

# Matematická logika – cvičení

Vilém Vychodil

## Abstrakt

*Následující dokument obsahuje řešené příklady a cvičení k předmětu Matematická logika. Pro zvládnutí cvičení je nutné mít zažité základní pojmy, které můžete nalézt v doporučených studijních materiálech. Některé partie, které nejsou studijními materiály dostatečně pokryty, jsou dále rozebrány v tomto textu. Komentáře zasílejte elektronickou poštou na adresu [<vilem.vychodil@upol.cz>](mailto:vilem.vychodil@upol.cz).*

Stav ke dni 17. 2. 2005.

## Obsah

Formule výrokového počtu  
Alternativní definice formulí I  
Alternativní definice formulí II  
Princip strukturální indukce  
Sémantika formulí výrokového počtu  
Adekvátní systémy spojek a funkční úplnost  
Úplné normální formy formulí  
Dokazatelnost ve VP  
Ekvivalence deduktivních systémů  
Sémantické vyplývání ve VP

Jazyk, termy a formule v predikátové logice  
Výskyty proměnných a substituovatelnost  
Slovní popis a formule  
Jazyky s rovností  
Kvantifikace

## Formule výrokového počtu

Příklady v následující sekci slouží k procvičení práce s formulemi a podformulemi. Při práci s formulemi budeme vycházet z následující indukční definice:

- (1) Každý výrokový symbol  $p$  je formule.
- (2) Nechť  $\varphi, \psi$  jsou formule. Pak  $\neg\varphi, (\varphi \Rightarrow \psi)$  jsou formule.
- (3) Všechny formule vznikají aplikací předchozích dvou bodů.

Analogicky lze definovat podformule:

- (1) Je-li  $\varphi$  formule, pak  $\varphi$  je podformule  $\varphi$ .
- (2) Je-li  $\varphi$  formule tvaru  $\neg\psi$  a  $\vartheta$  je podformule  $\psi$ , pak  $\vartheta$  je podformule  $\varphi$ .
- (3) Je-li  $\varphi$  formule tvaru  $(\psi \Rightarrow \chi)$  a  $\vartheta$  je podformule  $\psi$  nebo  $\chi$ , pak  $\vartheta$  je podformule  $\varphi$ .

### Cvičení.

1. Rozhodněte, které z následujících slov (ne)jsou formule a zdůvodněte proč.

$$\begin{array}{ccccccccc} p, & \neg p, & (\neg p), & \neg\neg p, & \neg\neg\neg p, \\ \neg(\neg\neg p), & \neg q \Rightarrow \neg p, & (\neg q \Rightarrow q), & \neg q \Rightarrow q, & \Rightarrow q, \\ (q \Rightarrow q), & (p \Rightarrow \neg), & (p \Rightarrow (p \Rightarrow \neg q)), & ((p \Rightarrow p) \Rightarrow \neg q), & \neg(q \Rightarrow \neg p). \end{array}$$

2. Z důvodů přehlednosti zápisu formulí obvykle připouštíme vynechání vnějších závorek ve formulích. V předchozím příkladu najděte slova, která jsou formulí až na absenci vnějších závorek.
- \*3. Formule VP mohou být uvažovány také v postfixovém bezzávorkovém tvaru. V tomto případě můžeme formule definovat opět induktivně: každý výrokový symbol  $p$  je formule a jsou-li  $\varphi, \psi$  formule, potom jsou i  $\varphi \neg, \varphi \psi \Rightarrow$  formule.

- (a) Následující formule vyjádřete v postfixovém tvaru.

$$(p \Rightarrow (q \Rightarrow r)), \quad ((p \Rightarrow q) \Rightarrow r), \quad (\neg p \Rightarrow \neg(q \Rightarrow r)), \quad \neg(\neg(\neg p \Rightarrow q) \Rightarrow \neg r).$$

- (b) Následující postfixové formule vyjádřete v klasickém (infixovém závorkovaném) tvaru.

$$q p \neg \Rightarrow, \quad q \neg p \Rightarrow, \quad p \neg q z \neg \Rightarrow \Rightarrow, \quad p q p q \neg \Rightarrow \neg \Rightarrow \Rightarrow.$$

Nápověda: uvědomte si, jak lze konkrétní formule sestavit užitím dvou předchozích definičních pravidel a tato pravidla aplikujte, pouze s druhým stylem zápisu formulí.

4. Zdůvodněte následující jednoduchá tvrzení.
  - (a) Každý výrokový symbol  $p$  má pouze jedinou podformuli.
  - (b) Každá podformule je formule.
  - (c) Je-li  $\psi$  podformule  $\varphi$  a  $\vartheta$  je podformule  $\psi$ , pak je  $\vartheta$  podformule  $\varphi$ .
  - (d) Je-li  $\psi$  podformule  $\varphi$ , pak má  $\psi$  nejvýš takový počet podformulí jako  $\varphi$ .
5. Dokažte následující tvrzení.

*Relace „býti podformulí“, to jest relace  $R = \{\langle \varphi, \psi \rangle; \varphi \text{ je podformule } \psi\}$  je relace uspořádání na množině všech formulí VP.*

## Alternativní definice formulí I

V některých případech je vhodné formuli definovat pomocí generující posloupnosti. Posloupnost slov  $\gamma_1, \dots, \gamma_n$  se nazývá *generující*, pokud pro každé  $1 \leq i \leq n$  platí, že  $\gamma_i$  je buďto výrokový symbol, nebo je v jednom z tvarů  $\neg\gamma_j$ ,  $(\gamma_k \Rightarrow \gamma_l)$ , kde  $j, k, l < i$ . Nyní lze definovat:

- Slovo  $\varphi$  je formule, pokud existuje generující posloupnost  $\varphi_1, \dots, \varphi_n$ , kde  $\varphi_n = \varphi$ .
- Slovo  $\psi$  je podformule  $\varphi$ , pokud se vyskytuje v každé generující posloupnosti formule  $\varphi$ .

Zavedení formulí a podformulí pomocí generující posloupnosti je praktické, pokud chceme dokazovat tvrzení o formulích pomocí matematické indukce přes délku jejich generující posloupnosti. Viz následující řešení příklad.

### Příklad.

6. Pro alternativní definici (pod)formule dokažte následující tvrzení.

*Nahradíme-li libovolnou podformuli formule jinou formulí, získáme opět formuli.*

#### Řešení.

Mějme formuli  $\varphi$  a její podformuli  $\psi$ . Pro každou generující posloupnost  $\varphi_1, \dots, \varphi_n = \varphi$ , máme  $\psi = \varphi_i$  pro některé  $1 \leq i \leq n$ . Nechť  $\vartheta$  je formule, kterou nahradíme podformuli  $\psi$ , a nechť  $\vartheta_1, \dots, \vartheta_m = \vartheta$  je její generující posloupnost.

Nyní můžeme zkonstruovat posloupnost  $\varphi'_1, \dots, \varphi'_{i-1}, \vartheta_1, \dots, \vartheta_{m-1}, \varphi'_i, \dots, \varphi'_n$ , pro jejíž členy platí následující,

$$\varphi'_j = \begin{cases} \varphi_j & \text{pro } j < i, \\ \vartheta & \text{pro } j = i, \\ \neg\varphi'_k & \text{je-li } j > i \text{ a formule } \varphi_j \text{ je tvaru } \neg\varphi_k, \\ (\varphi'_k \Rightarrow \varphi'_l) & \text{je-li } j > i \text{ a formule } \varphi_j \text{ je tvaru } (\varphi_k \Rightarrow \varphi_l). \end{cases}$$

Nyní lze jednoduše ověřit, že posloupnost  $\varphi'_1, \dots, \varphi'_{i-1}, \vartheta_1, \dots, \vartheta_{m-1}, \varphi'_i, \dots, \varphi'_n$  je generující, to jest  $\varphi'_n$  je formule vzniklá náhradením podformule  $\psi$  ve  $\varphi$  formulí  $\vartheta$ .

### Cvičení.

7. K následujícím formulím najděte generující posloupnosti.

$$(p \Rightarrow (\neg q \Rightarrow \neg(p \Rightarrow p))), \quad \neg(\neg q \Rightarrow p), \quad (\neg(p \Rightarrow p) \Rightarrow p), \quad ((p \Rightarrow \neg\neg q) \Rightarrow (q \Rightarrow \neg p)).$$

8. Pro alternativní definici (pod)formule dokažte následující tvrzení.

- (a) Každá podformule je formule.
- (b) Pro každou formuli  $\varphi$  je  $\varphi$  její podformule.
- (c) V každé podformuli  $\psi$  formule  $\varphi$  se vyskytuje nejvýš tolik logických spojek, jako ve formuli  $\varphi$ .
- (d) Nechť  $\psi$  je podformulí formule  $\varphi$ . Pak platí, že počet logických spojek obsažených v  $\psi$  je roven počtu logických spojek obsažených ve  $\varphi$ , právě když  $\varphi = \psi$ .

9. Ukažte, že alternativní definice (pod)formule jsou ekvivalentní původním definicím těchto pojmů. To jest ukažte, že ke každé formulí dle původní definice existuje generující posloupnost a naopak, že každá formule dle alternativní definice je i formulí podle výchozí definice.

## Alternativní definice formulí II

Pojem formule lze alternativně definovat pomocí stromů. Tento přístup je spíš názorný a v matematické logice je používán jen zřídka. Na druhou stranu, jsou-li formule representovány stromy, je na nich zřetelně vidět jejich struktura. Tato representace je také hojně používána při algoritmickém řešení úloh symbolické manipulace s výrazy.

Formule definujeme opět induktivně:

(1) Každý výrokový symbol  $p$  je formule (strom, který má pouze kořen).

(2) Necht' jsou  $\varphi, \psi$  formule. Pak  $\varphi \Rightarrow \psi$  a  $\neg \varphi$  jsou formule.

(3) Všechny formule vznikají aplikací předchozích dvou bodů.

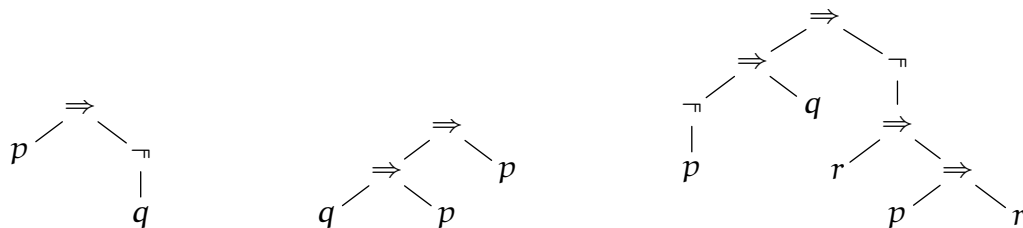
Jednoduše lze definovat pojem podformule – jsou to právě všechny podstromy dané formule.

**Příklad.**

10. Mezi formulími v klasickém smyslu a formulími definovanými pomocí stromů je opět vzájemně jednoznačná korespondence, například formule

$$(p \Rightarrow \neg q), \quad ((q \Rightarrow p) \Rightarrow p), \quad ((\neg p \Rightarrow q) \Rightarrow \neg(r \Rightarrow (p \Rightarrow r))),$$

lze vyjádřit následujícími stromy (v tomtéž pořadí):



Analogicky pro každý strom dle výše uvedené definice lze sestavit formuli v klasickém smyslu.

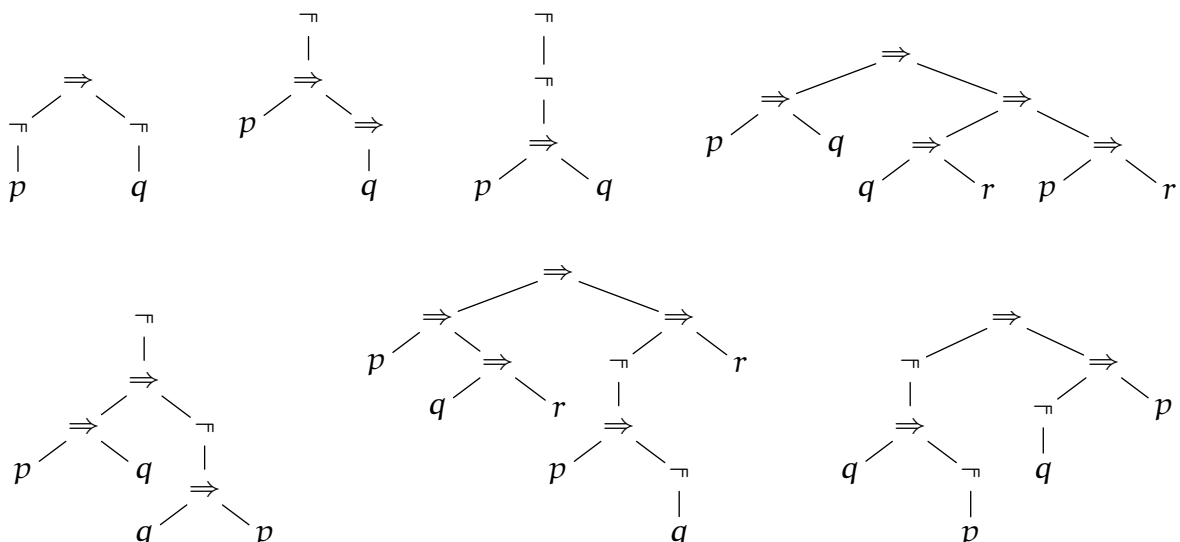
**Cvičení.**

11. Pro následující formule v klasickém smyslu najděte odpovídající stromy.

$$\begin{aligned} ((p \Rightarrow q) \Rightarrow (\neg q \Rightarrow \neg p)), & \quad (p \Rightarrow (\neg p \Rightarrow q)), & \quad (p \Rightarrow (q \Rightarrow \neg(p \Rightarrow \neg q))), \\ (p \Rightarrow \neg \neg \neg q), & \quad (\neg \neg p \Rightarrow (p \Rightarrow \neg q)), & \quad \neg \neg (\neg p \Rightarrow q). \end{aligned}$$

12. Které z následujících stromů representují formule?

Ke stromům representujícím formule najděte příslušné formule v klasickém smyslu.



## Princip strukturální indukce

Princip strukturální indukce je obecný dokazovací princip, který lze aplikovat například na formule výrokového počtu. K úplnému zavedení a prokázání principu se obvykle používá aparát universální algebry. Pro naše konkrétní účely to však zatím není nutné.

### Princip strukturální indukce pro formule VP

*K tomu, abychom prokázali, že všechny formule VP splňují vlastnost  $\mathcal{V}$ , stačí ukázat, že*

- (1) *každý výrokový symbol  $p$  splňuje vlastnost  $\mathcal{V}$ ,*
- (2) *jsou-li  $\varphi, \psi$  formule splňující vlastnost  $\mathcal{V}$ , pak i  $\neg\varphi$  a  $(\varphi \Rightarrow \psi)$  splňují vlastnost  $\mathcal{V}$ .*

### Důkaz správnosti principu.

Mějme vlastnost  $\mathcal{V}$ , pro kterou jsou splněny body (1), (2). Vezměme libovolnou formuli  $\varphi$  a některou její generující posloupnost  $\varphi_1, \dots, \varphi_n = \varphi$ . Nyní dokážeme, že každý prvek této posloupnosti splňuje vlastnost  $\mathcal{V}$ , tedy že ji splňuje i formule  $\varphi$ . Tvrzení dokážeme indukcí přes délku posloupnosti. První prvek  $\varphi_1$  musí být výrokový symbol  $p$ , pro výrokové symboly tvrzení platí dle bodu (1). Nyní předpokládejme, že tvrzení platí pro formule  $\varphi_1, \dots, \varphi_{l-1}$  – uvědomte si, že všechny prvky generující posloupnosti jsou formule. Pokud je  $\varphi_l$  opět výrokový symbol, použijeme předchozí úvahu, to jest  $\varphi_l$  splňuje  $\mathcal{V}$ . Pokud  $\varphi_l$  není výrokový symbol, pak je buďto ve tvaru  $\neg\varphi_i$  nebo ve tvaru  $(\varphi_j \Rightarrow \varphi_k)$ , kde  $i, j, k < l$ . Jelikož předpokládáme, že platí bod (2) a dle indukčního předpokladu formule  $\varphi_i, \varphi_j, \varphi_k$  splňují vlastnost  $\mathcal{V}$ , potom i formule  $\varphi_l$  splňuje vlastnost  $\mathcal{V}$ . V důsledku tedy každý člen generující posloupnosti  $\varphi_1, \dots, \varphi_n = \varphi$  splňuje  $\mathcal{V}$ . Jelikož byla úvaha vedena pro libovolnou formuli  $\varphi$ , každá formule VP splňuje vlastnost  $\mathcal{V}$ .

### Příklad.

13. Dokažte následující tvrzení.

*Všechny formule obsahují stejný počet levých i pravých závorek.*

#### Řešení.

V tomto případě uvažujeme vlastnost formulí: „Mít stejný počet levých i pravých závorek“. Výrokové symboly nemají žádné závorky, tedy tvrzení je pro ně splněno triviálně. Předpokládejme, že vlastnost platí pro formule  $\varphi$  a  $\psi$ , to jest  $\varphi$  má  $n$  levých a  $n$  pravých závorek a  $\psi$  má  $m$  levých a  $m$  pravých závorek. Pak formule  $\neg\varphi$  má stejný počet závorek jako  $\varphi$ , protože negací jsme žádnou závorku nepřidali ani neubrali. Formule  $(\varphi \Rightarrow \psi)$  má  $n + m + 1$  levých závorek a  $n + m + 1$  pravých závorek, to jest i  $(\varphi \Rightarrow \psi)$  splňuje deklarovanou vlastnost. Užitím principu strukturální indukce dostáváme požadované tvrzení.

### Poznámka.

Pomocí strukturální indukce je možné nejen dokazovat tvrzení o všech formulích, ale je rovněž možné prokazovat správnost definovaných pojmů či vlastností formulí.

### Příklad.

14. Pro libovolnou formuli  $\varphi$  můžeme definovat nezáporné celé číslo  $d(\varphi)$ , které nazveme *hloubka formule  $\varphi$*  a to tak, že položíme,

- pro každý výrokový symbol  $p$  je  $d(p) = 0$ ,
- jsou-li  $\varphi, \psi$  formule, pak  $d(\neg\varphi) = d(\varphi) + 1$  a  $d(\varphi \Rightarrow \psi) = \max(d(\varphi), d(\psi)) + 1$ .

Strukturální indukcí můžeme nyní dokázat, že pro všechny formule platí vlastnost

„Každá formule má jednoznačně definovanou svou hloubku.“

### Řešení.

Pro výrokové symboly je tvrzení zřejmé. Nechť  $\varphi, \psi$  jsou formule, které mají jednoznačně dány své hloubky  $d(\varphi), d(\psi)$ . Pak jsou zřejmě i  $d(\neg\varphi) = d(\varphi) + 1$  a  $d(\varphi \Rightarrow \psi) = \max(d(\varphi), d(\psi)) + 1$  jednoznačně dány. Tvrzení platí.

### Cvičení.

15. Pro každou formuli  $\varphi$  lze zavést množinu  $\text{At}(\varphi)$  všech výrokových symbolů vyskytujících se ve formuli  $\varphi$  následovně,
  - pro každý výrokový symbol  $p$  je  $\text{At}(p) = \{p\}$ ,
  - jsou-li  $\varphi, \psi$  formule, pak  $\text{At}(\neg\varphi) = \text{At}(\varphi)$  a  $\text{At}(\varphi \Rightarrow \psi) = \text{At}(\varphi) \cup \text{At}(\psi)$ .
 Dokažte, že množina  $\text{At}(\varphi)$  je dobře definovaná a že lze psát  $\text{At}(\varphi) = \{p; p \text{ je podformule } \varphi\}$ .
16. Analogicky jako v předchozím příkladě definujte pro každou formuli  $\varphi$  a pro každý výrokový symbol  $p$  nezáporné celé číslo  $|\varphi|_p$  jako četnost výskytu výrokového symbolu  $p$  ve formuli  $\varphi$ . Pomocí strukturální indukce dokažte, že
  - $|\varphi|_p$  je dobře definovaná,
  - je-li  $\psi$  podformule  $\varphi$ , pak je  $|\psi|_p \leq |\varphi|_p$ .
17. Pomocí strukturální indukce dokažte, že každá formule obsahuje závorky, které jsou dobře strukturované. Tím máme na mysli, že formule například nemůže obsahovat závorky ve tvaru „()“ atd. Uvědomte si, že tvrzení nelze dokázat pouze na základě kontroly stejného počtu levých a pravých závorek, protože například „)()“ nemá dobře strukturované závorky.
18. Uvažujme, že jsme pro každou formuli  $\varphi$  definovali nezáporné celé číslo  $g(\varphi)$  předpisem,
  - pro každý výrokový symbol  $p$  je  $g(p) = 1$ ,
  - jsou-li  $\varphi, \psi$  formule, pak  $g(\neg\varphi) = g(\varphi)$  a  $g(\varphi \Rightarrow \psi) = g(\varphi) + g(\psi)$ .
 Najděte a slovně popište intuitivní význam čísla  $g(\varphi)$ .

