{x \in D(n);\ \cup_n(\Omega\phi((\chi_A)_n(x)), \Omega\phi((\chi_B)_n(x))) = \Omega\phi((\chi_A)_n(x)$ pro každé $\phi : n \to m\}$
$= \{x \in D(n);\ \{\varphi \colon m \to l;\ \Omega\varphi(\Omega\phi((\chi_A)_n(x))) = T_l(0)$ a $\Omega\varphi(\Omega\phi((\chi_B)_n(x))) = T_l(0)\} =$
$\Omega\phi((\chi_A)_n(x)$ pro každé $\phi \colon n \to m\}$
$= \{x \in D(n);\ \{\varphi \colon m \to l; \Omega(\varphi \circ \phi)((\chi_A)_n(x)) = \Omega(\varphi \circ \phi)((\chi_B)_n(x)) = T_l(0)\} =$
$\Omega\phi((\chi_A)_n(x)$ pro každé $\phi \colon n \to m\}$
$= \{x \in D(n);\ (\Omega(\varphi \circ \phi)((\chi_A)_n(x)) = \Omega(\varphi \circ \phi)((\chi_B)_n(x)) = T_l(0)$ právě tehdy, když

$\varphi \circ \phi \in (\chi_A)_n(x))$ pro každé $\phi \colon n \to m\}$
$= \{x \in D(n);\ (D(\varphi \circ \phi)(x) \in A(l) \cap B(l)$ právě tehdy, když $D(\varphi \circ \phi)(x) \in A(l))$
pro každé $\phi \colon n \to m\}$
$= \{x \in D(n);\ $ pro každé $\omega \colon n \to l$ platí $(D\omega(x) \in A(c) \cap B(c)$ právě tehdy, když
$D\omega(x) \in A(c))\}$
$= \{x \in D(n);\ $ pro každé $\omega \colon n \to l$ platí $(D\omega(x) \in B(c)$ kdykoliv $D\omega(x) \in A(c))\}$

Věta 4.1.1. Nechť $\mathcal{C}$ je malá kategorie, n je $\mathcal{C}-$objekt a Ω je $\mathbf{Set}^{\mathcal{C}}-$classifier. Pak $(\Omega(n), \subseteq, \cup, \cap, \rightarrowtriangle)$ je Heytingova algebra.
Důkaz je analogický k důkazu věty 2.4.3. □

4.2 Posety

Pomocí výpočtů v sekci **4.1** vidíme, že logické funkce se v $\mathrm{Sub}(D)$ chovají podobně, jako v $\mathbb{P}^+$ ze sekce **2.4**. Jak souvisí funktorové kategorie s Kripkeho sémantikou?

Kripkeho sémantika ve framu $\mathbb{P}$ (tj. v Heytingově algebře $\mathbb{P}^+$) je vnitřní logika toposu $\mathbf{Set}^{\mathbb{P}}$. Pokud se nacházíme ve stavu a, máme vždy právě jeden způsob, jak se dostat do

stavu b, kdykoliv $a \sqsubseteq b$. Přechody $a \to b$ tedy nemusíme chápat jako šipky, ale stačí je určit koncovým bodem b. Uzavřenost nad skládáním zleva pak znamená kauzální uzavřenost, a tudíž $a-$sievy jsou kauzálně uzavřené podmnožiny $\mathbb{P}$, jejichž všechny prvky jsou v uspořádání $\sqsubseteq$ napravo od a. Zejména pokud má $\mathbb{P}$ nejmenší prvek (iniciální objekt) 0, platí

$$\Omega(0) = \mathbb{P}^+.$$

Obecněji, pokud označíme *principální množinu* $[a) = \{b; a \sqsubseteq b\} \subseteq P$ množinu všech prvků napravo od a, dostaneme $\Omega(a) = [a)^+$. Při přechodu mezi stavy $f\colon p \to q$ pravdivostní hodnoty v $\Omega(p)$ projdou změnou $\Omega f\colon [p)^+ \to [q)^+$, která $p-$siev X změní na $q-$siev

$$\Omega f(X) = \{\phi\colon q \to b;\ \phi \circ f \in X\} \cong \{b \in [q);\ b \in X\} = X \cap [q).$$

Při přechodu f *zapomeneme*, co se dělo před stavem q a vidíme jen *průnik* s $[q)$.

Z axiomu přirozenosti pro $V(\alpha) : 1 \to \Omega$ plyne, že diagram

$$\begin{array}{ccc} \{0\} & \xrightarrow{id_{\{0\}}} & \{0\} \\ \downarrow{\scriptstyle V_p(\alpha)} & & \downarrow{\scriptstyle V_q(\alpha)} \\ \Omega(p) & \xrightarrow{\Omega f} & \Omega(q) \end{array}$$

komutuje, takže $V_q(\alpha)(0) = \Omega f(V_p(\alpha)(0)) = V_p(\alpha)(0) \cap [q)$.

Co přináší kategoriální popis? U kripkeho modelů nám $\mathbb{P}^+-$valuace $V(\alpha)$ říkala, ve kterých stavech α platí. Chápání problému pomocí toposů nám umožňuje dvě nové věci:

1) Můžeme se dívat lokálně „z pohledu konkrétního stavu". Jakmile se ocitneme ve stavu p, z něhož se nejde dostat do q, vůbec nás nezajímá, jestli α platí v q. Proto se díváme na „lokální pravdivost" $V_p(\alpha)(0)$.
2) Můžeme studovat, jak přechody $f\colon p \to q$ mezi stavy změní pravdivost pomocí $\Omega f(V_p(\alpha)(0))$. Například pokud α po přechodu začne platit, musí být $\Omega f(V_p(\alpha)(0)) = [q)$.

Příklad 4.2.1. Nechť $\mathbb{P} = (I, \Delta_I)$, kde Δ_I je diskrétní uspořádání na I. $\mathbf{Set}^I$-objekty jsou soubory $\{F(i); i \in I\}$, kde $F\colon I \to \mathbf{Set}$ (I chápeme jako diskrétní kategorii). Šipky jsou soubory funkcí $\{\eta_i\colon F(i) \to G(i)\}$, kvůli diskrétnosti I nám axiom přirozenosti nedává žádné podmínky mezi komponentami.

