KAPITOLA I

VÝROKOVÝ POČET

Robot Radius: Já dovedu všechno.
Karel Čapek, RUR

Název kapitoly již předznamenává, že se v ní budeme zabývat výrokovým počtem. Místo o výrokovém počtu se někdy též hovoří o *výrokové logice* nebo o *výrokovém kalkulu* (anglicky propositional calculus nebo sentential logic). Vztah výrokového a predikátového počtu jsme diskutovali v úvodu textu. Připojme ještě, že výrokový počet je možno přirovnat i k větnému rozboru, při kterém se také obsahem jednotlivých vět nezabýváme, zajímají nás pouze vztahy mezi větami. Výrokový počet chápeme jako část logiky zabývající se způsoby, kterými lze z jednodušších výroků vytvořit výroky složitější, a zejména popisem vlastností a vztahů takto vzniklých výroků.

Výrokem rozumíme tvrzení (intuitivně chápáno oznamovací větu), které je dostatečně smysluplné, aby bylo *možno* uvažovat, zda je pravdivé nebo nepravdivé (nemusíme ale být schopni o pravdivosti rozhodnout; sousloví „V posledních pěti minutách, než jste dočetli až sem, nebyl na Zemi nikdo zavražděn“ je výrok). Pravdivým[1] výrokům je zvykem přiřazovat **pravdivostní hodnotu** 1 (případně $\top$ nebo **t** — true), nepravdivým hodnotu 0 (případně $\perp$ nebo **f** — false). Podané vysvětlení není formální definice, ale pouhé vymezení, přesně tak jako v geometrii „přímka je délkou bez šířky“ nedefinuje přímku, ale pouze ukazuje, jak si máme přímku představovat. Pojem přímky je pro geometrii pojmem základním (nedefinujeme ho na základě jiných pojmů), chování přímek je popsáno axiomy. Analogicky se ve výrokovém počtu nesnažíme pojem výroku formálně definovat, ale „pouze“ zkoumáme jeho vlastnosti a vztahy výroků. Ze základních výroků vytvoříme další výroky; *složenými výroky* se nazývají ty, které vzniknou z jednodušších pomocí logických operací (tzn. aplikací negace, implikace, etc., viz dále).

V sémantice výrokového počtu se na začátku předpokládá, že základní výroky[2] jsou nějak ohodnoceny (je jim přiřčena pravda nebo nepravda), a za tohoto předpokladu se definuje ohodnocení výroků složených. Při tom si ale uvědomme, že není důvod a ani možnost zamezit, aby výroky, které při jednom pohledu pokládáme za složené, nebyly pokládány při jiném pohledu za základní.

*

[1] Opět vidíme, jak matematická logika omezuje obor svého zkoumání: otázky „Co je pravda?“, „Jak pravdu poznáme?“, etc. jsou hluboké lidské problémy. Matematická logika však pouze předpokládá, že výroky (resp. výrokové proměnné) jsou *nějak* ohodnoceny.

[2] Výroky, které nejsou složenými, se někdy nazývají *jednoduchými*.

Terminologie „výrok“, „složený výrok“, etc. zdůrazňuje sémantickou stránku. V matematické logice v žádném případě nepomíjíme syntax, a je proto běžnější mluvit o formulích výrokového počtu, což také učiníme. V syntaxi výrokového počtu se např. zkoumá, které z formulí tohoto počtu jsou dokazatelné.

V matematické logice se obecně definuje **formule** (induktivní definicí; použité pojmy budeme podrobněji vysvětlovat v dalším textu) tak, že:

(a) každá ze základních formulí je formulí,
(b) vznikne-li $\mathscr{A}$ unární logickou operací z formule $\mathscr{B}$ nebo binární logickou operací z formulí $\mathscr{B}$ a $\mathscr{C}$, je $\mathscr{A}$ také formulí,
(c) každou formuli dostaneme postupnou aplikací pravidel (a) a (b)[3].

Popsaná forma definice formule bude užita ve výrokovém i predikátovém počtu, ale systémy logických operací a základních formulí budou pro tyto počty různé. V pravidle (b) je implicitně obsažen předpoklad potenciálního nekonečna. V prvních paragrafech kapitol I a II budeme upřesňovat definice pro jednotlivé počty a definice tam uvedené také zpřesňují (z hlediska finitisty) výše uvedené pravidlo (c).

*

Aby hrubá kostra definice výrokové formule byla vyplněna, je potřeba nejprve popsat, co budeme pokládat za základní formule výrokového počtu a co budeme pokládat za logické operace výrokového počtu. Základní formule výrokového počtu budou **výrokové proměnné,** přitom výroková proměnná, intuitivně řečeno, představuje blíže neurčený výrok. Popis logických operací pochopitelně provedeme na základě rozboru přirozeného jazyka, ke kterému nyní přistoupíme.

Zcela zřejmý, ale podstatný, je rozdíl mezi běžným a formalizovaným jazykem spočívající v míře neurčitosti. Slova v češtině (ani v jiném přirozeném jazyce) nejsou zcela jednoznačná; mluvené slovo je doplňováno důrazem, mimikou, etc., což umožňuje porozumět, co mluvčí míní; rozhodující pro pochopení však bývá celkový kontext. Pro běžný jazyk je jistá míra neurčitosti vítaná, dodává mu půvabu a umožňuje plodné asociace. Naproti tomu formální jazyk musí být zcela přesný (např. negaci výroku musí být přiřazena pravdivostní hodnota na základě pravdivostní hodnoty původního výroku zcela jednoznačně).

Přirozený jazyk je také velmi bohatý; při jeho formalizaci stačí vybrat jen některé obraty vytvářející z tvrzení nová složitější tvrzení a další způsoby vytváření složitějších tvrzení již vyjadřujeme jen s jejich pomocí. Při formalizaci se tak potýkáme se dvěma problémy: vybrat obraty běžného jazyka, které budeme formalizovat a určit jejich přesný formální význam (pravdivostní hodnoty). Obvykle se za vhodné pro formalizaci pokládají následující obraty běžného jazyka (popřípadě jazyka matematiky):

(1) „není pravda, že …“, „neplatí …“ nebo vznikající změnou slovesa přidáním předpony „ne-“ (popř. z latiny převzaté „non …“), které budeme formalizovat **negací** používajíce přitom symbolu $\neg$ (používá se též $\sim$ nebo $'$),

(2) „jestliže …, pak …“, „z … plyne …“, „… implikuje …“ se formalizují

[3] Předpokládáme-li aktuální nekonečno, můžeme upřesnit bod (c) tak, že množina formulí je nejmenší množina, která naplňuje body (a) a (b).

implikací a je zvykem přitom používat symbolu $\rightarrow$ (někdy též $\Rightarrow$, případně $\supset$)[4],

(3) „... a ...“, „... i ...“, „... a zároveň ...“ (případně z latiny převzaté „... et ...“) jsou formalizovány **konjunkcí,** při jejím zápisu budeme používat symbolu & (používá se též $\wedge$),

(4) „... nebo ...“ (případně z latiny přijaté „... vel ...“) bude formalizováno **disjunkcí,** při použití symbolu $\vee$ [5],

(5) „..., právě když ...“, „... tehdy a jen tehdy, když ...“, „... je ekvivalentní s ...“ budeme formalizovat **ekvivalencí** (někdy se také používá sousloví „*oboustranná implikace*“), přitom používáme znaku $\equiv$ (též $\Leftrightarrow$ nebo $\leftrightarrow$)[6].

Pravdivostní hodnoty příslušné k uvedeným obratům a popisující jejich obvyklé chápání jsou formulovány v §1, tam jsou také zmíněny příklady situací, kdy v běžné řeči dáváme obratům jiný význam.

Někteří autoři používají všech těchto obratů rovnoprávně, zaplatí za to však větším počtem axiomů, neboť obraty nejsou na sobě nezávislé a axiomy musí tento vztah popsat. Jiní autoři volí za základní obraty jen některé z nich a zaplatí za to tím, že ostatní obraty je potřeba chápat jako zkratky za složitější výroky obsahující pouze vybrané základní obraty. Hlavní výhodou tohoto druhého přístupu je zjednodušení demonstrací postupujících podle složitosti formule, protože je potřeba prověřovat méně případů. Dokonce ani volba základních obratů při druhém přístupu není jednotná (nicméně téměř vždy je jako jeden z nich volena negace), záleží na vkusu a účelu. Je dokonce možné zvolit jenom jediný obrat, ale ten pak už musí být volen z obratů méně intuitivních (např. Shefferova operace; viz cv. 11 této kapitoly). V dalším textu zvolíme za základní obraty první dva, pro zkoumání důsledku se zdá volba implikace jako nejvhodnější, jinými přístupy se budeme zabývat ve cvičeních.

Běžnými **logickými operacemi** tedy jsou negace (unární), implikace, konjunkce, disjunkce, ekvivalence (všechny binární), v predikátovém počtu pak navíc kvantifikace (viz následující kapitola); již jsme však uvedli, že v této kapitole se většinou omezíme jen na první dvě logické operace (a ostatní, relevantní pro výrokový počet, budeme chápat jako pouhé zkratky). Je nutno rozlišit logické operace od logických funkcí (neboli operací), kterými se budeme zabývat v predikátovém počtu.

Symboly používané k označení negace, implikace, konjunkce, disjunkce a ekvivalence formulí (tzn. symboly $\neg$, $\rightarrow$, &, $\vee$, $\equiv$) se nazývají **logické** (též *výrokové*) **spojky.**

V našem textu zásadně nebudeme používat $\Rightarrow$ a $\Leftrightarrow$ jako symbolů ve formálním jazyce, ale vyhradíme tyto symboly v odpovídajícím významu do metamatematické hladiny.

*

[4] Místo „$\mathscr{A}$ implikuje $\mathscr{B}$“ říkáme také, že „$\mathscr{B}$ je ***nutnou podmínkou*** pro $\mathscr{A}$“ nebo „$\mathscr{A}$ je ***postačující podmínkou*** pro $\mathscr{B}$“. Analogicky při ekvivalenci místo „$\mathscr{A}$, právě když $\mathscr{B}$“ říkáme také, že „$\mathscr{A}$ je ***nutnou a postačující podmínkou*** pro $\mathscr{B}$“.

[5] Místo o disjunkci se někdy mluví o ***alternativě***, což ale může vést k nedorozumění, protože někteří autoři chápou alternativu (příp. alternaci) jako disjunkci ve vylučovacím smyslu.

[6] Někdy se formalizuje i obrat „... nebo ... ve vylučovacím smyslu“, dnes *v logice* nepatří mezi nejobvyklejší. Antičtí Řekové ho však užívali často (viz např. cvičení 7 této kapitoly) a také v souvislosti s počítači je hojně využíván. Uvědomme si, že vylučující disjunkce je nahraditelná negací ekvivalence (viz cv. 5).

V Kritice slov K. Čapek s půvabem jemu vlastním napadá logiku: „O logickém důkazu je jediná pravda, že se nic nedá logicky dokazovat; což vám dokážu logicky. Buď dokazuji své tvrzení samými evidentními soudy; ale kdyby mé tvrzení plynulo evidentně z evidentních vět, bylo by samo evidentní, a tu by ovšem naprosto nepotřebovalo být dokazováno. Nebo dokazuji své tvrzení větami neevidentními, ale pak bych musel logicky dokazovat všechny tyto věty „usque ad infinitum“, …, z čehož logicky plyne, že logický důkaz je nemožný; a není-li tento logický důkaz naprosto přesvědčující, vidíte z toho, že logické dokazování opravdu za nic nestojí“.

K. Čapek zpochybňuje samu podstatu logiky, neboť pojem důkazu je jedním z jejích nejdůležitějších pojmů. Pokud bychom však přijali Čapkovy výhrady, musili bychom revidovat náš přístup k mnohem širší oblasti zahrnující celé lidské rozumové vyvozování. Připomeňme, že Eukleidés (315–271 př. Kr.) ve svých Základech jako prvý vyvozuje z několika axiomů celou nauku (geometrii, ale protože aritmetiku chápe jako součást geometrie, je možno říci, že celou tehdejší matematiku). Deduktivní metoda však neovlivnila pouze matematiku a vědy blízké matematice (např. teoretickou fyziku), ale zasahuje — a to dokonce i ve své formalizované podobě — do velice mnoha oblastí lidského poznání; jako příklad uveďme knihu B. Spinozy Etika (s podtitulem: vyložená metodou geometrickou), kde je podávána filozofie metodou věta – důkaz[7]. Naštěstí za chvíli nahlédneme, že Čapkovy námitky naprosto nereflektují lidskou zkušenost.

V této kapitole budeme formálně definovat pojem **důkazu** pro počet výrokový, v příští pro predikátový. Pojetí je v obou případech naprosto stejné, liší se pouze **axiomy** logiky a **dedukčními** (*odvozovacími*) **pravidly** přijímanými v tom kterém počtu. Je nutno velice zdůraznit, že v obou případech volíme axiomy logiky a dedukční pravidla tak, aby formalizovaly kroky přijímané v intuitivních úvahách. Tedy např. dedukční pravidla budou formalizace intuitivních postupů odvozujících další pravdivá tvrzení z tvrzení, která jsme již za pravdivá přijali. Jinak řečeno axiomy a dedukční pravidla můžeme volit různě, ale vždy mají popisovat „intuitivní pojem odvozování“, a v tomto ohledu jejich volba naprosto nemůže být nahodilá — podstatným cílem logiky již od antiky bylo popsat ty principy, kterými se řídí lidské uvažování.