## Sémantika formulí výrokového počtu

Formule je čistě syntaktický pojem, to jest bez dodatečné informace nemá smysl uvažovat, zda-li je formule pravdivá či nikoliv. Sémantiku formulí definujeme pomocí pravdivostního ohodnocení, což je zobrazení  $e: V \rightarrow \{0, 1\}$ , kde  $V$  je množina všech výrokových symbolů. Pravdivost formule při daném ohodnocení značíme  $\|\varphi\|_e$  a definujeme ji následovně:

- (1) Je-li formule  $\varphi$  výrokovým symbolem  $p$ , pak klademe  $\|\varphi\|_e = e(p)$ .
- (2) Nechť  $\varphi, \psi$  jsou formule. Pak  $\|\neg\varphi\|_e = 1$ , právě když  $\|\varphi\|_e = 0$ ;  $\|\varphi \Rightarrow \psi\|_e = 1$ , právě když  $\|\varphi\|_e = 0$  nebo  $\|\psi\|_e = 1$ .

Pro řešení dalších příkladů je rovněž nutné znát pojmy *tautologie* (formule pravdivá v každém ohodnocení), *splnitelná formule* (formule pravdivá v některém ohodnocení), *kontradikce* (formule nepravdivá ve všech ohodnoceních) a *formule logicky ekvivalentní* (formule  $\varphi, \psi$  mají ve všech ohodnoceních stejnou pravdivost).

### Cvičení.

19. Dokažte následující tvrzení. U některých příkladů vhodně využijte strukturální indukci.
  - (a) Formule  $\varphi$  je tautologie, právě když je  $\neg\varphi$  kontradikce.
  - (b) Je-li formule  $\varphi$  tautologie a  $\psi$  vznikla nahrazením libovolného výrokového symbolu  $p \in \text{At}(\varphi)$  formulí  $\vartheta$ , pak je i  $\psi$  tautologie.
  - (c) Je-li formule  $\varphi$  tautologie a  $\vartheta$  je libovolná formule, pak je i formule  $\vartheta \Rightarrow \varphi$  tautologie.
  - (d) Nechť  $\varphi$  je tautologie a  $\psi$  je kontradikce, pak  $\psi \Rightarrow \varphi$  je tautologie a  $\varphi \Rightarrow \psi$  je kontradikce.
  - (e) Nechť  $\varphi \Rightarrow \psi$  a  $\neg\psi$  jsou tautologie. Pak  $\neg\varphi$  je rovněž tautologie.
  - (f) Formule  $\varphi, \psi$  jsou logicky ekvivalentní, právě když jsou  $\varphi \Rightarrow \psi$  a  $\psi \Rightarrow \varphi$  tautologiemi.

Tautologičnost formule VP lze rozhodnout mechanicky pomocí *tabulkové metody*. K jejímu použití nás opravňuje důkaz z následujícího řešeného příkladu.

### Příklad.

20. Dokažte tvrzení:

*Pravdivost formule  $\varphi$  při daném pravdivostním ohodnocení závisí pouze na ohodnocení výrokových symbolů vyskytujících se ve formuli  $\varphi$ .*

### Řešení.

Mějme formuli  $\varphi$ . Označme  $\text{At}(\varphi)$  množinu všech výrokových symbolů vyskytujících se ve  $\varphi$ . Pro množinu  $\text{At}(\varphi)$  platí  $\text{At}(\varphi) = \{p; p \text{ je podformule } \varphi\}$ . Nyní stačí ukázat, že pro dvě libovolná pravdivostní ohodnocení  $e, f$ , pro která je  $e(p) = f(p)$  pro libovolný  $p \in \text{At}(\varphi)$ , máme  $\|\varphi\|_e = \|\varphi\|_f$ . Tvrzení prokážeme strukturální indukcí přes složitost formule  $\varphi$ .

- Je-li  $\varphi$  výrokovým symbolem  $p$ , pak zřejmě  $p \in \text{At}(p)$  a dle indukčního předpokladu máme  $\|p\|_e = e(p) = f(p) = \|p\|_f$ .
- Je-li  $\varphi$  ve tvaru  $\neg\psi$ , pak za předpokladu, že platí  $\|\psi\|_e = \|\psi\|_f$  je z definice  $\|\varphi\|_e = 1$ , právě když  $\|\psi\|_e = 0$ , což je právě když  $\|\psi\|_f = 0$ , to jest právě když  $\|\varphi\|_f = 1$ .
- Uvažujme  $\varphi$  ve tvaru  $(\psi \Rightarrow \vartheta)$  a nechť předpoklad platí pro formule  $\psi$  a  $\vartheta$ . Pak platí  $\|\psi \Rightarrow \vartheta\|_e = 1$ , právě když  $\|\psi\|_e = 0$  nebo  $\|\vartheta\|_e = 1$ , což je dle indukčního předpokladu právě když  $\|\psi\|_f = 0$  nebo  $\|\vartheta\|_f = 1$ , to jest právě když  $\|\psi \Rightarrow \vartheta\|_f = 1$ .

Dohromady dostáváme, že  $\|\varphi\|_e = \|\varphi\|_f$ . Což bylo dokázat.

**Úvaha.**

Nyní je jasné, že k tomu, abychom vyšetřili tautologičnost libovolné formule se lze omezit pouze na zkoumání její pravdivosti v konečně mnoha ohodnoceních. Množina  $At(\varphi)$  libovolné formule  $\varphi$  je totiž konečná, množina pravdivostních hodnot taktéž (je dvouprvková). To jest existuje pouze  $2^{|At(\varphi)|}$  způsobů (variací s opakováním), jak lze symbolům z množiny  $At(\varphi)$  přiřadit pravdivostní hodnoty z množiny  $\{0, 1\}$ . Chceme-li tedy ověřit tautologičnost, stačí ověřit pouze  $2^{|At(\varphi)|}$  přiřazení pravdivostních hodnot.

**Příklad.**

21. Zjistěte, zda-li je následující formule  $\varphi$  tautologie,

$$\neg((p \Rightarrow r) \Rightarrow \neg(r \Rightarrow q)) \Rightarrow ((\neg p \Rightarrow q) \Rightarrow r).$$

**Řešení.**

$p$	$q$	$r$	$p \Rightarrow r$	$r \Rightarrow q$	$\neg(r \Rightarrow q)$	$\neg p$	$\neg p \Rightarrow q$	$\varphi_1$	$\varphi_2$	$\varphi_3$	$\varphi$
0	0	0	1	1	0	1	0	0	1	1	1
0	0	1	1	0	1	1	0	1	0	1	1
0	1	0	1	1	0	1	1	0	1	0	0
0	1	1	1	1	0	1	1	0	1	1	1
1	0	0	0	1	0	0	1	1	0	0	1
1	0	1	1	0	1	0	1	1	0	1	1
1	1	0	0	1	0	0	1	1	0	0	1
1	1	1	1	1	0	0	1	0	1	1	1

Přitom  $\varphi_1$ ,  $\varphi_2$  a  $\varphi_3$  označují tři podformule  $(p \Rightarrow r) \Rightarrow \neg(r \Rightarrow q)$ ,  $\neg((p \Rightarrow r) \Rightarrow \neg(r \Rightarrow q))$  a  $(\neg p \Rightarrow q) \Rightarrow r$ , v tomto pořadí. Formule  $\varphi$  *není tautologie*, protože v každém ohodnocení  $e$ , ve kterém je  $e(p) = 0$ ,  $e(q) = 1$  a  $e(r) = 0$  je  $\|\varphi\|_e = 0$ . Formule je ale splnitelná, to jest není kontradikce. V tomto případě měla tabulka osm řádků, pozorný čtenář si jistě všiml, že pravdivostní ohodnocení výrokových symbolů odpovídají binárním rozvojmům čísel 0 až  $7 = 2^3 - 1$ .

**Poznámka.**

V klasickém výrokovém kalkulu hilbertovského typu je obvyklé uvažovat dvě základní spojky, binární *implikaci*  $\Rightarrow$  a unární *negaci*  $\neg$ , jejich význam je čten jako „když, ..., pak, ...“ a „neplatí, že ...“. Kromě těchto dvou základních spojek zpravidla pracujeme s dalšími spojkami, jako jsou *disjunkce*  $\vee$ , *konjunkce*  $\wedge$ , *ekvivalence*  $\Leftrightarrow$  a podobně. Omezená množina spojek zeštíhluje množinu axiomových schémat, navíc výrazně zkracuje důkazy dalších tvrzení. Na druhou stranu je potřeba umět ostatní spojky vyjadřovat pomocí základních a formule tvarů  $\varphi \vee \psi$ ,  $\varphi \wedge \psi$ ,  $\varphi \Leftrightarrow \psi$  etc., chápat jako zkratky za formule složitější.

Logické spojky  $\neg$ ,  $\Rightarrow$ ,  $\vee$ ,  $\wedge$  a  $\Leftrightarrow$  jsou interpretovány logickými operacemi  $\neg$ ,  $\rightarrow$ ,  $\vee$ ,  $\wedge$  a  $\leftrightarrow$ , které jsou zapsány v následujících tabulkách (čti v pořadí řádek – sloupec).

	$\neg$	$\rightarrow$	$\vee$	$\wedge$	$\leftrightarrow$
0	1	0	0	0	0
1	0	1	1	1	1

Srovnaj definici pravdivosti formulí  $\neg p$ ,  $p \Rightarrow q$  při daném ohodnocení  $e$  s definicí logických operací  $\neg$  a  $\rightarrow$  uvedených v předcházející tabulce. Evidentně platí  $\|p \Rightarrow q\|_e = e(p) \rightarrow e(q)$  a  $\|\neg p\|_e = \neg \|p\|_e$ . Pomocí principu strukturální indukce pak lehce dostaneme

$$\begin{aligned}\|\neg \varphi\|_e &= \neg \|\varphi\|_e, \\ \|\varphi \Rightarrow \psi\|_e &= \|\varphi\|_e \rightarrow \|\psi\|_e.\end{aligned}$$



V dalším textu se budeme věnovat vlastnostem systémů spojek a logických operací. Zejména se budeme zabývat možnostmi vyjadřování odvozených spojek pomocí pevně zvolených spojek základních.

### Příklad.

22. Ukažte, že logické spojky  $\vee$ ,  $\wedge$  a  $\Leftrightarrow$  lze chápat jako zkratky za formule (v tomto pořadí),

$$(\neg p \Rightarrow q), \quad \neg(p \Rightarrow \neg q), \quad \neg((p \Rightarrow q) \Rightarrow \neg(q \Rightarrow p)).$$

### Řešení.

Ukážeme pro první formuli, zbytek nechte si čtenář provést sám. Stačí ukázat, že pro libovolné přiřazení pravdivostních hodnot  $e$  výrokovým symbolům  $p$  a  $q$  platí  $\|p \vee q\|_e = \|\neg p \Rightarrow q\|_e$ . Potom již stačí strukturální indukcí ověřit, že i  $\|\varphi \vee \psi\|_e = \|\neg\varphi \Rightarrow \psi\|_e$ . Logickou ekvivalenci obou výrazů můžeme ověřit následující tabulkou.

$p$	$q$	$\neg p$	$\neg p \Rightarrow q$	$p \vee q$
0	0	1	0	0
0	1	1	1	1
1	0	0	1	1
1	1	0	1	1

To jest  $\neg p \Rightarrow q$  odpovídá disjunkci. Analogicky lze ověřit i pro ostatní spojky.

### Cvičení.

23. Ukažte, že následující formule lze chápat jako zkratky za spojku ekvivalenci,

$$(p \Rightarrow q) \wedge (q \Rightarrow p), \quad (p \wedge q) \vee (\neg p \wedge \neg q), \quad (\neg p \vee q) \wedge (p \vee \neg q).$$

### Příklad.

24. Zjistěte, zda-li je následující formule  $\varphi$  tautologie.

$$(\neg p \Rightarrow (q \wedge \neg r)) \Leftrightarrow (\neg(q \Rightarrow r) \vee p)$$

### Řešení.

$p$	$q$	$r$	$\neg p$	$\neg r$	$q \wedge \neg r$	$\neg p \Rightarrow (q \wedge \neg r)$	$\neg(q \Rightarrow r)$	$\neg(q \Rightarrow r) \vee p$	$\varphi$
0	0	0	1	1	0	0	0	0	1
0	0	1	1	0	0	0	0	0	1
0	1	0	1	1	1	1	1	1	1
0	1	1	1	0	0	0	0	0	1
1	0	0	0	1	0	1	0	1	1
1	0	1	0	0	0	1	0	1	1
1	1	0	0	1	1	1	1	1	1
1	1	1	0	0	0	1	0	1	1

Formule  $\varphi$  je tautologie.

### Poznámka.

Každá formule  $\varphi$ , kde  $\text{At}(\varphi) = \{p_1, \dots, p_n\}$ , je z pohledu tabelace předpisem pro  $n$ -ární booleovskou funkci, to jest pro  $n$ -ární zobrazení  $f^\varphi(x_1, \dots, x_n): \{0, 1\}^n \rightarrow \{0, 1\}$ , přitom  $f^\varphi(p_1, \dots, p_n) = 1$ , právě když pro ohodnocení  $e: \{p_1, \dots, p_n\} \rightarrow \{0, 1\}$ , kde  $e(p_1) = p_1, \dots, e(p_n) = p_n$ , je  $\|\varphi\|_e = 1$ .

**Cvičení.**

25. Vyšetřete, které z následujících formulí jsou tautologie, splnitelné nebo kontradikce.

$$\begin{aligned} p \Rightarrow (\neg p \Rightarrow q), & \quad p \Rightarrow (\neg q \Rightarrow \neg(q \Rightarrow \neg p)), & p \vee (\neg q \wedge \neg r), & \quad p \Rightarrow \neg p, \\ (q \wedge \neg p) \Leftrightarrow \neg(\neg q \vee p), & \quad r \Rightarrow (\neg(p \Rightarrow p) \Rightarrow q), & \neg q \wedge ((p \Rightarrow q) \wedge p), & \quad p \Leftrightarrow \neg\neg p. \end{aligned}$$

26. Určete pravdivost následujících formulí ve všech ohodnoceních  $e: V \rightarrow \{0, 1\}$ , ve kterých je formule  $p \Rightarrow \neg q$  pravdivá.

$$p \Rightarrow (\neg q \Rightarrow (q \wedge p)), \quad (p \vee q) \Rightarrow (\neg q \Rightarrow \neg p), \quad \neg(p \Rightarrow q) \vee \neg p.$$

27. Dokažte následující tvrzení.

*Relace  $E = \{\langle \varphi, \psi \rangle; \varphi \text{ je logicky ekvivalentní } \psi\}$  na množině všech formulí  $VP$  je relace ekvivalence.*

28. Necht'  $\varphi \vee \vartheta$ ,  $\psi \vee \neg\vartheta$  jsou splnitelné formule. Dokažte, že pak je  $\varphi \vee \psi$  splnitelná.

\*29. Dokažte, že formule obsahující pouze spojky  $\vee$  a  $\wedge$  nemůže být ani tautologie, ani kontradikce.

\*30. Dokažte, že formule  $\varphi$ , ve které se vyskytuje pouze spojka  $\Leftrightarrow$  je tautologie, právě když má každý  $p \in \text{At}(\varphi)$  ve formuli  $\varphi$  sudý počet výskytů.

## Adekvátní systémy spojek a funkční úplnost

Některé systémy logických spojek jsou významné z toho pohledu, že je pomocí nich možné vyjádřit libovolnou další spojku – říkáme jim *adekvátní systémy spojek*. Na úrovni sémantiky spojek to znamená, že libovolnou logickou operaci lze zkonstruovat pouze ze základních logických operací – této vlastnosti se říká *funkční úplnost*. Mezi adekvátní systémy logických spojek patří například systémy  $\{\Rightarrow, \neg\}$ ,  $\{\Rightarrow, \emptyset\}$  ( $\emptyset$  je nulární spojka, která je interpretována pravdivostní hodnotou 0),  $\{\wedge, \neg\}$ ,  $\{\vee, \Leftrightarrow, \emptyset\}$ ,  $\{\wedge, \vee, \Rightarrow, \Leftrightarrow, \neg\}$  atd. Čím větší je systém základních spojek, tím jednodušší je vyjadřování ostatních spojek, naopak, pokud je systém spojek malý, vyjadřování ostatních formulí může být komplikované a formule jsou obvykle dlouhé.

Speciální význam mají Pierceova spojka  $\Downarrow$  a Shefferova spojka  $\Uparrow$ , které samy o sobě tvoří adekvátní systém spojek. Obě dvě spojky jsou interpretovány následujícími logickými operacemi,

$\Downarrow$	0	1	$\Uparrow$	0	1
0	1	0	0	1	1
1	0	0	1	1	0

V následující tabulce je uveden souhrn všech binárních logických operací, které jsou vyjádřeny pomocí čtyř různých systémů spojek, v prvním sloupci se jedná o systém  $\{\wedge, \vee, \Rightarrow, \Leftrightarrow, \neg\}$ , v druhém sloupci  $\{\Rightarrow, \neg\}$ , dále  $\{\emptyset, \vee, \Leftrightarrow\}$  a  $\{\Uparrow\}$ .

	$\Rightarrow, \neg$	$\emptyset, \vee, \Leftrightarrow$	$\Uparrow$
$\neg(p \Rightarrow p)$	$\neg(p \Rightarrow p)$	$\emptyset$	$(p \Uparrow (p \Uparrow p)) \Uparrow (p \Uparrow (p \Uparrow p))$
$p \wedge q$	$\neg(p \Rightarrow \neg q)$	$(p \Leftrightarrow q) \Leftrightarrow (p \vee q)$	$(p \Uparrow q) \Uparrow (p \Uparrow q)$
$\neg(p \Rightarrow q)$	$\neg(p \Rightarrow q)$	$q \Leftrightarrow (\emptyset \Leftrightarrow (p \vee q))$	$(p \Uparrow (p \Uparrow p)) \Uparrow (p \Uparrow (p \Uparrow q))$
$p$	$p$	$p$	$p$
$\neg(q \Rightarrow p)$	$\neg(q \Rightarrow p)$	$p \Leftrightarrow (\emptyset \Leftrightarrow (p \vee q))$	$(p \Uparrow (p \Uparrow p)) \Uparrow (q \Uparrow (p \Uparrow p))$
$q$	$q$	$q$	$q$
$\neg(p \Leftrightarrow q)$	$(p \Rightarrow q) \Rightarrow \neg(q \Rightarrow p)$	$\emptyset \Leftrightarrow (p \Leftrightarrow q)$	$(p \Uparrow (p \Uparrow q)) \Uparrow (q \Uparrow (p \Uparrow p))$
$p \vee q$	$\neg p \Rightarrow q$	$p \vee q$	$(p \Uparrow p) \Uparrow (q \Uparrow q)$
$\neg(p \vee q)$	$\neg(\neg p \Rightarrow q)$	$\emptyset \Leftrightarrow (p \vee q)$	$(p \Uparrow (p \Uparrow p)) \Uparrow ((p \Uparrow p) \Uparrow (q \Uparrow q))$
$p \Leftrightarrow q$	$\neg((p \Rightarrow q) \Rightarrow \neg(q \Rightarrow p))$	$p \Leftrightarrow q$	$(p \Uparrow q) \Uparrow ((p \Uparrow p) \Uparrow (q \Uparrow q))$
$\neg q$	$\neg q$	$q \Leftrightarrow \emptyset$	$q \Uparrow q$
$q \Rightarrow p$	$q \Rightarrow p$	$p \Leftrightarrow (p \vee q)$	$q \Uparrow (p \Uparrow p)$
$\neg p$	$\neg p$	$p \Leftrightarrow \emptyset$	$p \Uparrow p$
$p \Rightarrow q$	$p \Rightarrow q$	$q \Leftrightarrow (p \vee q)$	$p \Uparrow (p \Uparrow q)$
$\neg(p \wedge q)$	$p \Rightarrow \neg q$	$\emptyset \Leftrightarrow ((p \Leftrightarrow q) \Leftrightarrow (p \vee q))$	$p \Uparrow q$
$p \Rightarrow p$	$p \Rightarrow p$	$\emptyset \Leftrightarrow \emptyset$	$p \Uparrow (p \Uparrow p)$

### Cvičení.

31. Pouze pomocí základních spojek  $\Rightarrow, \neg$  najděte vyjádření pro logické spojky, jejichž sémantiku definují následující čtyři tabulky.

	0	1		0	1		0	1		0	1
0	0	1	0	0	1	0	0	0	0	1	0
1	0	1	1	1	0	1	1	0	1	1	1

32. Určete kolik je navzájem různých  $n$ -árních logických operací.

Vypište si všechny unární logické operace a zkuste si pro ně vymyslet přirozené názvy.

33. Logickou nonekvivalenci (vylučovací nebo)  $*$  lze chápat jako zkratku za formuli  $\neg(p \Leftrightarrow q)$ .  
Ověřte, že formule  $(p * q) * q$  je ekvivalentní  $p$  a formule  $(p * q) * p$  je ekvivalentní  $q$ . Pokuste se zdůvodnit, jaký mohou mít tyto dvě ekvivalence praktický význam.

34. Uvažujme jako základní spojky implikaci  $\Rightarrow$  a nonekvivalenci  $*$ .  
Určete, které spojky jsou určeny následujícími formulami.

$$\begin{array}{llll} p * (p \Rightarrow q), & q * (p \Rightarrow p), & (p \Rightarrow p) * (p \Rightarrow q), & p * ((p \Rightarrow p) * (p \Rightarrow q)) \\ p \Rightarrow (p * p), & q \Rightarrow ((p * p) \Rightarrow p), & (p * q) \Rightarrow (q * p), & (p * q) \Rightarrow q. \end{array}$$

\*35. Jako základní spojky uvažujte  $\wedge$ ,  $\Leftrightarrow$ ,  $\mathbb{O}$ .

Pokuste se pomocí nich vyjádřit všechny ostatní binární a unární spojky.