Classifier v $\mathbf{Set}^I$ má složky $\Omega(i) = \{\emptyset, \{i\}\}$. Každá podmnožina I je kauzálně uzavřená, takže $\mathbb{I}^+ = \mathcal{P}(I)$. Pokud $V(\alpha) = S \subseteq I$, platí

$$V_i(\alpha)(0) = S \cap \{i\} = \begin{cases} \emptyset & \text{pokud } i \notin S, \\ \{i\} & \text{pokud } i \in S. \end{cases}$$

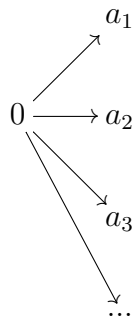
Charakter $\mathbf{Set}^I$-šipky $\eta\colon F \rightarrowtail G$ má komponenty $(\chi_\eta)_i\colon G(i) \to \{\emptyset, \{i\}\}$ s předpisem

$$(\chi_\eta)_i(x) = \{q : x \sqsubseteq q \text{ a } x \in F(q)\} = \begin{cases} \emptyset & \text{pokud } x \notin F(i), \\ \{i\} & \text{pokud } x \in F(i). \end{cases}$$

Interpretace: Stejná jako příklad 1.2.12, ale obohacená vybudovaným aparátem. $V(\alpha) = S$ znamená, že α platí v bodech S. $\mathbb{I}^+-$valuace neměří jen, jestli α platí nebo ne, ale uvažuje

platnost α v každém bodě prostoru I. Charakter $\chi_{\eta i}\colon G(i) \to 2$ se na otázku „patří x do F?" ptá *lokálně* v každém bodě I. Pravdivostní hodnoty v $\mathrm{Hom}_{\mathbf{Set}^{\hat{I}}(1,\Omega)}$ tvoří Booleovu algebru $(\mathcal{P}(I), \subseteq, \cap, \cup, \Rightarrow, \neg)$, nám známou z příkladu 1.2.12. ■

Příklad 4.2.2. Nechť $\mathbb{P} = \{0; a_1, a_2, a_3..., a_n\}$, netriviální relace jsou $0 \sqsubseteq a_i$ pro $1 \leq i \leq n$.



Výrok může platit ve všech stavech, v žádném stavu, nebo jen v některých a_i :

$$\mathbb{P}^+ = \{\emptyset; [0)\} \cup \mathcal{P}(\{a_i; 1 \leq i \leq n\})$$

Výrok $\alpha \in \Phi$ ohodnotíme $\mathbb{P}-$valuací $V\colon \Phi \to \mathbb{P}^+$ předpisem

$$V(\alpha) = \begin{cases} [0) & \alpha \text{ platí,} \\ \bigcup\{a_i\} & \alpha \text{ platí ve stavech } a_i \\ \emptyset & \alpha \text{ neplatí nikdy} \end{cases}$$

Pak pro $V(\alpha)\colon 1 \to \Omega$ platí $V_0(\alpha)(0) = V(\alpha)$ a

$$V_{a_i}(\alpha)(0) = V_0(\alpha)(0) \cup [a_i) = \begin{cases} [a_i) & \text{výrok platí ve stavu } a_i \\ \emptyset & \text{výrok neplatí ve stavu } a_i \end{cases}$$

Interpretace: Začínáme ve stavu 0 a máme n možných budoucností, které mohou nastat. $V_0(\alpha)(0)$ se ptá na otázku „Ve kterých možných budoucnostech bude α platit?"a $V_{a_i}(\alpha)(0)$ se ptá na otázku „Bude v budoucnosti a_i platit α?". Pro příklad uvažujme možné budoucnosti

a_1 : bude pršet
a_2 : bude zataženo
a_3 : bude jasno.

Pak α : „Půjdu na kolo"má hodnotu $V_0(\alpha)(0) = \{a_2; a_3\}$. Pravdivostní hodnoty v možných budoucnostech jsou $V_{a_1}(\alpha)(0) = \emptyset = \bot_{[a_1)^+}$, $V_{a_2}(\alpha)(0) = \{a_2\} = \top_{[a_2)^+}$ a $V_{a_3}(\alpha)(0) = \{a_3\} = \top_{[a_3)^+}$. ■

Poznámka. Prvek $x \in \mathbb{P}$ je *maximální,* pokud platí $x = p$ kdykoliv $x \sqsubseteq p$. Intuitivně řečeno: z maximálních prvků „nevedou"jiné šipky, než identity. Sievy takového prvku tvoří množinu

$$[x)^+ = \{\emptyset; \{x\}\} \cong \{\bot;\ \top\} = 2.$$

V maximálních stavech už nezbývají žádné stavy, do kterých se posunout. Výrok v takovém stavu může být jen pravdivý, či nepravdivý, a logika tento stav popisující je klasická logika ze sekce **1.1**.

Příklad 4.2.3. Uvažujme $\mathbb{P} = \mathbb{N}$ s přirozeným uspořádání $0 \leq 1 \leq 2 \leq ...$

$$0 \longrightarrow 1 \longrightarrow 2 \longrightarrow 3 \longrightarrow 4 \longrightarrow 5 \longrightarrow ...$$

$\mathbb{N}$-valuace výroku $\alpha \in \Phi$ může být buď $[n)$ pro $n \in \mathbb{N}$ nebo $\emptyset$ ($\mathbb{N}$ je dobře uspořádaná.) V prvním případě komponenty $\mathbf{Set}^{\mathbb{N}}$-valuace $V(\alpha) : 1 \to \Omega$ tvoří posloupnost

$$[n) \longrightarrow [n) \longrightarrow [n) \longrightarrow ... \longrightarrow [n) \longrightarrow [n+1) \longrightarrow [n+2) \longrightarrow [n+3) \longrightarrow ...$$

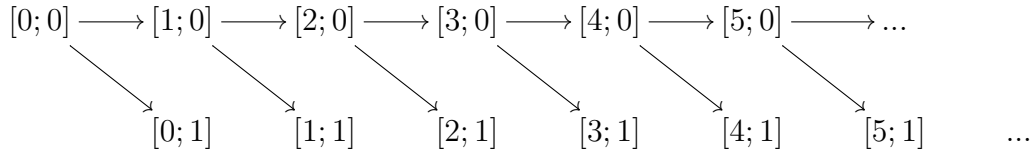
Ze začátku pravdivostní hodnota vyjadřuje, že α začne platit ve stavu n. Jakmile překročíme tento stav, uvidíme jen, že α prostě platí ($V(\alpha)_p(0)$ je $\top$ v Heytingově algebře $\Omega(p)$). V druhém případě je $\mathbf{Set}^{\mathbb{N}}$-valuace posloupnost

$$\emptyset \longrightarrow \emptyset \longrightarrow \emptyset \longrightarrow ...,$$

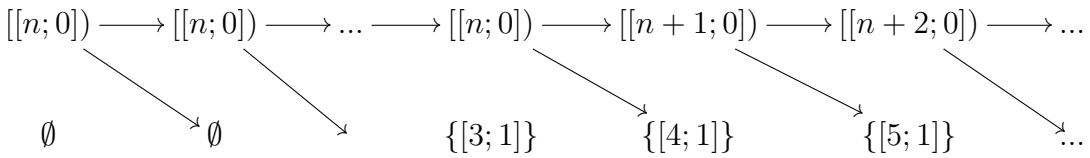
která vyjadřuje, že α nezačne platit v žádném stavu (tj. nikdy).

