Úlohy - výroková logika (přepis)

Martin Všetička

20.11.2008

1 Značení a některé pojmy

- $|X|$ značí velikost množiny X
- $\mathbb{P}$ označuje množinu prvovýroků.
- ${}^{x}2$ je množina všech zobrazení z X do $2 = \{0, 1\}$.
  - ${}^{\mathbb{P}}2$ je množina všech pravdivostních ohodnocení prvovýroků čili všech modelů výrokové logiky nad $\mathbb{P}$.
  - $M(T)$ je množina všech modelů teorie T; je-li T tvaru $\{A\}$, píšeme $M(A)$
  - Zřejmě je $M(T) \subseteq {}^{\mathbb{P}}2$.
  - Množina $K \subseteq {}^{\mathbb{P}}2$ je [konečně] axiomatizovaná, existuje-li [konečná] teorie $T \subseteq FmP^{\mathbb{P}}$ tak, že $K = M(T)$.
- $\mathbb{N}$ je množina všech přirozených čísel.
- Symbol A^1 značí A, A^0 značí $\neg A$
- $P^{\mathbb{P}}$ je jazyk výrokové logiky s množinou všech prvovýroků $\mathbb{P}$ ($FmP^{\mathbb{P}}$ je množina všech výroků jazyka $P^{\mathbb{P}}$).
- $p, q, r, p', p_0, \ldots$ značí prvovýroky
- $A, B, C, D, \ldots$ značí výroky
- $Con(T) = \{A; T \vdash A\}$ je množina všech teorému neboli dokazatelných výroku teorie T.
  - Teorie T a S (v témže jazyce) jsou **ekvivalentní**, mají-li stejné množiny teorému (tj. $\{A|T \vdash A\} = \{A|S \vdash A\}$, tj. $Con(T) = Con(S)$)
  - Teorie T je slabší než S a S je silnejší než T, když platí $Con(T) \subseteq Con(S)$.
- $(A \dot{-} B)$ je zkratka za výrok $(A\&\neg B) \vee (B\&\neg A)$, zvaný **výlučná disjunkce** (XOR)

P.1.1 Logika s konečně prvovýroky

P.1.1.1 Buď $|\mathbb{P}| = l$ konečné nenulové

1. **Zadání:** $|\mathbb{P}| = l \in \mathbb{N}$. Existuje 2^{2^l} neekvivalentních teorií a právě 2^l kompletních neekvivalentních teorií v $P^{\mathbb{P}}$.

   Pojmy:

   - **Kompletní teorie** jsou právě ty, které mají jediný model.
   - Teorie T a S (v témže jazyce) jsou **ekvivalentní**, mají-li stejné množiny teorémů (tj. $\{A|T \vdash A\} = \{A|S \vdash A\}$, tj. $Con(T) = Con(S)$)

Řešení: Máme dvě tvrzení, takže postupně:

1. část:

> **Lemma 1** T je ekvivalentní s $S \Leftrightarrow M(T) = M(S)$
> $\Rightarrow$ TODO
> $\Leftarrow$ TODO
> Tedy neekvivalentních teorií je právě tolik, kolik je podmnožin ${}^{\mathbb{P}}2$, neboť každá taková podmnožina je třídou všech modelů nějaké teorie.
>
> **Řečeno čísly:** Mám l prvovýroků a každému prvovýroku můžu přiřadit hodnotu 1 nebo 0, tj. 2^l možností, resp. 2^l pravdivostních ohodnocení (funkce) - tím jsem dostal $|{}^{\mathbb{P}}2|$. Nyní spočítám počet podmnožin ${}^{\mathbb{P}}2$, což se počítá pomocí vzorečku na mohutnost potenční množiny - tj. 2^n, kde n je počet prvků množiny. V našem případě je prvkem množiny nějaká ohodnocovací funkce v. Dostáváme tedy 2^{2^l}.

2. část: Kompletní teorie jsou právě ty, které mají jediný model [1]. Pro každý prvovýrok se tedy mužeme rozhodnout, zda mu přiřadíme 1 nebo 0. Voleb máme $l = |\mathbb{P}|$. Možností je tedy 2^l.

2. **Zadání:** $|\mathbb{P}| = l \in \mathbb{N}$. Teorie T má $2^{2^l - |M(T)|}$ neekvivalentních teorémů a vyvratitelných formulí a dále $(2^{|M(T)|} - 2) \cdot 2^{2^l - |M(T)|} (= 2^{2^l}(1 - 2^{1+|M(T)|}))$ neekvivalentních nezávislých výroků.