## Úplné normální formy formulí

V předchozí sekci jsme ke každé formuli  $\varphi$  sestrojovali tabulku, kterou jsme vyšetřovali pravdivost formule v závislosti na ohodnocení výrokových symbolů. Nabízí se přirozená otázka, zda-li není možné provést opačný proces. To jest k libovolné tabulce reprezentující  $n$ -ární booleovskou funkci najít formuli  $\varphi$  tak, že její tabelací získáme výchozí tabulku pravdivostních hodnot.

Vzhledem k funkční úplnosti logických operací interpretujících spojky  $\neg, \Rightarrow$  je to možné a lze jednoduše popsat algoritmus, kterým lze k zadané tabulce najít příslušnou formuli. Formule je navíc ve speciálním tvaru – v *konjunktivní* nebo *disjunktivní normální formě*, zkráceně KNF a DNF.

### Definice.

Každý výrokový symbol  $p$  a jeho negaci  $\neg p$  nazveme *literál*. Formuli ve tvaru  $(l_1 \vee \dots \vee l_k)$ , kde  $l_i$  je literál pro každé  $1 \leq i \leq k$  nazveme *elementární disjunkce literálů*, neboli *klausule*. Formuli ve tvaru  $(l_1 \wedge \dots \wedge l_k)$  kde  $l_i$  je literál pro každé  $1 \leq i \leq k$  nazveme *elementární konjunkce literálů*.

Formule  $\varphi$  je v

- *disjunktivní normální formě*, pokud je ve tvaru  $\vartheta_1 \vee \dots \vee \vartheta_n$ , kde  $\vartheta_1, \dots, \vartheta_n$  jsou elementární konjunkce literálů,
- *konjunktivní normální formě*, pokud je ve tvaru  $\vartheta_1 \wedge \dots \wedge \vartheta_n$ , kde  $\vartheta_1, \dots, \vartheta_n$  jsou klausule.

### Poznámka.

Jednotlivé normální formy, ani elementární disjunkce a konjunkce jsme nezávorkovali ani jsme neuváděli pořadí jednotlivých formulí, můžeme si to dovolit vzhledem k dokazatelnosti asociativity a komutativity spojek  $\vee$  a  $\wedge$ . Viz učební materiály.

### Algoritmus (Nalezení DNF).

VSTUP: booleovská funkce  $s: \{0, 1\}^n \rightarrow \{0, 1\}$ , kde  $s(p_1, \dots, p_n) = 1$  pro některá  $p_1, \dots, p_n \in \{0, 1\}$ ,

VÝSTUP: formule  $\varphi$  v DNF

Předpokládejme, že máme dáno  $n$ -ární zobrazení  $s: \{0, 1\}^n \rightarrow \{0, 1\}$ . Nyní můžeme pro každou  $n$ -tici  $\langle p_1, \dots, p_n \rangle \in \{0, 1\}^n$ , uvažovat elementární konjunkci  $p_1^\circ \wedge \dots \wedge p_n^\circ$ , kde  $p_i^\circ$  je buďto literál  $p_i$ , pokud je  $p_i = 1$ , nebo literál  $\neg p_i$  v opačném případě. Sestrojíme formuli  $\varphi = \vartheta_1 \vee \dots \vee \vartheta_k$ , kde  $\vartheta_i$  jsou právě všechny formule ve tvaru  $p_1^\circ \wedge \dots \wedge p_n^\circ$ , pro které je  $s(p_1, \dots, p_n) = 1$ . Výsledná formule  $\varphi$  je v DNF.

### Algoritmus (Nalezení KNF).

VSTUP: booleovská funkce  $s: \{0, 1\}^n \rightarrow \{0, 1\}$  kde  $s(p_1, \dots, p_n) = 0$  pro některá  $p_1, \dots, p_n \in \{0, 1\}$ ,

VÝSTUP: formule  $\varphi$  v KNF

Předpokládejme, že máme dáno  $n$ -ární zobrazení  $s: \{0, 1\}^n \rightarrow \{0, 1\}$ . Nyní můžeme pro každou  $n$ -tici  $\langle p_1, \dots, p_n \rangle \in \{0, 1\}^n$ , uvažovat klausuli  $p_1^\bullet \vee \dots \vee p_n^\bullet$ , kde  $p_i^\bullet$  je buďto literál  $p_i$ , pokud je  $p_i = 0$ , nebo literál  $\neg p_i$  v opačném případě. Sestrojíme formuli  $\varphi = \vartheta_1 \wedge \dots \wedge \vartheta_k$ , kde  $\vartheta_i$  jsou právě všechny klausule  $p_1^\bullet \vee \dots \vee p_n^\bullet$ , pro které je  $s(p_1, \dots, p_n) = 0$ . Výsledná formule  $\varphi$  je v KNF.

### Úvaha.

Uvažujme booleovskou funkci  $s: \{0, 1\}^n \rightarrow \{0, 1\}$ , kde  $s(p_1, \dots, p_n) = 0$  pro libovolné hodnoty  $p_i$ . Dle předchozího algoritmu nalezení DNF neexistuje ani jedna elementární konjunkce  $p_1^\circ \wedge \dots \wedge p_n^\circ$ , kde  $s(p_1, \dots, p_n) = 1$ , to jest příslušnou formuli  $\varphi$  v DNF nelze tímto algoritmem sestavit, stejně tak pro booleovskou funkci  $t: \{0, 1\}^n \rightarrow \{0, 1\}$ , kde  $t(p_1, \dots, p_n) = 1$  nelze sestavit KNF. Na druhou stranu ale existují formule, které jsou předpisem těchto booleovských funkcí a jsou v DNF a KNF. Uvažujme formule  $p \wedge \neg p$ ,  $p \vee \neg p$ , pak zřejmě máme  $s = f^{p \wedge \neg p}$ ,  $t = f^{p \vee \neg p}$ .

**Poznámka.**

Za pozornost rovněž stojí, že formule vytvořené předcházejícími algoritmy obsahují v každé elementární konjunkci či v každé klausuli libovolný výrokový symbol z množiny  $\{p_1, \dots, p_n\}$  jako literál *právě jednou*. Takovým formulím říkáme, že jsou v *úplné* DNF, případně *úplné* KNF. Na druhou stranu  $p \wedge \neg p$  a  $p \vee \neg p$  obsahují jeden výrokový symbol jako literál dvakrát.

**Příklady.**

36. K následující tabulkou zadané booleovské funkci  $s: \{0, 1\}^3 \rightarrow \{0, 1\}$  nalezněte DNF a KNF. Tabulka je z úsporných důvodů rozdělena na dvě části.

$p$	$q$	$r$	$s(p, q, r)$	$p$	$q$	$r$	$s(p, q, r)$
0	0	0	1	1	0	0	0
0	0	1	0	1	0	1	1
0	1	0	1	1	1	0	0
0	1	1	1	1	1	1	1

**Řešení.**

Máme  $s(0, 0, 0) = s(0, 1, 0) = s(0, 1, 1) = s(1, 0, 1) = s(1, 1, 1) = 1$ , to jest úplná DNF má tvar

$$(\neg p \wedge \neg q \wedge \neg r) \vee (\neg p \wedge q \wedge \neg r) \vee (\neg p \wedge q \wedge r) \vee (p \wedge \neg q \wedge r) \vee (p \wedge q \wedge r),$$

dále máme  $s(0, 0, 1) = s(1, 0, 0) = s(1, 1, 0) = 0$ , to jest úplná KNF má tvar

$$(p \vee q \vee \neg r) \wedge (\neg p \vee q \vee r) \wedge (\neg p \vee \neg q \vee r).$$

Intuitivně lze říct, že DNF byla zkonstruována podle těch ohodnocení, ve kterých byla výchozí booleovská funkce pravdivá. Naopak KNF je sestavena tak, aby vyloučila platnost v ohodnoceních, ve kterých nebyla původní booleovská funkce pravdivá. Čtenář se může tabulkovou metodou přesvědčit, že obě zkonstruované formy jsou skutečně předpisem výchozí funkce  $s$ .

37. Dokažte správnost algoritmu stanovení DNF.

**Řešení.**

Mějme danou booleovskou funkci  $s: \{0, 1\}^n \rightarrow \{0, 1\}$ . V případě, že je  $s(p_1, \dots, p_n) = 0$  pro libovolné hodnoty  $p_i$ , pak snadno nahlédneme, že  $f^{p \wedge \neg p}(p, p_1, \dots, p_{n-1}) = s(p, p_1, \dots, p_{n-1}) = 0$ . V opačném případě předpokládejme, že  $\varphi$  je DNF zkonstruovaná dle  $s$  výše uvedeným algoritmem. Dokážeme, že  $f^\varphi(p_1, \dots, p_n) = s(p_1, \dots, p_n)$  pro libovolné  $p_1, \dots, p_n \in \{0, 1\}$ . Jednoduchým ale důležitým pozorováním lehce dojdeme k tomu, že  $f^\varphi(p_1, \dots, p_n) = 1$  právě když je  $p_1^o \wedge \dots \wedge p_n^o$  elementární konjunkce obsažená ve  $\varphi$  (nebo některá elementární konjunkce s ní ekvivalentní – opět aplikujeme asociativitu a komutativitu), ale to je právě když je  $s(p_1, \dots, p_n) = 1$ . Což bylo dokázat.

38. K libovolné formuli  $\varphi$  existují formule  $\vartheta, \chi$  takové, že  $\vartheta$  je v DNF a  $\varphi$  a  $\vartheta$  jsou logicky ekvivalentní a  $\chi$  je v KNF a  $\varphi$  a  $\chi$  jsou logicky ekvivalentní.

**Řešení.**

Uvažujme výchozí formuli  $\varphi$  a příslušnou booleovskou funkci  $f^\varphi$ . Nechť  $\vartheta$  je DNF booleovské funkce  $f^\varphi$ . Pak jsou zřejmě  $\vartheta$  i  $\varphi$  logicky ekvivalentní. Důkaz pro KNF je analogický.

Poslední tvrzení nás opravňuje mluvit o *normální disjunktivní a normální konjunktivní formě* dané formule  $\varphi$ , která je dle předchozího s výchozí formulí logicky ekvivalentní. Do DNF či KNF lze formuli  $\varphi$  převést tak, že ji nejprve tabelujeme a poté aplikujeme předchozí dva algoritmy.

**Cvičení.**

39. Dokažte správnost algoritmu stanovení KNF.

40. K následujícím formulím nalezněte jejich DNF a KNF.

$$\begin{array}{lll} p \Rightarrow \neg(\neg r \Rightarrow (p \Rightarrow q)), & \neg p \wedge (q \Rightarrow \neg p), & p \Rightarrow (q \Rightarrow (\neg r \wedge q)), \\ (p \Rightarrow q) \vee \neg(\neg p \Rightarrow (p \Rightarrow \neg r)), & \neg(r \wedge (p \Rightarrow q)), & (p \vee \neg q) \wedge (p \vee \neg r). \end{array}$$

## Dokazatelnost ve VP

Dokazatelnost (syntaktické vyplývání) formalizuje intuitivní pojetí důkazu. Při úvahách o dokazatelnosti formulí z nějakého systému formulí nebo při práci s konkrétními důkazy, což pro nás budou speciální posloupnosti formulí, se však *nikterak neopíráme o pojem pravdivost*.

Klasický výrokový kalkul Hilbertova typu má tři axiomová schémata,

$$\text{H1)} \quad \varphi \Rightarrow (\psi \Rightarrow \varphi),$$

$$\text{H2)} \quad (\varphi \Rightarrow (\psi \Rightarrow \vartheta)) \Rightarrow ((\varphi \Rightarrow \psi) \Rightarrow (\varphi \Rightarrow \vartheta)),$$

$$\text{H3)} \quad (\neg\psi \Rightarrow \neg\varphi) \Rightarrow (\varphi \Rightarrow \psi).$$

Podotkněme že se skutečně jedná o schémata. Axiom je každá formule, která je ve tvaru H1–H3. Například tedy  $p \Rightarrow ((\neg\neg p \Rightarrow r) \Rightarrow p)$  a  $(\neg r \Rightarrow \neg\neg p) \Rightarrow (\neg p \Rightarrow r)$  jsou axiomy, ale například  $p \Rightarrow \neg q$  a  $p \Rightarrow (q \Rightarrow r)$  nikoliv. Axiomů je evidentně nekonečně mnoho. Dále používáme odvozovací pravidlo *modus ponens*, pomocí nějž z formulí  $\varphi$  a  $\varphi \Rightarrow \psi$  odvodíme formuli  $\psi$ . Schématicky

$$\text{MP: } \frac{\varphi, \varphi \Rightarrow \psi}{\psi}.$$

Posloupnost  $\delta_1, \dots, \delta_n$  se nazývá *důkaz ze systému formulí  $\mathcal{T}$* , pokud je každá  $\delta_i$  instancí některého axiomového schématu H1–H3, nebo je  $\delta_i \in \mathcal{T}$ , nebo  $\delta_i$  vznikla použitím modus ponens z formulí  $\delta_j$  a  $\delta_k$ , kde  $\delta_k$  je ve tvaru  $\delta_j \Rightarrow \delta_i$  a platí  $j, k < i$ . Formule  $\varphi$  je *dokazatelná z  $\mathcal{T}$*  (symbolicky  $\mathcal{T} \vdash \varphi$ ), pokud existuje důkaz  $\delta_1, \dots, \delta_n = \varphi$  z  $\mathcal{T}$ . Pokud  $\mathcal{T} = \emptyset$ , pak píšeme zkráceně  $\vdash \varphi$  místo  $\emptyset \vdash \varphi$ . Zápis  $\mathcal{T}, \varphi \vdash \psi$  chápeme jako zkratku za  $\mathcal{T} \cup \{\varphi\} \vdash \psi$ .

Dále budeme využívat následujících faktů:

$$\vdash \varphi \Rightarrow \varphi,$$

$$\vdash \neg\varphi \Rightarrow (\varphi \Rightarrow \psi) \quad \text{tzv. zákon Dunse Scotta, aneb „z nemožného plyne cokoliv“,}$$

$$\vdash \neg\neg\varphi \Rightarrow \varphi,$$

$$\vdash \varphi \Rightarrow \neg\neg\varphi \quad \text{s předchozím vztahem vyjadřuje zákon dvojí negace,}$$

$$\vdash (\varphi \Rightarrow \psi) \Rightarrow (\neg\psi \Rightarrow \neg\varphi) \quad \text{duální forma schématu H3,}$$

$$\vdash \varphi \Rightarrow (\neg\psi \Rightarrow \neg(\varphi \Rightarrow \psi)) \quad \text{z platnosti } \varphi \text{ a } \neg\psi \text{ plyne } \varphi \wedge \psi.$$

Rovněž budeme používat známé dokazovací principy, jako je *věta o dedukci*, *důkaz sporem*, *důkaz rozбором případů*, *věta o neutrální formuli*, *věta o nahrazení*, *věta o ekvivalenci* a další. Viz další učební materiály.

Uveďme si příklady jednoduchých, ale často používaných dokazovacích principů.

### Příklady.

41. Dokažte že pokud  $\mathcal{T} \vdash \varphi$  a pro každou  $\psi \in \mathcal{T}$  máme  $\mathcal{S} \vdash \psi$ , pak také  $\mathcal{S} \vdash \varphi$ .

#### Řešení.

Předpokládejme že platí  $\mathcal{T} \vdash \varphi$ . To jest existuje důkaz  $\delta_1, \dots, \delta_n = \varphi$  z  $\mathcal{T}$ . Uvažujme posloupnost  $\gamma_1, \dots, \gamma_m$ , kterou vytvoříme z posloupnosti  $\delta_1, \dots, \delta_n$  tak, že každý člen  $\delta_i \in \mathcal{T}$  nahradíme některým jeho důkazem ze systému  $\mathcal{S}$  (důkaz vždy existuje jelikož  $\mathcal{S} \vdash \delta_i$ ). Posloupnost  $\gamma_1, \dots, \gamma_m$  je evidentně důkazem ze  $\mathcal{S}$  a  $\gamma_m = \varphi$ . Dostáváme tedy  $\mathcal{S} \vdash \varphi$ . Důkaz  $\gamma_1, \dots, \gamma_m$  zkonstruovaný výše uvedeným postupem není nikdy kratší než výchozí důkaz  $\delta_1, \dots, \delta_n$ .

42. Dokažte platnost dvou často používaných dokazovacích principů.

(a) *důkaz obměnou*:  $\mathcal{T} \vdash \varphi \Rightarrow \psi$ , právě když  $\mathcal{T} \vdash \neg\psi \Rightarrow \neg\varphi$ ,



- (b) *důkaz ekvivalence tvrzení*: Platí  $\mathcal{T} \vdash \varphi_i \Rightarrow \varphi_j$  pro každé  $i, j \in \{1, \dots, n\}$ , právě když  $\mathcal{T} \vdash \varphi_i \Rightarrow \varphi_{i+1}$  pro všechna  $i = 1, \dots, n-1$  a  $\mathcal{T} \vdash \varphi_n \Rightarrow \varphi_1$ .

**Řešení.**

Tvrzení (a) plyne z axiomu H3 a principu modus ponens a z faktu, že  $(\varphi \Rightarrow \psi) \Rightarrow (\neg\psi \Rightarrow \neg\varphi)$  je dokazatelná z prázdného systému formulí.

Všimněte si že (b) formalizuje klasický princip, kterým se na intuitivní úrovni dokazuje *ekvivalence několika tvrzení*—formuli  $\varphi \Leftrightarrow \psi$  přitom chápeme jako zkratku za  $(\varphi \Rightarrow \psi) \wedge (\psi \Rightarrow \varphi)$ . Dále je dobré uvědomit si, že „ $\Rightarrow$ “ tvrzení (b) platí triviálně. Ukážeme tedy obrácenou implikaci. Předpokládejme že platí  $\mathcal{T} \vdash \varphi_i \Rightarrow \varphi_{i+1}$  pro všechna  $i = 1, \dots, n-1$  a  $\mathcal{T} \vdash \varphi_n \Rightarrow \varphi_1$ . Vezměme libovolná  $i, j \in \{1, \dots, n\}$ . Rozlišíme tři případy:

- (i) Pokud je  $i = j$ , tvrzení plyne přímo ze známého faktu  $\vdash \varphi \Rightarrow \varphi$ .
- (ii) Je-li  $i < j$ , pak  $\mathcal{T} \vdash \varphi_i \Rightarrow \varphi_j$  dostaneme násobným použitím *transitivity implikace* (z platnosti  $\mathcal{T} \vdash \varphi \Rightarrow \psi$  a  $\mathcal{T} \vdash \psi \Rightarrow \vartheta$  plyne  $\mathcal{T} \vdash \varphi \Rightarrow \vartheta$ ), což je důsledek věty o dedukci.
- (iii) Pokud  $i > j$ , pak aplikací transitivity implikace dostáváme  $\mathcal{T} \vdash \varphi_i \Rightarrow \varphi_n$  ( $i \leq n$ ) a z předpokladu  $\mathcal{T} \vdash \varphi_n \Rightarrow \varphi_1$  a transitivity implikace máme  $\mathcal{T} \vdash \varphi_i \Rightarrow \varphi_1$ . Jelikož  $\mathcal{T} \vdash \varphi_1 \Rightarrow \varphi_j$  platí podle bodu (i) nebo (ii), užitím transitivity implikace na  $\mathcal{T} \vdash \varphi_i \Rightarrow \varphi_1$  a  $\mathcal{T} \vdash \varphi_1 \Rightarrow \varphi_j$  dostáváme  $\mathcal{T} \vdash \varphi_i \Rightarrow \varphi_j$ .

Tím je důkaz hotov.

**Cvičení.**

43. Dokažte následující tvrzení.

- (a)  $\mathcal{T}$  je sporný systém, právě když  $\mathcal{T} \vdash \varphi$  a zároveň  $\mathcal{T} \vdash \neg\varphi$ ,
- (b)  $\mathcal{T}$  je bezsporný systém, právě když  $\neg(\vartheta \Rightarrow \vartheta)$  není dokazatelná z  $\mathcal{T}$ .
- (c) Položme  $\mathcal{T} \trianglelefteq \mathcal{S}$ , právě když platí, že z  $\mathcal{T} \vdash \varphi$  plyne  $\mathcal{S} \vdash \varphi$ . Dokažte, že  $\trianglelefteq$  je transitivní.
- (d) Pokud  $\mathcal{T} \vdash \varphi$ , pak existuje nekonečně mnoho vzájemně různých důkazů  $\varphi$  z  $\mathcal{T}$ .
- (e) Pokud  $\mathcal{T} \vdash \varphi \Rightarrow \psi$  a  $\mathcal{S} \vdash \psi \Rightarrow \vartheta$ , pak  $\mathcal{T} \cup \mathcal{S} \vdash \varphi \Rightarrow \vartheta$ .
- (f)  $\mathcal{T} \vdash \varphi \Rightarrow (\psi \Rightarrow \vartheta)$ , právě když  $\mathcal{T} \vdash \psi \Rightarrow (\varphi \Rightarrow \vartheta)$ .
- (g) Pokud  $\mathcal{T} \vdash \varphi$ , pak existuje konečná  $\mathcal{T}' \subseteq \mathcal{T}$  tak, že  $\mathcal{T}' \vdash \varphi$ .
- (h) Pokud  $\mathcal{T} \vdash \varphi$ , pak  $\mathcal{S} \vdash \varphi$  pro každou  $\mathcal{S}$ , kde  $\mathcal{T} \subseteq \mathcal{S}$ .
- (i)  $\mathcal{T}$  je bezsporný, právě když je každý konečný  $\mathcal{T}' \subseteq \mathcal{T}$  bezsporný.