Interpretace: Stejná, jako příklad 4.2.3, ale opět obohacená. $V_a(\alpha)(0)$ je čas, ve kterém α začne platit. Pokud α začne platit v čase a nebo dříve, musí už být $V_a(\alpha)(0) = [a) = \top_{[a)^+}$, tj. ve stavu a výrok α platí. Přechod $f\colon p \to q$ je posun o $q-p$ jednotek času. Pokud ve stavu p výrok α ještě neplatí (začne platit až ve stavu n, kde $p \leq n$) a posuneme se o $q \geq n-p$ jednotek času, pravdivost výroku se změní na $V_q(\alpha)(0) = [n) \cap [q) = [q) = \top_{[q)^+}$, takže výrok začne platit. Pro monickou šipku $\eta\colon F \to G$ se charakter $\chi_{\eta p}(x) \in [p)^+$ ptá na otázku „Kdy začne x patřit do F?". ■

Příklad 4.2.4. Uvažujme $\mathbb{P} = \mathbb{N} \times 2$, kde prvky $[n;0]$ porovnáváme v prvním komponentu jako přirozená čísla a prvky $[n;1]$ splňují jen $[n;0] \leq [n;1]$.



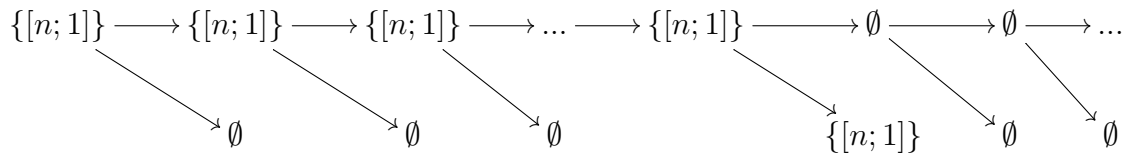
$\mathbb{N}$-valuace výroku $\alpha \in \Phi$ jsou buď $[[n;0])$ pro $n \in \mathbb{N}$ nebo $[m;1]$ pro $m \in \mathbb{N}$. V prvním případě komponenty $\mathbf{Set}^{\mathbb{N}}$-valuace tvoří poset



$V(\alpha) = [[n;0])$ znamená, že α začne platit ve stavu $[n;0]$. Pokud spadneme do některého ze stavů $[0;1], [1;1], ..., [n-1;1]$, nikdy se už nedostaneme do stavu $[n;0]$, a α tedy nikdy nezačne platit. Proto je

$$V(\alpha)_{[0;1]}(0) = V(\alpha)_{[1;1]}(0) = ... = V(\alpha)_{[n-1;1]}(0) = \emptyset,$$

neboli $\perp$ ve všech **HA** $\Omega([0;1]), ..., \Omega([n-1;1])$. V druhém případě komponenty $\mathbf{Set}^{\mathbb{N}}$-valuace tvoří poset



$V(\alpha) = \{[n;1]\}$ znamená, že α platí jen ve stavu $[n;1]$. Pokud spadneme do některého ze stavů $[0;1], [1;1], ..., [n-1;1]$, nebo stav $[n;1]$ „promeškáme" a pokračujeme do stavů v $[[n+1;0])$, nikdy se už do $\{[n;1]\}$ nedostaneme, a tedy

$$\begin{aligned} V(\alpha)_{[0;1]}(0) = V(\alpha)_{[1;1]}(0) = ... = V(\alpha)_{[n-1;1]}(0) = \emptyset, \\ V(\alpha)_{[n+1;0]}(0) = V(\alpha)_{[n+2;0]}(0) = ... = \emptyset, \\ V(\alpha)_{[n+1;1]}(0) = v(\alpha)_{[n+2;1]}(0) = ... = \emptyset, \end{aligned}$$

jsou $\perp$ v korespondujících **HA**. Jinak řečeno,

$$\neg\{[n;1]\} = \{[0;1]; [1;1]; ...; [n-1;1]\} \cup [[n+1;0]).$$

■

Příklad 4.2.5. Buď (X, τ) topologický prostor. Množina τ otevřených podmnožin X tvoří poset $(\tau, \subseteq)$. Můžeme zkonstruovat opačný poset $\mathbb{P} = (\tau, \subseteq)^{op} = (\tau, \sqsubseteq)$ kde

$$U \sqsubseteq V \quad \text{právě tehdy, když} \quad V \subseteq U$$

Pak principální množiny $[U)$ jsou právě otevřené podmnožiny U. Ty můžeme z otevřených podmnožin X dostat pomocí průniku:

$$[U) = \{S \cap U;\ S \in \tau\}$$

Pohled z množiny U je „lokální" pohled na množinu X. Kauzálně uzavřené množiny jsou sjednocení principálních množin, jenže sjednocení otevřených množin je zase otevřená množina! Každá kauzálně uzavřená množina v $\mathbb{P}^+$ tedy lze vyjádřit jako $[U)$ pro nějaké $U \in \tau$. Infima a suprema jsou jednoduše sjednocení a průnik:

$$\begin{aligned} [U) \sqcup [V) = [U \cup V), \\ [U) \sqcap [V) = [U \cap V), \end{aligned}$$

zatímco relativní pseudokomplement je vyjádřen vztahem

$$\begin{aligned} [U) \Rightarrow_W [V) &= \{x; x \in W \text{ a } [U \cap W; V \cap W] \in \mathrm{Eq}(\cap, \pi_1)(x)\} \\ &= \{x \in W;\ (U \cap W) \cap (V \cap W) = U \cap W\} = \{x \in W;\ U \cap V \cap W = U \cap W\}, \end{aligned}$$

tj. $[U) \Rightarrow_W [V)$ je největší otevřená podmnožina W, ve které lokálně platí $U \cap V = U$. Množinově-teoreticky toto je splněno množinou $A = (X \setminus U) \cup V$ a tedy $[U) \Rightarrow_W [V)$ je největší otevřená množina „uvnitř" $A \cap W$:

$$[U) \Rightarrow_W [V) = (A \cap W)^{\mathrm{int}} = ((X \setminus U)^{\mathrm{int}} \cup V) \cap W.$$

Zejména, když se podíváme z pohledu celé množiny X, relativní pseudokomplement

$$[U) \Rightarrow_X [V) = (X \setminus U)^{\mathrm{int}} \cup V$$

nabývá tvaru nám známého z příkladu 2.3.3. ■

4.3 Akce monoidů

Monoid $\mathbb{M}$ lze podle příkladu 3.2.4 chápat jako kategorii s jedním objektem M, kde šipky $M \to M$ značí prvky $\mathbb{M}$. V následující kapitole popíšeme $\mathbf{Set}^{\mathbb{M}}$ jako topos.