   Pojmy:

   - **ekvivalentní teorémy** - teorémy, které mají stejné množiny modelů (viz lemma v P.1.1.1.1)
   - **vyvratitelná formule** - formule A je vyvratitelná, je-li $\neg A$ dokazatelná
   - **nezávislá formule** - nelze dokázat ani A, ani $\neg A$

   ⚓ **Příklad:**

   Vezměme si třeba $\mathbb{P} = \{p, q\}$ (logika se dvěma prvovýroky) a teorii $T = \{p\}$. Z věty o úplnosti víme: $T \vdash q \Leftrightarrow T \models q$. Formule q je nezávislá formule, jelikož neplatí:

   – ani $T \models q$ (protipříklad: $v = \{p \to 1, q \to 0\}$ je modelem T, ale není modelem q)
   – ani $T \models \neg q$ (protipříklad: $v = \{p \to 1, q \to 1\}$ je modelem T, ale není modelem $\neg q$)

   Podle vzorečku ze zadání příkladu je nezávislých formulí: $(2^2 - 2) \cdot 2^{2^2-2} = (4-2) \cdot 4 = 8$
   Vypišme si nejdříve dokazatelné[2] formule v T:

   (a) p
   (b) $\neg q \to p$ (což je $q \vee p$)
   (c) $q \to p$ (což je $\neg q \vee p$)
   (d) $q \to q$

   Vyvratitelné[3] jsou právě negace formulí výše.
   Nezávislé[4] formule jsou ty, které zbývají:

   (a) q $(v_{1,1}, v_{0,1})$
   (b) $\neg q$ $(v_{1,0}, v_{0,0})$
   (c) $p \ \& \ q$ $(v_{1,1})$
   (d) $p \ \& \ \neg q$ $(v_{1,0})$
   (e) ??
   (f) ??
   (g) ??
   (h) ??

   Řešení:

[1] Právě jeden model má teorie $T = \{p^{v(p)}; p \in \mathbb{P}\}$, modelem je pravdivostní ohodnocení v, tj. $M(T) = \{v\}$
[2] formule jsou pravdivé pro každý model T
[3] každá formule je nepravdivé pro každý model T
[4] alespoň jednou je formule pravdivá a alespoň jednou je formule nepravdivá v rámci modelů T

Lemma 2 $T \vdash A \Leftrightarrow M(T) \subseteq M(A)$

Důkaz. Dokazujeme obě implikace:

"$\Rightarrow$" Stačí se odvolat na větu o úplnosti, která říká, že $T \vdash A \Leftrightarrow T \models A$.
$T \models A$ však znamená, že A je tautologickým důsledkem množiny formulí T a formule A je pravdivá při každém ohodnocení, které je modelem množiny T. Tím jsme ukázali, že platí $M(T) \subseteq M(A)$.
Stojí za to si však uvědomit, kdy nastane $M(T) \subset M(A)$. Vezměme si teorií T takto:
$T = \{p, p \to q\}$. Pomocí pravidla modus ponens dostáváme:
$T \vdash q$. Podívejme se nyní podíváme na modely $M(q)$ a $M(T)$.
$M(T)$ má jediný model: $v_1 = \{p \to 1, q \to 1\}$
$M(q)$ má však modely dva: $v_1 = \{p \to 1, q \to 1\}, v_2 = \{p \to 0, q \to 1\}$!!

"$\Leftarrow$" $M(T) \subseteq M(A) \Rightarrow T \models A \overbrace{\Rightarrow}^{\text{věta o úplnosti}} T \vdash A$

□

Tudíž neekvivalentních teorémů teorie T je tolik, kolik je množin M takových, že $M(T) \subseteq M \subseteq {}^{\mathbb{P}}2$, tj. právě $2^{2^l - |M(T)|}$. Tolik je i vyvratitelných formulí a tedy nezávislých je $2^{2^l} - 2 \cdot 2^{2^l - |M(T)|}$.

Podstata tohoto důkazu tkví v myšlence, že převedeme důkaz na důkaz prvního příkladu.

3. **Zadání:** $|\mathbb{P}| = l \in \mathbb{N}$. Teorie T má $|M(T)|$ neekvivalentních kompletních rozšíření a $2^{|M(T)|}$ neekvivalentních rozšíření (z nichž jediné je sporné).

   Pojmy:

   - T' **je rozšíření (je silnější než)** $T \Leftrightarrow Cont(T) \subseteq Con(T')$, z toho plyne: $Cont(T) \subseteq Cont(T') \Leftrightarrow M(T') \subseteq M(T)$
   - T' **je kompletní rozšíření** T - pokud $M(T')$ obsahuje právě jeden prvek.

   Řešení: Každá množina $M \subseteq M(T)$ představuje až na ekvivalenci právě jednu teorii rozšiřující T; jednoprvkové M jsou pak právě modely kompletních rozšíření T.

   Přípisek: Nyní řešíme, dalo by se říci, opačný příklad k 1. a 2. příkladu. Nehledáme nadmnožiny $M(T)$, ale podmnožiny.