44. Pro každý systém formulí  $\mathcal{T}$  definujme systém formulí  $\mathcal{T}^+ = \{\varphi; \mathcal{T} \vdash \varphi\}$ .

Dokažte následující tvrzení.

- (a)  $\mathcal{T}^+ = (\mathcal{T}^+)^+$ ,
- (b) Je-li  $\mathcal{T}$  bezsporný, pak je  $\mathcal{T}^+$  bezsporný systém obsahující  $\mathcal{T}$ .
- (c) Mějme bezsporný systém  $\mathcal{T}$ , kde pro každou formuli  $\varphi$  máme buď  $\varphi \in \mathcal{T}$ , nebo  $\neg\varphi \in \mathcal{T}$ . Pak platí, že  $\mathcal{T} = \mathcal{T}^+$  a  $\mathcal{T}$  je maximální bezsporný systém.

**Příklady.**

45. Bez použití věty o úplnosti VP dokažte následující tvrzení.

- (a)  $\varphi \wedge \psi \vdash \varphi$ ,
- (b)  $\varphi \wedge \psi \vdash \psi$ ,
- (c)  $\vdash (\varphi \wedge \psi) \Rightarrow \vartheta$ , právě když  $\vdash \varphi \Rightarrow (\psi \Rightarrow \vartheta)$ ,

(d)  $\mathcal{T} \vdash \varphi$  a zároveň  $\mathcal{T} \vdash \psi$ , právě když  $\mathcal{T} \vdash \varphi \wedge \psi$ .

(e)  $\mathcal{T} \vdash \varphi \Rightarrow \psi$  a zároveň  $\mathcal{T} \vdash \psi \Rightarrow \varphi$ , právě když  $\mathcal{T} \vdash \varphi \Leftrightarrow \psi$ .

### Řešení.

(a) Připomeňme, že  $\varphi \wedge \psi$  chápeme jako zkratku za formuli  $\neg(\varphi \Rightarrow \neg\psi)$ . Platí

$\vdash \neg\varphi \Rightarrow (\varphi \Rightarrow \neg\psi)$	<i>zákon Dunse Scotta,</i>
$\vdash (\neg\varphi \Rightarrow (\varphi \Rightarrow \neg\psi)) \Rightarrow (\neg(\varphi \Rightarrow \neg\psi) \Rightarrow \neg\neg\varphi)$	<i>duální forma H3,</i>
$\vdash \neg(\varphi \Rightarrow \neg\psi) \Rightarrow \neg\neg\varphi$	<i>modus ponens,</i>
$\vdash \neg(\varphi \Rightarrow \neg\psi) \Rightarrow \varphi$	<i>věta o ekvivalenci,</i>
$\vdash (\varphi \wedge \psi) \Rightarrow \varphi$	<i>zkratka za formuli.</i>

Tvrzení (b) se dokazuje analogicky jako (a), využijte přitom axiom H1.

Nyní ukážeme (c). Nechť  $\vdash (\varphi \wedge \psi) \Rightarrow \vartheta$ . Z věty o dedukci máme  $\varphi \wedge \psi \vdash \vartheta$ . Navíc platí

$\varphi \Rightarrow \neg\psi, \varphi \vdash \neg\psi$	<i>princip modus ponens,</i>
$\varphi \vdash (\varphi \Rightarrow \neg\psi) \Rightarrow \neg\psi$	<i>věta o dedukci,</i>
$\varphi \vdash ((\varphi \Rightarrow \neg\psi) \Rightarrow \neg\psi) \Rightarrow (\neg\neg\psi \Rightarrow \neg(\varphi \Rightarrow \neg\psi))$	<i>duální forma H3, monotonie,</i>
$\varphi \vdash \neg\neg\psi \Rightarrow \neg(\varphi \Rightarrow \neg\psi)$	<i>princip modus ponens,</i>
$\varphi \vdash \psi \Rightarrow \neg(\varphi \Rightarrow \neg\psi)$	<i>věta o ekvivalenci,</i>
$\varphi \vdash \psi \Rightarrow (\varphi \wedge \psi)$	<i>zkratka za formuli,</i>
$\varphi, \psi \vdash \varphi \wedge \psi$	<i>věta o dedukci.</i>

Nyní z  $\varphi, \psi \vdash \varphi \wedge \psi$  a  $\varphi \wedge \psi \vdash \vartheta$  dostáváme  $\varphi, \psi \vdash \vartheta$  (zdůvodněte proč). Dále dvojnásobným užitím věty o dedukci dostáváme  $\vdash \varphi \Rightarrow (\psi \Rightarrow \vartheta)$ , což bylo dokázat.

Předpokládejme  $\vdash \varphi \Rightarrow (\psi \Rightarrow \vartheta)$ . Z věty o dedukci  $\varphi, \psi \vdash \vartheta$ . Aplikací bodů (a), (b) dostáváme  $\varphi \wedge \psi \vdash \varphi$  a  $\varphi \wedge \psi \vdash \psi$ . To jest v důsledku  $\varphi \wedge \psi \vdash \vartheta$ . Užitím věty o dedukci  $\vdash (\varphi \wedge \psi) \Rightarrow \vartheta$ , což je požadované tvrzení. Dohromady jsme prokázali platnost bodu (c).

Tvrzení (d) plyne z bodů (a), (b), věty o dedukci a užitím  $\vdash \varphi \Rightarrow (\psi \Rightarrow (\varphi \wedge \psi))$ .

Bod (e) je bezprostředním důsledkem (d) a opravňuje nás přijmout platnost  $\mathcal{T} \vdash \varphi \Leftrightarrow \psi$  pokud prokážeme obě implikace, to jest  $\mathcal{T} \vdash \varphi \Rightarrow \psi$  a  $\mathcal{T} \vdash \psi \Rightarrow \varphi$ , což je opět dokazovací princip často používaný při dokazování na úrovni intuice.

### Cvičení.

46. Bez použití věty o úplnosti VP dokažte následující tvrzení.

- |   |   |
|---|---|
| (a) $(\neg\varphi \Rightarrow \psi) \Rightarrow (\neg\psi \Rightarrow \varphi)$ ,       | (h) $\varphi, \neg\neg\psi \vdash \varphi \wedge \psi$ ,  |
| (b) $\vdash (\varphi \wedge \psi) \Rightarrow (\varphi \vee \psi)$ .                    | (i) $\psi \vdash (\varphi \Rightarrow (\psi \Rightarrow \vartheta)) \Rightarrow (\varphi \Rightarrow \vartheta)$ .          |
| (c) $\neg(\varphi \Rightarrow \varphi) \Rightarrow (\varphi \Leftrightarrow \varphi)$ , | (j) $\vdash ((\varphi \Rightarrow \psi) \wedge (\psi \Rightarrow \vartheta)) \Rightarrow (\varphi \Rightarrow \vartheta)$ , |
| (d) $\psi \vee \neg\varphi \vdash \varphi \Rightarrow \psi$ .                           | (k) $\vdash (\varphi \Rightarrow \varphi) \Rightarrow (\varphi \Rightarrow \varphi)$ ,                                      |
| (e) $\vdash \neg\varphi \vee \varphi$ ,   | (l) $\vdash \neg(\psi \Rightarrow \psi) \Rightarrow \varphi$ ,  |
| (f) $\varphi \vdash \varphi \wedge \varphi$ ,   | (m) $\vdash \neg(\varphi \wedge \neg\varphi)$ ,   |
| (g) $\varphi \vdash \psi \vee \varphi$ ,  | (n) $\vdash \varphi \vee (\varphi \Rightarrow \psi)$ .  |

## Ekvivalence deduktivních systémů

Výroková dokazatelnost formule  $\varphi$  ze systému  $\mathcal{T}$  je definovaná pomocí pojmu důkaz. Přitom s důkazem pracujeme jako se speciální konečnou posloupností formulí, která musí splňovat jisté podmínky. Z hlediska důkazu jsou podstatná *axiomová schémata* a *odvozovací pravidla*. V klasickém výrokovém kalkulu (Hilbertova typu) se používají tradičně axiomová schémata H1–H3 a odvozovací pravidlo modus ponens. Můžeme však uvažovat i jiná schémata, případně jiná odvozovací pravidla a lze zkoumat jejich vztah k H1–H3 a pravidlu modus ponens.

Množinu uvažovaných axiomových schémat a odvozovacích pravidel budeme stručně nazývat *deduktivní systém*. Označme  $L$  deduktivní systém a necht'  $\mathcal{T}$  je systém formulí. Posloupnost  $\delta_1, \dots, \delta_n$  je  $L$ -*důkazem* ze systému formulí  $\mathcal{T}$ , pokud je každá  $\delta_i$  instancí některého axiomového schématu z  $L$ , nebo je  $\delta_i \in \mathcal{T}$ , nebo  $\delta_i$  vznikla z nějakých  $n$  formulí  $\delta_{i_1}, \dots, \delta_{i_n}$  ( $i_1, \dots, i_n < i$ ) užitím jistého  $n$ -árního odvozovacího pravidla z  $L$ . Formule  $\varphi$  je  $L$ -*dokazatelná* z  $\mathcal{T}$  (symbolicky  $\mathcal{T} \vdash_L \varphi$ ), pokud existuje  $L$ -důkaz  $\delta_1, \dots, \delta_n = \varphi$  z  $\mathcal{T}$ . Předchozí pojmy evidentně zobecňují dokazatelnost z  $\mathcal{T}$  pro deduktivní systém  $L$ . Pokud je  $L$  systém skládající se z axiomových schémat H1–H3 a pravidla modus ponens, dostáváme triviálně  $\mathcal{T} \vdash_L \varphi$ , právě když  $\mathcal{T} \vdash \varphi$  pro každou  $\mathcal{T}$  a  $\varphi$ .

Deduktivní systémy  $L_1$  a  $L_2$  nazýváme *ekvivalentní*, pokud platí  $\mathcal{T} \vdash_{L_1} \varphi$ , právě když  $\mathcal{T} \vdash_{L_2} \varphi$  pro každý systém formulí  $\mathcal{T}$  a libovolnou formuli  $\varphi$ .

Nyní si ukážeme typickou metodu jak prokázat ekvivalenci deduktivních systémů.

### Příklad.

47. Mějme deduktivní systém  $L$ , který vznikne z deduktivního systému klasického výrokového kalkulu Hilbertova typu nahrazením axiomového schématu H3 schématem

$$\text{H3}') \quad (\neg\psi \Rightarrow \neg\varphi) \Rightarrow ((\neg\psi \Rightarrow \varphi) \Rightarrow \psi).$$

Dokažte, že  $L$  je ekvivalentní ded. systému klasického výrokového kalkulu Hilbertova typu.

### Řešení.

Pro libovolný systém formulí  $\mathcal{T}$  a libovolnou formuli  $\varphi$  stačí dokázat, že  $\mathcal{T} \vdash \varphi$ , právě když  $\mathcal{T} \vdash_L \varphi$ . Jelikož první dvě axiomová schémata nebyla změněna a odvozovací pravidlo modus ponens zůstalo opět jako jediné dokazovací pravidlo, můžeme v deduktivním systému  $L$  bez újmy používat *větu o dedukci* ( $\mathcal{T} \vdash_L \varphi \Rightarrow \psi$ , právě když  $\mathcal{T}, \varphi \vdash_L \psi$ ). V důkazu věty o dedukci se totiž využívají pouze schémata H1 a H2, to jest změna třetího schématu nemůže způsobit její neplatnost (podrobně si ověřte sami).

Vezměme libovolný systém formulí  $\mathcal{T}$  a formuli  $\varphi$ . Směr „ $\mathcal{T} \vdash_L \varphi \Rightarrow \mathcal{T} \vdash \varphi$ “ je jednodušší a podrobně si jej rozebereme. Předpokládejme platnost  $\mathcal{T} \vdash_L \varphi$ . Budeme postupovat tak, že vyjdeme z  $L$ -důkazu formule  $\varphi$  z  $\mathcal{T}$  a transformujeme jej na posloupnost formulí, která bude důkazem  $\varphi$  z  $\mathcal{T}$ . Z předpokladu  $\mathcal{T} \vdash_L \varphi$  plyne existence posloupnosti  $\delta_1, \dots, \delta_n = \varphi$ , která je  $L$ -důkazem. To jest pro každé  $i = 1, \dots, n$  je  $\delta_i$  buďto instancí H1, H2 a H3', předpokladem z množiny  $\mathcal{T}$ , nebo vznikla použitím pravidla modus ponens z  $\delta_j, \delta_k$  pro  $j, k < i$ . Dále platí

$$\begin{array}{ll} \neg\psi \Rightarrow \neg\varphi, \neg\psi \Rightarrow \varphi, \neg\psi \vdash \neg\varphi & \text{princip MP na } \neg\psi \Rightarrow \neg\varphi \text{ a } \neg\psi, \\ \neg\psi \Rightarrow \neg\varphi, \neg\psi \Rightarrow \varphi, \neg\psi \vdash \varphi & \text{princip MP na } \neg\psi \Rightarrow \varphi \text{ a } \neg\psi, \\ \neg\psi \Rightarrow \neg\varphi, \neg\psi \Rightarrow \varphi \vdash \psi & \text{princip důkazu sporem,} \\ \vdash (\neg\psi \Rightarrow \neg\varphi) \Rightarrow ((\neg\psi \Rightarrow \varphi) \Rightarrow \psi) & \text{dvakrát věta o dedukci.} \end{array}$$

To jest  $\vdash (\neg\psi \Rightarrow \neg\varphi) \Rightarrow ((\neg\psi \Rightarrow \varphi) \Rightarrow \psi)$  pro libovolné formule  $\psi, \varphi$ . Což znamená že pro každou instanci  $\vartheta$  schématu H3' platí  $\vdash \vartheta$ , neboli existuje důkaz  $\vartheta_1, \dots, \vartheta_n = \vartheta$  z prázdného

systému předpokladů. Nyní můžeme uvažovat posloupnost formulí  $\gamma_1, \dots, \gamma_m = \varphi$  vzniknuvší z  $\delta_1, \dots, \delta_n$  nahrazením každé instance  $\vartheta$  schématu H3' jejím důkazem  $\vartheta_1, \dots, \vartheta_n = \vartheta$  z axiomů H1, H2 a H3. Posloupnost  $\gamma_1, \dots, \gamma_m$  je evidentně důkazem, ve kterém jsou využita pouze schémata H1–H3, předpoklady z  $\mathcal{T}$  a odvozovací pravidlo modus ponens. Platí tedy  $\mathcal{T} \vdash \varphi$ .

Směr „ $\mathcal{T} \vdash \varphi \Rightarrow \mathcal{T} \vdash_L \varphi$ “, nyní již stručněji. Stačí ukázat  $\vdash_L (\neg\psi \Rightarrow \neg\varphi) \Rightarrow (\varphi \Rightarrow \psi)$ .

Zbývající úvaha je vedena jako v předchozím případě.

$\vdash_L (\neg\psi \Rightarrow \neg\varphi) \Rightarrow ((\neg\psi \Rightarrow \varphi) \Rightarrow \psi)$	<i>instance schématu H3',</i>
$\neg\psi \Rightarrow \neg\varphi \vdash_L (\neg\psi \Rightarrow \varphi) \Rightarrow \psi$	<i>věta o dedukci,</i>
$\vdash_L \varphi \Rightarrow (\neg\psi \Rightarrow \varphi)$	<i>instance schématu H1,</i>
$\neg\psi \Rightarrow \neg\varphi \vdash_L \varphi \Rightarrow (\neg\psi \Rightarrow \varphi)$	<i>monotonie,</i>
$\neg\psi \Rightarrow \neg\varphi \vdash_L \varphi \Rightarrow \psi$	<i>transitivita implikace,</i>
$\vdash_L (\neg\psi \Rightarrow \neg\varphi) \Rightarrow (\varphi \Rightarrow \psi)$	<i>věta o dedukci.</i>

Použití principu transitivity implikace bylo v pořádku, protože plyne přímo z věty o dedukci.

### Poznámka.

Uveďme že z předchozího příkladu plyne  $\mathcal{T} \vdash_L \varphi$ , právě když  $\mathcal{T} \vdash \varphi$ , což je právě když platí  $\mathcal{T} \models \varphi$  (viz další paragraf). Pro deduktivní systém  $L$  jsme tedy automaticky získali *větu o úplnosti*. Pochopitelně existují i deduktivní systémy, které nejsou ekvivalentní se systémem klasické výrokové logiky Hilbertova typu. Stačilo by například uvažovat systém, který vznikne z klasického výrokového systému Hilbertova typu odejmutím některého ze schémat H1–H3. Zkuste zdůvodnit proč.

### Cvičení.

48. Uvažujme deduktivní systém  $L$ , který vznikne z deduktivního systému klasické výrokové logiky Hilbertova typu (dále jen KH) přidáním odvozovacího pravidla *nahrazení* (z formule  $\varphi$  odvoď  $\psi$ , kde  $\psi$  vznikla z  $\varphi$  nahrazením všech výskytů výrokového symbolu  $p$  ve  $\varphi$  formulí  $\vartheta$ ). Dokažte že  $L$  je ekvivalentní deduktivnímu systému HK.
49. Mějme deduktivní systém  $L$ , který neobsahuje žádná axiomová schémata, ale obsahuje odvozovací pravidla modus ponens a pravidlo nahrazení z předchozího příkladu.  $L$  evidentně není ekvivalentní deduktivnímu systému HK. Ukažte ale, že  $\mathcal{T} \vdash \varphi$  platí, právě když  $\mathcal{T} \cup \mathcal{S} \vdash_L \varphi$ , kde  $\mathcal{S} = \{p \Rightarrow (q \Rightarrow p), (p \Rightarrow (q \Rightarrow r)) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r)), (\neg q \Rightarrow \neg p) \Rightarrow (p \Rightarrow q)\}$ .

\*50. Hilbertův-Ackermannův deduktivní systém (dále značený  $A$ ) má čtyři axiomová schémata:

- A1)  $(\varphi \vee \varphi) \Rightarrow \varphi$ ,
- A2)  $\varphi \Rightarrow (\varphi \vee \psi)$ ,
- A3)  $(\varphi \vee \psi) \Rightarrow (\psi \vee \varphi)$ ,
- A4)  $(\varphi \Rightarrow \psi) \Rightarrow ((\vartheta \vee \varphi) \Rightarrow (\vartheta \vee \psi))$ ,

a odvozovací pravidlo modus ponens. Dokažte že  $A$  je ekvivalentní deduktivnímu systému HK. Uvědomte si, že pracujeme s deduktivním systémem neobsahujícím schémata H1, H2. To znamená, že nemůžeme automaticky v  $A$  přijmout platnost věty o dedukci. Všechny používané dokazovací principy v  $A$  musíme nejprve explicitně prokázat analogicky jako jsme to dělali u deduktivního systému HK.

## Sémantické vyplývání ve VP

Mějme pravdivostní ohodnocení  $e: V \rightarrow \{0, 1\}$ . Pro libovolný systém formulí  $\mathcal{T}$  píšeme  $e \models \mathcal{T}$ , pokud je každá formule  $\psi \in \mathcal{T}$  pravdivá v ohodnocení  $e$ , to jest  $\|\psi\|_e = 1$  pro každou formuli  $\psi \in \mathcal{T}$ . Ohodnocení  $e$ , pro které  $e \models \mathcal{T}$ , se někdy nazývá *model*  $\mathcal{T}$ . Formule  $\varphi$  *sémanticky vyplývá* z množiny formulí  $\mathcal{T}$ , pokud je  $\varphi$  pravdivá v každém ohodnocení  $e$ , kde  $e \models \mathcal{T}$ .

Zkoumání vztahů mezi syntaktickým vyplýváním, je test *dokazatelnosti*, a sémantickým vyplýváním, to jest *pravdivostí ve všech modelech*, je jedním z ústředních bodů matematické logiky. Je dobré si uvědomit, že pokud například prokážeme, že  $\mathcal{T} \vdash \varphi$  platí právě když  $\mathcal{T} \models \varphi$  (věta o úplnosti), pak můžeme dokazovací principy uvedené v předchozím paragrafu, třeba větu o dedukci, automaticky přenést na sémantickou úroveň. Například sémantická verze věty o dedukci má tvar:  $\mathcal{T} \models \varphi \Rightarrow \psi$ , právě když  $\mathcal{T}, \varphi \models \psi$ . Všechny tyto běžné principy lze však na sémantické úrovni prokázat bez použité věty o úplnosti VP.

### Příklad.

51. Bez použití věty o úplnosti VP dokažte  $\mathcal{T} \models \varphi \Rightarrow \psi$ , právě když  $\mathcal{T}, \varphi \models \psi$ .

#### Řešení.

Nejprve ukážeme stranu  $\Rightarrow$ . Tedy předpokládáme  $\mathcal{T} \models \varphi \Rightarrow \psi$  a dokazujeme  $\mathcal{T}, \varphi \models \psi$ . Stačí ověřit, že pro každé ohodnocení  $e$ , kde  $e \models \mathcal{T}, \varphi$ , máme  $\|\psi\|_e = 1$ . Pokud ale  $e \models \mathcal{T}, \varphi$ , pak  $e \models \mathcal{T}$  a zároveň  $\|\varphi\|_e = 1$ . Jelikož  $\mathcal{T} \models \varphi \Rightarrow \psi$  platí dle předpokladu, ihned dostáváme  $\|\varphi \Rightarrow \psi\|_e = 1$ . Nyní již z  $\|\varphi\|_e = 1$  a z  $\|\varphi \Rightarrow \psi\|_e = \|\varphi\|_e \rightarrow \|\psi\|_e = 1$  plyne  $\|\psi\|_e = 1$ . To jest  $\mathcal{T}, \varphi \models \psi$ .