Navíc ovšem při běžném uvažování vycházíme z nějakých **předpokladů**. V diskusích běžného života obvykle tyto předpoklady neformulujeme přesně, jsou přítomny v našem uvažování pouze implicitně a právě toto běžné neujasnění základních východisek vede v mnoha diskusích k nedorozuměním, neboť co pro jednoho diskutujícího je zcela zřejmé (a na čem staví svou argumentaci), může být pro druhého nejasné, nebo dokonce nepřijatelné. Naproti tomu v matematické logice žádáme, aby předpoklady, které můžeme v důkaze použít, byly vymezeny zcela přesně.

Předpoklady představují ta tvrzení, z kterých při dokazování dalších tvrzení vycházíme. Je totiž zřejmé, že při zdůvodňování nějakého tvrzení se nemohu do nekonečna odvolávat na stále zřejmější a zřejmější fakta: někdy musím již prohlásit, že tato fakta jsou (alespoň pro mne) tak zřejmá, že je již nebudu dokazovat. S partnerem se v diskusi buďto na nich shodneme (tzn. formálně řečeno přijmeme stejnou

[7] Pro zajímavost uveďme první Spinozův axiom: „Vše co jest, jest buďto samo v sobě, anebo v něčem jiném.“

teorii, viz §3 následující kapitoly[8)]), nebo jsme ochotni nadále společně přijatelné základy hledat, anebo zjistíme, že jeden přijímá jako základní fakt (o kterém odmítá diskutovat) přesně negaci základního faktu (příp. důsledku základních faktů) toho druhého. V posledním případě je již předem zřejmé, že diskuse, využívající jako argument zmíněný fakt, nemůže vést ke shodě.

Při volbě předpokladů nejsme po formální stránce nijak omezeni, při nevhodné volbě se může „pouze“ stát, že z nich dokážeme jakýkoli nesmysl (předpoklady jsou sporné). Je však jasné, že z intuitivního hlediska nejsou jednotlivé systémy předpokladů rovnocenné. Popis vhodné volby je závislý na filozofickém pojetí pravdy a skutečnosti, a přesahuje tedy rámec matematické logiky.

Poznamenejme, že volba axiomů logiky, dedukčních pravidel a předpokladů je možná až po zvolení systému formulí, které budeme vyšetřovat. Ve výrokovém počtu je potřeba dříve zvolit spojky, což jsme před okamžikem učinili, v predikátovém počtu je potřeba zvolit jazyk (formální definici viz §1 kap. II), tzn. rozhodnout o jaké vlastnosti a vztahy se budeme zajímat a s jakými objekty budeme pracovat.

Přistupme k formálnímu pojmu důkazu.

V matematické logice definujeme **důkaz** z nějakých předpokladů jako konečnou posloupnost formulí, při jejíž tvorbě smíme v každém jednotlivém kroku učinit některou z následujících činností:

(a) napsat (vyslovit, myslet, etc.) jeden z předpokladů,
(b) napsat axiom logiky,
(c) napsat formuli, kterou dostaneme aplikací dedukčního pravidla na některé formule, které *v posloupnosti předcházejí*.

Formule je **dokazatelná** (z nějakých předpokladů), jestliže existuje důkaz (z těchto předpokladů), jehož je posledním členem.

Uvědomme si, že pokud má mít uvedený pojem důkazu rozumný smysl, musíme zvolit alespoň jedno dedukční pravidlo a alespoň jeden axiom nebo předpoklad[9)]. Zdůrazněme, že pravidla uvedená v následujících kapitolách jsou ryze syntaktická a neodvolávají se na sémantiku a že triviálně existuje algoritmus umožňující rozhodnout, zda formule je axiomem logiky či nikoli, a analogicky umožňující rozhodnout, zda jedna formule plyne z druhé/druhých pomocí některého z uvedených dedukčních pravidel. Máme-li předloženu nějakou posloupnost formulí, je ověření, zda se jedná o důkaz z určitých předpokladů, zcela mechanickou záležitostí (existuje algoritmus).

Po vyslovení definice důkazu je již možné, a nutné, zdůraznit, v čem se matematický logik naprosto rozchází s citovaným výrokem K. Čapka. Parafrázuji-li jeho

---

8) Důkaz z předpokladů ve výrokovém počtu je v jistém smyslu jen pomocný pojem, podstatná je dokazatelnost bez předpokladů. Naproti tomu v predikátovém počtu bychom se sice také bez předpokladů obešli, ale bylo by to nevýhodné (a hlavně naprosto nepřehledné, protože bychom neustále museli tyto předpoklady opakovat). Proto je v predikátovém počtu zvykem mluvit o důkazu ve zkoumané teorii, jinak řečeno sumarizovat předpoklady na začátku zkoumání jakožto **axiomy teorie**.

9) Jako kuriozitu uveďme systém, který jednak pracuje s jedinou logickou spojkou (Shefferovou, viz cv. 11, která má význam „není pravda, že $\mathcal{A}$ nebo není pravda, že $\mathcal{B}$“) značenou $|$, ale hlavně má jediný axiom a jediné dedukční pravidlo. Tato minimalizace je pochopitelně zaplacena ztrátou přehlednosti a intuitivního náhledu. Axiomem je $[\mathcal{P}|(\mathcal{Q}|\mathcal{R})]|\big[[\mathcal{S}|(\mathcal{S}|\mathcal{S})]|\big((\mathcal{T}|\mathcal{Q})|[(\mathcal{P}|\mathcal{T})|(\mathcal{P}|\mathcal{T})]\big)\big]$ a dedukční pravidlo dovoluje odvození formule $\mathcal{R}$ výrokového počtu z formulí $\mathcal{P}$ a $\mathcal{P}|(\mathcal{Q}|\mathcal{R})$ výrokového počtu.

úvahu, mohu také jednoduše „dokázat“, že nikdy nedojdu z Prahy do Prčic: při každém kroku se má pozice změní jen málo a Prčice jsou od Prahy dost daleko. Chyba Čapkovy úvahy spočívá v tom, že mnoha (byť malými) kroky je možno urazit velkou vzdálenost, což řada účastníků pochodu na uvedené trase prakticky prokázala. Analogicky není možno popřít, že i pomocí evidentních důkazových kroků je možno dojít (je-li jich hodně) k tvrzením značně neevidentním.

*

V lidském uvažování je možno vysledovat mnoho správných dokazovacích postupů a v průběhu vývoje logiky bylo velmi mnoho takovýchto pravidel formulováno a vyučováno (stále s možností nalézání dalších pravidel). Důležitým objevem matematické logiky je možnost volby poměrně malého počtu základních dokazovacích principů, které již pro popsání našeho usuzování (vyvozování) *„plně postačí“*. Pro výrokový i predikátový počet popíšeme konkrétně takovéto dostatečně silné systémy — pro výrokový počet bude složený ze tří typů axiomů a jediného dedukčního pravidla.

V textu je uvedena řada dokazovacích postupů (často včetně klasických názvů), nicméně je to jen zlomek těch, které byly v průběhu vývoje logiky formulovány. Matematická logika však přinesla obrovský posun: principy budeme uvádět jako *příklady* toho, co lze v námi zvoleném systému dokázat, a jako to, co máme *používat*, ale nikoli jako zákony, které je třeba se naučit vyjmenovávat. Přístup k logice jako k rozsáhlému systému pravidel, která je třeba se naučit, je zřetelný zejména od scholastiky a pokračuje až do 20. stol. Toto pojetí je sice nyní překonané, zdržme se však jakýchkoli negativních soudů, protože scholastický přístup reálně přispěl k rozvoji lidského myšlení.

Slovním spojením „plně postačí“ rozumíme, že jakýkoli jiný dokazovací princip, který je formalizací intuitivně správného vyvozovacího kroku (speciálně tedy i každý dodatečný axiom logiky popisující intuitivně pravdivé tvrzení), je dovoditelný ze zvolených základních dokazovacích principů. Vyjádřeme předchozí tvrzení pro výrokový počet ještě jinými slovy: přidáme-li k námi zvoleným axiomům výrokového počtu a/nebo k jedinému dedukčnímu pravidlu výrokového počtu jakýkoli další dokazovací princip, jsou jen dvě možnosti. Buďto i „důkazy“, v kterých je tento dokazovací princip povolen, umožní dokázat jen (vždy) pravdivé výrokové formule, pak ale je dodatečný dokazovací princip zbytečný, neboť tytéž výrokové formule je možno dokázat i bez něho, anebo se pomocí nějakého „důkazu“ povolujícího i dodatečný dokazovací princip podaří dokázat nějakou výrokovou formuli, která není (vždy) pravdivá, ale pak je tento dokazovací princip nepřijatelný. Odporovalo by přece naší intuici o pojmu dokazatelnosti, kdybychom dokázali nepravdivý výrok. Dokonce bychom považovali za absurdní, kdybychom dokázali nějakou výrokovou formuli, která by byla nepravdivá, byť jen při jediném ohodnocení výrokových proměnných, ze kterých je vytvořena.

Tímto pochopitelně nezpochybňujeme užitečnost různých jiných dokazovacích postupů (také jich řadu uvedeme), protože takovéto postupy mohou velice urychlovat a zpřehledňovat důkazy, pouze tvrdíme, že takovéto postupy jsou již nahraditelné pomocí vybraných základních dokazovacích principů. A už vůbec netvrdíme, že existuje jediná vhodná volba základních dokazovacích principů, dokonce i některé jiné možné volby základních dokazovacích principů ukážeme (viz závěr §2 a také cvičení 18–21).

Systémy dokazovacích pravidel můžeme zhruba dělit na dvě skupiny:

(a) hilbertovské systémy mající málo dedukčních pravidel a více axiomů,

(b) gentzenovské systémy mající naopak více pravidel a co nejméně axiomů.

Systém popsaný v §2 je hilbertovský, příklady gentzenovských systémů lze nalézt ve cvičeních.

*

Je nutné poznamenat, že nebývá — dokonce ani v matematice — zvykem vytvářet důkazy tak, aby přesně vyhovovaly uvedené definici, bylo by to velmi zdlouhavé a špatně čitelné, ale každý správný důkaz *musíme být schopni* předělat na důkaz vyhovující výše uvedené definici. V celém našem textu je jediný důkaz, který je skutečně posloupností mající vlastnost vyžadovanou v definici důkazu. Je to důkaz naprosto triviálního tvrzení $\mathcal{A} \to \mathcal{A}$ (viz §2). Na tomto důkazu by čtenář měl nahlédnout již uvedený fakt, že otázka prozkoumání, zda uvedená posloupnost formulí je důkazem, je skutečně zcela mechanickou záležitostí. Na druhé straně ale čtenář pravděpodobně také prožije, že volba formulí výrokového počtu, které důkaz vytvářejí, je méně triviální a že vyžaduje jistou zkušenost a intuici. K problému, zda vystačíme se zkušeností nebo zda potřebujeme současně jak zkušenost tak i intuici, se vrátíme na konci tohoto úvodu.

Ve čtvrté kapitole budeme způsobem běžným v matematice prokazovat aritmetická tvrzení. K prvému tam uvedenému důkazu však připojujeme komentář poukazující na to, které postupy matematické logiky (včetně postupů predikátového počtu) jsou v předvedeném důkazu použity *implicitně*. Těmito poukazy vlastně podáváme návod, jak by se musel k předvedenému důkazu konstruovat příslušný zcela formální důkaz.

Hlavní náplní syntaxe výrokového počtu je ukázat metody, jak z existujících důkazů tvoříme důkazy jiné, a zejména prokázat možnost používat „důkazové bloky (schémata)“. S pomocí takovýchto bloků pak ukazujeme dokazatelnost dalších tvrzení, a to podstatně jednodušeji.

*

Zmínili jsme se, že sémantiku výrokového počtu je možno popsat tak, že vystačíme s jediným modelem. Je jím pochopitelně dvouprvkový soubor $\{1, 0\}$, jehož prvky představují pravdu a nepravdu, přičemž budeme uvažovat různá ohodnocení výrokových proměnných, tj. zobrazení souboru výrokových proměnných do $\{1, 0\}$. Toto pojetí je v souladu s pojetím v predikátovém počtu, kde se také uvažují ohodnocení jako zobrazení do zkoumaného modelu. V jiné terminologii pokládáme každé jednotlivé ohodnocení za „model“, a tedy je potřeba uvažovat řadu „modelů“.

*

V úvodu celého textu již bylo uvedeno, že vztah syntaxe a sémantiky je obsahem vět o korektnosti a o úplnosti. Věta o korektnosti v případě výrokového počtu vypovídá, že každá dokazatelná formule výrokového počtu je vždy pravdivá, tzn. je pravdivá při každém ohodnocení základních výroků. Takováto výpověď evidentně odpovídá intuici, neboť požadavek, aby vše, co dokážeme, bylo také pravdivé, je zcela přirozený. Nadto intuitivně budeme pokládat za vhodný jen takový popis usuzování, který ho popíše „úplně“, a tato idea je obsahem věty o úplnosti. Věta o úplnosti ve výrokovém počtu tvrdí, že každá vždy pravdivá formule výrokového počtu je v tomto počtu dokazatelná. Druhá z uvedených vět má za důsledek výše zmíněnou postačitelnost vybraných základních dokazovacích principů pro popis veškerého vyvozování relevantního pro výrokový počet, ale jejím důsledkem je také, že *vyplnění tabulky pravdivostních hodnot představuje algoritmus, který rozhoduje, zda formule výrokového počtu je dokazatelná či nikoli* (tedy výrokový počet je rozhodnutelný). Demonstrace věty o úplnosti navíc popisuje algoritmus, jak k dokazatelným výrokům příslušný důkaz sestrojit. Pro tvorbu důkazů ve výrokovém počtu lze napsat program, a pak už stačí pouhý stroj a není potřeba intuice matematika. Tedy z hlediska výrokového počtu matematika zcela *nahradí robot*[10]. Ke zcela jiným závěrům dojdeme však v případě predikátového počtu.