Objekty: Funktor $F\colon \mathbb{M} \to \mathbf{Set}$ je množina $F(M)$ spolu s funkcemi $Fm\colon F(M) \to F(M)$ pro každé $m \in \mathbb{M}$. Pak snadno definujeme $\mathbb{M}$-akci (viz. [n-l]) $A_F\colon \mathbb{M} \times F(M) \to F(M)$ předpisem $A_F(m,x) = Fm(x)$. Z definice funktoru získáme vlastnosti

$$A_F(e,x) = x \quad \text{a} \quad A_F(m, A_F(n,x)) = A_F(m \circ n, x),$$

což jsou přesně axiomy pro akci monoidu. Objekty $\mathbf{Set}^{\mathbb{M}}$ jsou právě $\mathbb{M}$-akce.

Šipky: Axiom přirozenosti pro $\eta : F \to G$

$$\begin{array}{ccc} F(M) & \xrightarrow{\eta_M} & G(M) \\ \downarrow{\scriptstyle Fm} & & \downarrow{\scriptstyle Gm} \\ F(M) & \xrightarrow{\eta_M} & G(m) \end{array}$$

říká, že η_M je ekvivariantní zobrazení mezi $\mathbb{M}-$akcemi:

$$\eta_M(A_F(m,-)) = A_G(m, \eta_M(-)).$$

Classifier: $M-$siev, tedy množina šipek $M \to M$ zleva uzavřená nad kompozicí, je levý ideál $\mathbb{M}$:

$$\Omega(M) = \{L;\ L \text{ je levý ideál } \mathbb{M}\}.$$

Jediné globální prvky $1 \to \Omega$ jsou $\bot, \top\colon 1 \rightrightarrows \Omega$, jejichž komponenty mají předpis $\bot_M(0) = \emptyset$ a $\top_M(0) = M$ (viz. [EM01]). Proto je zajímavější studovat Heytingovu algebru $(\Omega(M), \subseteq)$. $\mathbb{M}$ na $\Omega(M)$ působí akcí $A_\Omega(m,-) = \Omega m\colon \Omega(M) \to \Omega(M)$ s předpisem

$$A_\Omega(m,x) = \{\phi\colon M \to M;\ \phi \circ m \in x\} = \{\phi \in \mathbb{M};\ \phi \cdot m \in x\}.$$

Funktor $F \in \mathrm{Sub(G)}$ má charakter

$$(\chi_F)_M(x) = \{\phi : M \to M;\ G\phi(x) \in F(M)\} = \{\phi \in \mathbb{M}; A_G(\phi, x) \in F(M)\}$$

Zejména pak $(\chi_\bot)_M = \neg_M\colon \Omega(M) \to \Omega(M)$ definovaná pullbackem

$$\begin{array}{ccc} \{\emptyset\} & \hookrightarrow & \Omega(M) \\ \downarrow{\scriptstyle !} & & \downarrow{\scriptstyle \neg} \\ \{0\} & \xrightarrow{\top} & \Omega(M) \end{array}$$

má předpis

$$\neg_M(L) = \{\phi \in M;\ A_\Omega(\phi, L) = \emptyset\} = \{\phi \in M;\ \varphi \cdot \phi \notin L \ \text{ pro každé } \ \phi \in \mathbb{M}\}.$$

Pokud je monoid $\mathbb{M}$ komutativní a L je neprázdná, ϕ lze vždy vynásobit prvkem $l \in L$ a tím dostat $l \cdot \phi = \phi \cdot l$ do L, takže $\neg_M L = \emptyset$. V příkladech tedy negace nebudeme zmiňovat, poněvadž jsou triviální.

Interpretace: Prvky $\mathbb{M}$ kategoriálně chápeme jako šipky $M \to M$, pohybování po nichž vyjadřuje *rozhodování*. Při rozhodování se ovšem neposunujeme do dalšího stavu, ale měníme náš momentální stav. $V(\alpha) = L$ znamená, že α začne platit, pokud se posuneme do ideálu L. Dále $A_\Omega(m, V(\alpha)) = S$ znamená, že při vynásobení prvkem $m \in \mathbb{M}$ (tj. přechodu po šipce $m\colon M \to M$, neboli rozhodnutím m) se pravdivostní hodnota α změní na S. Zejména pak $A_\Omega(m, V(\alpha)) = M = \top_M(0)$ znamená, že po přechodu po šipce $m\colon M \to M$ začne α platit.

Příklad 4.3.1. Nechť $\mathbb{M}$ je grupa. Pak $\Omega(M) = \{\emptyset; M\} \cong \{\bot; \top\}$ tvoří Booleovu algebru známou z klasické logiky se standartními logickými funkcemi.

Interpretace: v grupě má každý prvek inverzi, takže každé rozhodnutí $m : M \to M$ lze navrátit rozhodnutím $m^{-1} : M \to M$. Stav nikdy nezměníme nenávratným způsobem, takže pokud α platí v $V(\alpha)$, musí platit i v $A_\Omega(m, V(\alpha)) = V(\alpha)$. Rozhodnutími pravdivost výroku nezměníme, může tedy být jen absolutně pravdivý ($V(\alpha) = M$), či absolutně nepravdivý ($V(\alpha) = \emptyset$).

Příklad 4.3.2. Nechť $\mathbb{M} = (\mathbb{N}, +, 0)$. Levé ideály jsou množiny tvaru

$$[n) = \{n;\ n+1;\ n+2;\ ...\}.$$

Předpis

$$\begin{aligned} \emptyset &\mapsto \emptyset \\ [n) &\mapsto n \\ n &\mapsto [n) \end{aligned}$$

určuje bijekci $\Omega(M) \cong \mathbb{N} \cup \{\emptyset\}$. Dále

$$\phi + m \geq n \text{ právě tehdy, když } \phi \geq max(0; n - m),$$

takže $A_\Omega(m, [n)) = [max(0; n - m))$. Logické funkce $\sqcup, \sqcap, \Rightarrow, \neg$ jsou stejné jako v příkladu 2.4.2. Model slouží jako alternativní popis příkladu 2.4.2 (postup času).