Ukážeme opačnou implikaci. Předpokládejme  $\mathcal{T}, \varphi \models \psi$ , stačí ověřit, že pro každé ohodnocení  $e$ , kde  $e \models \mathcal{T}$  máme  $\|\varphi \Rightarrow \psi\|_e = 1$ . Nechť tedy  $e \models \mathcal{T}$ . Pokud  $\|\varphi\|_e = 0$ , pak  $\|\varphi \Rightarrow \psi\|_e = 1$  plyne přímo ze sémantiky implikace. Pokud  $\|\varphi\|_e = 1$ , pak i  $e \models \mathcal{T}, \varphi$  a z předpokladu  $\mathcal{T}, \varphi \models \psi$  dostáváme  $\|\psi\|_e = 1$ . Tedy  $\|\varphi \Rightarrow \psi\|_e = \|\varphi\|_e \rightarrow \|\psi\|_e = 1 \rightarrow 1 = 1$ , to jest  $\mathcal{T} \models \varphi \Rightarrow \psi$ .

### Cvičení.

52. Bez použití věty o úplnosti VP dokažte následující tvrzení.

- $\mathcal{T} \models \varphi$  a pro každou  $\psi \in \mathcal{T}$  platí  $\mathcal{S} \models \psi$ , pak  $\mathcal{S} \models \varphi$ ,
- $\mathcal{T} \models \varphi$  a  $\mathcal{T} \subseteq \mathcal{S}$ , pak  $\mathcal{S} \models \varphi$ ,
- systém formulí  $\mathcal{T}, \neg\varphi$  není splnitelný, právě když  $\mathcal{T} \models \varphi$ ,
- $\mathcal{T}, \varphi \models \psi$  a  $\mathcal{T}, \neg\varphi \models \psi$ , právě když  $\mathcal{T} \models \psi$ ,
- $\mathcal{T}$  není splnitelný, právě když  $\mathcal{T} \models \varphi$  pro libovolnou formuli  $\varphi$ ,
- $\mathcal{T} \models \neg(\varphi \Rightarrow \neg\psi)$ , právě když  $\mathcal{T} \models \varphi$  a zároveň  $\mathcal{T} \models \psi$ ,
- pokud  $\mathcal{T} \models \varphi$  a  $\mathcal{T} \models \varphi \Rightarrow \psi$ , pak  $\mathcal{T} \models \psi$ ,
- každý splnitelný systém formulí je bezesporný,
- $\mathcal{T}, \neg\varphi \models \varphi \Rightarrow \psi$ ,
- $\varphi$  a  $\psi$  jsou logicky ekvivalentní, právě když  $\varphi \models \psi$  a  $\psi \models \varphi$ .

53. Pro každý systém formulí  $\mathcal{T}$  definujme systém formulí  $\mathcal{T}^{\models} = \{\varphi; \mathcal{T} \models \varphi\}$ . Dokažte následující tvrzení.

- $\mathcal{T}^{\models} = (\mathcal{T}^{\models})^{\models}$ ,
- $\mathcal{T}^{\models}$  je vždy nekonečný systém formulí,
- $\varphi \in \mathcal{T}^{\models}$ , právě když  $\mathcal{T}, \neg\varphi$  není splnitelný,
- je-li  $\mathcal{T}$  splnitelný systém, pak je  $\mathcal{T}^{\models}$  splnitelný systém obsahující  $\mathcal{T}$ .

**Příklad.**

54. Rozhodněte, které z následujících formulí sémanticky plynou z  $\mathcal{T} = \{p \Rightarrow \neg(\neg r \Rightarrow q), \neg r\}$ :

$$q \Rightarrow \neg p, \quad \neg(p \Rightarrow q) \Rightarrow r, \quad s \Rightarrow (q \Rightarrow p), \quad s \Rightarrow ((p \Rightarrow \neg q) \Rightarrow s).$$

**Řešení.**

Označme  $\varphi = p \Rightarrow \neg(\neg r \Rightarrow q)$ ,  $\psi = \neg r$ . Provedeme tabelaci:

	$p$	$q$	$r$	$\varphi$	$\psi$		$p$	$q$	$r$	$\varphi$	$\psi$
$e_1$ :	0	0	0	1	1	$e_3$ :	1	0	0	1	1
	0	0	1	1	0		1	0	1	0	0
$e_2$ :	0	1	0	1	1		1	1	0	0	1
	0	1	1	1	0		1	1	1	0	0

Z předchozí tabulky je vidět, že stačí vyšetřovat pravdivost formulí v ohodnoceních, která jsou v tabulce representována řádky označenými  $e_1, e_2, e_3$ . Nyní zřejmě  $\mathcal{T} \models q \Rightarrow \neg p$ , protože formule  $q \Rightarrow \neg p$  je pravdivá v každém z ohodnocení  $e_1, e_2, e_3$ . Dále  $\| \neg(p \Rightarrow q) \Rightarrow r \|_{e_3} = 0$ , to jest formule  $\neg(p \Rightarrow q) \Rightarrow r$  sémanticky neplyne z  $\mathcal{T}$  – ohodnocení  $e_3$  nám slouží jako *protipříklad*. Stejně tak třetí formule  $s \Rightarrow (q \Rightarrow p)$  neplyne z  $\mathcal{T}$ , uvažujeme-li například ohodnocení  $e$ , kde  $e(p) = e_2(p)$ ,  $e(q) = e_2(q)$ ,  $e(r) = e_2(r)$  a  $e(s) = 1$ , pak  $e \models \mathcal{T}$ , ale  $\| s \Rightarrow (q \Rightarrow p) \|_e = 0$ . Konečně formule  $s \Rightarrow ((p \Rightarrow \neg q) \Rightarrow s)$  je tautologie, to jest plyne z libovolného systému formulí, tedy i ze zkoumaného systému  $\mathcal{T}$ .

**Příklad.**

55. Dokažte, že formule  $q \Rightarrow p$  není dokazatelná ze systému  $\mathcal{T} = \{(p \Rightarrow \neg q) \Rightarrow \neg r, p \Rightarrow r\}$ .

**Řešení.**

Využijeme věty o korektnosti VP: pokud  $\mathcal{T} \vdash \varphi$ , pak  $\mathcal{T} \models \varphi$ . Reformulací dostáváme, že pokud  $\varphi$  sémanticky neplyne z  $\mathcal{T}$ , pak  $\varphi$  není dokazatelná z  $\mathcal{T}$ . V našem případě to tedy znamená najít ohodnocení  $e$  takové, že  $e \models \mathcal{T}$ , ale  $\| q \Rightarrow p \|_e = 0$ . Takovým ohodnocením je například  $e$ , kde  $e(p) = 0$ ,  $e(q) = 1$  a  $e(r) = 0$ . Přesvědčte se tabelací.

**Cvičení.**

56. Rozhodněte, které z formulí

$$\begin{aligned} r \Rightarrow (\neg r \Rightarrow (q \Rightarrow r)), & \quad p \Rightarrow \neg(q \Rightarrow \neg r), & \quad p \Rightarrow (q \Rightarrow \neg(p \Rightarrow q)), \\ (p \Rightarrow q) \Rightarrow \neg r, & \quad (r \Rightarrow p) \Rightarrow (\neg q \Rightarrow \neg r), & \quad \neg((\neg p \Rightarrow q) \Rightarrow r), \end{aligned}$$

sémanticky plynou ze systému  $\mathcal{T} = \{p \Rightarrow \neg q, r \Rightarrow (\neg p \Rightarrow r), r \Rightarrow \neg(p \Rightarrow q)\}$ .

57. S využitím věty o korektnosti VP *vyvráťte* následující tvrzení.

- (a)  $p \vdash p \Rightarrow q$ ,
- (b) pro každé  $\varphi, \psi, \vartheta$  platí: pokud  $\varphi, \psi \vdash \vartheta$ , pak  $\varphi \vdash \vartheta$ ,
- (c) pro každé  $\varphi, \psi, \vartheta$  platí: pokud  $\varphi \vdash \vartheta$  a  $\psi \vdash \varphi$ , pak  $\vartheta \vdash \varphi \Rightarrow \psi$ ,
- (d)  $p, \neg q \Rightarrow r \vdash p \Rightarrow (q \Rightarrow r)$ .

## Jazyk, termy a formule v predikátové logice

Formule *výrokové logiky* formalizují vztahy mezi *výroky*. Naproti tomu formule predikátové logiky formalizují vztahy mezi *individui* neboli *objekty* (jejich funkční závislosti, vlastnosti a vzájemné vztahy). Formule predikátové logiky musí tento rozdíl zohledňovat. Například tvrzení „*pokud je  $x$  sudé číslo, pak je  $x + 1$  liché*“ je z pohledu výrokové logiky ve tvaru implikace dvou výroků a je tudíž formalizovatelné výrokovou formulí  $p \Rightarrow q$ . Z pohledu predikátové logiky se ale ve tvrzení vyskytují individua (*čísla*), jejich vlastnosti (*být sudé, být liché*) a funkční závislosti ( *$x + 1$  je následníkem  $x$* , podrobněji 1 označuje *individuum* a „+“ označuje funkční závislost dvou individuí, v našem případě individua označeného proměnnou  $x$  a konstantou 1). Zdůrazněme že stejně jako ve výrokové logice se soustředíme na *formu (tvar)* formulí a abstrahujeme od jejich obsahu.

Při popisu jednotlivých problémových domén (vlastností čísel, popisu struktury počítačové sítě, etc.) je obecně potřeba pracovat s různými vlastnostmi a vztahy, například „být sudý“, „být menší než“, nebo „být propojen s daným uzlem“, „mít záložní zdroj“ a tak dále. Formule predikátové logiky proto vždy vztahujeme ke konkrétnímu *jazyku*, který nám určuje, jaké funkční závislosti, vlastnosti a vztahy mohou formule popisovat. Předmětem matematické logiky není *nezkoumání* problém návrhu jazyka a konstrukce formulí ze slovního popisu. Na druhou stranu je ale nutné mít v těchto postupech jistý cvik, je to například potřeba při programování v *logických programovacích jazycích*. Formulím a slovnímu popisu se věnuje jedna z dalších částí cvičení.

Každý uvažovaný jazyk je určen svým typem. *Typ jazyka* predikátové logiky je trojice  $\langle R, F, \sigma \rangle$ , kde  $R$  je množina *relačních symbolů* (jména pro vlastnosti a vztahy),  $F$  je množina *funkčních symbolů* (jména pro funkční závislosti). Dále předpokládáme  $R \cap F = \emptyset$  a  $\sigma$  je zobrazení  $\sigma : R \cup F \rightarrow \mathbb{N}_0$ , které každému relačnímu a funkčnímu symbolu přiděluje jeho *aritu* (neformálně řečeno „počet argumentů“). Je-li  $\sigma(f) = 0$ , pak se symbol  $f$  nazývá *nulární*, pro  $\sigma(f) = 1$  se  $f$  nazývá *unární*, pro  $\sigma(f) = 2$  se  $f$  nazývá *binární*, pro  $\sigma(f) = 3$  se  $f$  nazývá *ternární*, pro  $\sigma(f) = 4$  se  $f$  nazývá *kvaternární* a tak dále. Nulární relační symboly nazýváme *výroky*. Nulární funkční symboly nazýváme *konstanty*.

Speciálním způsobem chápeme *jazyky s rovností*. Za jazyk s rovností považujeme jazyk, který obsahuje binární relační symbol  $\approx$  označující *rovnost*. Důvod explicitního rozlišení jazyků s rovností bude patrný dále.

### Příklad.

58. Navrhněte jazyky pro formalizaci následujících tvrzení.

- (a) „*Pokud je  $x$  sudé číslo, pak je  $x + 1$  liché.*“
- (b) „*Některé dopravní prostředky mají dvě kola.*“
- (c) „*Každý uzel v počítačové síti má aspoň jednoho souseda.*“

### Řešení.

- (a) Můžeme uvažovat například  $F = \{plus, 1\}$ , kde  $\sigma(plus) = 2$ ,  $\sigma(1) = 0$  a  $R = \{sudé, liché\}$ , kde shodně  $\sigma(sudé) = \sigma(liché) = 1$ . Upozorníme na fakt, že funkční symbol 1 je pro nás konstanta, kterou v žádném případě *nelze ztotožňovat* s přirozeným číslem 1. Definicí jazyka pouze vymezujeme formule (viz dále), se kterými vedeme další úvahy. Jazyk (coby součást syntaxe predikátové logiky) nemá sám o sobě žádnou sémantickou interpretaci.
- (b) Uvažujme jazyk s rovností, kde  $F = \{dvě, pkol\}$ ,  $\sigma(dvě) = 0$ ,  $\sigma(pkol) = 1$  a dále mějme  $R = \{prostředek\}$ , kde  $\sigma(prostředek) = 1$ . Relační symbol *prostředek* reprezentuje vlastnost „být dopravním prostředkem“, konstanta *dvě* reprezentuje počet a *pkol* můžeme

chápat jako funkční závislost mezi individuem (třeba dopravním prostředkem) a jeho počtem kol. Navržený jazyk není jediný přípustný. Pokuste se pro tento příklad navrhnout vhodný jazyk bez rovnosti, ve kterém bude  $F = \emptyset$ .

- (c) Nyní již stručně,  $F = \emptyset$ ,  $R = \{uzel, sousedí\}$ , kde  $\sigma(uzel) = 1$ ,  $\sigma(sousedí) = 2$ . Unární relační symbol *uzel* reprezentuje vlastnost „být uzlem v síti“, binární relační symbol *sousedí* představuje „sousedský vztah“ mezi dvěma uzly. Pokuste se zdůvodnit proč není vhodné (i když ne nemožné) chápat „sousedství uzlů“ jako funkční závislost mezi uzly?

Pro každý jazyk daného typu  $\langle R, F, \sigma \rangle$  definujeme množinu *termů*:

- (1) Každá proměnná  $x$  je term (proměnné označujeme písmeny  $x, y, z, \dots$ ).
- (2) Nechť  $f \in F$ ,  $\sigma(f) = k$  a  $t_1, \dots, t_k$  jsou libovolné termy. Pak  $f(t_1, \dots, t_k)$  je term.
- (3) Všechny termy vznikají aplikací předchozích dvou bodů.

Dále definujeme množinu *formulí*:

- (1) Je-li  $r \in R$ ,  $\sigma(r) = n$  a  $t_1, \dots, t_n$  jsou libovolné termy. Pak  $r(t_1, \dots, t_n)$  je (*atomická*) formule.
- (2) Nechť  $\varphi, \psi$  jsou formule a nechť  $x$  je libovolná proměnná. Pak  $\neg\varphi$ ,  $(\varphi \Rightarrow \psi)$ ,  $(\forall x)\varphi$  jsou formule.
- (3) Všechny formule vznikají aplikací předchozích dvou bodů.

Dále budeme používat běžné konvence o vynechávání vnějších závorek. Stejně jako ve výrokové logice chápeme výrazy  $\varphi \wedge \psi$ ,  $\varphi \vee \psi$ ,  $\varphi \Leftrightarrow \psi$  jako zkratky za formule obsahující pouze spojky  $\neg$  a  $\Rightarrow$ .

V některých případech nemáme dán jazyk explicitně, ale chápeme jej jako *minimální množinu funkčních a relačních symbolů*, ve kterých daný řetězec symbolů, případně množina řetězců symbolů, *splňuje definici formule*. Například řetězec  $(\forall x)r(x, c)$  je formule za předpokladu, že pracujeme s jazykem, kde  $r$  je binární relační symbol,  $x$  je proměnná a  $c$  je proměnná nebo konstanta. Ve výrazu  $(\forall x)r(x, c)$  by symbol  $c$  mohl označovat konstantu i proměnnou, na druhou stranu  $x$  musí být v tomto případě pouze proměnná (rozmyslete si proč).

### Cvičení.

59. Uvažujme jazyk, kde  $F = \{f, g, h\}$ ,  $R = \{r, s\}$  a  $\sigma(f) = \sigma(h) = \sigma(r) = 1$ ,  $\sigma(s) = 2$ ,  $\sigma(g) = 3$ . Rozhodněte, které z následujících slov (ne)jsou formule tohoto jazyka a zdůvodněte proč.

$$\begin{array}{llll} f(x), & r(f(x)), & (\forall x)r(x) \Rightarrow s(x, h(x)), & (\forall x)(r(x) \Rightarrow \neg r(x)), \\ (\forall x)\neg h(x), & s(g(x, x, h(x))), & s(h(x), h(f(x))), & s(x, x) \Rightarrow (\forall y)s(x, x), \\ (\forall x)(\forall y)\neg r(g(x, y, z)), & r(\neg r(x)), & r(y) \Rightarrow (\forall s)s(x, y), & \neg(\forall x)(k(x) \Rightarrow r(x)). \end{array}$$

60. Mějme jazyk s rovností, kde  $F = \{c, f\}$ ,  $R = \{r\}$  a  $\sigma(c) = 0$ ,  $\sigma(f) = 1$ ,  $\sigma(r) = 2$ . Pojmy *podterm* a *podformule* se v predikátové logice zavádí analogickým způsobem jako se zaváděl pojem podformule ve výrokové logice, nebudeme je tedy uvádět. Rozhodněte, které z následujících výrazů jsou termy a které jsou formule výše uvedeného jazyka a vypište všechny jejich podtermy, případně podformule.

$$\begin{array}{llll} c, & r(c, x) \Rightarrow \neg r(c, f(c)), & f(f(c)), & r(x, y) \Rightarrow (\forall x)\neg r(x, c), \\ c \approx c, & (c \approx f(c)) \Rightarrow (\forall y)r(f(y), y), & \neg f(f(x)) \approx f(c), & (\forall x)x \approx c \Rightarrow (\forall y)r(f(y), c). \end{array}$$

61. Napište typ minimálního jazyka, ve kterém lze uvažovat následující výrazy jako formule.

$$\begin{array}{llll} r(x) \Rightarrow y \approx f(x), & p \Rightarrow \neg p, & x \approx x, & (\forall x)(x \approx f(x) \Rightarrow q(x, g(x, 0))), \\ f(g(h(c))), & f(x, y) \Rightarrow (f(y, z) \Rightarrow f(x, z)), & r(x, x), & c \approx d \Rightarrow (\forall x)x \approx c. \end{array}$$



## Výskyty proměnných a substituovatelnost

Formule v predikátové logice můžeme samozřejmě definovat i jinými způsoby než jak tomu bylo v předchozí sekci. V logickém programování se formule často uvažují jako *uzlově ohodnocené stromy*. Tuto názornou definici lze přirozeně rozšířit i pro formule predikátové logiky.

Všechny *termy* vznikají aplikací následujících dvou bodů.

- (1) Každá proměnná  $x$  je term.
- (2) Nechť  $f \in F$ ,  $\sigma(f) = k$  a  $t_1, \dots, t_k$  jsou libovolné termy. Pak  $t_1 \begin{array}{c} \diagup \\ f \\ \diagdown \end{array} \begin{array}{c} t_2 \\ \dots \\ t_k \end{array}$  je term.

Všechny *formule* vznikají aplikací následujících dvou bodů.

- (1) Je-li  $r \in R$ ,  $\sigma(r) = n$  a  $t_1, \dots, t_n$  jsou libovolné termy. Pak  $t_1 \begin{array}{c} \diagup \\ r \\ \diagdown \end{array} \begin{array}{c} t_2 \\ \dots \\ t_n \end{array}$  je formule.
- (2) Nechť  $\varphi, \psi$  jsou formule. Pak  $\varphi \Rightarrow \psi$ ,  $\neg \varphi$  a  $\forall x \varphi$  jsou formule.

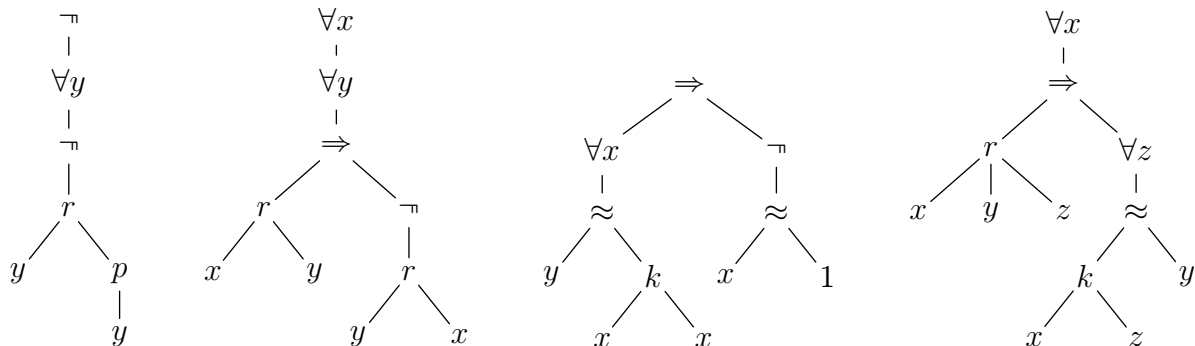
### Příklad.

62. Následující formule vyjádřete pomocí stromů.

$$\begin{array}{ll} \neg(\forall y)\neg r(y, p(y)), & (\forall x)(\forall y)(r(x, y) \Rightarrow \neg r(y, x)), \\ (\forall x)y \approx k(x, x) \Rightarrow \neg x \approx 1, & (\forall x)(r(x, y, z) \Rightarrow (\forall z)k(x, z) \approx y). \end{array}$$

### Řešení.

Formule přepíšeme podle definice:



Za pozornost stojí, že všechny *listové uzly* stromů reprezentujících formule jsou označeny buďto *proměnnou*, *konstantou*, nebo *výrokem* (nulárním relačním symbolem). Pomocí strukturální indukce se přesvědčte, že ke každé formuli predikátového počtu existuje jednoznačně definovaný strom dle předchozí definice a obráceně. Formule jsou ve *vzájemně jednoznačné korespondenci* se speciálními uzlově ohodnocenými stromy. Pro formuli  $\varphi$  budeme označovat  $\mathfrak{t}_\varphi$  příslušný strom.