[10] Zkoumanou otázkou až dosud bylo, zda existuje důkaz. Pokud položíme otázku, zda existuje důkaz, který má nějakou vlastnost (např. je dostatečně jednoduchý), přestane být konstrukce takovéhoto důkazu triviálním problémem.

§1

FORMULE A SÉMANTIKA VÝROKOVÉHO POČTU

V úvodu této kapitoly jsme již uvedli, že ve výrokovém počtu budeme pracovat s následujícími pojmy (a jejich znaky), a ukazovali jsme jejich intuitivní význam:

(1) znaky pro výrokové proměnné (někdy se místo výrokové proměnné používá i název ***prvotní formule***, případně (***výrokový***) ***atom***);
předpokládáme, že výrokových proměnných máme k dispozici nekonečně mnoho, i když v jakékoli úvaze (formálněji: v jakékoli formuli, v jakémkoli důkaze, etc.) se jich vyskytne jen *konečný* počet[1)];
výrokové proměnné budeme označovat $\mathsf{p}, \mathsf{q}, \mathsf{r}, \ldots$;

(2) logické spojky $\neg, \rightarrow$ (alternativně navíc připouštíme $\&, \vee, \equiv$);

(3) nadto budeme ještě používat pomocné symboly (závorky, méně obvyklé je použití teček); jejich význam spočívá „pouze" v určení, na které formule se ta která logická operace vztahuje, tzn. závorky vymezují rozsah výrokových spojek, neboli intuitivně řečeno pomocné symboly popisují, jak posloupnost symbolů „číst"; např. $(\neg\mathcal{A}) \rightarrow \mathcal{B}$ čteme: jestliže neplatí $\mathcal{A}$, pak $\mathcal{B}$, ale jiné „uzávorkování" $\neg(\mathcal{A} \rightarrow \mathcal{B})$ čteme: neplatí, že z $\mathcal{A}$ plyne $\mathcal{B}$; ve cvičení se zmíníme o tzv. polské notaci, která se zcela obejde bez závorek[2)].

Slovem nad určitou **abecedou** budeme rozumět konečnou posloupnost[3)] znaků (symbolů) z dané abecedy (prázdné slovo se připouští; pořadí symbolů v posloupnosti je podstatné, změnou pořadí symbolů změníme slovo). Říkáme, že znak Φ_i se vyskytuje na i-tém místě ve slově $\Phi_1 \ldots \Phi_n$. Např. znak 0 se ve slově 1005 vyskytuje na druhém a třetím místě, tedy má dva výskyty. Slovo $\Psi_1 \ldots \Psi_m$ nazýváme podslovem slova $\Phi_1 \ldots \Phi_n$, jestliže existuje $l < n$ tak, že znak Ψ_j je totožný se znakem Φ_{l+j} pro každé $j \leqq m$. Nahrazení podslova začínajícího na popsaném místě v daném slově jiným slovem vyjadřuje intuitivní představu (formálně: jsou-li slovo $\Phi_1 \ldots \Phi_k$, slovo $\Psi_1 \ldots \Psi_i$ a slovo $\Theta_1 \ldots \Theta_j$ tři slova nad danou abecedou a je-li $i' \leqq k$, pak slovem vzniklým nahrazením slova $\Psi_1 \ldots \Psi_i$ začínajícího na místě i' ve slově $\Phi_1 \ldots \Phi_k$ slovem $\Theta_1 \ldots \Theta_j$ rozumíme slovo $\Phi_1 \ldots \Phi_{i'-1}\Theta_1 \ldots \Theta_j\Phi_{i'+i} \ldots \Phi_k$ za předpokladu, že $\Psi_1 \ldots \Psi_i$ je slovem $\Phi_{i'} \ldots \Phi_{i'+i-1}$, a v případě, že neplatí předpoklad, nebudeme náhradu provádět, tzn. slovem vzniklým „nahrazením" bude slovo $\Phi_1 \ldots \Phi_k$).

---

1) Tudíž postačí *potenciálně* nekonečně mnoho výrokových proměnných. Nadto je možno si představovat výrokové proměnné ze spočetného systému jako konečné posloupnosti dvou symbolů (např. nul a jedniček), a níže uvažovaná slova je tedy možno chápat jako slova nad konečnou abecedou.

2) Někdy se za základní stavební kameny pokládají i ***logické konstanty*** $\top$ a $\bot$, které se syntakticky chovají jako výrokové proměnné, ale při každém ohodnocení nabývá první z nich hodnoty 1 a druhá hodnoty 0.

3) Již jsme uvedli, že intuitivně budeme používat některých termínů blízkých teorii množin (např. konečná posloupnost); současně však upozorněme, že celou syntax lze vybudovat v řeči aritmetiky (viz §3 kap. IV). Posloupnost $\Phi_1 \ldots \Phi_n$ formálněji chápeme jako (množinovou) funkci přiřazující číslu i hodnotu Φ_i pro $i \leqq n$; pro $n = 0$ se přitom jedná o prázdnou posloupnost. Definici funkce v teorii množin připomínáme ve cv. 13 kap. III.

Definice. **Formulí výrokového počtu** (nazývanou též *výrokovou formulí*) rozumíme takové slovo $\mathscr{A}$ (nad abecedou, která obsahuje symboly pro výrokové proměnné, logické spojky a závorky), že k tomuto slovu existuje posloupnost $\mathscr{B}_1, \ldots, \mathscr{B}_k$ slov taková, že $\mathscr{B}_k$ je slovem $\mathscr{A}$ a pro každé jednotlivé $i \leqq k$ má slovo $\mathscr{B}_i$ *některý* z následujících tvarů:
(a) je výrokovou proměnnou,
(b) je tvaru $\neg\mathscr{B}_j$ pro některé $j < i$,
(c) je tvaru $(\mathscr{B}_j \to \mathscr{B}_{j'})$ (alternativně navíc připouštíme tvary $(\mathscr{B}_j \mathbin{\&} \mathscr{B}_{j'})$, $(\mathscr{B}_j \vee \mathscr{B}_{j'})$ a $(\mathscr{B}_j \equiv \mathscr{B}_{j'})$) pro některá $j, j' < i$.

Posloupnost $\mathscr{B}_1, \ldots, \mathscr{B}_k$ vyhovující uvedeným podmínkám nazýváme **vytvářející posloupností formule** $\mathscr{A}$ výrokového počtu[4].

Formuli výrokového počtu, která se vyskytuje ve všech vytvářejících posloupnostech formule $\mathscr{A}$ výrokového počtu, nazýváme **podformulí** formule $\mathscr{A}$. □

Značení. Pro formule výrokového počtu budeme používat znaky $\mathcal{A}, \mathcal{B}, \ldots$

Například posloupnost

$$\mathsf{p}, \mathsf{q}, (\mathsf{p} \to \mathsf{q}), \neg(\mathsf{p} \to \mathsf{q}), \neg\mathsf{p}, (\neg\mathsf{p} \to \neg(\mathsf{p} \to \mathsf{q}))$$

je vytvářející posloupností formule $(\neg\mathsf{p} \to \neg(\mathsf{p} \to \mathsf{q}))$.

Jestliže bude ze souvislosti patrné, že se jedná o formule výrokového počtu, budeme někdy sousloví „výrokového počtu“ vynechávat. Uvědomme si, že slovo $\&\ \mathsf{p})$ je podslovem formule $(\mathsf{p} \mathbin{\&} \mathsf{p})$, nikoli však podformulí a že ke každé formuli existuje její vytvářející posloupnost obsahující pouze její podformule (toto můžeme rigorózně prokázat postupně indukcí pro jednotlivé formule z vytvářející posloupnosti). Ve vytvářející posloupnosti formule jsou evidentně všechny členy formulemi, a tedy je také zřejmé, že volba termínu „pod*formule*“ je vhodná, neboť každé slovo, které je podformulí formule, je samo formulí.

Někdy se vytvářející posloupnost definuje tak, že obsahuje pouze podformule zkoumané formule (tzn. jako minimální možná).

Umluvme se, že budeme závorky vynechávat, pokud to neohrozí čitelnost zápisu. Již v definici jsme nevyžadovali závorky kolem negované formule, v dalším textu budeme také vynechávat poslední („zcela vnější“) dvojici závorek — tzn. budeme psát např. $\mathsf{p} \mathbin{\&} (\mathsf{p} \to \mathsf{q})$ místo $(\mathsf{p} \mathbin{\&} (\mathsf{p} \to \mathsf{q}))$. Navíc od okamžiku, kdy prokážeme asociativitu konjunkce a disjunkce, budeme vynechávat závorky i v případech vícečetných konjunkcí a disjunkcí, etc.[5] Při popisu abecedy, nad kterou vytváříme formule výrokového počtu, jsme uvažovali jediný typ závorek, neboť s ním vystačíme, ale pro *usnadnění čtení* se v matematickém textu běžně používá (což i my budeme činit v dalším textu) více typů závorek. V takovém případě je zvykem používat nejprve typ (,), a poté typ [,], pro ještě složitější výrazy je zvykem odlišovat závorky velikostí.

[4] V knize [K-Š-Ch] se používá termínu *konstrukce formule*.

[5] Někdy se dokonce přijímá úmluva, že $\to$ má nižší prioritu než ostatní spojky, což umožní psát místo $(\mathcal{A} \mathbin{\&} \mathcal{B}) \to (\mathcal{C} \vee \mathcal{D})$ prostě $\mathcal{A} \mathbin{\&} \mathcal{B} \to \mathcal{C} \vee \mathcal{D}$.

Zopakujme, že definice formule záleží na volbě systému logických spojek. V naší definici jsme volili spojky $\neg$ a $\rightarrow$, ale jako alternativu jsme připouštěli i další spojky (viz bod (2) a v definici formule bod (c); při ještě jiné volbě systému spojek jest třeba definici upravit obdobně). Při omezenější volbě, které dáme přednost, budeme slova typu $\mathcal{A} \,\&\, \mathcal{B}$, $\mathcal{A} \vee \mathcal{B}$ a $\mathcal{A} \equiv \mathcal{B}$ chápat po řadě jako *zkratky* formulí $\neg(\mathcal{A} \rightarrow \neg\mathcal{B})$, $\neg\mathcal{A} \rightarrow \mathcal{B}$ a $(\mathcal{A} \rightarrow \mathcal{B}) \,\&\, (\mathcal{B} \rightarrow \mathcal{A})$, které jsou vytvořeny na základě formulí $\mathcal{A}$ a $\mathcal{B}$. Zopakujme, že při preferovaném pojetí se při demonstracích obejdeme bez indukčních kroků pro konjunkci, disjunkci a ekvivalenci, což je značná výhoda. Prosím čtenáře, aby se přesvědčil (pochopitelně až po definování pravdivostních hodnot formulí nad rozsáhlejší ze zmíněných abeced), že příslušné dvojice formulí (tedy např. formule $\mathcal{A} \,\&\, \mathcal{B}$ a $\neg(\mathcal{A} \rightarrow \neg\mathcal{B})$) nabývají téže pravdivostní hodnoty pro každé ohodnocení. Takovéto zjištění bude intuitivním ospravedlněním možnosti chápat formule vzniklé konjunkcí, disjunkcí a ekvivalencí jako pouhé zkratky.

Věta. *Nahradíme-li ve formuli její podformuli na kterémkoli místě jinou formulí, dostáváme opět formuli.*

Demonstrace. Buď $\mathcal{B}_1, \ldots, \mathcal{B}_k$ vytvářející posloupnost formule $\mathcal{A}$. Dále buď dána podformule $\mathcal{B}$ formule $\mathcal{A}$ a buď dána formule $\mathcal{C}$. Metamatematickou indukcí ukážeme, že pro $i \leqq k$ je slovo, vzniklé z $\mathcal{B}_i$ nahrazením slova $\mathcal{B}$ slovem $\mathcal{C}$ na kterémkoli místě, opět formulí.

Je-li formule $\mathcal{B}_i$ výrokovou proměnnou, není co ukazovat, neboť $\mathcal{B}_i$ nemá podslova různá od sama sebe.

Jestliže $\mathcal{B}_i$ vznikla logickou operací aplikovanou na formule $\mathcal{B}_j$ a $\mathcal{B}_{j'}$ (případně na jednu formuli $\mathcal{B}_j$), musí být $\mathcal{B}$ podformulí jedné z těchto formulí (nebo samotnou formulí $\mathcal{B}_i$) anebo vůbec není podslovem.

Poslední tvrzení je sice velice intuitivní, avšak přesné prokázání provedeme opět metamatematickou indukcí podle složitosti formule (neboli podle její vytvářející posloupnosti). Nejprve si však uvědomme že (v důsledku správného „uzávorkování“) pro žádné slovo $\Phi_1 \ldots \Phi_n$, které je formulí nemůže existovat $k' < n$ takové, aby buďto $\Phi_1 \ldots \Phi_{k'}$ nebo $\Phi_{k'+1} \ldots \Phi_n$ bylo formulí — avšak abychom byli schopni tvrzení prokázat musíme přesně dodržet definici formule, tzn. nesmíme žádné závorky vynechat.