Interpretace: $V(\alpha) = [n)$ znamená, že n začne platit za n jednotek času (např. sekund). $A_\Omega(m, -)$ vyjadřuje postup času o m jednotek: když α začne platit za n sekund, po uplynutí m sekund buď α platí (pokud $n \leq m$) a nebo začne platit za $n - m$ sekund (pokud $m \leq n$). ■

Příklad 4.3.3. $\mathbb{M} = (\mathbb{N}, \cdot, 1)$. Levé ideály jsou množiny tvaru

$$n\mathbb{N} = \{0;\ n;\ 2n;\ 3n;\ ...\}.$$

Předpis

$$\begin{aligned} \emptyset &\mapsto \emptyset \\ n\mathbb{N} &\mapsto n \\ n &\mapsto n\mathbb{N} \end{aligned}$$

určuje bijekci $\Omega(M) \cong \mathbb{N} \cup \{\emptyset\}$. Dále

$$n \mid \phi \cdot m \quad \text{právě tehdy, když} \quad \frac{\mathrm{nsn}(n,m)}{m} \mid \phi,$$

takže $A_\Omega(m, n\mathbb{N}) = \frac{\mathrm{nsn}(n,m)}{m}\mathbb{N}$.

Důkaz: Rozepišme

$$\begin{aligned} n &= p_1^{n_1} \cdot p_2^{n_2} \cdot ... \cdot p_l^{n_l}, \\ m &= p_1^{m_1} \cdot p_2^{m_2} \cdot ... \cdot p_l^{m_l}, \\ \text{a} \quad \phi &= p_1^{\phi_1} \cdot p_2^{\phi_2} \cdot ... \cdot p_l^{\phi_l}, \end{aligned}$$

kde p_i je $i-$té prvočíslo. Pak $n|\phi \cdot m$ znamená $n_i \leq \phi_i + m_i$ pro každé $1 \leq i \leq l$, což je ekvivalentní s $\max(n_i, m_i) - m_i = \max(0, n_i - m_i) \leq \phi_i$, neboli

$$\frac{\mathrm{nsn}(n,m)}{m} = \frac{p_1^{\max(n_1,m_1)} \cdot p_2^{\max(n_2,m_2)} \cdot ... \cdot p_l^{\max(n_l,m_l)}}{p_1^{m_1} \cdot p_2^{m_2} \cdot ... \cdot p_l^{m_l}} \mid \phi$$

□

Konjunkce a disjunkce jsou

$$\begin{aligned} n\mathbb{N} \cup m\mathbb{N} &= \mathrm{NSD}(n,m)\mathbb{N}, \\ n\mathbb{N} \cap m\mathbb{N} &= \mathrm{nsn}(n,m)\mathbb{N}. \end{aligned}$$

Relativní pseudokomplement $n\mathbb{N} \Rightarrow mN$ je složitější, neboť ho nelze vyjádřit přímo z n, m (aspoň dle mých znalostí). Po rozepsání

$$\begin{aligned} n &= p_1^{n_1} \cdot p_2^{n_2} \cdot ... \cdot p_l^{n_l}, \\ m &= p_1^{m_1} \cdot p_2^{m_2} \cdot ... \cdot p_l^{m_l}, \\ \text{a} \quad \phi &= p_1^{\phi_1} \cdot p_2^{\phi_2} \cdot ... \cdot p_l^{\phi_l}, \end{aligned}$$

se podmínka

$$n\mathbb{N} \Rightarrow mN \subseteq \phi\mathbb{N} \quad \text{právě tehdy, když} \quad \mathrm{nsn}(n,m)\mathbb{N} \subseteq \phi\mathbb{N}$$

změní na

$$\begin{aligned} &\phi_i \quad \text{je největší takové, že} \quad \max(n_i, \phi_i) \leq m_i, \\ &\phi_i = \begin{cases} 0 & m_i \leq n_i, \\ m_i & n_i \leq m_i \end{cases} \end{aligned}$$

Např. $18\mathbb{N} \Rightarrow 60\mathbb{N} = 20\mathbb{N}$.

Interpretace: Svůj stav můžeme změnit nekonečně mnohokrát rozhodnutími $p_1, p_2, p_3, ...$, kde $i-$té rozhodnutí je označeno $i-$tým prvočíslem p_i. Každé prvočíslo si můžeme vybrat vícekrát: do stavu

$$n = p_1^{n_1} \cdot p_2^{n_2} \cdot ... \cdot p_l^{n_l}$$

se dostaneme n_1-násobným zvolením možnosti p_1, n_2-násobným zvolením možnosti p_2 atd. Takto nám každé přirozené číslo určuje právě jednu kombinaci možností. $V(\alpha) = m = p_1^{m_1} \cdot p_2^{m_2} \cdot ... \cdot p_l^{m_l}$ znamená, že α začne platit, až se příslušným rozhodováním dostaneme do stavu m. Jinak řečeno, $V(\alpha)$ je odpověď na otázku „Po jakých rozhodnutích začne platit α?", zatímco $A_\Omega(m, V(\alpha))$ je odpověď na otázku „Po jakých rozhodnutích začne platit α, když jsou má dosavadní rozhodnutí m?". ■

Příklad 4.3.4. $\mathbb{M} = (\{0; 1\}, \cdot, 1)$. Levé ideály tvoří množinu

$$\Omega(M) = \{\emptyset;\ \{0\},\ \{0; 1\}\}$$

Máme dvě možnosti, jak změnit svůj stav: násobením jedničkou $A_\Omega(1, -) = id_{\Omega(M)}$ nic neuděláme a vynásobením nulou $A_\Omega(0, -)$ změníme svůj stav nevratným způsobem. Tím naše logika „spadne" do klasické logiky: možné hodnoty $A_\Omega(0, L)$ jsou $\emptyset$ a M, což tvoří Heytingovu algebru $\{\bot; \top\}$ (příklad 1.2.11).

Pravdivostní hodnoty v $\Omega(M)$ tvoří Heytingovu algebru znázorněnou diagramem

$$\emptyset \longrightarrow \{0\} \longrightarrow M.$$

Logické funkce na jsou určeny tabulkami

$\neg$	
$\emptyset$	M
$\{0\}$	$\emptyset$
M	$\emptyset$

$\sqcap$	$\emptyset$	$\{0\}$	M
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
1	$\emptyset$	$\{0\}$	$\{0\}$
M	$\emptyset$	$\{0\}$	M

$\sqcup$	$\emptyset$	$\{0\}$	M
$\emptyset$	$\emptyset$	$\{0\}$	M
$\{0\}$	$\{0\}$	$\{0\}$	M
M	M	M	M

$\Rightarrow$	$\emptyset$	$\{0\}$	M
$\emptyset$	M	M	M
$\{0\}$	$\emptyset$	M	M
M	$\emptyset$	$\{0\}$	M

Interpretace: Zafixujme si výrok $X \in \Phi$ a sledujme, jak jiné výroky platí v závislosti na X. Valuaci $V\colon \Phi_0 \to \Omega(M)$ definujeme předpisem

$$V(\alpha) = \begin{cases} \emptyset & \alpha \text{ neplatí nezávisle na } X, \\ \{0\} & \alpha \text{ platí jen, pokud platí } X, \\ \{0; 1\} & \alpha \text{ platí nezávisle na } X. \end{cases}$$