Pro každou formuli  $\varphi$  a proměnnou zavádíme následující pojmy.

- Každý list  $\mathfrak{t}_\varphi$  označený proměnnou  $x$  se nazývá *výskyt proměnné  $x$  ve  $\varphi$* . Proměnná  $x$  se *vyskytuje* ve  $\varphi$ , pokud má ve  $\varphi$  aspoň jeden výskyt.
- Výskyt proměnné  $x$  ve  $\varphi$  se nazývá *vázaný*, pokud se na cestě od tohoto výskytu směrem ke kořenu stromu  $\mathfrak{t}_\varphi$  nachází uzel označený  $\forall x$ .
- Pokud není výskyt proměnné  $x$  ve  $\varphi$  vázaný, pak jej nazýváme *volný výskyt*. Výrazem  $\varphi(x_1, \dots, x_k)$  označujeme fakt, že  $\varphi$  je formule a všechny proměnné vyskytující se volně ve  $\varphi$  jsou mezi  $x_1, \dots, x_k$ .

Všechny předchozí pojmy se obvykle zavádějí bez pomoci stromů reprezentujících formule (viz učební materiály pro srovnání). Jako cvičení si můžete prokázat, že je to vskutku totéž.

### Příklad.

63. Určete volné a vázané výskyty proměnných v následujících formulích.

$$\begin{array}{ll} \neg(\forall y)\neg r(y, p(y)), & (\forall x)(\forall y)(r(x, y) \Rightarrow \neg r(y, x)), \\ (\forall x)y \approx k(x, x) \Rightarrow \neg x \approx 1, & (\forall x)(r(x, y, z) \Rightarrow (\forall z)k(x, z) \approx y). \end{array}$$

### Řešení.

Ve formuli  $\neg(\forall y)\neg r(y, p(y))$  se vyskytuje pouze proměnná  $y$ , která má dva výskyty a oba dva jsou vázané. Ve formuli  $(\forall x)(\forall y)(r(x, y) \Rightarrow \neg r(y, x))$  se vyskytují proměnné  $x$  a  $y$  a všechny jejich výskyty jsou rovněž vázané. Ve formuli  $(\forall x)y \approx k(x, x) \Rightarrow \neg x \approx 1$  má proměnná  $y$  jeden volný výskyt. Proměnná  $x$  má tři výskyty, z nichž dva výskyty jsou vázané (výskyty v podformuli  $y \approx k(x, x)$ ) a jeden je volný (výskyt v podformuli  $x \approx 1$ ). Proměnná  $x$  má tedy v této formuli volný i vázaný výskyt. Konečně ve formuli  $(\forall x)(r(x, y, z) \Rightarrow (\forall z)k(x, z) \approx y)$  se vyskytují proměnné  $x, y$  a  $z$ . Proměnná  $x$  má dva vázané výskyty, proměnná  $y$  má dva volné výskyty a  $z$  má jeden vázaný a jeden volný výskyt.

### Poznámka.

V některých materiálech se lze setkat s poněkud odlišnou definicí pojmu *vázaná proměnná*: pokud je  $(\forall x)\psi$  podformulí formule  $\varphi$ , pak je  $x$  ve  $\varphi$  vázaná. Podle této definice je například  $x$  ve formuli  $(\forall x)r(y, z)$  vázaná, v našem pojetí však nikoliv – zdůvodněte proč.

Formule  $\varphi$  se nazývá *uzavřená*, pokud  $\varphi$  neobsahuje volný výskyt žádné proměnné. Ke každé formuli  $\varphi(x_1, \dots, x_n)$  zpravidla uvažujeme její *univerzální uzávěr*  $\bar{\varphi}$ , což je formule tvaru  $(\forall x_1) \dots (\forall x_n)\varphi$ . Formule  $\varphi$  se nazývá *otevřená*, pokud neobsahuje žádný kvantifikátor. Otevřenost a uzavřenost formule se *vzájemně nevylučují*. Například uvažujeme-li jazyk typu  $\langle R, F, \sigma \rangle$ , kde  $F = \{c\}$  a  $R = \{r\}$ ,  $\sigma(c) = 0$ ,  $\sigma(r) = 1$ , pak  $r(c)$  je atomická formule, která je uzavřená i otevřená – zdůvodněte proč.

Dále zavedme označení  $\text{var}(t)$  pro množinu všech proměnných v termu  $t$ , to jest

$$\text{var}(t) = \begin{cases} \{x\} & \text{je-li } t \text{ proměnná } x, \\ \text{var}(t_1) \cup \dots \cup \text{var}(t_n) & \text{je-li } t \text{ tvaru } f(t_1, \dots, t_n). \end{cases}$$

O správnosti definice se přesvědčte strukturální indukcí. Je obvyklé chápat zápis  $t(x_1, \dots, x_k)$  jako zkratku za fakt, že  $t$  je term a  $\text{var}(t) \subseteq \{x_1, \dots, x_k\}$ .

Mějme formuli  $\varphi$ , term  $t$  a proměnnou  $x$ . Term  $t$  je *substituovatelný za proměnnou  $x$  do formule  $\varphi$* , pokud se žádný volný výskyt proměnné  $x$  ve  $\varphi$  nevyskytuje volně v žádné formuli tvaru  $(\forall y)\psi$ , kde  $(\forall y)\psi$  je podformule  $\varphi$  a  $y \in \text{var}(t)$ .

Jinými slovy, je-li  $t$  substituovatelný za  $x$  do  $\varphi$ , pak nahradíme-li každý volný výskyt proměnné  $x$  ve  $\varphi$  termem  $t$ , pak *všechny nové výskyty proměnných z množiny  $\text{var}(t)$  ve formuli vzniklé nahrazením budou volné*. Každá proměnná je substituovatelná za sebe samu do libovolné formule (zdůvodněte).

Pro formuli  $\varphi$ , proměnnou  $x$  a term  $t$  označujeme  $\varphi(x/t)$  formuli, která vznikne nahrazením všech volných výskytů proměnné  $x$  ve formuli  $\varphi$  termem  $t$ . Formule  $\varphi(x/t)$  se nazývá *výsledek substituce termu  $t$  za proměnnou  $x$  ve formuli  $\varphi$* . Samotná dvojice  $(x/t)$  se někdy nazývá *substituce*.

**Příklady.**

64. Rozhodněte, zda-li jsou termy  $k(x, x)$ ,  $k(k(x, z), z)$  a  $k(x, y)$  substituovatelné do formule

$$(\forall z)r(x, 1) \Rightarrow (\forall y)(r(y, z) \Rightarrow \neg r(k(x, y), y)),$$

za proměnné  $x, y, z$ .

**Řešení.**

Nejprve si všimněte, že libovolný term je substituovatelný za  $y$  do předchozí formule, protože  $y$  nemá v této formuli žádný volný výskyt.

Term  $k(x, x)$  je substituovatelný za  $x$  (term  $k(x, x)$  obsahuje pouze proměnnou  $x$ ), i za  $z$  (volný výskyt  $z$  není obsažen v žádné podformuli tvaru  $(\forall x)\psi$ ). Term  $k(k(x, z), z)$  není substituovatelný za proměnnou  $x$ , protože  $x$  má volný výskyt v podformuli  $(\forall z)r(x, 1)$ . Dále  $k(k(x, z), z)$  je substituovatelný za  $z$ , protože volný výskyt  $z$  není v rozsahu kvantifikátorů  $(\forall x)$  ani  $(\forall z)$ . Term  $k(x, y)$  není substituovatelný ani za  $x$  ani za  $z$  – zdůvodněte proč.

65. Pro následující formule určete výsledky substituce  $(x/f(x, y))$ .

$$r(x) \Rightarrow (\forall x)\neg r(x), \quad \neg z \approx f(z, z) \Rightarrow r(z), \quad r(x, x) \Rightarrow (\forall y)r(x, y).$$

**Řešení.**

Všimněte si, že v prvních dvou formulích je term  $f(x, y)$  substituovatelný za proměnnou  $x$ , ale ve třetím případě tomu tak není.

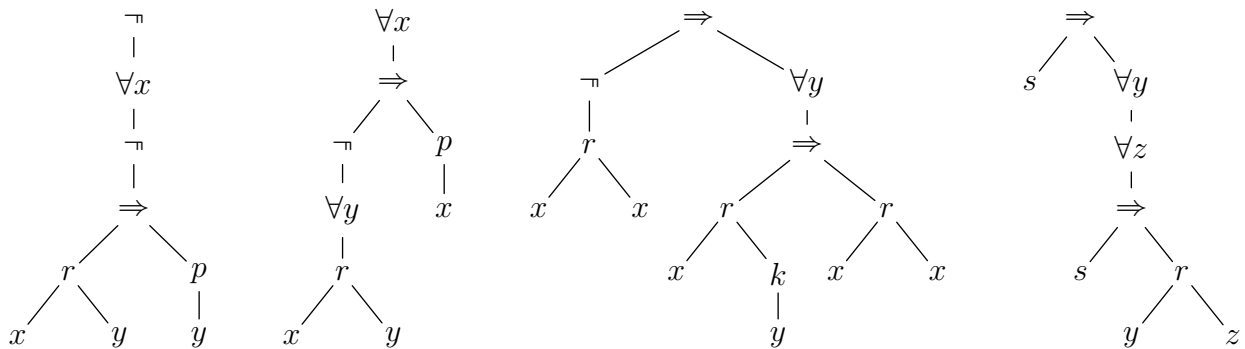
$$r(f(x, y)) \Rightarrow (\forall x)\neg r(x), \quad \neg z \approx f(z, z) \Rightarrow r(z), \quad r(f(x, y), f(x, y)) \Rightarrow (\forall y)r(f(x, y), y).$$

**Cvičení.**

66. Následující formule vyjádřete příslušnými uzlově ohodnocenými stromy.

$$\begin{aligned} r(x) \Rightarrow \neg(\forall x)\neg r(x), \quad (\forall x)(r(x) \Rightarrow (\forall y)y \approx k(x)), \quad x \approx f(x, y) \Rightarrow g(y, x) \approx x, \\ \neg(\forall x)(r(x) \Rightarrow r(c)), \quad f(c) \approx f(x) \Rightarrow (\forall x)r(x), \quad \neg(\forall x)\neg(\forall y)r(x, y) \Rightarrow (\forall y)\neg(\forall x)\neg r(x, y). \end{aligned}$$

Následující uzlově ohodnocené stromy vyjádřete formulemi.



67. Pro formule z předchozího příkladu určete výskyty všech proměnných. Dále rozhodněte, které z formulí z předchozího příkladu jsou otevřené a které jsou uzavřené.

68. Rozhodněte, zda-li jsou termy  $x$ ,  $p(x, y)$ ,  $p(y, p(x, z))$  a  $z + 1$  substituovatelné za proměnné  $x, y, z$  do následujících formulí. V případě že jsou, napište výsledky substitucí.

$$\begin{aligned} r(x) \Rightarrow \neg(\forall x)(\forall z)\neg r(x), \quad (\forall z)(r(y) \Rightarrow x \approx z), \quad \neg r(x, y) \Rightarrow (x \approx y \Rightarrow r(y, x)), \\ f(x) \approx x \Rightarrow (\forall z)f(x) \approx x, \quad (\forall x)(\forall y)(s \Rightarrow (\forall z)r(x, y, z)), \quad (\forall z)f(x) \approx k(x, z) \Rightarrow (\forall x)r(z). \end{aligned}$$

## Slovní popis a formule

Predikátová logika slouží k vyšetřování vztahů mezi jednotlivými objekty – individui. Před zahájením popisu konkrétní problémové domény musíme vždy zvolit *jazyk* a formulovat dostatek předpokladů, které budou tvořit zkoumanou *teorii*. V této teorii se zpravidla snažíme dokázat platnost tvrzení, případně nějaká tvrzení vyvrátit. Mnohdy jsou předpoklady tvořící teorii konstruovány ze slovního popisu. To jest je potřeba zvládnout vytváření formulí pouze na základě slovního popisu. Na začátek podotkneme, že metody formalizace slovního popisu, to jest metody návrhu jazyka a hledání vhodných formulí odpovídajících slovnímu popisu, nejsou přímo studovány *matematickou logikou*, která se snaží idealisovat a formalizovat usuzování. Návrh formulí může být naproti tomu věcí subjektivního hodnocení problémové domény, místy může hraničit s filosofií a podobně.

V první řadě je nutné uvědomit si, jaký je rozdíl mezi *termy* a *formulemi*. Jedním slovem – značný. Termy slouží k označování individuí, kdežto formule reprezentují výpovědi o vztazích a vlastnostech individuí označovaných termy. Oba pojmy nelze v žádném případě míchat nebo volně zaměňovat. V následujícím textu je postupně rozebrána formalizace slovního popisu, od návrhu termů až ke kvantifikovaným formulím.

### Proměnné, funkční symboly a termy.

*Proměnné* zastupují jednotlivá individua. Zde ovšem zdůrazníme, že dvě různé proměnné  $x, y$  mohou zastupovat totéž individuum. Složené *termy* vyjadřují rovněž individua, konkrétně *vyjadřují individua z jiných individuí*. Příkladem jsou obraty typu „bratrovo auto“, „včerejší oběd“, „přepona pravoúhlého trojúhelníka o stranách  $x, y$  a  $z$ “, „druhá mocnina  $x$ “ a podobně. Na *funkční symboly* se lze dívat jako na *jména*, která pojmenovávají funkční závislost mezi individui. Ve slovním popisu jsou individua zastoupena *podstatnými jmény – substantivy*, nebo *jmennými vazbami*.

Po rozlišení jednotlivých individuí obsažených ve slovním popisu a po klasifikaci jejich vzájemné funkční závislosti můžeme stanovit všechny funkční symboly, které se v daném jazyku budou vyskytovat. Speciální roli zde hrají *konstanty – nulární funkční symboly*, které označují jednotlivá individua. Na rozdíl od proměnných je však interpretace konstant dána na sémantické úrovni pouze strukturou, konkrétní ohodnocení proměnných nemá na interpretaci konstant vliv.

### Příklady.

69. V následujících větách nalezněte individua, funkční závislosti a tato individua formalizujte pomocí termů.

- (a) „Cigaretový kouř je nezdravý.“
- (b) „Rychlost kamarádova auta je v dešti nízká.“
- (c) „Součet vnitřních úhlů trojúhelníka je  $180^\circ$ “.

### Řešení.

- (a) V prvním případě je zřejmě individuem „kouř“. Otevřenou otázkou ale je, zda-li bychom měli chápat slovní spojení „cigaretový kouř“ jako vyjádření funkční závislosti, či nikoliv. To, že kouř je cigaretový, bychom mohli také chápat jako *vlastnost*, nikoliv funkční závislost.

V případě, že bychom potřebovali mít tento fakt vyjádřený funkční závislostí, měli bychom uvažovat funkční symboly  $F = \{\text{kouř}, \text{cigareta}\}$ , kde  $\sigma(\text{kouř}) = 1$ ,  $\sigma(\text{cigareta}) = 0$ . Funkční symbol *cigareta* je nulární, jedná se tudíž o *konstantu*. Funkční symbol *kouř* je unární, term tvaru *kouř*( $x$ ) chápeme jako vyjádření: „Kouř objektu  $x$ “. Term vyjadřující slovní spojení „cigaretový kouř“ by pak měl tvar *kouř*(*cigareta*). Tento term je uzavřený, neobsahuje žádnou proměnnou.

Další slovní obrat vyskytující se ve větě je „býti nezdravý“. Tento obrat nerepresentuje žádné individuum ani nepopisuje žádnou funkční závislost, to jest neformalizujeme jej termem.

- (b) V tomto případě se nabízí formalizovat termem sousloví „rychlost kamarádova auta v dešti“. Individuum označující rychlost je v tomto případě závislé na dvou argumentech – na vozidle a na podmínkách jeho provozu. Sousloví „kamarádovo auto“ pak můžeme vyjádřit analogicky jako sousloví „cigaretový kouř“ v předchozím příkladě. To jest položíme  $F = \{\text{rychlost}, \text{auto}, \text{kamarád}, \text{dešť}\}$ , kde  $\sigma(\text{kamarád}) = \sigma(\text{dešť}) = 0$ ,  $\sigma(\text{auto}) = 1$  a  $\sigma(\text{rychlost}) = 2$ . V následující tabulce jsou uvedeny termy a jejich význam.

<i>kamarádovo auto</i>	$\text{auto}(\text{kamarád}),$
<i>rychlost <math>x</math> v dešti</i>	$\text{rychlost}(x, \text{dešť}),$
<i>rychlost kamarádova auta v dešti</i>	$\text{rychlost}(\text{auto}(\text{kamarád}), \text{dešť}),$

Množinu funkčních symbolů bychom mohli zjednodušit. Například „kamarádovo auto“ bychom mohli označit jednou konstantou a podobně. Návrh jazyka a míru zjednodušení je vždy nutné pečlivě zvážit. Slovní spojení „být nízký“, které se ve větě vyskytuje, vyjadřuje vlastnosti (v tomto případě vlastnost individua reprezentující rychlost onoho vozidla za deště), takže se nejedná o individuum a vazbu proto neformalizujeme termem.

- (c) Zde můžeme popsat termem vazbu „součet vnitřních úhlů trojúhelníka“. Metod, kterak tohoto cíle dosáhnout je samozřejmě více. Je například možné zavést binární funkční symbol pro „sčítání“ a vyjádřit součet pomocí něj. Konkrétně, když položíme  $F = \{+\}$ ,  $\sigma(+) = 2$ , pak například termem  $+(+(x, y), z)$  vyjádříme požadovanou funkční závislost. Na úrovni termů však nemáme nijak zachyceno, že  $x$ ,  $y$  a  $z$  jsou strany trojúhelníka. Důležité je také uvědomit si, že pouhou definicí funkčního symbolu „+“ samozřejmě nijak nezajistíme „žádné očekávané vlastnosti sčítání“. Druhou možností, jak vyjádřit sčítání, je zavedení ternárního funkčního symbolu. Například pro  $F = \{\text{součet\_tří}\}$ ,  $\sigma(\text{součet\_tří}) = 3$  bychom mohli předchozí fakt vyjádřit termem  $\text{součet\_tří}(x, y, z)$ . Dalším individuem může být velikost úhlu  $180^\circ$ , i když opět ji můžeme chápat jako vlastnost „mít velikost  $180^\circ$ “.

## Cvičení.

70. V následujících větách se snažte vytipovat individua a jejich funkční závislosti. Proved'te diskusi.

„*S cizí ženou v cizím pokoji.*“

„*Pes, který šteká, nekouše.*“

„*Někteří ptáci nemohou létat.*“

„*Někteří lidé mají rádi jen sami sebe.*“

## Relační symboly a formule.

V předchozí ukázce jsme mohli vidět, že termy samy o sobě nedokážou popsat vlastnosti individuí nebo jejich vzájemné vztahy. K tomuto účelu slouží formule. Vlastnosti a vztahy jsou ve slovním popisu obvykle popisovány *přídavnými jmény* a *slovesnými vazbami*. *Relační symboly* zde mají úlohu *jmen*, která označují *jména vlastností a vztahů*. Množinu relačních symbolů můžeme stanovit ze slovního popisu jako množinu všech vlastností a vztahů, které se v daném popisu vyskytují. *Formule* pak zastupují jednotlivá sdělení, to jest na slovní úrovni mohou odpovídat větám nebo částem souvětí. Z jednotlivých formulí pak mohou být vytvářeny formule složitější pomocí spojek, což koresponduje s intuitivní představou skládání vět do souvětí. Uveďme si opět příklad.

## Příklady.

71. Navrhněte jazyk a následující tvrzení formalizujte formulími.

- (a) „Ptáci, kteří nelétají, umějí rychle běhat.“
- (b) „Čím více má člověk peněz, tím je šťastnější.“

## Řešení.

- (a) V textu se vyskytují vlastnosti „létat“ a „býti ptákem“. Sousedství „rychle běhat“ můžeme chápat jako atomickou vlastnosti, nebo jako vyjádření, že „rychlost běhu je velká“. V druhém případě ovšem musíme specifikovat funkční závislost mezi individuem a jeho rychlostí. Rozebereme postupně oba dva přístupy.

Mějme jazyk typu  $\langle R, \emptyset, \sigma \rangle$ , kde  $R = \{pták, létat, rychle\_běhat\}$ , přitom  $\sigma(r) = 1$  pro každý  $r \in R$ . Nyní můžeme požadovaný fakt vyjádřit formulí

$$(pták(x) \wedge \neg létat(x)) \Rightarrow rychle\_běhat(x).$$

Předchozí formule není jediná možná. Jelikož je  $(p \Rightarrow (q \Rightarrow r)) \Leftrightarrow ((p \wedge q) \Rightarrow r)$  tautologie výrokového počtu, pak principem dosazení do této tautologie dostáváme jedno z mnoha ekvivalentních vyjádření předchozí formule,

$$pták(x) \Rightarrow (\neg létat(x) \Rightarrow rychle\_běhat(x))$$

Uvažujme nyní jazyk typu  $\langle R, F, \sigma \rangle$ , kde  $F = \{rychlost\}$ ,  $R = \{pták, létat, rychlý\}$  a dále nechť  $\sigma(rychlost) = 1$  a  $\sigma(r) = 1$  pro každý  $r \in R$ . Pak můžeme požadovaný fakt vyjádřit například formulí v tomto tvaru,

$$pták(x) \Rightarrow (\neg létat(x) \Rightarrow rychlý(rychlost(x))).$$

přitom term  $rychlost(x)$  čteme jako „rychlost objektu  $x$ “. Příklad bychom mohli dále precisovat, například pojem „být rychlý“ může být chápán kontextově. V tomto případě by stačilo uvažovat relační symbol  $rychlý$  jako označení pro binární vztah „objekt  $x$  je při své rychlosti  $y$  rychlý“.