   Teorií rozšiřujících teorii T máme $2^{|M(T)|}$, jelikož z množiny modelů $M(T)$ vybíráme všechny možné podmnožiny. Opět jsme tedy použili vzorec pro výpočet potenční množiny. Číslo $2^{|M(T)|}$ však zahrnuje i prázdnou množinu a samotnou množinu $M(T)$, zatímco druhá jmenovaná nám nevadí (viz definice rozšíření teorie), tak první ano. Prázdná množina modelů značí kontradikce, které nás obecně příliš nezajímají, navíc bychom takto teorii T nijak nerozšířili (v přirozeném slova smyslu).

   Teorií kompletně rozšiřujících T je pouze $M(T)$, jelikož vybíráme jednoprvkové podmnožiny množiny $M(T)$ (proč viz definice)

P.1.1.2 Buď $|\mathbb{P}| = l$ konečné nenulové

1. **Zadání:** $|\mathbb{P}| = l \in \mathbb{N}$. Nechť A je výrok. Kolik je neekvivalentních výroků B takových, že $B \models A$ nebo $A \models B$?

   Návod: Pomocí l a $M(A)$ spočtěte, kolik je množin $M(B)$ pro uvažovaná B.

   Řešení: Podle předchozích příkladů máme obdobně: $2^{|M(A)|} + 2^{2^l - |M(A)|} - 1$. Výsledkem je počet množin $K \subseteq {}^{\mathbb{P}}2$ takových, že $K \subseteq M(A)$ nebo $M(A) \subseteq K$ a vynecháváme $K = \{\emptyset\}$

Přípisek: Pro objasnění výpočtu pro část "$B \models A$" se podívejte na lemma v druhém příkladu P.1.1.1.

"$A \models B$" odpovídá počtu neekvivalentních teorémů ze zadání druhého příkladu P.1.1.1.

2. **Zadání:** $|\mathbb{P}| = l \in \mathbb{N}$. Nechť $\{A, B\}$ je sporná teorie. Kolik je neekvivalentních teorémů teorie $\{A \vee B\}$?

   Návod: Vyjádřete výsledek pomocí $l, M(A), M(B)$.

   Řešení: Výsledek je $2^{2^l-(|M(A)|+|M(B)|)}$. Platí totiž $|M(A \vee B)| = |M(A) \cup M(B)| = |M(A)| + |M(B)|$. Poslední rovnost plyne z $M(A) \cap M(B) = M(A \;\&\; B) = \emptyset$

   Přípisek: Spornost teorie $\{A, B\}$ nám dovoluje tvrdit: $\{A, B\} \vdash p \;\&\; \neg p$, pro libovolné $p \in \mathbb{P}$, pro takovou teorii však nemůže existovat žádný model! Toto přesně vyjadřuje poslední rovnice v řešení výše.

3. **Zadání:** $|\mathbb{P}| = l \in \mathbb{N}$. Buď A výrok, $M(A) \neq \emptyset$

   (a) $\bigvee_{v \in M(A)} \bigwedge_{p \in \mathbb{P}} p^{v(p)}$ je disjunktivně normální tvar A.

   (b) $\bigwedge_{v \in {}^{\mathbb{P}}2 - M(A)} \bigvee_{p \in \mathbb{P}} (\neg p)^{v(p)}$ je konjuntivně normální tvar A.

P.1.1.3

1. Buď $\mathbb{P} = \{p, q, r\}$ množina všech prvovýroků

   (a) Ekvivalentními úpravami najděte disjunktivně normální tvar následujícího výroku D:

   $$(p \to \neg q) \;\&\; (\neg p \to q) \;\&\; r \tag{1}$$

   Řešení: Upravujeme ekvivalentními úpravami na DNF:

   $$(p \to \neg q) \;\&\; (\neg p \to q) \;\&\; r \tag{2}$$

   Použijeme zkratky:

   $$(\neg p \vee \neg q) \;\&\; (p \vee q) \;\&\; r \tag{3}$$

   Použijeme zákon o distributivitě:

   $$(((\neg p \vee \neg q) \vee p) \;\&\; ((\neg p \vee \neg q) \vee q)) \;\&\; r \tag{4}$$

   $$(((\underbrace{\neg p \;\&\; p)}_{\text{vyškrtneme}} \vee (\neg q \;\&\; p)) \vee ((\neg p \;\&\; q) \vee \underbrace{(\neg q \;\&\; q)}_{\text{vyškrtneme}})) \;\&\; r \tag{5}$$