Předpokládejme tedy, že pro formule $\mathcal{C}_1, \mathcal{C}_2$ je každá formule, která je podslovem kterékoli z této dvojice již podformulí příslušné formule. Nechť formule $\mathcal{D}$ je podslovem formule $\mathcal{C}_1 \rightarrow \mathcal{C}_2$, kteréžto slovo není podformulí žádné z formulí $\mathcal{C}_1$, $\mathcal{C}_2$. Pak $\mathcal{D}$ nemůže být podslovem ani $\mathcal{C}_1$, ani $\mathcal{C}_2$, musí být tudíž vytvořeno z nějakých slov $\mathcal{D}_1$ a $\mathcal{D}_2$ pomocí implikace. Ovšem je-li *formule* $\mathcal{D}$ tvaru $\mathcal{D}_1 \rightarrow \mathcal{D}_2$, jsou slova $\mathcal{D}_1$ a $\mathcal{D}_2$ formulemi, a tudíž $\mathcal{D}_1$ je podformulí formule $\mathcal{C}_1$ a $\mathcal{D}_2$ je podformulí formule $\mathcal{C}_2$. Protože však $\mathcal{D}_1$ je „koncem slova“ $\mathcal{C}_1$ a $\mathcal{D}_2$ je „počátkem slova“ $\mathcal{C}_2$, musí být $\mathcal{D}_1$ totožné s $\mathcal{C}_1$ a současně $\mathcal{D}_2$ totožné s $\mathcal{C}_2$.

Analogickou úvahu provedeme pro negaci, příp. pro další logické operace. Indukcí podle složitosti formule tedy prokážeme, že každá formule má požadovanou vlastnost.

Na základě právě prokázaného jsou indukční kroky pro negaci a implikaci evidentní. Pro implikaci např. stačí uvážit pouze, že pokud je $\mathcal{B}$ podformulí formule $\mathcal{B}_i$ a/nebo formule $\mathcal{B}_j$, je slovo $\mathscr{A}$ vzniklé z formule $\mathcal{B}_i \rightarrow \mathcal{B}_j$ nahrazením formule $\mathcal{B}$ formulí $\mathcal{C}$ implikací, a to implikací s antecedentem (formulí před znakem $\rightarrow$) vzniklým z formule $\mathcal{B}_i$ nahrazením formule $\mathcal{B}$ formulí $\mathcal{C}$ a konsekventem (formulí za znakem $\rightarrow$) vzniklým z formule $\mathcal{B}_j$ nahrazením formule $\mathcal{B}$ formulí $\mathcal{C}$ — speciálně je tedy slovo $\mathscr{A}$ formulí. ■

*

Zabývejme se teď pravdivostními hodnotami formulí výrokového počtu vzniklých pomocí logických spojek.

Intuitivně je přirozené pokládat negaci výroku za nepravdivou, jestliže původní výrok pokládáme za pravdivý, a naopak v případě, že nějaký výrok pokládáme za nepravdivý, jeho negaci pokládáme za pravdivou.

Již jsme zmínili, že v běžném jazyce nejsou obraty odpovídající logickým operacím chápány ve všech situacích stejně. Často uváděným příkladem nejednoznačnosti běžného jazyka je spojka „nebo“, kterou někdy používáme ve vylučovacím smyslu, ale běžně nikoli. Při běžném chápání tedy považujeme za pravdivý i případ, platí-li oba členy. Naproti tomu při emocionálním zvolání „buď tu budu já, nebo ten pes“ vylučujeme, že můžeme zůstat oba. V souhlase s obvyklejším přístupem budeme pokládat disjunkci za nepravdivou, pouze jsou-li nepravdivé *oba* její členy[6]. Chápání konjunkce a ekvivalence nebude činit potíže — konjunkce je pravdivá, právě když jsou pravdivé *oba* její členy (takto již Stoikové) a ekvivalence je pravdivá, jestliže její členy jsou buď oba pravdivé, nebo oba nepravdivé.

Hodnocení pravdivosti implikace v závislosti na ohodnocení pravdivosti výroků, z nichž je implikace složena, již nemusí být na první pohled tak zřejmé, ale jak již zdůrazněno v úvodu, při formalizaci uvažování musíme určit *jednoznačně* význam implikace (tedy hodnotit pravdivost implikace *pouze* v závislosti na hodnocení pravdivosti výroků do ní vstupujících). Řeknu-li „jestliže bude zítra pršet, pak budu celý den doma“ a druhý den venku lije a já jsem z domova pryč, pak jsem lhal; jestliže lije a jsem doma, pak jsem mluvil pravdu; jestliže svítí sluníčko, pak mohu dělat cokoli a vždy jsem mluvil pravdu, protože o tom, co budu dělat, když bude hezky, jsem nic netvrdil[7]. V souladu s intuitivním chápáním důsledku nám tedy nezbude než implikaci pokládat za nepravdivou jenom v případě, že první výrok, nazývaný **antecedent** nebo *předpoklad* či *premisa*, je pravdivý a druhý výrok, nazývaný **konsekvent** nebo *důsledek* (též *sukcedent* či *závěr*), je nepravdivý. Toto chápání je doložitelné již u Diodóra Krona[8].

Následující velice známé tabulky (někdy nazývané *základní pravdivostní tabulky*) shrnují právě popsané pravdivostní hodnoty. Uvědomte si, že každý sloupec druhé z následujících tabulek představuje funkci, která dvojici nul a jedniček přiřazuje hodnotu, která je nulou nebo jedničkou, přičemž přiřazená hodnota se nachází ve stejném řádku jako dvojice, které jest přiřazena. Analogicky první tabulka představuje funkci, která jedničce nebo nule přiřadí nulu nebo jedničku (srovnej cv. 10 a 11).

---

[6] Stoikové vyšetřovali více forem disjunkce, mezi nimi také námi zvolenou.

[7] Gramatika rozlišuje věty příčinné, které (podle pravidel českého pravopisu) vyjadřují „příčinu (důvod) obsahu věty řídící“ a jsou připojovány spojkami protože, poněvadž, že, jelikož a věty podmínkové, které vyjadřují „podmínku, při které může nastat děj věty řídící“ a které se připojují spojkami jestliže, -li, kdyby, jestli, když. Není vhodné formalizovat implikací věty příčinné: větu „přišel jsem pozdě, protože nejela tramvaj“ budeme brát za lživou v případě, že tramvaje jezdily.

[8] Diodóros Kronos vyžaduje navíc „souvislost“ mezi antecedentem a konsekventem, tzn. oproti pojetí dnes běžnému pojetí ještě omezuje obor, kde je aplikovatelná implikace. Formulace přesně odpovídající naší je u jeho následovníka Filóna z Megar. Spor o význam spojek (koncentrovaný převážně do sporu o význam implikace) pokračuje až do 20. stol., a to včetně, většinou však probíhá *vně* matematické logiky. Při snaze přesně vymezit chápání implikace ve smyslu našeho textu se někdy mluví o *materiální implikaci*.

p	¬p
0	1
1	0

p	q	p → q	p & q	p ∨ q	p ≡ q
0	0	1	0	0	1
0	1	1	0	1	0
1	0	0	0	1	0
1	1	1	1	1	1

Na rozdíl od implikace nezávisí hodnoty konjunkce (analogicky disjunkce a ekvivalence) na pořadí formulí v nich se vyskytujících, a proto mluvíme o **složkách** konjunkce, etc., někdy též o *konjunktech* resp. *disjunktech*.

Výše uvedené intuitivní zdůvodnění nám ukazuje, že následující formální definice je v souladu s běžným chápáním.

Definice. Ohodnocením (též *pravdivostním ohodnocením* nebo *valuací*) výrokových proměnných rozumíme jakékoli zobrazení $\mathbb{v}$ přiřazující jednotlivým výrokovým proměnným hodnoty 0 nebo 1 (a definované na jejich systému).

Metamatematickou indukcí (postupně pro členy vytvářející posloupnosti formule) definujeme **pravdivostní hodnotu** $\mathcal{A}[\mathbb{v}]$ (někdy značenou i $\mathbb{v}(\mathcal{A})$) jakékoli formule výrokového počtu $\mathcal{A}$ **při ohodnocení** $\mathbb{v}$ v souladu s výše uvedenými tabulkami následovně[9]:

(1) $\mathcal{B}[\mathbb{v}] = \mathbb{v}(\mathcal{B})$, je-li $\mathcal{B}$ výrokovou proměnnou,
(2) $(\neg\mathcal{B})[\mathbb{v}] = 1$, je-li $\mathcal{B}[\mathbb{v}] = 0$,
$(\neg\mathcal{B})[\mathbb{v}] = 0$, je-li $\mathcal{B}[\mathbb{v}] = 1$,
(3) $(\mathcal{B} \to \mathcal{C})[\mathbb{v}] = 1$ je-li $\mathcal{B}[\mathbb{v}] = 0$ nebo $\mathcal{C}[\mathbb{v}] = 1$,
$(\mathcal{B} \to \mathcal{C})[\mathbb{v}] = 0$, je-li $\mathcal{B}[\mathbb{v}] = 1$ a současně $\mathcal{C}[\mathbb{v}] = 0$.

Tautologií (nebo podrobněji *výrokovou tautologií*) nazýváme formuli $\mathcal{A}$ výrokového počtu, jejíž pravdivostní hodnota $\mathcal{A}[\mathbb{v}]$ je 1 při každém ohodnocení výrokových proměnných $\mathbb{v}$; **kontradikcí** nazýváme formuli $\mathcal{A}$, jejíž pravdivostní hodnota $\mathcal{A}[\mathbb{v}]$ je 0 při každém ohodnocení výrokových proměnných $\mathbb{v}$.

Je-li $\mathcal{A}[\mathbb{v}] = 1$, říkáme, že formule $\mathcal{A}$ je při ohodnocení $\mathbb{v}$ **pravdivá** (někdy též *splněna* nebo $\mathbb{v}$ *splňuje* $\mathcal{A}$). Není-li formule pravdivá při nějakém ohodnocení, říkáme (pochopitelně), že je při tomto ohodnocení **nepravdivá. Formule je splnitelná,** jestliže existuje ohodnocení, při kterém je pravdivá. **Systém formulí je splnitelný,** jestliže existuje ohodnocení, při kterém jsou (najednou) pravdivé všechny formule z tohoto systému[10].

Říkáme, že formule $\mathcal{A}$ (resp. systém formulí $\mathcal{S}$) je (**tautologickým**) **důsledkem systému formulí** $\mathcal{T}$ (a značíme $\mathcal{T} \models \mathcal{A}$, resp. $\mathcal{T} \models \mathcal{S}$)[11], je-li $\mathcal{A}$ (resp. každá formule ze systému $\mathcal{S}$) pravdivá při každém ohodnocení, při kterém jsou pravdivé všechny formule ze systému $\mathcal{T}$. Místo být důsledkem systému $\mathcal{T}$

[9] Jestliže bychom připustili i další spojky jako plnoprávné, museli bychom rozšířit následující definici, a to v souladu se základními pravdivostními tabulkami těchto spojek.

[10] Jestliže každé ohodnocení pokládáme za samostatný model, pak ohodnocení, při kterém je pravdivá formule (resp. jsou pravdivé všechny formule daného systému), nazýváme *modelem* této formule (resp. tohoto systému).

[11] Znak $\models$ je používán pro důsledek i v predikátovém počtu, ale používá se také ve významu splňování (pro predikátový počet viz §2 kap. II, pro výrokový počet někdy $\mathbb{v} \models \mathcal{A}$ místo $\mathcal{A}[\mathbb{v}] = 1$).

se říká také (*tautologicky*) *vyplývat z*, případně být (*tautologicky*) *odvoditelný z* $\mathcal{T}$. Speciálně zápis $\models \mathcal{A}$ znamená, že $\mathcal{A}$ je tautologickým důsledkem prázdného systému, tzn. že je tautologií[12]. □

Je dobré si uvědomit, že podmínky uváděné v jednotlivých dvouřádcích v předchozí definici jsou komplementární, a pro každé ohodnocení je tedy pravdivostní hodnota jakékoli formule určena, a to jednoznačně. Pokud systém $\mathcal{T}$ není splnitelný, je jeho důsledkem jakákoli formule.

Pravdivostní hodnota formule závisí pouze na pravdivostních hodnotách výrokových proměnných v ní se vyskytujících a připomeňme, že těch je jenom konečně mnoho. Pro ověření, zda uvažovaná formule je splnitelná nebo zda je tautologií, stačí tedy vyšetřit konečně mnoho případů ohodnocení. Jsou to tedy algoritmicky rozhodnutelné úlohy a totéž platí i pro vlastnost „být tautologickým důsledkem konečného systému předpokladů“.

Tautologie jsou formule, které nabývají pravdivostní hodnoty 1 při jakémkoli ohodnocení výrokových proměnných. Jedná se tedy o „vždy pravdivé“ formule, tzn. o formule jejichž pravdivost je zaručena pouze jejich formou (strukturou formule). Analogicky kontradikce nabývají pravdivostní hodnoty 0 při jakémkoli ohodnocení výrokových proměnných, a představují tudíž „vždy nepravdivé“ formule.

Ohodnocení je definováno na všech výrokových proměnných, kterých je nekonečně mnoho, a proto ohodnocení *není* konečným objektem. Nicméně již jsme uvedli, že splnitelnost jakékoli formule při daném ohodnocení závisí jen na hodnotách ohodnocení pro výrokové proměnné, které se vyskytují v uvažované formuli. Zastánce finitního směru tedy nebude uvažovat jedno ohodnocení, ale mnoho ohodnocení, z nichž každé je ale jen *konečným* zobrazením ze systému výrokových proměnných do $\{0,1\}$, a definici splňování modifikuje tak, že $\mathcal{A}[\mathbb{v}]$ je definováno, právě když v definičním oboru $\mathbb{v}$ jsou (přinejmenším) všechny výrokové proměnné vyskytující se ve formuli $\mathcal{A}$. Po této modifikaci je celá sémantika výrokového počtu k dispozici i finitistovi.