- (b) V tomto případě lze postupovat analogicky jako v předchozím. Nejprve ukážeme formalizaci nepoužívající žádné funkční symboly. Mějme jazyk typu  $\langle R, \emptyset, \sigma \rangle$ , přitom máme  $R = \{člověk, mít\_více\_peněz, být\_šťastnější\}$  a  $\sigma(člověk) = 1$ , ostatní dva relační symboly jsou binární. Tvrzení formalizujeme následující formulí.

$$(člověk(x) \wedge člověk(y) \wedge mít\_více\_peněz(x, y)) \Rightarrow být\_šťastnější(x, y).$$

Při formalizaci můžeme uvažovat i tak, že pro dané individuum budeme vyjadřovat počet peněz, jakožto funkční závislost a oba počtu budeme klasifikovat pomocí speciálního relačního symbolu. Podrobněji, mějme jazyk typu  $\langle R, F, \sigma \rangle$ , kde  $F = \{peníze\}$  a  $R = \{menší, člověk, být\_šťastnější\}$ , přitom  $\sigma(peníze) = 1$  a  $\sigma(menší) = 2$ , arity ostatních symbolů jsou stejné jako u předchozího jazyka. Nyní můžeme vyjádřit

$$(člověk(x) \wedge člověk(y) \wedge menší(peníze(y), peníze(x))) \Rightarrow být\_šťastnější(x, y).$$

U relačních symbolů s aritou vyšší jak 1 musíme dodržovat smluvené pořadí argumentů, evidentní je to například u vztahů typu „ $x$  je otcem  $y$ “ a podobně.

**Kvantifikace.**

Vyskytují-li se ve slovním popisu vazby jako „všichni (ne)jsou . . .“, „někteří (ne)jsou, . . .“ a podobně, při vytváření formulí bychom měli vhodně použít kvantifikátory. Některá ustálená slovní spojení, například „všechna  $A$  jsou  $B$ “, mají svoje specifická vyjádření. Uvažujme nyní dvě formule  $\varphi(x)$ ,  $\psi(x)$  s volnou proměnnou  $x$ , vyjadřující dvě vlastnosti.

V následujícím přehledu jsou uvedeny typické přepisy ustálených obrátů. U některých obrátů je uvedeno několik ekvivalentních přepisů.

Každé $\varphi$ je $\psi$ .	$(\forall x)(\varphi(x) \Rightarrow \psi(x))$
Žádné $\varphi$ není $\psi$ .	$(\forall x)(\varphi(x) \Rightarrow \neg\psi(x)), \quad (\forall x)\neg(\varphi(x) \wedge \psi(x)), \quad \neg(\exists x)(\varphi(x) \wedge \psi(x))$
Některá $\varphi$ jsou $\psi$ .	$(\exists x)(\varphi(x) \wedge \psi(x)), \quad \neg(\forall x)(\varphi(x) \Rightarrow \neg\psi(x))$
Některá $\varphi$ nejsou $\psi$ .	$(\exists x)(\varphi(x) \wedge \neg\psi(x)), \quad (\exists x)\neg(\varphi(x) \Rightarrow \psi(x)), \quad \neg(\forall x)(\varphi(x) \Rightarrow \psi(x))$

Za pozornost stojí přepis obrátu „někteřá  $\varphi$  jsou  $\psi$ “. Intuitivně by se mohlo zdát, že bychom ve formuli měli použít implikaci místo konjunkce. Při bližším pohledu je ale jasné, že formule  $\vartheta$  tvaru  $(\exists x)(\varphi(x) \Rightarrow \psi(x))$  by *neměla požadovaný význam*. Snadno totiž můžeme najít model, ve kterém „žádné  $\varphi$  není  $\psi$ “ ale formule  $\vartheta$  je v tomto modelu pravdivá – to jest formule nevystihuje požadovaný fakt, že „někteřá  $\varphi$  jsou  $\psi$ “.

**Zdůvodnění.**

Uvažujme jazyk typu  $\langle R, \emptyset, \sigma \rangle$  se dvěma relačními symboly  $R = \{r, s\}$ ,  $\sigma(r) = \sigma(s) = 1$  a strukturu tohoto jazyka  $\mathbf{M} = \langle M, \{r^{\mathbf{M}}, s^{\mathbf{M}}\}, \emptyset \rangle$ , kde  $M = \{a, b\}$  a relace  $r^{\mathbf{M}}, s^{\mathbf{M}}$  jsou definovány předpisy  $r^{\mathbf{M}} = \{a\}$ ,  $s^{\mathbf{M}} = \{b\}$ . Nyní můžeme chápat  $\varphi$  jako atomickou formuli  $r(x)$  a  $\psi$  jako atomickou formuli  $s(x)$ . Snadno nahlédneme, že ve struktuře  $\mathbf{M}$  žádné  $\varphi$  není  $\psi$ , protože v ohodnocení  $v$ , kde  $v(x) = a$  máme  $\|\varphi\|_{\mathbf{M},v} = 1$ , ale  $\|\psi\|_{\mathbf{M},v} = 0$ . Na druhou stranu, v ohodnocení  $w$ , kde  $w(x) = b$  máme  $\|\varphi\|_{\mathbf{M},v} = 0$ , to jest  $\|\varphi \Rightarrow \psi\|_{\mathbf{M},v} = 1$ , tedy  $\|(\exists x)(\varphi \Rightarrow \psi)\|_{\mathbf{M}} = 1$ . To jest formule  $(\exists x)(\varphi(x) \Rightarrow \psi(x))$  dobře nevystihuje slovní obrát „někteřá  $\varphi$  jsou  $\psi$ “.

**Příklady.**

72. (a) „Všichni studenti, kromě Petra, jsou pilní.“  
 (b) „Každý muž má otce, pokud je navíc sám otcem, jeho otec je dědečkem.“  
 (c) „Každé racionální číslo lze vyjádřit zlomkem.“  
 (d) „Existuje přirozené číslo, které je větší než všechna ostatní přirozená čísla.“  
 (e) „Číslo je sudé, právě když je rovno nule nebo je následovníkem lichého čísla.“

**Řešení.**

- (a) Nejprve navrhne jazyk. V popisu se vyskytují dvě vlastnosti, „býti student“ a „býti pilný“. Speciálním individuem je „Petr“. To jest uvažujme jazyk s rovností  $\approx$  typu  $\langle R, F, \sigma \rangle$ , kde  $F = \{petr\}$ ,  $R = \{pilný, student\}$ , přitom  $\sigma(petr) = 0$ . Pro relační symboly máme  $\sigma(pilný) = \sigma(student) = 1$ . Tvzení můžeme formalizovat následovně,

$$(\forall x)((student(x) \wedge \neg x \approx petr) \Rightarrow pilný(x)).$$

Mohli bychom rovněž uvažovat  $F = \emptyset$ , jazyk bez rovnosti a vlastnost „býti Petrem“, to jest  $R = \{pilný, student, je\_petr\}$ , kde  $\sigma(je\_petr) = 1$ . Potom bychom mohli tvrzení vyjádřit

$$(\forall x)((student(x) \wedge \neg je\_petr(x)) \Rightarrow pilný(x)).$$

Rozdíl proti předchozí formalizaci je v tom, v druhém případě obecně do úvah o interpretaci formule zahrnujeme i struktury, ve kterých nebude žádné nebo víc individuí

s vlastností *je\_petr*. U předchozí formalizace se jednalo vždy právě o jedno individuum, které bylo označeno konstantou. Na konec podotkněme, že předchozí tvrzení bychom mohli vyjádřit ekvivalentně i bez použití universálního kvantifikátoru.

- (b) V tomto případě budeme používat jazyk bez rovnosti. V popisu se vyskytují dvě vlastnosti „býti mužem“ a „býti dědečkem“. Vztah „býti otcem“ je přitom *binární*, to jest jedná se o vztah „ $x$  je otcem  $y$ “. Uvažujme tedy jazyk typu  $\langle R, \emptyset, \sigma \rangle$ , kde  $R = \{\text{muž}, \text{dědeček}, \text{otec}\}$  a  $\sigma(\text{muž}) = \sigma(\text{dědeček}) = 1$ ,  $\sigma(\text{otec}) = 2$ . Rozeberme tvrzení po částech, fakt „každý muž má otce“ lze zapsat formulí

$$(\forall x)(\text{muž}(x) \Rightarrow (\exists y)\text{otec}(y, x)),$$

formuli bychom mohli zkrátit i na  $(\forall x)(\exists y)\text{otec}(y, x)$ . Pokud bychom ovšem navrhovali jazyk pro vyšetřování vztahů různých individuí, mezi nimiž by byli muži (dále třeba ženy, auta a dýmky), pak bychom měli předpoklad  $\text{muž}(x)$  zachovat. Formalizace celého tvrzení může být následující,

$$(\forall x)(\text{muž}(x) \Rightarrow (\exists y)(\text{otec}(y, x) \wedge ((\exists z)\text{otec}(x, z) \Rightarrow \text{dědeček}(y))))).$$

Vázaná proměnná  $z$  ve formuli označuje individuum, které je potomkem individua  $x$ . Zároveň proměnná  $y$  označuje individuum, které je otcem individua  $x$ , to jest individuu označovanému  $y$  lze přiřadit vlastnost „býti dědečkem“. Formuli lze opět ekvivalentně vyjádřit i bez kvantifikace proměnné  $x$ .

- (c) Proto, abychom formalizovali tvrzení (c) nemusíme nutně budovat aritmetiku, dokonce ani nemusíme axiomaticky popisovat vlastnosti čísel. Stačí když budeme uvažovat vlastnost „býti racionální číslo“ a zavedeme označení pro individuum, které vznikne z čitatele a jmenovatele – z tohoto pohledu jde o funkční závislosti individuí, nikoliv o vlastnost. Podrobněji, uvažujme jazyk s rovností  $\approx$  typu  $\langle R, F, \sigma \rangle$ , kde  $F = \{\text{zlomek}\}$ ,  $R = \{\text{racionální}\}$  a  $\sigma(\text{racionální}) = 1$ ,  $\sigma(\text{zlomek}) = 2$ . Nyní můžeme uvažovat formuli

$$\text{racionální}(x) \Rightarrow (\exists y)(\exists z) x \approx \text{zlomek}(x, y),$$

která vystihuje popsany fakt.

- (d) Formalizace tohoto příkladu je velmi jednoduchá. Nenechte se prosím zmást, tím, že tvrzení je „proti intuici“. My nezkoumáme jeho obsah či snad pravdivost, pouze jej formalizujeme formulí. Struktury, ve kterých bude tato formule pravdivá, nemusejí svými vlastnostmi korespondovat s našimi představami o vlastnostech přirozených číslech. Můžeme uvažovat jazyk s rovností  $\approx$  typu  $\langle R, \emptyset, \sigma \rangle$ , kde  $R = \{\text{číslo}, \text{menší}\}$ , kde  $\sigma(\text{číslo}) = 1$ ,  $\sigma(\text{menší}) = 2$ . Nyní máme formuli,

$$(\exists x)(\text{číslo}(x) \wedge (\forall y)((\text{číslo}(y) \wedge \neg y \approx x) \Rightarrow \text{menší}(y, x))).$$

V předchozí formuli nelze vynechat universální kvantifikaci  $(\forall y)$ , pokuste se zdůvodnit proč. Poznamenejme, že s využitím věty o kompaktnosti PP lze dokázat, že skutečně existuje model axiomatizované aritmetiky (Peanovy aritmetiky), ve kterém existuje individuum, které je ostře větší než všechna ostatní. Tomuto modelu se říká *nestandardní model aritmetiky*.



- (e) Při práci s *aritmetikou* se často zavádí konstanta 0 a unární funkční symbol  $s$ , který má význam „následovníka“. Pracujeme tedy s jazykem, kde  $\{0, s\} \subseteq F$ ,  $\sigma(0) = 0$  a  $\sigma(s) = 1$ . Term 0 můžeme chápat jako označení pro nulu, term  $s(0)$  pro jedničku (následník nuly),  $s(s(0))$  pro dvojku a tak podobně. Reprezentace přirozených čísel pomocí složených termů se využívá například v logických programovacích jazycích, které nemají zabudovanou vlastní implementaci aritmetiky.

Pro naše účely formalizace tvrzení z bodu (e) zvolíme jazyk  $\langle R, F, \sigma \rangle$  s rovností  $\approx$  tak, že  $F = \{0, s\}$ ,  $R = \{sudé, liché\}$ , kde  $\sigma(0) = 0$ ,  $\sigma(s) = 1$  a  $\sigma(sudé) = \sigma(liché) = 1$ . Nyní můžeme tvrzení formalizovat následující formulí.

$$sudé(x) \Leftrightarrow (x \approx 0 \vee (\exists y)(x \approx s(y) \wedge liché(y))).$$

Za pozornost stojí vyjádření obratu „je následovníkem lichého čísla“. V předchozí ukázce jsme jej vyjádřili podformulí  $(\exists y)(x \approx s(y) \wedge liché(y))$ . Jinými slovy,  $x$  je následovníkem lichého čísla, právě když existuje liché  $y$  takové, že  $x$  je rovno  $s(y)$ .

### Cvičení.

73. Navrhněte jazyk a formalizujte slovně popsaná tvrzení formulemi.

- „Nejlepší programovací jazyk je Scheme.“
- „Čím jsou programy větší, tím více obsahují chyb.“
- „Nad jednoprvkovou abecedou existuje jazyk, který není regulární.“
- „Tučňáci kladou nejvýš jedno vejce za rok.“
- „Každý bezkontextový jazyk je přijímán některým nedeterministickým zásobníkovým automatem, ale ne každý bezkontextový jazyk je přijímán nějakým deterministickým zásobníkovým automatem.“

74. Uvažujme jazyk s rovností, kde  $F = \{matka/1, otec/1\}$ ,  $R = \{člověk/1, muž/1, manžel/2\}$ , arita symbolů je pro jednoduchost značena jako číslo za lomítkem. Funkční symboly budeme interpretovat jako „matka/otec daného individua“, relační symboly *člověk* a *muž* označují vlastnosti individuí a konečně *manžel* je binární vztah „ $x$  je manželem  $y$ “.

Přečtete následující formule. Pokud mají formule *volné proměnné*, lze je chápat jako vyjádření odvozených vlastností individuí, které jsou vyjádřené ze základních vlastností pojmenovaných relačními symboly. Zkuste tyto vlastnosti slovně vyjádřit.

$$(\forall x)(muž(x) \Rightarrow člověk(x)), \quad člověk(x) \wedge \neg muž(x), \quad člověk(x) \Rightarrow muž(otec(x)), \\ manžel(x, y) \Rightarrow \neg manžel(y, x), \quad manžel(x, y) \wedge (\exists z)otec(z) \approx x, \quad x \approx matka(y) \Rightarrow muž(y).$$

75. Uvažujte jazyk z předchozího příkladu a pomocí formulí s volnými proměnnými zkuste vyjádřit následující vlastnosti lidí a rodinné vztahy.

- „býti sirotkem“,
- „nemít žádné sourozence“,
- „ $x$  a  $y$  jsou sourozenci“,
- „ $x$  je nevlastním sourozencem  $y$ “,
- „ $x$  je švagrem  $y$ “.

## Jazyky s rovností

V predikátové logice musíme s jazyky obsahujícími rovnost zacházet speciálním způsobem. Po rovnosti totiž požadujeme, aby byla v každém modelu realizována identickou relací na nosiči. Této vlastnosti ovšem nelze dosáhnout pouhou definicí dodatečných axiomů. Při úvahách o jazycích s rovností však přijímáme dodatečné *axiomy rovnosti*, které zaručují, že rovnost bude v každé struktuře realizována jako *relace ekvivalence*, která bude navíc *kompatibilní s funkcemi a relacemi* této struktury.

### Poznámka.

Při úvahách o jazycích s rovností lze přijmout buďto pět základních axiomových schémat, nebo pouze tři z nich a posléze ukázat, že zbylá dvě schémata jsou z nich plynoucí. Druhý přístup je úspornější z pohledu dalšího dokazování, pouhé tři axiomy však nejsou na první pohled příliš intuitivní. Základní tři axiomy mají tvar,

$$\begin{array}{ll} x \approx x & \text{reflexivita,} \\ (x_1 \approx y_1 \wedge \dots \wedge x_n \approx y_n) \Rightarrow f(x_1, \dots, x_n) \approx f(y_1, \dots, y_n) & \text{kompatibilita s operacemi} \\ (x_1 \approx y_1 \wedge \dots \wedge x_n \approx y_n \wedge r(x_1, \dots, x_n)) \Rightarrow r(y_1, \dots, y_n) & \text{kompatibilita s relacemi,} \end{array}$$

přitom  $x, y, z, x_1, y_1, \dots, x_n, y_n$  jsou proměnné,  $f$  je  $n$ -ární funkční symbol a  $r$  je  $n$ -ární relační symbol. Z předchozích tří axiomů plynou dva následující,

$$\begin{array}{ll} x \approx y \Rightarrow y \approx x & \text{symetrie,} \\ (x \approx y \wedge y \approx z) \Rightarrow x \approx z & \text{transitivita,} \end{array}$$

### Příklady.

76. Dokažte, že axiomy *symetrie* a *transitivity* plynou z axiomů reflexivity a kompatibility.

#### Řešení.

Jednoduché, ale důležité pozorování je, že symbol pro rovnost  $\approx$  je binární relační symbol. To jest axiomové schéma kompatibility s relacemi můžeme aplikovat i pro  $r$  rovno  $\approx$ . Nyní prokážeme symetrii,

$$\begin{array}{ll} \vdash (x \approx y \wedge x \approx x \wedge \approx(x, x)) \Rightarrow \approx(y, x) & \text{instance axiomu kompatibility pro } r \text{ rovno } \approx, \\ \vdash (x \approx x \wedge x \approx x) \Rightarrow (x \approx y \Rightarrow y \approx x) & \text{tautologie výrokového počtu a modus ponens,} \\ \vdash x \approx y \Rightarrow y \approx x & \text{axiom reflexivity, modus ponens.} \end{array}$$

V důkazu byl použit princip dosazení do tautologie VP  $((p \wedge q) \Rightarrow r) \Rightarrow (q \Rightarrow (p \Rightarrow r))$ . Nyní s pomocí dokázané symetrie ukážeme transitivitu,

$$\begin{array}{ll} \vdash (y \approx x \wedge y \approx z \wedge \approx(y, y)) \Rightarrow \approx(x, z) & \text{instance kompatibility pro } r \text{ rovno } \approx, \\ \vdash y \approx y \Rightarrow ((y \approx x \wedge y \approx z) \Rightarrow x \approx z) & \text{tautologie VP a modus ponens,} \\ \vdash (y \approx x \wedge y \approx z) \Rightarrow x \approx z & \text{axiom reflexivity, modus ponens,} \\ \vdash (x \approx y \wedge y \approx z) \Rightarrow x \approx z & \text{symetrie, věta o ekvivalenci PP.} \end{array}$$

### Cvičení.

77. Dokažte, že axiomové schéma kompatibility s relacemi má následující ekvivalentní vyjádření,

$$(x_1 \approx y_1 \wedge \dots \wedge x_n \approx y_n) \Rightarrow (r(x_1, \dots, x_n) \Leftrightarrow r(y_1, \dots, y_n)).$$

## Kvantifikace

Následující řešené příklady a cvičení se věnují dokazatelnosti formulí s kvantifikátory. Při dokazování budeme používat větu o dedukci predikátového počtu a větu o konstantách. Připomeňme, že věta o dedukci má v PP omezený tvar, to jest pro libovolnou *uzavřenou formuli*  $\varphi$  a jakoukoliv formuli  $\psi$  platí  $\mathcal{T}, \varphi \vdash \psi$ , právě když  $\mathcal{T} \vdash (\varphi \Rightarrow \psi)$ .