Valuaci induktivně rozšíříme na $V'\colon \Phi \to \Omega(M)$. Konkrétně tedy $V(X) = \{0\}$. Možnost $V(\alpha) = \{1\}$ nemůže nastat, neboť pokud jsme dokázali α nezávisle na platnosti X, z X nelze dokázat $\sim \alpha$. Negace jsou z tohoto důvodu zvláštní - pokud by bylo

$$\neg S = \Omega(M) \setminus S,$$

pro každé $S \in \Omega(M)$, muselo by být $\neg\{0\} = \{1\} \notin \Omega(M)$. Pokud chceme negace počítat „po komponentech", musíme začít „od konce" a teprve uvažovat případ, kdy X platí: pokud $V(\alpha) = \{0\}$, pak α platí závisle na X, takže $\sim \alpha$ neplatí nezávisle na X, a tedy nemůže platit ani závisle na X. Proto $\neg\{0\} = V(\sim \alpha) = \emptyset$.

Pokud výrok $\alpha \in \Phi$ platí závisle na X ($V(\alpha) = \{0\}$), v případě neplatnosti X není ani pravdivý (nedokázali jsme ho) a ani nepravdivý (nevyvrátili jsme ho, v případě platnosti X stále může platit) a platí

$$V(\alpha \vee \sim \alpha) = \{0\} \cup \emptyset = \{0\} \neq \top_M(0),$$

takže $\mathbf{Set}^{\mathbb{M}} \not\models \alpha \vee \sim \alpha$. ■

4.4 Topos funkcí

V následující sekci popíšeme kategorii $\mathbf{Set}^{\to}$ definovanou příkladem 3.2.17 jako topos. Kategorie $\longrightarrow$ je poset znázorněný diagramem

$$0 \xrightarrow{f} 1.$$

Kauzálně uzavřené množiny tvoří množiny

$$\Omega(0) = \{\emptyset; \{1\}; \{0;1\}\}$$
$$\Omega(1) = \{\emptyset; \{1\}\}$$

Classifier je funkce $\Omega f\colon \Omega(0) \to \Omega(1)$ s předpisem

$$\Omega f(\emptyset) = \emptyset, \quad \Omega f(\{1\}) = \{1\}, \quad \text{a} \quad \Omega f(\{0;1\}) = \{1\}.$$

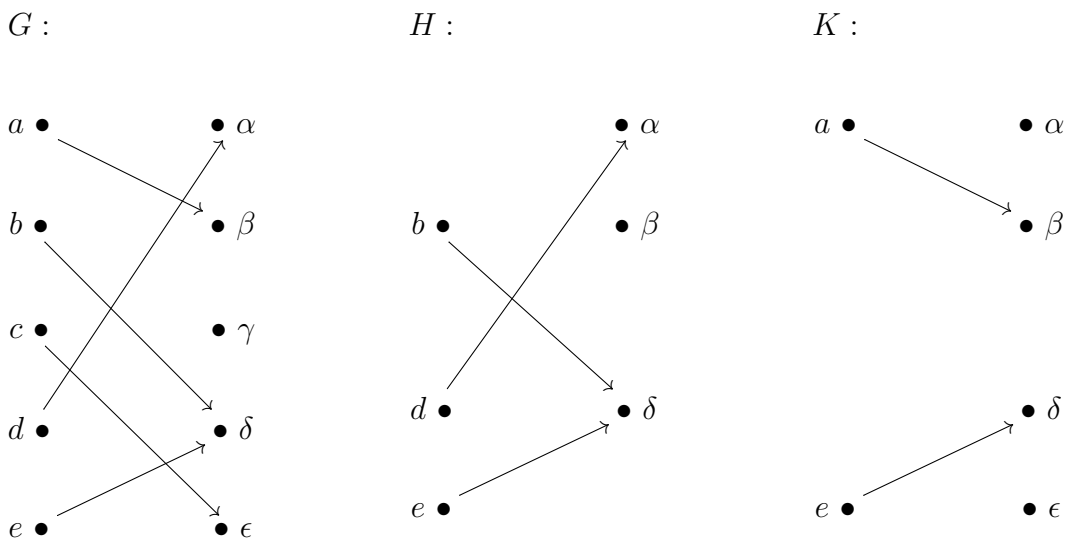
Předpis

$$\emptyset \mapsto \emptyset, \quad \{0\} \mapsto \{1\}, \quad M \mapsto \{0;1\}$$

určuje isomorfismus Heytingových algeber $\{\emptyset; \{1\}; \{0;1\}\} = \Omega(0) \cong \Omega(M) = \{\emptyset; \{0\}; \{0;1\}\}$ classifieru v $\mathbf{Set}^{\to}$ a v $\mathbf{Set}^{\mathbb{M}}$ z příkladu 4.3.4. Proto je vše (logické funkce, struktura $\Omega(0)$, interpretace) shodné s příkladem 4.3.4.

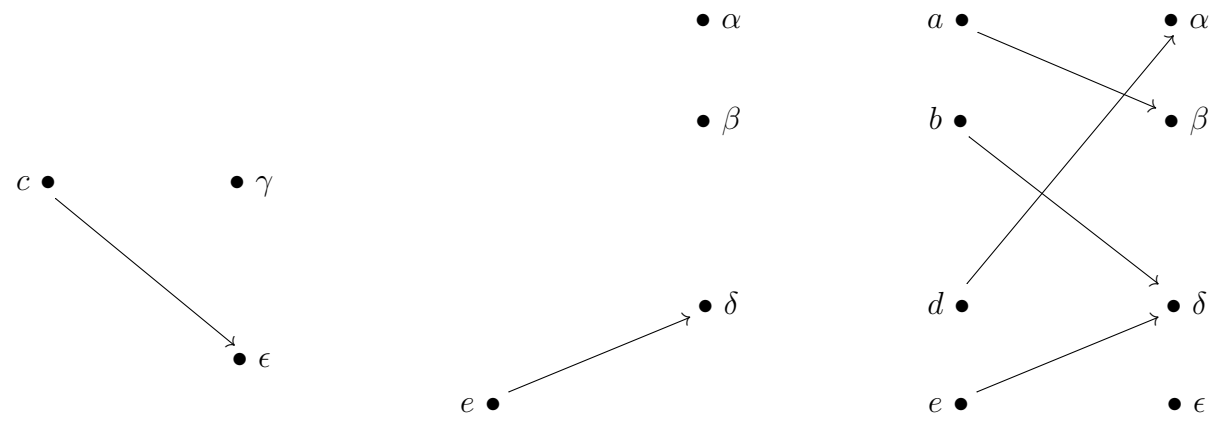
Příklad 4.4.1. Nechť F je koncept množiny protipříkladů Riemannovy hypotézy, přičemž ve stavu 0 jsme Riemannovu hypotézu nevyvrátili a ve stavu 1 už ano. Pak $F(0) = \emptyset$, ale $F(1)$ může být neprázdná. Říkáme, že F je *potenciálně neprázdná.* ■