*

Oblíbeným způsobem výpočtu pravdivostních hodnot jsou **tabulky pravdivostních hodnot**[13] (též *pravdivostní tabulky*). Jednu z nich ukazuje následující příklad (který vede k ohodnocení formule $\neg(\mathsf{p} \to \neg\mathsf{q}) \to \mathsf{p}$), ve kterém každý řádek přísluší jednomu ohodnocení dvojice výrokových proměnných p, q a v každém políčku se nachází pravdivostní hodnota formule uvedené v záhlaví sloupce při tomto ohodnocení. Je zapotřebí si uvědomit, že existují právě čtyři různá ohodnocení dvojice výrokových proměnných p a q, proto má následující tabulka čtyři řádky. Obecně tabulka pravdivostních hodnot formule vytvořené z k výrokových proměnných má 2^k řádků a alespoň tolik sloupců, kolik je podformulí dané formule (pokud nevyužijeme nějakého zjednodušení zápisu).

p	q	$\neg\mathsf{q}$	$\mathsf{p} \to \neg\mathsf{q}$	$\neg(\mathsf{p} \to \neg\mathsf{q})$	$\neg(\mathsf{p} \to \neg\mathsf{q}) \to \mathsf{p}$
0	0	1	1	0	1
0	1	0	1	0	1
1	0	1	1	0	1
1	1	0	0	1	1

[12] Formule, pro které platí $\models \mathcal{A} \equiv \mathcal{B}$ se někdy nazývají *ekvivalentní*, viz také cv. 15.

[13] Tabulky pravdivostních hodnot zavedl Ch. S. Peirce (1839–1914).

Formule $\neg(\mathsf{p} \to \neg\mathsf{q}) \to \mathsf{p}$ jest tedy tautologií, formule $\mathsf{p} \to \neg\mathsf{q}$ nikoli. Dále si uvědomme, že pravdivostní hodnota formule $\neg(\mathsf{p} \to \neg\mathsf{q})$ je stejná jako pravdivostní hodnota formule $\mathsf{p}\ \&\ \mathsf{q}$ pro každé ohodnocení (tedy, že chápání druhé formule jako zkratky za formuli první je v souladu s intuicí).

*

Jestliže $\mathfrak{T}$ je jakýkoli systém formulí výrokového počtu a $\mathcal{A}$ je jakákoli formule téhož počtu, pak $\mathfrak{T}, \mathcal{A}$ značí systém formulí $\mathfrak{T}$ rozšířený o formuli $\mathcal{A}$ (tj. v množinové terminologii $\mathfrak{T}, \mathcal{A}$ je množinou $\mathfrak{T} \cup \{\mathcal{A}\}$). Při této konvenci jest zřejmě $\mathfrak{T} \models \mathcal{A}$, právě když systém $\mathfrak{T}, \neg\mathcal{A}$ není splnitelný. Přes svou trivialitu je tento vztah často používán a je sémantickou analogií syntaktického tvrzení, že $\mathfrak{T}, \neg\mathcal{A}$ je sporná, právě když $\mathcal{A}$ je dokazatelná v $\mathfrak{T}$ (viz §2).

Dalším často používaným a opět jednoduchým vztahem je

$$(\mathfrak{T}, \mathcal{A} \models \mathcal{B}) \Leftrightarrow (\mathfrak{T} \models \mathcal{A} \to \mathcal{B}),$$

který je sémantickou obdobou syntakticky formulované věty o dedukci (viz opět následující paragraf). Jestliže totiž při každém ohodnocení výrokových proměnných, při kterém jsou pravdivé všechny formule ze systému $\mathfrak{T}$, je pravdivá i formule $\mathcal{A} \to \mathcal{B}$, pak stačí uvážit definici pravdivostní hodnoty přiřazené implikaci a vidíme, že při každém ohodnocení výrokových proměnných, při kterém jsou pravdivé všechny formule ze systému $\mathfrak{T}, \mathcal{A}$, je pravdivá i formule $\mathcal{B}$. Naopak jestliže předpokládáme, že při každém ohodnocení výrokových proměnných, při kterém jsou pravdivé všechny formule ze systému $\mathfrak{T}, \mathcal{A}$, je pravdivá i formule $\mathcal{B}$, pak uvažujeme-li jakékoli ohodnocení výrokových proměnných, při kterém jsou pravdivé všechny formule ze systému $\mathfrak{T}$, stačí opět pohlédnout na definici pravdivosti implikace a uvidíme, že při tomto ohodnocení je pravdivá i formule $\mathcal{A} \to \mathcal{B}$.

Pro každé systémy formulí $\mathfrak{T}, \mathfrak{S}, \mathfrak{R}$ platí evidentně

(a) je-li $\mathfrak{S}$ podsystémem $\mathfrak{T}$, je $\mathfrak{T} \models \mathfrak{S}$,

(b) je-li $\mathfrak{T} \models \mathfrak{S}$ a $\mathfrak{S} \models \mathfrak{R}$, je $\mathfrak{T} \models \mathfrak{R}$.

Podmínku (b) můžeme (využívajíce (a)) formulovat také ve tvaru

(b′) značí-li $\overline{\mathfrak{T}}$ systém všech formulí tautologicky odvoditelných ze systému $\mathfrak{T}$, jest $\overline{\overline{\mathfrak{T}}} = \overline{\mathfrak{T}}$.

Jako důsledek věty o kompaktnosti vyslovené v §3 této kapitoly dostaneme — po jejím prokázání — navíc podmínku

(c) jestliže $\mathfrak{T} \models \mathcal{A}$, pak existuje konečný podsystém $\mathfrak{Q}$ systému $\mathfrak{T}$ takový, že $\mathfrak{Q} \models \mathcal{A}$[14].

[14] Uvedené podmínky formuloval A. Tarski.

§2

SYNTAX VÝROKOVÉHO POČTU

Vytváření formulí je součástí syntaxe, takže o úplných základech syntaxe výrokového počtu jsme již pojednali v předchozím paragrafu. V právě počínajícím paragrafu se budeme věnovat zejména dokazatelnosti ve výrokovém počtu.

Za **axiomy výrokového počtu** vezmeme všechny formule, které jsou některého ze tří následujících tvarů, kde $\mathcal{P}, \mathcal{Q}$ a $\mathcal{R}$ označují *jakékoli* formule výrokového počtu:

VP1 $$\mathcal{P} \to (\mathcal{Q} \to \mathcal{P}),$$
VP2 $$[\mathcal{P} \to (\mathcal{Q} \to \mathcal{R})] \to [(\mathcal{P} \to \mathcal{Q}) \to (\mathcal{P} \to \mathcal{R})],$$
VP3 $$(\neg\mathcal{P} \to \neg\mathcal{Q}) \to (\mathcal{Q} \to \mathcal{P}).$$

Za dedukční (odvozovací) pravidlo přijmeme **modus ponens,** dovolující z dvojice formulí $\mathcal{P}$ a $\mathcal{P} \to \mathcal{Q}$ vyvodit formuli $\mathcal{Q}$.

Před intuitivním zdůvodněním pravidel **VP**1–**VP**3 si uvědomme, že se jedná o schémata, neboť axiomem je formule uvedeného typu pro libovolné formule $\mathcal{P}, \mathcal{Q}, \mathcal{R}$ výrokového počtu. Jde tedy o nekonečně mnoho axiomů konečně mnoha typů[1)].

Jestliže přijmeme nějaké tvrzení jako předpoklad, pak pro nás toto přijaté tvrzení již vyplývá z čehokoli (formalizací této úvahy je **VP**1). Zdůrazněme, že tuto úvahu provedeme i v případě, kdy nevíme, zda první tvrzení je pravdivé, a dokonce axiom přijímáme, i když $\mathcal{P}$ je nepravdivé — např. $\neg\mathcal{Q} \to (\mathcal{Q} \to \neg\mathcal{Q})$ je axiomem nezávisle na tom, zda $\mathcal{Q}$ je pravdivé!

Jestliže z prvního tvrzení vyplývá druhé a z druhého vyplývá třetí, pak z prvého tvrzení již musí vyplývat třetí (tzn. vyplývání je tranzitivní). Uvedený dokazovací princip uvádí již Theofrastos z Eresu (lze připisovat i Aristotelovi). Jeho formalizací je formule $(\mathcal{P} \to \mathcal{Q}) \to [(\mathcal{Q} \to \mathcal{R}) \to (\mathcal{P} \to \mathcal{R})]$ výrokového počtu[2)], kterou budeme pro snazší zapamatování nazývat **tranzitivitou implikace,** i když tradici by více odpovídal název *zákon hypotetického sylogismu*. Schéma **VP**2 je mírně „zesílenou“ verzí tranzitivity implikace (protože předpoklad $\mathcal{P} \to (\mathcal{Q} \to \mathcal{R})$ je slabší než předpoklad $\mathcal{Q} \to \mathcal{R}$) a v popsané podobě ho využijeme v demonstraci věty o dedukci (někdy je nazýváno *Fregův zákon*).

V matematice často místo toho, abychom dokazovali, že z jednoho tvrzení plyne druhé, ukazujeme, že z negace druhého tvrzení plyne negace prvního tvrzení; formalizací tohoto principu je **VP**3. Tento princip je obměnou *zákona transpozice*[3)] $(\mathcal{P} \to \mathcal{Q}) \to (\neg\mathcal{Q} \to \neg\mathcal{P})$, přijímaného již Stoiky (viz (4) třetí věty tohoto paragrafu a (2) z cvičení 7). Uvedený princip je i podstatou často užívaného principu **důkazu sporem** (viz dále, princip důkazu sporem se také nazývá *reductio ad absurdum*): jestliže z nějakého tvrzení dovodíme něco nepravdivého, pak princip důkazu sporem

---

1) Obměna našeho systému, mající pouze konečně mnoho axiomů (tři) a konečně mnoho dedukčních pravidel (dvě), je uvedena na konci paragrafu.

2) či ekvivalentně $(\mathcal{Q} \to \mathcal{R}) \to [(\mathcal{P} \to \mathcal{Q}) \to (\mathcal{P} \to \mathcal{R})]$

3) nazývaného někdy též *zákonem kontrapozice*

nám dovolí uzavřít, že nemůže být udržitelný náš původní předpoklad, tzn. že jsme dokázali negaci výchozího tvrzení.

Dokazovací pravidlo modus ponens se ve starší literatuře označuje jako *modus ponendo ponens* (viz cvičení 8), česky se nazývá *pravidlo odloučení* a anglicky převážně detachment rule. Je uváděno také již Theofrastem a bylo užíváno už před Aristotelem. Intuitivní správnost tohoto pravidla je zcela zřejmá, neboť jestliže ukážeme, že z jednoho tvrzení plyne druhé, a jestliže prokážeme první tvrzení, pak musíme přijmout za prokázané i druhé. Formule $\mathcal{Q}$ se někdy nazývá **bezprostředním důsledkem formulí** $\mathcal{P}$ a $\mathcal{P} \to \mathcal{Q}$.

Pokud někdo věří více kalkulaci než odvolání na intuici, může se ubezpečit o správnosti axiomů ověřením, že jde o tautologie (tento výpočet budeme stejně potřebovat pro větu o korektnosti v příštím paragrafu).

Definice. Je-li $\mathfrak{T}$ jakýkoli systém formulí výrokového počtu, pak **důkazem ze systému předpokladů** (*axiomů*) $\mathfrak{T}$[4] (též prostě **důkazem z předpokladů** $\mathfrak{T}$) rozumíme posloupnost formulí $\mathcal{D}_1, \dots, \mathcal{D}_k$ výrokového počtu takovou, že pro každé $i \leqq k$ vznikne formule $\mathcal{D}_i$ *některým* z následujících způsobů:

(a) je axiomem výrokového počtu,
(b) je jedním z předpokladů systému $\mathfrak{T}$,
(c) vyplývá z formulí v důkazu předcházejících pomocí dedukčního pravidla modus ponens (podrobněji: existují $j, j' < i$ tak, že $\mathcal{D}_{j'}$ je formulí $\mathcal{D}_j \to \mathcal{D}_i$).

Posloupnost $\mathcal{D}_1, \dots, \mathcal{D}_k$, vyhovující výše uvedené podmínce, nazýváme také **důkazem** (poslední) **formule** výrokového počtu $\mathcal{D}_k$ ze systému předpokladů $\mathfrak{T}$.

Formuli $\mathcal{A}$ výrokového počtu nazýváme **dokazatelnou** ze systému předpokladů $\mathfrak{T}$, jestliže existuje její důkaz z uvedeného systému. Dokazatelnost formule $\mathcal{A}$ ze systému předpokladů $\mathfrak{T}$ značíme $\mathfrak{T} \vdash \mathcal{A}$. **Dokazatelností ve výrokovém počtu** rozumíme dokazatelnost bez předpokladů (tj. pro prázdný systém $\mathfrak{T}$) a v souhlase s předchozím ji značíme $\vdash \mathcal{A}$.

Formuli nazveme **vyvratitelnou** ze systému předpokladů $\mathfrak{T}$, jestliže její negace je dokazatelná ze systému předpokladů $\mathfrak{T}$.