Pomocí věty o konstantách můžeme omezení věty o dedukci „obejít“, pokud budeme *fixovat* všechny *volné proměnné* ve formuli  $\varphi$  *konstantami*. Přesněji řečeno, z věty o konstantách  $\mathcal{T} \vdash (\varphi \Rightarrow \psi)$  platí, právě když  $\mathcal{S} \vdash (\varphi(x_1/\mathbf{c}_1, \dots, x_n/\mathbf{c}_n) \Rightarrow \psi(x_1/\mathbf{c}_1, \dots, x_n/\mathbf{c}_n))$ , kde  $\mathcal{S}$  je teorie vzniklá z  $\mathcal{T}$  přidáním konstant  $\mathbf{c}_1, \dots, \mathbf{c}_n$ , ale bez přidání axiomů. Konstanty a jednotlivé proměnné  $x_1, \dots, x_n$  přitom můžeme zvolit tak, aby byla  $\varphi(x_1/\mathbf{c}_1, \dots, x_n/\mathbf{c}_n)$  uzavřená formule. To jest nyní z věty o dedukci

$$\mathcal{T} \vdash (\varphi \Rightarrow \psi), \text{ právě když } \mathcal{S}, \varphi(x_1/\mathbf{c}_1, \dots, x_n/\mathbf{c}_n) \vdash \psi(x_1/\mathbf{c}_1, \dots, x_n/\mathbf{c}_n).$$

Řečeno jinými slovy, k tomu abychom prokázali  $\mathcal{T} \vdash (\varphi \Rightarrow \psi)$  stačí ukázat, že z množiny předpokladů  $\mathcal{S}, \varphi(x_1/\mathbf{c}_1, \dots, x_n/\mathbf{c}_n)$  je dokazatelná formule  $\psi(x_1/\mathbf{c}_1, \dots, x_n/\mathbf{c}_n)$ . V tomto důkazu narozdíl od důkazu formule  $\psi$  z předpokladů  $\mathcal{T}, \psi$ , nemá smysl používat pravidlo generalisace přes proměnné  $x_1, \dots, x_n$ , jelikož ve  $\varphi(x_1/\mathbf{c}_1, \dots, x_n/\mathbf{c}_n)$  ani  $\psi(x_1/\mathbf{c}_1, \dots, x_n/\mathbf{c}_n)$  nemají volný výskyt.

### Příklad.

78. Dokažte následující dvě tvrzení,

- |  |                           |
|--|---------------------------|
| (i) $\mathcal{T} \vdash \varphi$ , právě když $\mathcal{T} \vdash \bar{\varphi}$ | věta o uzávěru,           |
| (ii) $\vdash \varphi \Rightarrow (\exists x)\varphi(x/t)$                        | duální forma specifikace, |

kde  $\varphi$  je libovolná formule,  $\bar{\varphi}$  je její *uzávěr* a term  $t$  je substituovatelný za  $x$  do  $\varphi$ .

### Řešení.

Pro tvrzení (i) nejprve ukážeme implikaci  $\Rightarrow$ . Nechť  $\mathcal{T} \vdash \varphi$ , pak jsou-li  $x_1, \dots, x_n$  právě všechny volné proměnné z formule  $\varphi$ , pak opakováním generalisace dostáváme  $\mathcal{T} \vdash (\forall x_1)\varphi$ ,  $\mathcal{T} \vdash (\forall x_2)(\forall x_1)\varphi$  až  $\mathcal{T} \vdash (\forall x_n) \dots (\forall x_2)(\forall x_1)\varphi$ . Ale  $(\forall x_n) \dots (\forall x_2)(\forall x_1)\varphi$  je právě uzávěr  $\bar{\varphi}$ . Opačně, mějme  $\mathcal{T} \vdash \bar{\varphi}$ , pak  $\bar{\varphi}$  je ve tvaru  $(\forall x_1)(\forall x_2) \dots (\forall x_n)\varphi$ . Opakovaným užitím specifikace a modus ponens dostáváme

$$\begin{aligned} \mathcal{T} &\vdash (\forall x_1)(\forall x_2) \dots (\forall x_n)\varphi \Rightarrow (\forall x_2) \dots (\forall x_n)\varphi, \\ \mathcal{T} &\vdash (\forall x_2) \dots (\forall x_n)\varphi \Rightarrow (\forall x_3) \dots (\forall x_n)\varphi, \\ &\vdots \\ \mathcal{T} &\vdash \varphi. \end{aligned}$$

Axiom specifikace jsme použili ve tvaru  $(\forall x)\varphi \Rightarrow \varphi(x/x)$ , libovolná proměnná  $x$  je triviálně substituovatelná za sebe samu. Zajímavým důsledkem věty o uzávěru je fakt, že teorie  $\mathcal{T}, \varphi$  a  $\mathcal{T}, \bar{\varphi}$  jsou ekvivalentní. Vskutku,  $\mathcal{T}, \varphi \vdash \varphi$ , tedy  $\mathcal{T}, \varphi \vdash \bar{\varphi}$ , analogicky  $\mathcal{T}, \bar{\varphi} \vdash \varphi$ . Při dokazování někdy využíváme tohoto faktu a říkáme, že můžeme bez újmy předpokládat, že všechny předpoklady z  $\mathcal{T}$  jsou uzavřené formule.

Nyní ukážeme (ii). Využijeme přitom axiom specifikace,

- |  |  |
|--|--|
| $\vdash (\forall x)\neg\varphi \Rightarrow \neg\varphi(x/t)$         | axiom specifikace,   |
| $\vdash \neg\neg\varphi(x/t) \Rightarrow \neg(\forall x)\neg\varphi$ | transposice implikace, modus ponens,                             |
| $\vdash \neg\neg\varphi(x/t) \Rightarrow (\exists x)\varphi$         | zkratka formule,   |
| $\vdash \varphi(x/t) \Rightarrow (\exists x)\varphi$                 | transitivita implikace a tautologie $p \Rightarrow \neg\neg p$ . |

V prvním kroku důkazu jsme využili jednoduchého pozorování, že je-li  $t$  je substituovatelný za  $x$  do  $\varphi$ , pak je i  $t$  substituovatelný za  $x$  do  $\neg\varphi$ .

### Poznámka.

Podmínka substituovatelnosti v duální formě specifikace je nutná. Uvažujme jazyk typu  $\langle R, \emptyset, \sigma \rangle$ , kde  $R = \{r\}$ ,  $\sigma(r) = 2$  a strukturu tohoto jazyka  $\mathbf{M} = \langle M, \{r^{\mathbf{M}}\}, \emptyset \rangle$ , kde  $M = \{a, b\}$  a relace  $r^{\mathbf{M}}$  je definována  $r^{\mathbf{M}} = \{\langle a, a \rangle, \langle b, b \rangle\}$ . Nyní  $(\forall y)r(x, y)$  je formule, ve které není term  $y$  substituovatelný za proměnnou  $x$ , protože po substituci by došlo k navázání  $y$ . Kdybychom tedy připustili duální formu specifikace v plném rozsahu, obdrželi bychom pro formuli  $(\forall y)r(x, y)$ , zkráceně označovanou  $\varphi$ , že platí  $\vdash \varphi(x/y) \Rightarrow (\exists x)\varphi$ , to jest  $\vdash (\forall y)r(y, y) \Rightarrow (\exists x)(\forall y)r(x, y)$ . Ve struktuře  $\mathbf{M}$  při libovolném ohodnocení  $v$  máme  $\|(\forall y)r(y, y)\|_{\mathbf{M},v} = 1$ , ale  $\|(\exists x)(\forall y)r(x, y)\|_{\mathbf{M},v} = 0$ . To jest dostali bychom se do sporu s větou o korektnosti.

### Příklad.

79. Dokažte následující dvě tvrzení o distribuci kvantifikace,

- (i)  $\vdash (\forall x)(\varphi \Rightarrow \psi) \Rightarrow ((\forall x)\varphi \Rightarrow (\forall x)\psi)$ ,
- (ii)  $\vdash (\forall x)(\varphi \Rightarrow \psi) \Rightarrow ((\exists x)\varphi \Rightarrow (\exists x)\psi)$ .

kde  $\varphi, \psi$  jsou libovolné formule.

### Řešení.

Nejprve ukážeme (i). Využijeme věty o konstantách a budeme předpokládat, že formule  $\varphi$  a  $\psi$  mají nejvýše jednu volnou proměnnou a to  $x$ . Ostatní volné proměnné můžeme „fixovat konstantami“. Potom budou formule  $(\forall x)(\varphi \Rightarrow \psi)$ ,  $(\forall x)\varphi$  uzavřené a budeme moci použít větu o dedukci.

$(\forall x)(\varphi \Rightarrow \psi), (\forall x)\varphi \vdash \varphi \Rightarrow \psi$	<i>specifikace a modus ponens,</i>
$(\forall x)(\varphi \Rightarrow \psi), (\forall x)\varphi \vdash \varphi$	<i>specifikace a modus ponens,</i>
$(\forall x)(\varphi \Rightarrow \psi), (\forall x)\varphi \vdash \psi$	<i>modus ponens,</i>
$(\forall x)(\varphi \Rightarrow \psi), (\forall x)\varphi \vdash (\forall x)\psi$	<i>generalisace,</i>
$\vdash (\forall x)(\varphi \Rightarrow \psi) \Rightarrow ((\forall x)\varphi \Rightarrow (\forall x)\psi)$	<i>dvakrát věta o dedukci.</i>

Pomocí předchozího důkazu dokážeme (ii). Opět předpokládáme, že  $\varphi$  a  $\psi$  nemají mimo  $x$  žádné jiné volné proměnné.

$(\forall x)(\varphi \Rightarrow \psi) \vdash \varphi \Rightarrow \psi$	<i>specifikace,</i>
$(\forall x)(\varphi \Rightarrow \psi) \vdash \neg\psi \Rightarrow \neg\varphi$	<i>transposice implikace,</i>
$(\forall x)(\varphi \Rightarrow \psi) \vdash (\forall x)(\neg\psi \Rightarrow \neg\varphi)$	<i>generalisace,</i>
$(\forall x)(\varphi \Rightarrow \psi) \vdash (\forall x)\neg\psi \Rightarrow (\forall x)\neg\varphi$	<i>bod (i) a modus ponens,</i>
$(\forall x)(\varphi \Rightarrow \psi) \vdash \neg(\forall x)\neg\varphi \Rightarrow \neg(\forall x)\neg\psi$	<i>transposice implikace,</i>
$(\forall x)(\varphi \Rightarrow \psi) \vdash (\exists x)\varphi \Rightarrow (\exists x)\psi$	<i>zkratka za formule,</i>
$\vdash (\forall x)(\varphi \Rightarrow \psi) \Rightarrow ((\exists x)\varphi \Rightarrow (\exists x)\psi)$	<i>věta o dedukci.</i>

### Poznámka.

Ukažme, že implikace u obou vztahů (i), (ii) z předchozího příkladu nelze obrátit. To jest neplatí  $\vdash ((\forall x)\varphi \Rightarrow (\forall x)\psi) \Rightarrow (\forall x)(\varphi \Rightarrow \psi)$  ani  $\vdash ((\exists x)\varphi \Rightarrow (\exists x)\psi) \Rightarrow (\forall x)(\varphi \Rightarrow \psi)$ . Vezměme si jazyk typu  $\langle R, \emptyset, \sigma \rangle$ , kde  $R = \{r, s\}$ ,  $\sigma(r) = \sigma(s) = 1$  a strukturu tohoto jazyka  $\mathbf{M} = \langle M, \{r^{\mathbf{M}}, s^{\mathbf{M}}\}, \emptyset \rangle$ , kde

$M = \{a, b\}$  a  $r^{\mathbf{M}} = \{a\}$ ,  $s^{\mathbf{M}} = \{b\}$ . Uvažujme, že  $\varphi$  je formule  $r(x)$  a  $\psi$  je formule  $s(x)$ . Pak v  $\mathbf{M}$  při libovolném ohodnocení  $v$  máme  $\|(\forall x)r(x) \Rightarrow (\forall x)s(x)\|_{\mathbf{M},v} = 1$  a  $\|(\exists x)r(x) \Rightarrow (\exists x)s(x)\|_{\mathbf{M},v} = 1$ . Na druhou stranu ale  $\|(\forall x)(r(x) \Rightarrow s(x))\|_{\mathbf{M},v} = 0$ . To jest našli jsme model, ve kterém nejsou formule s obrácenými implikacemi splněny.

### Příklad.

80. Dokažte následující tvrzení o *záměně pořadí implikace a kvantifikace*,

- (i)  $\vdash (\forall x)(\varphi \Rightarrow \psi) \Leftrightarrow (\varphi \Rightarrow (\forall x)\psi)$ ,  $\varphi, \psi$  jsou formule a  $\varphi$  nemá volný výskyt  $x$ ,
- (ii)  $\vdash (\forall x)(\varphi \Rightarrow \psi) \Leftrightarrow ((\exists x)\varphi \Rightarrow \psi)$ ,  $\varphi, \psi$  jsou formule a  $\psi$  nemá volný výskyt  $x$ ,
- (iii)  $\vdash (\exists x)(\varphi \Rightarrow \psi) \Leftrightarrow (\varphi \Rightarrow (\exists x)\psi)$ ,  $\varphi, \psi$  jsou formule a  $\varphi$  nemá volný výskyt  $x$ ,
- (iv)  $\vdash (\exists x)(\varphi \Rightarrow \psi) \Leftrightarrow ((\forall x)\varphi \Rightarrow \psi)$ ,  $\varphi, \psi$  jsou formule a  $\psi$  nemá volný výskyt  $x$ .

Z uvedených tvrzení dokážeme první dvě z nich. Při dokazování budeme využívat známého faktu, že ekvivalence je zaváděna jako konjunkce dvou implikací. Pokud dokážeme obě implikace, můžeme využít principu dosazení do tautologie výrokového počtu  $p \Rightarrow (q \Rightarrow (p \wedge q))$ .

### Řešení.

Nejprve ukažme (i). Triviálně  $\vdash (\forall x)(\varphi \Rightarrow \psi) \Rightarrow (\varphi \Rightarrow (\forall x)\psi)$ , jelikož se jedná o instanci axiomu distribuce, podmínka, že  $x$  nemá volný výskyt v  $\varphi$  je splněna z předpokladů. Dále prokážeme opačnou nerovnost. Opět předpokládejme, že  $\varphi$  nemá volné proměnné a  $\psi$  má nejvýše volnou proměnnou  $x$ . Kdyby tomu tak nebylo, můžeme volné proměnné fixovat konstantami. Máme,

$\vdash (\forall x)\psi \Rightarrow \psi$	<i>instance axiomu specifikace,</i>
$\varphi \Rightarrow (\forall x)\psi \vdash (\forall x)\psi \Rightarrow \psi$	<i>monotonie dokazatelnosti,</i>
$\varphi \Rightarrow (\forall x)\psi \vdash \varphi \Rightarrow \psi$	<i>transitivita implikace,</i>
$\varphi \Rightarrow (\forall x)\psi \vdash (\forall x)(\varphi \Rightarrow \psi)$	<i>generalisace,</i>
$\vdash (\varphi \Rightarrow (\forall x)\psi) \Rightarrow (\forall x)(\varphi \Rightarrow \psi)$	<i>věta o dedukci.</i>

Princip transitivity implikace lze použít, jelikož se jedná o použití principu dosazení do tautologie výrokového počtu  $(p \Rightarrow q) \Rightarrow ((q \Rightarrow r) \Rightarrow (p \Rightarrow r))$ . Dohromady tedy dostáváme požadované tvrzení.

Nyní prokážeme (ii). V tomto důkazu budeme vhodně využívat větu o ekvivalenci. Vyjdeme z již dokázaného bodu (i),

$\vdash (\forall x)(\neg\psi \Rightarrow \neg\varphi) \Leftrightarrow (\neg\psi \Rightarrow (\forall x)\neg\varphi)$	<i>tvrzení z bodu (i),</i>
$\vdash (\forall x)(\neg\psi \Rightarrow \neg\varphi) \Leftrightarrow (\neg(\forall x)\neg\varphi \Rightarrow \psi)$	<i>třetí axiom, věta o ekvivalenci,</i>
$\vdash (\forall x)(\neg\psi \Rightarrow \neg\varphi) \Leftrightarrow ((\exists x)\varphi \Rightarrow \psi)$	<i>zkratka za formulí,</i>
$\vdash (\forall x)(\varphi \Rightarrow \psi) \Leftrightarrow ((\exists x)\varphi \Rightarrow \psi)$	<i>třetí axiom, věta o ekvivalenci.</i>

Což bylo dokázat.

### Poznámka.

Podmínka omezující předchozí tvrzení pouze na formule bez volného výskytu proměnné  $x$  je opět nutná a snadno najdeme protipříklad. Uvažujme typ jazyka  $\langle R, \emptyset, \sigma \rangle$ , kde  $R = \{r\}$ ,  $\sigma(r) = 1$  a strukturu tohoto jazyka  $\mathbf{M} = \langle M, \{r^{\mathbf{M}}\}, \emptyset \rangle$ , kde  $M = \{a, b\}$  a relace  $r^{\mathbf{M}}$  je definována  $r^{\mathbf{M}} = \{a\}$ . Kdyby platila tvrzení (i)–(iv) v plném rozsahu, pak bychom pro formule  $\varphi, \psi$  rovny  $r(x)$  měli

$\|(\forall x)(r(x) \Rightarrow r(x))\|_{\mathbf{M},v} = 1$  v libovolném ohodnocení  $v$ . Pokud ale například pro (i) zvolíme ohodnocení  $v$  tak, že  $v(x) = a$ , pak platí  $\|r(x) \Rightarrow (\forall x)r(x)\|_{\mathbf{M},v} = 0$ . To jest dostali bychom se do sporu s větou o korektnosti.

### Cvičení.

81. Najděte protipříklady k tvrzením (ii)–(iv) z předchozího řešeného příkladu. Při hledání modelů se snažte najít struktury s co možná nejmenšími nosiči.
- \*82. Pokuste se dokázat tvrzení (iii) a (iv) z předchozího příkladu nebo alespoň některou z implikací. Například pro dokázání implikace  $\Rightarrow$  z (iii) stačí vhodně využít duální formu specifikace, transitivitu implikace a již prokázaný princip (ii).
83. Dokažte tvrzení o *záměně pořadí kvantifikace a negace*,

- (i)  $\vdash \neg(\forall x)\varphi \Leftrightarrow (\exists x)\neg\varphi$ ,  
(ii)  $\vdash \neg(\exists x)\varphi \Leftrightarrow (\forall x)\neg\varphi$ .

Využijte faktu, že existenční kvantifikaci  $(\exists x)\varphi$  chápeme jako zkratku za formuli  $\neg(\forall x)\neg\varphi$ .

### Příklad.

84. Dokažte následující tvrzení o *záměně pořadí kvantifikací*,

- (i)  $\vdash (\forall x)(\forall y)\varphi \Leftrightarrow (\forall y)(\forall x)\varphi$ ,  
(ii)  $\vdash (\exists x)(\exists y)\varphi \Leftrightarrow (\exists y)(\exists x)\varphi$ ,  
(iii)  $\vdash (\exists x)(\forall y)\varphi \Rightarrow (\forall y)(\exists x)\varphi$ ,

kde  $\varphi$  je libovolná formule. Zdůrazněme, že první dvě tvrzení mají tvar ekvivalence, kdežto ve třetím případě nelze opačnou implikaci prokázat.

### Řešení.

Tvrzení (i) dostaneme jednoduše aplikací axiomu specifikace a modus ponens a pravidla generalisace. Ekvivalenci opět chápeme jako konjunkci dvou implikací.

V případě tvrzení (ii) si pomůžeme zavedením  $(\exists x)\varphi$  jakožto zkratky za formuli  $\neg(\forall x)\neg\varphi$  a platností bodu (i) spolu s větou o ekvivalenci a s větami o *záměně pořadí kvantifikace a negace*. Podrobněji,

$\vdash (\exists x)(\exists y)\varphi \Leftrightarrow \neg(\forall x)\neg\neg(\forall y)\neg\varphi$	<i>rozepsání zkratky za formuli,</i>
$\vdash (\exists x)(\exists y)\varphi \Leftrightarrow \neg(\forall x)(\forall y)\neg\neg\neg\varphi$	<i>dvakrát záměna pořadí negace a kvantifikace spolu s větou o ekvivalenci,</i>
$\vdash (\exists x)(\exists y)\varphi \Leftrightarrow \neg(\forall y)(\forall x)\neg\neg\neg\varphi$	<i>bod (i) a věta o ekvivalenci,</i>
$\vdash (\exists x)(\exists y)\varphi \Leftrightarrow \neg(\forall y)\neg\neg(\forall x)\neg\varphi$	<i>zpětná záměna pořadí negace a kvantifikace,</i>
$\vdash (\exists x)(\exists y)\varphi \Leftrightarrow (\exists y)(\exists x)\varphi$	<i>zkratka za formuli.</i>

Nyní ukážeme bod (iii),

$\vdash \varphi \Rightarrow (\exists x)\varphi$	<i>duální forma specifikace,</i>
$\vdash (\forall y)(\varphi \Rightarrow (\exists x)\varphi)$	<i>generalisace,</i>
$\vdash (\forall y)\varphi \Rightarrow (\forall y)(\exists x)\varphi$	<i>distribuce kvantifikace,</i>
$\vdash (\forall x)((\forall y)\varphi \Rightarrow (\forall y)(\exists x)\varphi)$	<i>generalisace,</i>
$\vdash (\exists x)(\forall y)\varphi \Rightarrow (\forall y)(\exists x)\varphi$	<i>záměna pořadí kvantifikace a implikace,</i>

Což jsme chtěli ukázat.

**Poznámka.**

Pro tvrzení (iii) opět ukážeme, že jej nelze prokázat pro obrácenou implikaci. Uvažujme jazyk typu  $\langle R, \emptyset, \sigma \rangle$ , kde  $R = \{r\}$ ,  $\sigma(r) = 2$  a strukturu tohoto jazyka  $\mathbf{M} = \langle M, \{r^{\mathbf{M}}\}, \emptyset \rangle$ , kde  $M = \{a, b\}$  a relace  $r^{\mathbf{M}}$  je definována  $r^{\mathbf{M}} = \{\langle a, b \rangle, \langle b, a \rangle\}$ . Ve struktuře  $\mathbf{M}$  máme  $\|(\forall y)(\exists x)r(x, y)\|_{\mathbf{M}, v} = 1$  při libovolném ohodnocení  $v$ . Na druhou stranu však  $\|(\exists x)(\forall y)r(x, y)\|_{\mathbf{M}, v} = 0$ . To jest našli jsme model, kde není opačná implikace pravdivá.