   Znovu zákon o distributivitě:

   $$((\neg q \;\&\; p) \vee (\neg p \;\&\; q)) \;\&\; r \tag{6}$$

   Výsledek:

   $$(\neg q \;\&\; p \;\&\; r) \vee (\neg p \;\&\; q \;\&\; r) \tag{7}$$

   (b) Uveďte počet neekvivalentních nezávislých výroků teorie $\{D\}$

   Řešení: $2^{2^3-2} \cdot (2^2 - 2) = 2^7 = 128$

   Přípisek: Použijeme vzorec z druhého příkladu P.1.1.1 pro výpočet nezávislých výroků a pouze do něj dosadíme:
   $(2^{|M(D)|} - 2) \cdot 2^{2^l - |M(D)|} = (2^2 - 2) \cdot 2^{8-2} = 2 \cdot 2^6 = 2^7 = 128$

- $l = 3$ ... plyne ze zadání P.1.1.3 - 1
- $|M(D)| = 2$ ... stačí se podívat na formuli D v DNF tvaru (řešení příkladu a)) a vidíme, jak musíme ohodnotit prvovýroky, aby toto ohodnocení bylo modelem D

(c) Uveďte počet neekvivalentních výroků D' takových, že $Con(D') \subseteq Con(D)$.

Řešení: $2^{2^l-2} = 2^6$

Přípisek: Znovu podle druhého příkladu P.1.1.1.

2. Buď $\mathbb{P} = \{p, q, r\}$ množina všech prvovýroků.

(a) Ekvivalentními úpravami najděte disjunktně normální tvar následujícího výroku D:

$$\neg(p \ \& \ q) \ \& \ (p \vee q) \ \& \ r \tag{1}$$

Řešení: Zákon o distributivitě:

$$\neg(p \ \& \ q) \ \& \ ((p \ \& \ r) \vee (q \ \& \ r)) \tag{2}$$

Zákon o distributivitě (na celou formuli)

$$((\neg p \vee \neg q) \ \& \ (r \ \& \ p)) \vee ((\neg p \vee \neg q) \ \& \ (r \ \& \ q)) \tag{3}$$

Zákon o distributivitě:

$$((\neg p \ \& \ p \ \& \ \neg p) \vee (r \ \& \ \neg q \ \& \ p)) \vee ((r \ \& \ q \ \& \ \neg q) \vee (r \ \& \ q \ \& \ \neg p)) \tag{4}$$

Zákon o distributivitě:

$$\underbrace{(\neg p \ \& \ p \ \& \ \neg p)}_{\textit{můžeme škrtnout}} \vee (r \ \& \ \neg q \ \& \ p) \vee \underbrace{(r \ \& \ q \ \& \ \neg q)}_{\textit{můžeme škrtnout}} \vee (r \ \& \ q \ \& \ \neg p) \tag{5}$$

Výsledek:

$$(r \ \& \ \neg q \ \& \ p) \vee (r \ \& \ q \ \& \ \neg q) \vee (r \ \& \ q \ \& \ \neg p) \tag{6}$$

Přípisek: Mathematica má funkci LogicalExpand pro hledání DNF tvaru.

(b) Uveďte počet neekvivalentních logických důsledků výroku $\{D\}$

Řešení: $2^{2^3-2} = 2^6 = 64$

Pozn: logický důsledek = nějaký theorém $A \Leftrightarrow T \vdash A$; takže opět dle př. P.1.1.1.2

(c) Uveďte počet neekvivalentních kompletních teorií, rozšiřujících $\{D\}$

Řešení: 2

Přípisek: Teorie D má dva modely (viz řešení a)). Podle definice[5] je kompletní teorie rozšiřující jinou teorii taková, která má jediný model. Tedy výsledek je 2.

P.1.2 Sémantická kompaktnost

P.1.2.1

1. **Zadání:** Buď T maximální množina výroků taková, že každá její konečná část má model. Pak platí pro výroky A, B:

[5] Pro definici viz příklad P.1.1.1.3

(a) $A \in T, A \to B \in T \Rightarrow B \in T$

Řešení: Pro $T' \subseteq T \cup \{B\}$ konečnou existuje model. Tedy díky maximalitě T je $B \in T$

Přípisek: Věta *"Maximální množina výroků taková, že každá její konečná část má model"* by se dala také říci tak, že neexistuje teorie T' různá od T, která jednak splňuje, že každá její konečná část má model a zároveň obsahuje T (tj. neexistuje $T' \supset T$).

$$A \in T, A \to B \in T \overbrace{\Rightarrow}^{\textit{Modus ponens}} T \vdash B \Rightarrow \textit{Uvažme } T' \subseteq T \cup \{B\} \overbrace{\Rightarrow}^{\textit{maximalita } T} T' \equiv T \Rightarrow B \in T$$

(b) $A \in T \Leftrightarrow \neg A \notin T$

Řešení: Dokazujeme postupně obě implikace:

"$\Rightarrow$" Když $A \in T$, není $\neg A \in T$, neboť by $\{A, \neg A\}$ měla model.