Systém formulí výrokového počtu nazýváme **sporný** (též *inkonzistentní*), jestliže je v něm dokazatelná každá formule výrokového počtu (nad zkoumanou abecedou). Systém formulí, který není sporný, nazýváme **bezesporný** (též *konzistentní*). □

Naprosto triviálním, ale často používaným pozorováním je, že důkaz ze systému předpokladů $\mathfrak{T}$ je důkazem i z každého systému předpokladů $\mathfrak{S}$ obsahujícího všechny formule z $\mathfrak{T}$. Každá formule vyskytující se v důkazu ze systému předpokladů je pochopitelně dokazatelná z těchto předpokladů.

Je také zcela zřejmé, že lze zobecnit pravidlo modus ponens na tvrzení, že je-li ze systému předpokladů $\mathfrak{T}$ dokazatelná jak formule $\mathcal{A} \to \mathcal{B}$, tak i formule $\mathcal{A}$, pak je z téhož systému předpokladů $\mathfrak{T}$ dokazatelná formule $\mathcal{B}$ — na toto jednoduché tvrzení se budeme odvolávat jako na **princip modus ponens.** Stačí totiž prodloužit

[4] V takovéto souvislosti budeme formule ze systému $\mathfrak{T}$ nazývat **předpoklady** (*axiomy*).

(jakožto posloupnost formulí) důkaz formule $\mathcal{A} \to \mathcal{B}$ o důkaz formule $\mathcal{A}$, ověřit, že takto vznikne důkaz ze systému předpokladů $\mathcal{T}$, a tento důkaz dále prodloužit o jediný další krok použitím odvozovacího *pravidla* modus ponens.

V dalším budeme konstruovat různé důkazy. V těchto konstrukcích je řada kroků zcela rutinních (např. použití modus ponens), avšak některé kroky se jeví pro ten který důkaz klíčové. Pro snazší pochopení podstaty každého jednotlivého důkazu se budu, jak již uvedeno při popisu značení, snažit podtržením zdůraznit kroky, které jsou pro sestrojovaný důkaz — dle mého názoru — nejdůležitější. Pro přehlednost budeme také na pravé straně uvádět zdůvodnění jednotlivých kroků.

Věta 1[5]**.** $\vdash \mathcal{A} \to \mathcal{A}$.

Demonstrace. Následující posloupnost je důkazem ve výrokovém počtu:

$$\underline{\big(\mathcal{A} \to [(\mathcal{A} \to \mathcal{A}) \to \mathcal{A}]\big) \to \big([\mathcal{A} \to (\mathcal{A} \to \mathcal{A})] \to (\mathcal{A} \to \mathcal{A})\big)},$$

	VP2, do kterého dosadíme za $\mathcal{P}$ a $\mathcal{R}$ formuli $\mathcal{A}$ a za $\mathcal{Q}$ dosadíme formuli $\mathcal{A} \to \mathcal{A}$,
$\mathcal{A} \to [(\mathcal{A} \to \mathcal{A}) \to \mathcal{A}]$,	**VP**1, do kterého dosadíme za $\mathcal{P}$ formuli $\mathcal{A}$ a za $\mathcal{Q}$ dosadíme formuli $\mathcal{A} \to \mathcal{A}$,
$[\mathcal{A} \to (\mathcal{A} \to \mathcal{A})] \to (\mathcal{A} \to \mathcal{A})$,	modus ponens,
$\mathcal{A} \to (\mathcal{A} \to \mathcal{A})$,	**VP**1, do kterého dosadíme za $\mathcal{P}$ i $\mathcal{Q}$ formuli $\mathcal{A}$,
$\mathcal{A} \to \mathcal{A}$,	modus ponens. ■

*

Následující věta o dedukci je jedním z prostředků, které zpřehledňují demonstrace a usnadňují nalezení potřebných důkazů. Princip, který vyjadřuje věta o dedukci, bude mnohokrát použit v našem textu. Potřeba takovýchto prostředků (další budou formulovány v poslední větě tohoto paragrafu) je zcela očividná, neboť důkaz zcela triviálního tvrzení $\mathcal{A} \to \mathcal{A}$ měl pět kroků, plně provedené důkazy složitějších tvrzení by byly velice těžko průhledné a přetěžce bychom pro každé jednotlivé tvrzení hledali znovu a znovu metodu konstrukce důkazu (na druhé straně po nalezení důkazu by ověření, že se jedná o důkaz, již obtížné nebylo, bylo by jenom zdlouhavé). Poznamenejme, že podobná věta o dedukci v predikátovém počtu má ještě širší použití. Pro některé účely je potřeba zdůraznit, že v demonstraci věty o dedukci *není* (a ani v predikátovém počtu nebude) použit **VP**3. Nadto si uvědomme, že **VP**3 nebyl použit ani v důkazu formule $\mathcal{A} \to \mathcal{A}$.

Věta 2 (o dedukci). *Pro každý systém formulí výrokového počtu $\mathcal{T}$ a pro každé formule výrokového počtu $\mathcal{A}, \mathcal{B}$ platí*

$$\mathcal{T}, \mathcal{A} \vdash \mathcal{B} \quad \Leftrightarrow \quad \mathcal{T} \vdash \mathcal{A} \to \mathcal{B}.$$

Demonstrace. $\Leftarrow$ K důkazu formule $\mathcal{A} \to \mathcal{B}$ ze systému předpokladů $\mathcal{T}$ stačí přidat dvojici formulí

[5] Formule $\mathcal{A} \to \mathcal{A}$ se někdy nazývá ***zákon totožnosti***, srovnej také s dále uvedeným zákonem vyloučeného třetího.

$\mathcal{A}$,	jeden předpoklad ze systému $\mathfrak{T}, \mathcal{A}$,
$\mathcal{B}$,	modus ponens

a získáme důkaz formule $\mathcal{B}$ ze systému předpokladů $\mathfrak{T}, \mathcal{A}$.

$\Rightarrow$ Nechť $\mathcal{D}_1, \ldots, \mathcal{D}_k$ je důkaz formule $\mathcal{B}$ ze systému předpokladů $\mathfrak{T}, \mathcal{A}$ (tedy $\mathcal{D}_k$ je totožná s $\mathcal{B}$). Indukcí budeme pro formule $\mathcal{D}_1, \ldots, \mathcal{D}_k$ demonstrovat, že $\mathfrak{T} \vdash \mathcal{A} \to \mathcal{D}_i$ (dokonce induktivně dáme návod, jak transformovat důkaz formule $\mathcal{B}$ ze systému předpokladů $\mathfrak{T}, \mathcal{A}$ na důkaz formule $\mathcal{A} \to \mathcal{B}$ ze systému předpokladů $\mathfrak{T}$). Rozeberme jednotlivé možnosti, jakými se pro $i \leqq k$ mohla do důkazu dostat formule $\mathcal{D}_i$:

(1) $\mathcal{D}_i$ je buďto axiomem logiky a nebo některým z předpokladů z $\mathfrak{T}$. Pak posloupnost formulí

$\mathcal{D}_i \to (\mathcal{A} \to \mathcal{D}_i)$,	axiom typu **VP1**,
$\mathcal{D}_i$,	axiom výrokového počtu nebo jeden předpoklad ze systému $\mathfrak{T}$,
$\mathcal{A} \to \mathcal{D}_i$,	modus ponens

je důkazem formule $\mathcal{A} \to \mathcal{D}_i$ ze systému předpokladů $\mathfrak{T}$.

(2) Je-li $\mathcal{D}_i$ formulí $\mathcal{A}$ (což je jeden z předpokladů z $\mathfrak{T}, \mathcal{A}$), pak $\vdash \mathcal{A} \to \mathcal{A}$ je obsahem předchozí věty, a stačí si tedy uvědomit, že $\vdash \mathcal{C}$ zaručuje $\mathfrak{T} \vdash \mathcal{C}$.

(3) Jestliže $\mathcal{D}_i$ je bezprostředním důsledkem formulí $\mathcal{D}_j$ a $\mathcal{D}_{j'}$ (tzn. užíváme-li na uvedené formule modus ponens), pak $\mathcal{D}_{j'}$ je formulí $\mathcal{D}_j \to \mathcal{D}_i$ a $j, j' < i$. Tedy dle indukčního předpokladu existuje posloupnost $\mathcal{C}_1, \ldots, \mathcal{C}_{n_j}, \mathcal{A} \to \mathcal{D}_j$, která je důkaz formule $\mathcal{A} \to \mathcal{D}_j$ ze systému předpokladů $\mathfrak{T}$ (je-li $n_j = 0$, je posloupnost $\mathcal{C}_1, \ldots, \mathcal{C}_{n_j}$ prázdnou posloupností). Současně indukční předpoklad také zaručuje existenci posloupnosti $\mathcal{B}_1, \ldots, \mathcal{B}_{n_{j'}}, \mathcal{A} \to (\mathcal{D}_j \to \mathcal{D}_i)$, která je důkaz formule $\mathcal{A} \to \mathcal{D}_{j'}$ ze systému předpokladů $\mathfrak{T}$. Přidáme-li k posloupnosti $\mathcal{C}_1, \ldots, \mathcal{C}_{n_j}, \mathcal{A} \to \mathcal{D}_j, \mathcal{B}_1, \ldots, \mathcal{B}_{n_{j'}}$, $\mathcal{A} \to (\mathcal{D}_j \to \mathcal{D}_i)$ tři formule

$(\mathcal{A} \to (\mathcal{D}_j \to \mathcal{D}_i)) \to ((\mathcal{A} \to \mathcal{D}_j) \to (\mathcal{A} \to \mathcal{D}_i))$,	axiom typu **VP2**,
$(\mathcal{A} \to \mathcal{D}_j) \to (\mathcal{A} \to \mathcal{D}_i)$,	modus ponens,
$\mathcal{A} \to \mathcal{D}_i$,	modus ponens,

dostaneme důkaz formule $\mathcal{A} \to \mathcal{D}_i$ z předpokladů $\mathfrak{T}$. ∎

Poznamenejme, že věta o dedukci je asi nejdůležitější ze všech prostředků zpřehledňujících demonstrace. V následujících větách uvedeme některé často používané typy formulí dokazatelných ve výrokovém počtu a zejména další často užívané „důkazové bloky“, tzn. principy umožňující zkracování a zpřehledňování důkazů. Pro začátek si uvědomme, že princip modus ponens můžeme při použití věty o dedukci reformulovat tak, že

$$\text{jestliže } \mathfrak{T} \vdash \mathcal{A} \ \text{ a } \ \mathfrak{T}, \mathcal{A} \vdash \mathcal{B}, \ \text{ pak } \ \mathfrak{T} \vdash \mathcal{B}$$

neboli intuitivně „vše co je dokázáno, lze použít při dalším dokazování“.

Dále je také evidentní, že pro libovolné $\mathfrak{T}$ a libovolné formule $\mathcal{A}$, $\mathcal{B}$ a $\mathcal{C}$ výrokového počtu

$$\text{jestliže } \mathfrak{T} \vdash \mathcal{A} \to \mathcal{B} \ \text{ a } \ \mathfrak{T} \vdash \mathcal{B} \to \mathcal{C}, \ \text{ pak } \ \mathfrak{T} \vdash \mathcal{A} \to \mathcal{C},$$

neboť za uvedeného předpokladu je

$\mathcal{T}, \mathcal{A} \vdash \mathcal{B}$, věta o dedukci aplikovaná na $\mathcal{A} \to \mathcal{B}$,
$\mathcal{T}, \mathcal{A} \vdash \mathcal{C}$, princip modus ponens užívající $\mathcal{T} \vdash \mathcal{B} \to \mathcal{C}$,
$\mathcal{T} \vdash \mathcal{A} \to \mathcal{C}$, věta o dedukci.

Na uvedený princip se budeme odvolávat jako na **princip tranzitivity implikace.** Zkrátí nám mnohokrát demonstrace (tento princip můžeme chápat i jako jinou formulaci tranzitivity implikace). Možnost odvodit vyslovený princip (při jehož odvození jsme použili **VP**2) lze pojímat jako upřesnění již deklarovaného faktu, že **VP**2 je „zesílením" principu tranzitivity implikace.

Uvědomme si, že věta o dedukci (spolu s modus ponens) stírá poněkud rozdíl mezi ukázáním dokazatelnosti formule ve výrokovém počtu a prokázáním, že k ní příslušný odvozovací princip je nahraditelný (tedy i správný) ve zvoleném systému. Např. přijímáme-li princip tranzitivity implikace, dostaneme dokazatelnost tranzitivity implikace tj. $\vdash (\mathcal{A} \to \mathcal{B}) \to [(\mathcal{B} \to \mathcal{C}) \to (\mathcal{A} \to \mathcal{C})]$ dvojnásobným užitím věty o dedukci a naopak místo použití principu tranzitivity implikace bychom do důkazu mohli napsat posledně zmíněnou formuli (spolu s jejím důkazem) a použít dvakrát modus ponens. V jistém ohledu je tedy aplikace principu tranzitivity implikace téměř totéž jako užití dokazatelnosti tranzitivity implikace.

*

Formule výrokového počtu, jejichž dokazatelnost ukážeme ve větě příští, použijeme při demonstraci poslední věty tohoto paragrafu a věty o úplnosti v následujícím paragrafu. Tyto formule mají navíc jasný intuitivní význam:

(1) „z nemožného plyne cokoli"[6] — **zákon Dunse Scota**; jestliže totiž přijmeme $\neg\mathcal{A}$, pak již z $\mathcal{A}$ plyne cokoli[7];
(2) a (3) lze chápat jako „dvojitou negaci je možno vynechat" (ve formě $\neg\neg\mathcal{A} \equiv \mathcal{A}$ se nazývají *zákonem dvojité negace*, tento princip lze připsat již stoicko-megarské škole[8]);
(4) je obrácením implikace v axiomu **VP**3 a bylo zmíněno jako zákon transpozice na začátku paragrafu;
(5) lze vykládat „z $\mathcal{A}$ a $\mathcal{B}$ plyne $\mathcal{A}$ & $\mathcal{B}$", neboť $\mathcal{A}$ & $\mathcal{B}$ je definováno jako zkratka za $\neg(\mathcal{A} \to \neg\mathcal{B})$ (podrobnější rozbor viz dále, kde je použit k motivaci další věty).