Příklad 4.4.2. Uvažujme funktor G, korespondující funkci $Gf : \{a;\ b;\ c;\ d;\ e\} \to \{\alpha;\ \beta;\ \gamma;\ \delta;\ \epsilon\}$ a $H, K \in \mathrm{Sub}(g)$, jejichž předpisy jsou znázorněny diagramy



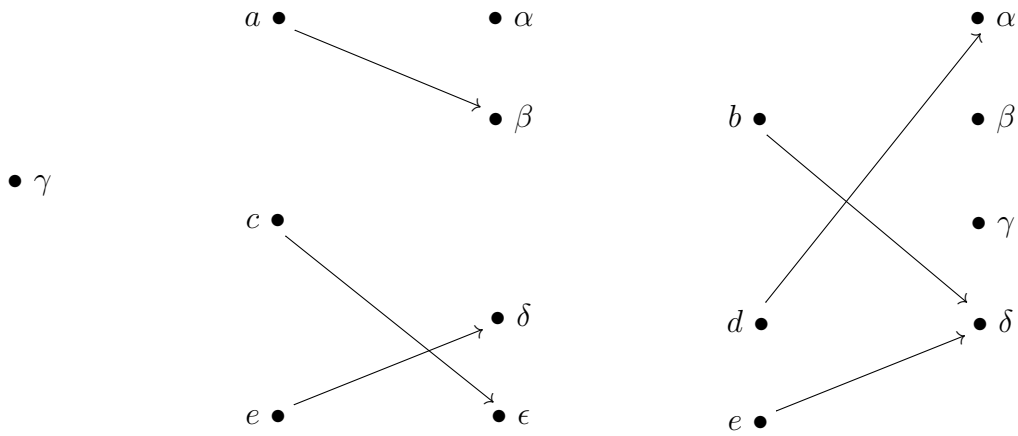
$\cap, \cup$ se počítají po komponentách. Při počítání $\neg$ musíme v analogii s příkladem 4.3.4 začít od konce: $\neg H(1) = G(1) \setminus H(1) = \{\gamma, \epsilon\}$ je množinový doplněk a $\neg H(0) = Hf^{-1}(\neg H(1)) = \{c\}$ je množina všech prvků $G(0)$, které se funkcí Gf pošlou do $\neg H(1)$.

$\neg H$: $H \cap K$: $H \cup K$:



Relativní pseudokomplement $\Rightarrow$ počítáme podobně „odzadu"jako pseudokomplement: $(K \Rightarrow H)(1) = (G(1) \setminus K(1)) \cup H(1)$ funguje stejně jako v Booleově algebře $\mathcal{P}(X)$. Pro vyšetření množiny $(K \Rightarrow H)(0)$ se podíváme, kdy začne „koncept"a patřit do K. Pro $a \in G(0)$ nastává $a \in (K \Rightarrow H)(0)$, kdykoliv jsou splněny následující podmínky:
1) pokud $a \in K(0)$, musí platit $a \in H(0)$,
2) pokud $a \notin K(0)$, ale $Gf(a) \in K(1)$, musí platit $Gf(a) \in H(1)$.

$\neg K$: $H \Rightarrow K$: $K \Rightarrow H$:



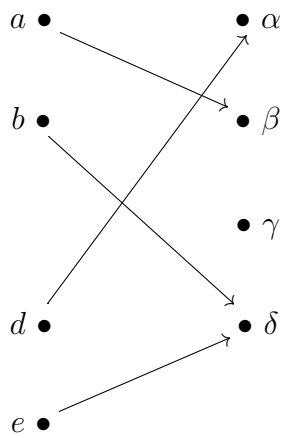
Zajímavá je taktéž dvojitá negace:

$$\begin{aligned}\neg\neg A(n) &= \{x \in D(n);\ D\phi(x) \notin \neg A(l) \text{ pro každé } \phi\colon n \to l\}\\ &= \{x \in D(n);\ (D\phi(x) \notin \neg A(l) \text{ pro každé } \varphi\colon l \to k) \text{ nenastane pro žádné } \phi\colon n \to l\}\\ &= \{x \in D(n);\ \text{ pro každé } \phi : n \to l \text{ existuje } \varphi\colon l \to c \text{ takové, že } D(\circ\phi)(x) \in A(c)\}\end{aligned}$$

Dvojitá negace $\sim\sim$ má podle sekce **4.1** význam „vždy může platit, že ...". Její interpretace, dvojitý pseudokomplement $\neg\neg$, je *zúplnění*: $\neg\neg H$ je množina všech bodů, které funkce

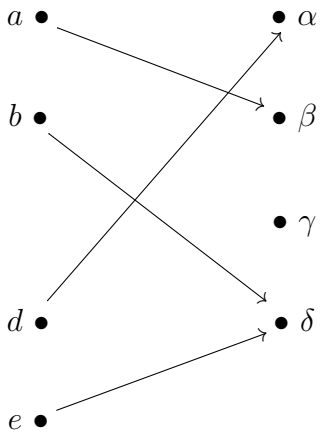
Gf „pošle do H". Množiny v $\neg\neg H$ se pak počítají jako $\neg\neg H(1) = H(1)$ a $\neg\neg H(0) = Gf^{-1}(H(1))$:

$\neg\neg H$:

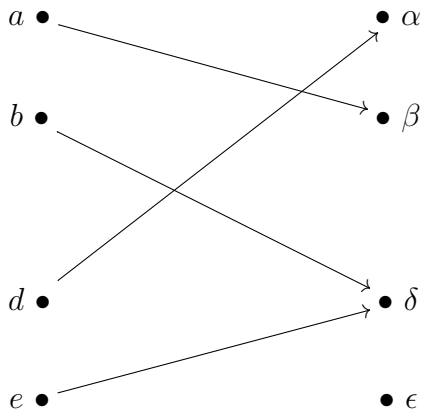


V tomto příkladu neplatí modus tollens, neboť $((\neg H \Rightarrow \neg K) \Rightarrow (K \Rightarrow H))(0) \neq G(0)$:

$\neg H \Rightarrow \neg K$:

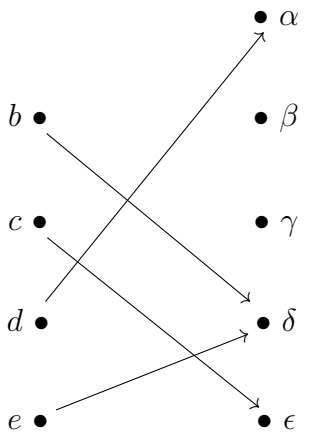


$(\neg H \Rightarrow \neg K) \Rightarrow (K \Rightarrow H)$:

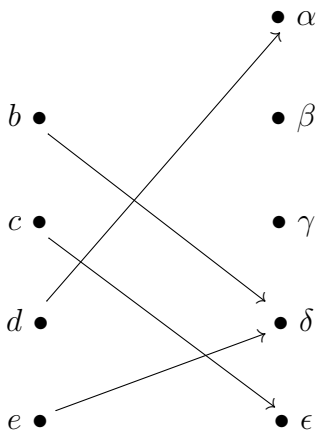


Dále v tomto příkladu neplatí **LEM** a $\alpha \to \sim\sim \alpha$:

$H \cup \neg H$:



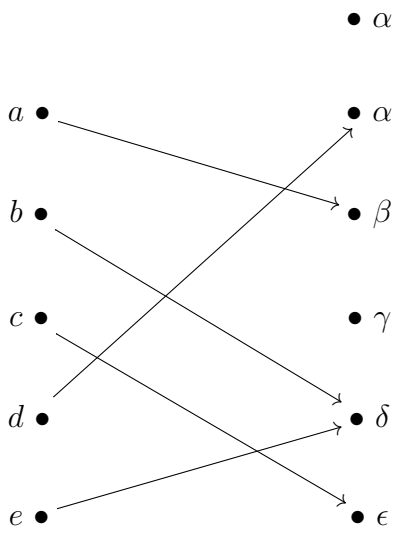
$\neg\neg H \Rightarrow H$:



Výše uvedené protipříklady ovšem nesplňují klasické tautologie pouze ve stavu 0. Najít skutečný protipříklad tautologie **LEM** by znamenalo najít $F \in Sub(G)$ takové, že $(F \cup \neg F)(1) \neq G(1)$. To ovšem nelze, neboť $(F \cup \neg F)(1) = F(1) \cup (G(1) \setminus F(1)) = G(1)$, takže formule **LEM** selže jen ve stavu 0. Tyto *slabé protipříklady* jsme už potkali v sekci **2.1**.

Formule $(\alpha \to \beta) \vee (\beta \to \alpha)$ ovšem platí:

$(H \Rightarrow K) \cup (K \Rightarrow H)$:



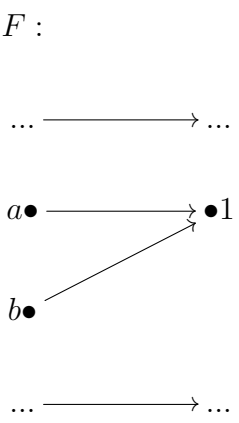
Obecněji platí $\mathbf{Set}^{\mathbb{P}} \models (\alpha \to \beta) \vee (\beta \to \alpha)$, kdykoliv poset $\mathbb{P}$ je úplně uspořádaný. Výrok $(\alpha \to \beta) \vee (\beta \to \alpha)$ znamená, že α a β spolu „kauzálně souvisí."

Úplně uspořádaný poset můžeme chápat jako momenty „zobecněného času": např. pokud bychom v příkladu 4.3.3 měli jen možnost $p_1 = 2$, naše stavy se mohou změnit jen jedním způsobem. Naše jediná možnost je pokračovat, nebo se zastavit. Toto rozhodování, zda-li jít či nejít dál, tvoří tok onoho zobecněného času. Formálně řečeno, exponenciální funkce $x \mapsto 2^x$ tvoří isomorfismus Heytingových algeber (iso šipku v **HeytAlg**) mezi $(\mathbb{N}, \leq)^+$ vyjadřující plynutí času a $(\{1; 2; 4; 8; 16; ...\}, |)^+$ vyjadřující jedno možné rozhodnutí. ■

Příklad 4.4.3. Někteří lidé neví, že $1 = 0,\overline{9}$. Jejich koncept reálných čísel F tedy obsahuje „koncept" $a\colon 1 \to F$ čísla 1 s hodnotou $a_0(0) \in F(0)$ a koncept $b\colon 1 \to F$ čísla $0,\overline{9}$ s hodnotou $b_0(0) \in F(0)$ jako dva různé prvky $a_0(0) \neq b_0(0)$. Jakmile ale zjistí, že supremum na $\mathbb{R}$ je jedinečné, hned si uvědomí, že

$$1 = \sup\{0,9;\ 0,99;\ 0,999;\ ...\} = 0,\overline{9}$$

Pak koncepty a a b splynou v $a_1(0) = Ff(a_0(0)) = Ff(b_0(0)) = b_1(0) \in F(1)$:



Zde ve stavu 0 tvrzení $1 = 0,\overline{9}$ není pravdivé (ještě nevíme, že je pravdivé), ale ve stavu 1 tvrzení pravdivé je.

Důkaz jedinečnosti můžeme vždy chápat podobným způsobem jako „splývání" konceptů. ■

Bibliografie

[Gol84] Robert Goldblatt. *Topoi: The Categorial Analysis of Logic*. 1984. ISBN: 0444867112.

[EM01] Mehdi Ebrahimi a Mojgan Mahmoudi. "The category of M-sets". In: *Italian Journal of Pure and Applied Mathematics [electronic only]* 9 (led. 2001).

[WD15] William Weiss a Cherie D'Mello. *Fundamentals of Model Theory*. 2015.

[Wal17] Michał Walicki. *Introduction to mathematical logic*. World Scientific, 2017.

[Bri19] Mark Bridger. *Real analysis: A constructive approach through interval arithmetic*. American Mathematical Society, 2019.

[Tri19] Todd Trimble. *An Elementary Approach to Elementary Topos Theory*. 2019. URL: `https://ct-octoberfest.github.io/2019-slides/ttrimble.pdf`.

[CKA] Leran Cai, Ambrus Kaposi a Thorsten Altenkirch. *Formalising the Completeness Theorem of Classical Propositional Logic in Agda (Proof Pearl)*. URL: `https://akaposi.github.io/proplogic.pdf`.

[n-l] n-lab. URL: `http://nlab-pages.s3.us-east-2.amazonaws.com/nlab/show/action`.

[Sha] Talk Shawn. *Introduction to Kripke semantics*. URL: `http://therisingsea.org/notes/talk-shawn-kripke.pdf`.

[Zal] Edward N. Zalta. URL: `https://plato.stanford.edu/entries/intuitionistic-logic-development/#Bib`.