"$\Leftarrow$" Nechť $A \notin T$ [6]. Pak existuje konečné $T' \subseteq T$ tak, že $T' \cup A$ nemá model. Pro každé $S \subseteq T$ konečné existuje model $S \cup T'$; v něm ovšem platí $\neg A$. Tudíž $T, \neg A \subseteq T$ díky maximalitě T, tudíž $\neg A \in T$.

Přípisek: Důkaz těží ze skutečnosti, že každá konečná podmnožina T má model. V důkazu je velmi podstatný moment, že existuje model pro *libovolnou* konečnou podmnožinu $S \subseteq T$.

(c) $A \to B \in T \Leftrightarrow \neg A \in T$ nebo $B \in T$

Řešení: Dokazujeme postupně obě implikace:

"$\Rightarrow$" Když $\neg A \notin T$, tak $A \in T$ dle b) a $B \in T$ dle a), tedy i $A \to B \in T$.

"$\Leftarrow$" Když $\neg A \in T$, pro nějakou $T' \subseteq T$ konečnou existuje model $v \models T' \cup \{\neg A\}$; pak $v(A \to B) = 1$ (neplatí premisa, proto implikace platí vždy), tj. $v \models T', A \to B$. Díky maximalitě T je tedy $A \to B$. Stejně je tomu, když $B \in T$.

Přípisek: "$\Rightarrow$" Technika důkazu je uvedena v poznámce 6.

(d) Buď T maximální ohodnocení $v \in^{\mathbb{P}} 2$ definováno takto: $v(p) = 1 \Leftrightarrow p \in T$. Pak $v \models T$

Návod: Indukcí podle složitosti formule A dokažte, že $\overline{v}(A) = 1 \Leftrightarrow A \in T$.

Řešení: Indukcí podle složitosti formule A plyne užitím b) a c), že $\overline{v}(A) = 1 \Leftrightarrow A \in T$.

2. Když každá konečná část teorie T má model, existuje maximální $T' \supseteq T$, taková, že každá konečná část teorie T' má model.

   Návod: Užijte princip maximality na uspořádání $< \mathbb{T}, \subseteq >$, kde $\mathbb{T}$ je množina všech teorií $S \supseteq T$ takových, že každá konečná část teorie S má model.

   Přípisek: Pro princip maximality viz: `http://cs.wikipedia.org/wiki/Princip_maximality`

P.1.3 Vlastnosti Con(T)

P.1.3.1 Buďte T, S teorie a A, B výroky v jazyce $P^{\mathbb{P}}$

Úvod:

Definice: Množinu všech formulí dokazatelných z T označíme $Con(T)$, tedy $Con(T) = \{A \mid T \vdash A\}$.

Věta: Platí následující tvrzení:

1. $T \subseteq Con(T)$
2. Je-li $T \subseteq S$ potom $Con(T) \subseteq Con(S)$

[6] Technika důkazu: $X \to Y \Leftrightarrow \neg Y \to \neg X$

3. Con(Con(T)) = Con(T)

4. Je-li T bezesporná, potom také $Con(T)$ je bezesporná.

Tato tvrzení jsou ve slidech prof. Štěpánka k dokázání jako cvičení.

Příklady:

1. (a) $Con(\underbrace{Con(T) \cup Con(S)}_{ozn.A}) = \underbrace{Con(T \cup S)}_{ozn.B}$.

   Řešení: $\underbrace{Con(T) \cup Con(S))}_{A} \underbrace{\subseteq}_{A \subseteq B} \underbrace{Con(T \cup S)}_{B} \underbrace{\subseteq}_{B \subseteq A} Con(\underbrace{Con(T) \cup Con(S)}_{A}));$
   aplikací Con() dostaneme požadované.

   (b) $Con(Con(T) \cap Con(S)) = Con(T) \cap Con(S)$.

   Řešení: Podobně jako u minulého příkladu:

   i. $Con(Con(T) \cap Con(S)) \subseteq Con(Con(T)) \subseteq Con(T)$
   ii. $Con(Con(T) \cap Con(S)) \subseteq Con(Con(S)) \subseteq Con(S)$
   iii. Z předchozích dvou plyne:

   $Con(Con(T) \cap Con(S)) \subseteq Con(T) \cap Con(S) \overbrace{\subseteq}^{\text{věta 1.}} Con(Con(T) \cap Con(S))$ a odtud dostaneme požadovanou rovnost. "První znak $\subseteq$"plyne z průniku levých a pravých stran prvních dvou formulí.

2. $Con(T, A \vee B) = Con(T, A) \cap Con(T, B)$.

   Řešení: Tvrzení plyne z *lemma o rozboru případů*, říkající: $T, A \vee B \vdash C \Leftrightarrow T, A \vdash C$ a $T, B \vdash C$.