Příklady mnoha dalších dokazatelných formulí výrokového počtu budou uvedeny v druhé polovině příštího paragrafu.

Věta 3. *Jsou-li $\mathcal{A}$ a $\mathcal{B}$ formule výrokového počtu, pak máme:*

(1) $\vdash \neg\mathcal{A} \to (\mathcal{A} \to \mathcal{B})$,
(2) $\vdash \neg\neg\mathcal{A} \to \mathcal{A}$,

---

[6] Od scholastické logiky je známo jako „Ex impossibili sequitur quodlibet"; užitím pravidla (4) komentované věty na tento princip dostaneme (viz cv. 6) „Nutné vyplývá z čehokoli" neboli „Necessarium sequitur ad quodlibet".

[7] Zákon Dunse Scota bychom mohli napsat $(\neg\mathcal{A}$ & $\mathcal{A}) \to \mathcal{B}$, protože $\neg\mathcal{A}$ & $\mathcal{A}$ je „nemožné", srovnej „vyloučení kontradikce", tj. formuli (17) ze seznamu ke konci příštího paragrafu. Při převádění (1) věty 3 na tvar $(\neg\mathcal{A}$ & $\mathcal{A}) \to \mathcal{B}$ je vhodné využít formule (21) z téhož seznamu.

[8] V této souvislosti je poněkud překvapující, že není známo, že by se tato škola pokusila explicitně popsat pravdivostní hodnotu negace v závislosti na pravdivostní hodnotě příslušné formule. Naproti tomu popis pro implikaci, kterou je možno považovat za „složitější", je dokumentován.

(3) $\vdash \mathcal{A} \to \neg\neg\mathcal{A}$,
(4) $\vdash (\mathcal{A} \to \mathcal{B}) \to (\neg\mathcal{B} \to \neg\mathcal{A})$,
(5) $\vdash \mathcal{A} \to [\neg\mathcal{B} \to \neg(\mathcal{A} \to \mathcal{B})]$.

Demonstrace.

(1)	$\underline{\vdash \neg\mathcal{A} \to (\neg\mathcal{B} \to \neg\mathcal{A})}$,	**VP**1,
	$\vdash (\neg\mathcal{B} \to \neg\mathcal{A}) \to (\mathcal{A} \to \mathcal{B})$,	**VP**3,
	$\vdash \neg\mathcal{A} \to (\mathcal{A} \to \mathcal{B})$,	princip tranzitivity implikace;
(2)	$\underline{\vdash \neg\neg\mathcal{A} \to (\neg\mathcal{A} \to \neg\neg\neg\mathcal{A})}$,	aplikace (1),
	$\neg\neg\mathcal{A} \vdash (\neg\mathcal{A} \to \neg\neg\neg\mathcal{A})$,	věta o dedukci,
	$\vdash (\neg\mathcal{A} \to \neg\neg\neg\mathcal{A}) \to (\neg\neg\mathcal{A} \to \mathcal{A})$,	**VP**3,
	$\neg\neg\mathcal{A} \vdash \neg\neg\mathcal{A} \to \mathcal{A}$,	princip modus ponens,
	$\neg\neg\mathcal{A} \vdash \mathcal{A}$,	věta o dedukci,
	$\vdash \neg\neg\mathcal{A} \to \mathcal{A}$,	věta o dedukci;
(3)	$\underline{\vdash \neg\neg\neg\mathcal{A} \to \neg\mathcal{A}}$,	aplikace (2),
	$\vdash (\neg\neg\neg\mathcal{A} \to \neg\mathcal{A}) \to (\mathcal{A} \to \neg\neg\mathcal{A})$,	**VP**3,
	$\vdash \mathcal{A} \to \neg\neg\mathcal{A}$,	princip modus ponens;
(4)	$\mathcal{A} \to \mathcal{B} \vdash \neg\neg\mathcal{A} \to \neg\neg\mathcal{B}$,	(2) a (3) a dvojnásobně princip tranzitivity implikace,
	$\vdash (\neg\neg\mathcal{A} \to \neg\neg\mathcal{B}) \to (\neg\mathcal{B} \to \neg\mathcal{A})$,	**VP**3,
	$\mathcal{A} \to \mathcal{B} \vdash \neg\mathcal{B} \to \neg\mathcal{A}$,	princip modus ponens,
	$\vdash (\mathcal{A} \to \mathcal{B}) \to (\neg\mathcal{B} \to \neg\mathcal{A})$,	věta o dedukci;
(5)	$\mathcal{A}, \mathcal{A} \to \mathcal{B} \vdash \mathcal{B}$,	aplikace modus ponens na předpoklady,
	$\mathcal{A} \vdash (\mathcal{A} \to \mathcal{B}) \to \mathcal{B}$,	věta o dedukci aplikovaná na formuli $\mathcal{A} \to \mathcal{B}$,
	$\underline{\mathcal{A} \vdash ((\mathcal{A} \to \mathcal{B}) \to \mathcal{B}) \to (\neg\mathcal{B} \to \neg(\mathcal{A} \to \mathcal{B}))}$,	(4) aplikované na formuli $(\mathcal{A} \to \mathcal{B})$ a formuli $\mathcal{B}$,
	$\mathcal{A} \vdash \neg\mathcal{B} \to \neg(\mathcal{A} \to \mathcal{B})$,	princip modus ponens,
	$\vdash \mathcal{A} \to (\neg\mathcal{B} \to \neg(\mathcal{A} \to \mathcal{B}))$,	věta o dedukci. ■

Předchozí věta je formulována pro libovolné formule $\mathcal{A}, \mathcal{B}$ výrokového počtu. První část následující věty však ukazuje, že případná formulace pouze pro výrokové proměnné by byla slabší jenom zdánlivě.

Uvědomme si, že zákon Dunse Scota (spolu s modus ponens) umožňuje ukázat, že systém formulí $\mathfrak{T}$ je sporný, právě když existuje formule $\mathcal{A}$ taková, že z předpokladů $\mathfrak{T}$ je dokazatelná jak formule $\mathcal{A}$, tak i formule $\neg\mathcal{A}$.

*

Motivujme nyní poněkud podrobněji tvrzení následující věty. Jak jsme již uvedli, jedná se o formulaci dalších odvozovacích principů. Na jedné straně použití těchto dodatečných odvozovacích principů podstatně zjednoduší konstrukci důkazů, ale na druhé straně následující věta prokazuje, že tyto principy jsou v každém jednotlivém případě nahraditelné pomocí jediného dedukčního pravidla modus ponens (při současném využití axiomů **VP**1–**VP**3).

Výše jsme vlastně intuitivně zdůvodňovali vztah (5) předchozí věty jeho reformulací tvaru $\vdash \mathcal{A} \to [\mathcal{B} \to \neg(\mathcal{A} \to \neg\mathcal{B})]$ (viz (2) ze seznamu uvedeného v §3). Pokud v tvrzení (5) místo $\mathcal{B}$ píšeme $\neg\mathcal{B}$, získáme $\vdash \mathcal{A} \to [\neg\neg\mathcal{B} \to \neg(\mathcal{A} \to \neg\mathcal{B})]$. Je celkem jednoduché reformulaci $\vdash \mathcal{A} \to [\mathcal{B} \to \neg(\mathcal{A} \to \neg\mathcal{B})]$ z dokazatelnosti $\vdash \mathcal{A} \to [\neg\neg\mathcal{B} \to \neg(\mathcal{A} \to \neg\mathcal{B})]$ ukázat[9)]. Je však pochopitelně výhodnější prokázat jednou provždy možnost nahradit podformule formulemi s nimi ekvivalentními než hledat konstrukci důkazu pro každý jednotlivý případ zvlášť.

Princip, o kterém je řeč, můžeme formulovat $\mathcal{P}_1 \equiv \mathcal{Q}_1, \ldots, \mathcal{P}_k \equiv \mathcal{Q}_k \vdash \mathcal{A} \equiv \mathcal{B}$, kde $\mathcal{B}$ vznikne nahrazením *některých* (tzn. ne nutně všech[10)]) výskytů podformulí $\mathcal{P}_1, \ldots, \mathcal{P}_k$ formule $\mathcal{A}$ po řadě formulemi $\mathcal{Q}_1, \ldots, \mathcal{Q}_k$. Dosud jsme však podrobněji nepopsali chování spojek, které zavádíme jako zkratky, a proto budeme princip formulovat raději ve tvaru $\mathcal{P}_1 \to \mathcal{Q}_1, \mathcal{Q}_1 \to \mathcal{P}_1, \ldots, \mathcal{P}_k \to \mathcal{Q}_k, \mathcal{Q}_k \to \mathcal{P}_k \vdash \mathcal{A} \to \mathcal{B}$. Při této formulaci také více vynikne, že pro *jednu* implikaci, svazující formule $\mathcal{A}$ a $\mathcal{B}$, potřebujeme (v obecném případě) *obě* implikace svazující $\mathcal{P}_i$ a $\mathcal{Q}_i$. Na druhé straně již pak triviálně symetrií dokážeme i druhou implikaci svazující formule $\mathcal{A}$ a $\mathcal{B}$. K problematice popisu chování dalších spojek se vrátíme na konci příštího paragrafu poté, co dokončíme, pokud možno v sevřené podobě, popis vlastností negace a implikace. Pak bude také zřejmé, že obě uvedené formulace vyjadřují totéž.

Poznamenejme, že v demonstraci analogické věty pro predikátový počet budeme muset rozlišit více případů (kvantifikace), ale podstatné je, že příslušná část demonstrace z tohoto paragrafu je aplikovatelná i při dosazování formulí predikátového počtu (viz formulaci v §3 kap. II). V příští kapitole již nebudeme demonstraci tudíž znovu opakovat.

Důkaz sporem a **důkaz rozborem případů** jsou tak běžné odvozovací principy v matematice, že by neměly potřebovat přílišné vysvětlování. Běžnost těchto principů naopak způsobuje, že kdybychom nebyli schopni možnost použití těchto dovozovacích prostředků předvést, pokládali bychom náš systém za „slabý“ (uveďme však, že např. intuicionistická logika nepřipouští důkaz sporem). Pro lepší orientaci připomeňme, že např. běžný důkaz, že součin dvou po sobě jdoucích přirozených čísel je sudý, používá rozbor případů, protože v něm rozlišíme případ, že x je sudé (a pak součin s čímkoli je sudý), a případ, kdy x je liché, ve kterémžto případu si uvědomíme, že potom je $x + 1$ sudé.

Nicméně *formulace* principu důkazu rozborem případů může vyvolat jisté obtíže. Rozeberme tedy trochu podrobněji formulaci tvrzení (4) následující věty. Na první pohled se zdá nepřirozené, že na jedné (levé) straně se mluví o dokazatelnosti z předpokladu $\mathcal{A} \vee \mathcal{B}$ (tedy z disjunkce) a na straně druhé (pravé) se vyžaduje *současná* dokazatelnost jak z předpokladu $\mathcal{A}$, tak i z předpokladu $\mathcal{B}$ (pro jednoduchost výkladu teď předpokládám, že systém $\mathfrak{T}$, použitý při obecné formulaci ve větě 4, je prázdný). Mnozí studenti by však pokládali za intuitivně přijatelnější, kdyby i na pravé straně se požadovala dokazatelnost z předpokladu $\mathcal{A}$ *nebo* z předpokladu $\mathcal{B}$. Takovéto oslabení požadavku na pravé straně však není přijatelné, jak vzápětí ukážeme. Uvažujme výrokové proměnné p a q a formuli $\mathsf{p} \vee \mathsf{q}$. Podle první věty tohoto

9) Stačí použít na začátku i na konci demonstrace větu o dedukci a jako jádro demonstrace užít tvrzení (3) předchozí věty, formuli $\mathcal{A} \to [\neg\neg\mathcal{B} \to \neg(\mathcal{A} \to \neg\mathcal{B})]$ a princip tranzitivity implikace.

10) Tedy korektně dostaneme např. $\mathcal{P} \equiv \mathcal{Q} \vdash (\mathcal{P} \to \mathcal{P}) \equiv (\mathcal{P} \to \mathcal{Q})$.

paragrafu a podle věty o dedukci je $\mathsf{p} \vdash \mathsf{p}$, a tedy $(\mathsf{p} \vdash \mathsf{p}$ nebo $\mathsf{q} \vdash \mathsf{p})$; naproti tomu není $\mathsf{p} \vee \mathsf{q} \vdash \mathsf{p}$. Z věty o dedukci bychom pak totiž dostali $\vdash (\mathsf{p} \vee \mathsf{q}) \rightarrow \mathsf{p}$, ale tato formule *není pravdivá* při ohodnocení, které proměnné p přiřazuje 0 a proměnné q přiřazuje 1, a tedy intuitivně cítíme, že posledně uvedená formule nemůže být dokazatelná ve výrokovém počtu (zcela rigorózně úvahu dokončíme použitím věty o korektnosti uvedené v následujícím paragrafu).