   Pozn: $Con(T, A \vee B)$ je zkratka za $Con(T \cup \{A \vee B\})$

3. (a) $M(T) = M(Con(T))$

   Řešení: "$\Rightarrow$" $M(T) \subseteq M(Con(T)) \equiv M(\{A \mid T \vdash A\}) \overbrace{=}^{\text{věta o úplnosti}} M(\{A \mid T \models A\})$.
   Protože $T \models A$ znamená, že formule A je pravdivá při každém ohodnocení, které je modelem množiny T, máme tím dokázanou dopřednou implikaci.

   "$\Leftarrow$" Chceme dokázat: $M(T) \supseteq M(\{A \mid T \models A\})$. Pro libovolné $B \in T$ platí: $T \models B$, tedy každý model $Con(T)$ musí být zároveň modelem T.

   (b) $Con(T) \subseteq Con(S) \Leftrightarrow M(T) \supseteq M(S)$.

   Přípisek: Hospodsky: "Když mám menší množinu modelů, tak se Con může víc rozmáchnout, protože je svázaný méně podmínkami."

   (c) $Con(T)$ je maximální bezesporná $\Leftrightarrow |M(T)| = 1$

   Řešení: Dokazujeme obě implikace:

   "$\Rightarrow$" Protože je množina maximální bezesporná, tak jistě obsahuje formuli ve tvaru: $\&\{q^{v_1(q)} \mid q \in \mathbb{P}\}$, ta však má pouze jeden model.

   "$\Leftarrow$" (sporem) Nechť $|M(T)| > 1$.
   Existuje tedy nějaká dvě pravdivostní ohodnocení $v_1, v_2 \models T$, která se liší minimálně ohodnocením nějakého prvovýroku p.
   Definujme formuli D takto: $D = \&\{q^{v_1(q)} \mid q \in \mathbb{P}\}$
   Nechť $T' = T \cup \{D\}$, pak T' je bezesporná a různá od T (jelikož v_1, v_2 jsou modely T lišící se v ohodnocení p, tak formule $D \notin T$), tedy T nemůže být maximální bezesporná.

P.1.3.2 Buďte T, S teorie v jazyce $P^{\mathbb{P}}$

1. (a) $Con(T) \cup Con(S) \subseteq Con(T \cup S)$.

   Řešení: TODO

   (b) $Con(T) \cup Con(S) = Con(T \cup S) \Leftrightarrow Con(T) \cup Con(S)$ je uzavřeno na $\&$.

   Pozn: Uzavřenost na & (konjunkci) znamená, že mohu vzít libovolné dvě formule z množiny a jejich konjunkce opět bude v množině.

   Řešení: Dokazujeme obě implikace:

   "$\Rightarrow$" Nechť platí rovnost. Protože $Con(T \cup S)$ je uzavřeno na &, $Con(T) \cup Con(S)$ je uzavřeno na $\&$.

   "$\Leftarrow$" Buď $Con(T) \cup Con(S)$ uzavřeno na $\&$.
   Dokazujeme $Con(T) \cup Con(S) \supseteq Con(T \cup S)$ [7].
   Nechť $T \cup S \vdash A$, tedy musíme dokázat $T \vdash A$ nebo $S \vdash A$.

   ⚓ **Příklad:**

   Situaci, která je důležitá, demonstrujme na příkladu:
   Vezměme například $T = \{p \ \& \ q\}, S = \{s \ \& \ t\}$. Podle známého lemma[8] dostáváme, že $T \cup S \vdash p \ \& \ q \ \& \ s \ \& \ t$ - tato formule leží v $Con(T \cup S)$, ale neleží v $Con(T) \cup Con(S)$!

   Je $\bigwedge T' \ \& \ \bigwedge S' \vdash A$ (pozn. [9]) pro jisté $T' \subseteq T, S' \subseteq S$ konečné.
   Díky uzavřenosti $Con(T) \cup Con(S)$ na $\&$ máme[10] buď $T \vdash \bigwedge T' \ \& \ \bigwedge S'$; pak $T \vdash A$, nebo $S \vdash \bigwedge T' \ \& \ \bigwedge S'$; pak $S \vdash A$.

   (c) $Con(T) \cup Con(S)$ je uzavřeno na $\& \Leftrightarrow T \subseteq Con(S)$ nebo $S \subseteq Con(T)$

   Řešení: Dokazujeme obě implikace:

   "$\Rightarrow$" Nechť $Con(T) \cup Con(S)$ je uzavřeno na &. Když $T \nsubseteq Con(S)$, existuje $A \in T, S \nvdash A$. Pro $B \in S$ máme nutně $A \ \& \ B \in T$, tedy $T \vdash B$, tudíž $S \subseteq Con(T)$.

   "$\Leftarrow$" Když $T \subseteq Con(S)$, tak $Con(S) \subseteq Con(S) \cup Con(T) \subseteq Con(S)$ a $Con(S) \cup Con(T)$ je uzavřeno na &, neboť $Con(S)$ je. Díky symetrii v T, S z $S \subseteq Con(T)$ plyne uzavřenost $Con(S) \cup Con(T)$ na &.

2. (a) $Con(A) \cup Con(B) = Con(A \ \& \ B) \Leftrightarrow A \vdash B$ nebo $B \vdash A$, jsou-li A, B výroky.

   Řešení: Dokazujeme obě implikace:

   "$\Rightarrow$" Nechť platí uvažovaná rovnost. Když $A \nvdash B$, není $A \vdash A \ \& \ B$ [11], tedy je $B \vdash A \ \& \ B$ a tedy $B \vdash A$.

   "$\Leftarrow$" BÚNO: $A \vdash B$ (1)
   $A \ \& \ B \vdash C \underbrace{\Rightarrow}_{\text{věta o dedukci}} A \vdash B \to C$ (2), pomocí Modus ponens z (1) a (2) máme $A \vdash C$

   (b) $Con(p) \cup Con(q) \subseteq Con(p \ \& \ q)$ pro různé prvovýroky p, q.

   Řešení: $p \ \& \ q \notin Con(p) \cup Con(q)$

P.1.4 Axiomatizovatelnost

P.1.4.1 Vlastnosti axiomatizovatelnosti

1. (a) Buď $v \in {}^{\mathbb{P}}2$. Pak existuje teorie T v $P^{\mathbb{P}}$ tak, že $M(T) = \{v\}$

[7] druhou implikaci máme z příkladu a)
[8] $T \vdash A \ \& \ B \Leftrightarrow T \vdash A$ a $T \vdash B$
[9] Výrokovou logiku jsme si založili na dvou log. spojkách: implikaci a negaci. Ale jde to i pomocí konjunkce a negace!
[10] Jistě $T \vdash \bigwedge T'$ a $S \vdash \bigwedge S'$, podle předpokladu musí být dokazatelná i konjunkce: $Con(T) \cup Con(S) \vdash \bigwedge T' \ \& \ \bigwedge S$
[11] Jedna ze základních vlastností konjunkce, viz skripta prof. Štěpánka

Řešení: $T = \{p^{v(p)} : p \in \mathbb{P}\}$

(b) Buď $K \subseteq {}^{\mathbb{P}}2$ konečná. Pak existuje teorie T v $P^{\mathbb{P}}$ tak, že $M(T) = K$

Řešení: Buď $K = \{v_0, \ldots, v_{n-1}\}$. Pro $i < n$ existuje T_i tak, že $M(T_i) = \{v_i\}$. Pak $T = \{A_0 \vee \ldots \vee A_{n-1} : A_i \in T_i\}$ splňuje $M(T) = \{v_0, \ldots, v_{n-1}\}$.

2. Buďte T, S takové teorie, že $M(T) = {}^{\mathbb{P}}2 - M(S)$. Pak existuje $S' \subseteq S$ konečné tak, že $M(T) = M(\neg \bigwedge S'); T$ je tedy konečně axiomatizovatelná.

Návod: Dokažte sporem a užitím věty o kompaktnosti, že $M(T) = {}^{\mathbb{P}}2 - M(S')$ pro jisté $S' \subseteq S$ konečné.

Řešení: Je $M(T) = {}^{\mathbb{P}}2 - M(S) \supseteq {}^{\mathbb{P}}2 - M(S')$ pro každé konečné $S' \subseteq S$. Kdyby uvedená inkluze (tj. inkluze $S' \subseteq S$) byla vždy ostrá, bylo by vždy $M(T) \cap M(S') \neq \emptyset$, tj. $T \cup S'$ by měla pro každé $S' \subseteq S$ konečný model, tedy dle věty o kompaktnosti by měla $T \cup S$ model, tj. bylo by $\emptyset \neq M(T \cup S) = M(T) \cap M(S)$. Avšak $M(T) \cap M(S) = \emptyset$. Tudíž $M(T) = {}^{\mathbb{P}}2 - M(S')$ pro jisté $S' \subseteq S$ konečné; pak $M(T) = M(\neg \bigwedge S')$.

3. Nechť množina $\mathbb{P}$ prvovýroků je nekonečná.

(a) Buď T bezesporná teorie, která má jen konečně mnoho modelů. Pak neexistuje konečná teorie S, tak že $M(S) = M(T)$.

Návod: Zjistěte velikost množiny $M(A)$ pro výrok A.

Řešení: Pro výrok A je $M(A)$ nekonečná (kardinality $2^{|\mathbb{P}|}$).

(b) Buď $K \subseteq {}^{\mathbb{P}}2$ konečná neprázdná. Pak $K \subseteq {}^{\mathbb{P}}2 - K$ není axiomatizovatelná.

Návod: K je axiomatizovatelná, avšak není konečně axiomatizovatelná. Tedy $K \subseteq {}^{\mathbb{P}}2 - K$ není axiomatizovatelná, neboť jinak by byla K konečně axiomatizovatelná.

Řešení: K je axiomatizovatelná, avšak není konečně axiomatizovatelná. Tedy ${}^{\mathbb{P}}2 - K$ není axiomatizovatelná, neboť jinak by byla K konečně axiomatizovatelná.

P.1.4.2 Axiomatizovatelnost konkrétních

1. Nechť A je výrok a v nějaké ohodnocení. Která z následujících teorií T_i axiomatizuje $M(A) \cup \{v\}$, tj. splňuje $M(T_i) = M(A) \cup \{v\}$? (p^0 je $\neg p$, (p^1 je p)

$T_1 = \{p^{v(p)}; p \in \mathbb{P}\} \cup \{A\}$
$T_2 = \{A \vee p^{v(p)}; p \in \mathbb{P}\}$
$T_3 = \{A \ \& \ p^{v(p)}; p \in \mathbb{P}\}$
$T_4 = \{\neg(p^{v(p)}) \to A; p \in \mathbb{P}\}$

Řešení: T_2, T_4

2. Buď $p_0 \in \mathbb{P}, v : \mathbb{P} \to 2$ takové, že $v(p) = 1 \Leftrightarrow p = p_0$.

(a) Buď $\mathbb{P}$ nekonečná. Která teorie axiomatizuje množinu ${}^{\mathbb{P}}2 - \{v\}$?

Řešení: Žádná. Je totiž $\{v\}$ axiomatizovatelná; kdyby byla T axiomatizovatelná, byla by $\{v\}$ konečně axiomatizovatelná, což není.

(b) Buď $\mathbb{P} = \{p_0, \ldots, p_{n-1}$ konečná. Která teorie axiomatizuje množinu ${}^{\mathbb{P}} - \{v\}$?

Řešení: $T = \{\bigvee_{i<1} \neg p_i^{v(i)}\}$

3. Která z následujících teorií T_i axiomatizuje $M(\{A, B\}) \cup M(T)$?

$T_1 = \{(A \ \& \ B) \vee C; C \in T\}$

$T_2 = \{A \ \& \ C; C \in T\} \cup \{B \ \& \ C; C \in T\}$

$T_3 = \{(A \vee B) \ \& \ C; C \in T\}$

Řešení: T_1

Názorně: modely, ohodnocovací funkce a vzájemné vztahy

Mějme množinu prvovýroků $\mathbb{P} = \{p, q\}$, $l = 2$. Máme 4 možné ohodnocovací funkce:

- $v_1 = \{p \to 0, q \to 0\}$
- $v_2 = \{p \to 0, q \to 1\}$
- $v_3 = \{p \to 1, q \to 0\}$
- $v_4 = \{p \to 1, q \to 1\}$

V příkladu P.1.1.1.1 jsme si ukázali, že existuje 2^{2^l} (v našem případě $2^{2^2} = 16$) neekvivalentních teorií. Napišme si všechny možné podmnožiny množiny $\{v_1, v_2, v_3, v_4\}$ (tyto množiny modelů rozdělují všechny možné teorie na třídy ekvivalence):

Množiny modelů s příklady teorií	
$\{\varnothing\}$	$T_1 = \{p \& \neg p\}, T_2 = \{\neg(p \vee \neg p)\}$
$\{v_1\}$	$T = \{\neg(p \& q)\}$
$\{v_2\}$	$T = \{p \& \neg q\}$
$\{v_3\}$	$T = \{TODO\}$
$\{v_4\}$	$T = \{p \& q\}$
$\{v_1, v_2\}$	$T = \{TODO\}$
$\{v_1, v_3\}$	$T = \{TODO\}$
$\{v_1, v_4\}$	$T = \{TODO\}$
$\{v_2, v_3\}$	$T = \{TODO\}$
$\{v_2, v_4\}$	$T = \{TODO\}$
$\{v_3, v_4\}$	$T = \{TODO\}$
$\{v_1, v_2, v_3\}$	$T = \{TODO\}$
$\{v_1, v_2, v_4\}$	$T = \{p \to q\}$
$\{v_1, v_3, v_4\}$	$T = \{TODO\}$
$\{v_2, v_3, v_4\}$	$T = \{p \vee q\}$
$\{v_1, v_2, v_3, v_4\}$	$T = \{A \to (B \to A)\}$ (axiom A1)