Poslední princip je speciálním případem rozboru případů, neboť formule $\mathsf{p} \vee \neg \mathsf{p}$ je zkratkou za formuli $\neg \mathsf{p} \rightarrow \neg \mathsf{p}$, a je tedy dokazatelná ve výrokovém počtu. Uveďme, že formule $\mathsf{p} \vee \neg \mathsf{p}$ je označována jako **zákon vyloučeného třetího** (*tertium non datur*), který byl velmi zdůrazňován již Chrýsippem ze Soloi.

Prosím čtenáře, aby si uvědomil, že důkaz sporem je svou strukturou dosti výjimečný. Běžně z předpokladů, které pokládáme za správné, vyvozujeme další tvrzení, při důkazu sporem naopak předpokládáme platnost toho, co chceme vyvrátit.

Ve znění věty o nahrazení se uvažuje posloupnost výrokových proměnných $\mathsf{p}_1, \ldots, \mathsf{p}_k$; chceme-li být naprosto přesní, musíme explicitně přijmout (implicitně evidentně přijímaný) předpoklad, že uvedené výrokové proměnné jsou od sebe různé, tj. že i-tá hodnota posloupnosti $\mathsf{p}_1, \ldots, \mathsf{p}_k$ je různá od j-té pro různá $i, j \leqq k$. Naproti tomu různost formulí $\mathcal{P}_1, \ldots, \mathcal{P}_k$ se nevyžaduje.

Věta 4. (1) **(Věta o nahrazení).** *Jestliže formule $\mathcal{B}$ výrokového počtu vznikne nahrazením* ***všech*** *výskytů (od sebe různých) výrokových proměnných $\mathsf{p}_1, \ldots, \mathsf{p}_k$ po řadě formulemi $\mathcal{P}_1, \ldots, \mathcal{P}_k$ výrokového počtu ve formuli $\mathcal{A}$, pak*

$$(\vdash \mathcal{A}) \;\Rightarrow\; (\vdash \mathcal{B}).$$

(2) **(Věta o ekvivalenci).** *Vznikne-li formule $\mathcal{B}$ výrokového počtu z formule $\mathcal{A}$ výrokového počtu nahrazením jejích podformulí $\mathcal{P}_1, \ldots, \mathcal{P}_k$ po řadě formulemi $\mathcal{Q}_1, \ldots, \mathcal{Q}_k$ výrokového počtu, pak*

$$\mathcal{P}_1 \rightarrow \mathcal{Q}_1, \mathcal{Q}_1 \rightarrow \mathcal{P}_1, \ldots, \mathcal{P}_k \rightarrow \mathcal{Q}_k, \mathcal{Q}_k \rightarrow \mathcal{P}_k \vdash \mathcal{A} \rightarrow \mathcal{B},$$

tedy speciálně $\vdash \mathcal{A}$ zaručí $\mathcal{P}_1 \rightarrow \mathcal{Q}_1, \mathcal{Q}_1 \rightarrow \mathcal{P}_1, \ldots, \mathcal{P}_k \rightarrow \mathcal{Q}_k, \mathcal{Q}_k \rightarrow \mathcal{P}_k \vdash \mathcal{B}$.

Nadto pro každý systém $\mathcal{T}$ a všechny formule $\mathcal{A}, \mathcal{B}$ a $\mathcal{C}$ výrokového počtu platí

(3) **(Věta o důkazu sporem).** $\mathcal{T} \vdash \mathcal{A} \;\Leftrightarrow\; [\mathcal{T}, \neg\mathcal{A} \vdash \neg(\mathcal{C} \rightarrow \mathcal{C})]$,

(4) **(Věta o důkazu rozborem případů).** $\mathcal{T}, \mathcal{A} \vee \mathcal{B} \vdash \mathcal{C} \;\Leftrightarrow$
$\Leftrightarrow\; [\mathcal{T}, \mathcal{A} \vdash \mathcal{C}$ *a současně* $\mathcal{T}, \mathcal{B} \vdash \mathcal{C}]$,

(5) **(Věta o neutrální formuli).** $\mathcal{T} \vdash \mathcal{C} \;\Leftrightarrow$
$\Leftrightarrow\; [\mathcal{T}, \mathcal{A} \vdash \mathcal{C}$ *a současně* $\mathcal{T}, \neg\mathcal{A} \vdash \mathcal{C}]$.

Demonstrace. (1) Buď $\mathcal{D}_1, \ldots, \mathcal{D}_{k'}$ důkaz formule $\mathcal{A}$. Uvažme posloupnost formulí $\mathcal{C}_1, \ldots, \mathcal{C}_{k'}$, kde $\mathcal{C}_i$ jsou (pro $i \leqq k'$) formule vzniklé nahrazením výrokových proměnných $\mathsf{p}_1, \ldots, \mathsf{p}_k$ po řadě formulemi $\mathcal{P}_1, \ldots, \mathcal{P}_k$ výrokového počtu ve formuli $\mathcal{D}_i$. Ukážeme, že posloupnost $\mathcal{C}_1, \ldots, \mathcal{C}_{k'}$ je opět důkazem.

Je-li $\mathcal{D}_i$ axiomem výrokového počtu, je axiomem téhož typu i formule $\mathcal{C}_i$.

Tato úvaha je korektní v případě nahrazování výrokových proměnných. Avšak v případě nahrazování *podformulí* jinými formulemi již korektní *není*[11]. Je také zřejmé, že pro korektnost uvedené úvahy potřebujeme, aby výrokové proměnné v posloupnosti $\mathsf{p}_1, \ldots, \mathsf{p}_k$ byly různé[12].

---

[11] Například nahrazením podformule $\mathsf{q} \rightarrow \mathsf{p}$ výrokovou proměnnou q dostáváme z formule $\mathsf{p} \rightarrow (\mathsf{q} \rightarrow \mathsf{p})$, která je axiomem, formuli $\mathsf{p} \rightarrow \mathsf{q}$, která již dokazatelná není (což by intuitivně mělo být zřejmé, přesná demonstrace využije větu o korektnosti z následujícího paragrafu).

[12] Ku příkladu nahradíme-li r v axiomu $[\mathsf{p} \rightarrow (\mathsf{q} \rightarrow \mathsf{r})] \rightarrow [(\mathsf{p} \rightarrow \mathsf{q}) \rightarrow (\mathsf{p} \rightarrow \mathsf{r})]$ jednou formulí p

Jestliže formule $\mathcal{D}_i$ byla odvozena pomocí modus ponens aplikovaného na formule $\mathcal{D}_j, \mathcal{D}_{j'}$, kde $j, j' < i$, pak formule $\mathcal{D}_{j'}$ je formulí $\mathcal{D}_j \to \mathcal{D}_i$. Po nahrazení výrokových proměnných $\mathsf{p}_1, \ldots, \mathsf{p}_k$ po řadě formulemi $\mathcal{P}_1, \ldots, \mathcal{P}_k$ výrokového počtu ve formuli $\mathcal{D}_j \to \mathcal{D}_i$ dostaneme formuli $\mathcal{C}_j \to \mathcal{C}_i$ (tzn. provedeme-li napřed nahrazení a pak spojíme formule do implikace, dostaneme totéž, jako když napřed spojíme formule do implikace, a pak provedeme nahrazení; viz demonstrace věty §1). Formule $\mathcal{C}_i$ tedy opět vyplývá z formulí $\mathcal{C}_j$ a $\mathcal{C}_{j'}$ pravidlem modus ponens.

(2) Prokážeme opět indukcí, tentokrát postupně pro formule vyskytující se ve vytvářející posloupnosti formule $\mathcal{A}$ výrokového počtu. K prověření kroku pro konstrukci formule negací stačí prokázat tvrzení $\mathsf{p} \to \mathsf{q}, \mathsf{q} \to \mathsf{p} \vdash \neg\mathsf{p} \to \neg\mathsf{q}$, což je důsledkem (4) předchozí věty a věty o dedukci. Pro krok odpovídající konstrukci implikace stačí prokázat $\mathsf{p}_1 \to \mathsf{q}_1, \mathsf{q}_1 \to \mathsf{p}_1, \mathsf{p}_2 \to \mathsf{q}_2, \mathsf{q}_2 \to \mathsf{p}_2 \vdash (\mathsf{p}_1 \to \mathsf{p}_2) \to (\mathsf{q}_1 \to \mathsf{q}_2)$, což získáme dvojnásobnou aplikací principu tranzitivity implikace a věty o dedukci.

(3) $\Rightarrow$	$\vdash \neg\mathcal{A} \to [\mathcal{A} \to \neg(\mathcal{C} \to \mathcal{C})]$	(1) předchozí věty
	$\mathfrak{T}, \neg\mathcal{A} \vdash \mathcal{A} \to \neg(\mathcal{C} \to \mathcal{C})$	věta o dedukci
	$\mathfrak{T}, \neg\mathcal{A} \vdash \neg(\mathcal{C} \to \mathcal{C})$	princip modus ponens využívající $\mathfrak{T} \vdash \mathcal{A}$
$\Leftarrow$	$\mathfrak{T} \vdash \neg\mathcal{A} \to \neg(\mathcal{C} \to \mathcal{C})$	věta o dedukci
	$\mathfrak{T} \vdash (\mathcal{C} \to \mathcal{C}) \to \mathcal{A}$	**VP**3 a princip modus ponens
	$\mathfrak{T} \vdash \mathcal{A}$	princip modus ponens využívající $\vdash \mathcal{C} \to \mathcal{C}$
(4) $\Leftarrow$	$\mathfrak{T} \vdash \mathcal{A} \to \mathcal{C}$	věta o dedukci aplikovaná na $\mathfrak{T}, \mathcal{A} \vdash \mathcal{C}$
	$\mathfrak{T} \vdash \mathcal{B} \to \mathcal{C}$	věta o dedukci aplikovaná na $\mathfrak{T}, \mathcal{B} \vdash \mathcal{C}$
	$\mathfrak{T} \vdash \neg\mathcal{C} \to \neg\mathcal{A}$	(4) předchozí věty a princip modus ponens
	$\mathfrak{T}, (\neg\mathcal{A} \to \mathcal{B}) \vdash \neg\mathcal{C} \to \mathcal{C}$	dvakrát užitý princip tranzitivity implikace
	$\vdash \neg\mathcal{C} \to [\neg\mathcal{C} \to \neg(\neg\mathcal{C} \to \mathcal{C})]$	(5) předchozí věty použité pro $\neg\mathcal{C}$ a $\mathcal{C}$
	$\vdash \neg\mathcal{C} \to \neg(\neg\mathcal{C} \to \mathcal{C})$	třikrát užitá věta o dedukci; uvědomte si, že $\mathcal{P}, \mathcal{P} \vdash \mathcal{Q}$, právě když $\mathcal{P} \vdash \mathcal{Q}$
	$\vdash (\neg\mathcal{C} \to \mathcal{C}) \to \mathcal{C}$	**VP**3 a princip modus ponens
	$\mathfrak{T}, (\neg\mathcal{A} \to \mathcal{B}) \vdash \mathcal{C}$	princip modus ponens.

Nyní si stačí uvědomit, že $\mathcal{A} \vee \mathcal{B}$ je zkratkou za $\neg\mathcal{A} \to \mathcal{B}$.

Obrácená implikace je triviální, neboť $\vdash \mathcal{A} \to (\neg\mathcal{A} \to \mathcal{B})$ a současně máme $\vdash \mathcal{B} \to (\neg\mathcal{A} \to \mathcal{B})$.

Jak už zmíněno, (5) je speciálním případem (4), neboť $\mathcal{A} \vee \neg\mathcal{A}$ (tj. formule $\neg\mathcal{A} \to \neg\mathcal{A}$) je dokazatelná dle první věty tohoto paragrafu, a postačí tedy použít princip modus ponens (a větu o dedukci). ■

Uvědomme si, že reformulací věty o důkazu sporem je tvrzení, že

$$\mathfrak{T} \vdash \mathcal{A}, \quad \text{právě když systém formulí} \quad \mathfrak{T}, \neg\mathcal{A} \text{ je sporný,}$$

a jednou ponecháme beze změny (tj. nahradíme r formulí r) a současně nahradíme-li q formulí p (tzn. uvažujeme-li posloupnost $\mathsf{p}_1, \mathsf{p}_2, \mathsf{p}_3$, kde p_1 a p_2 jsou rovny r a p_3 je rovné q), dostaneme formuli $[\mathsf{p} \to (\mathsf{p} \to \mathsf{p})] \to [(\mathsf{p} \to \mathsf{p}) \to (\mathsf{p} \to \mathsf{r})]$ a po dvojnásobném užití principu modus ponens bychom dále dostali, že je dokazatelná formule $\mathsf{p} \to \mathsf{r}$, jejíž nedokazatelnost jsme již deklarovali.

neboť dle zákona Dunse Scota $\vdash \neg(\mathcal{C} \to \mathcal{C}) \to [(\mathcal{C} \to \mathcal{C}) \to \mathcal{B}]$ pro libovolnou formuli $\mathcal{B}$ výrokového počtu, a k ukázání spornosti teorie $\mathcal{T}, \neg\mathcal{A}$ z předpokladu $\mathcal{T}, \neg\mathcal{A} \vdash \neg(\mathcal{C} \to \mathcal{C})$ tedy stačí použít dvojnásobně princip modus ponens a $\vdash \mathcal{C} \to \mathcal{C}$.

*

Již jsme zdůraznili, že zkoumaný systém axiomů a dokazovacího pravidla není jediný možný. Pokud by někdo chtěl mít jen konečně mnoho axiomů (nestačilo by mu konečně mnoho *typů* axiomů), mohl by přijmout za axiomy

VP1′ $\quad \mathsf{p} \to (\mathsf{q} \to \mathsf{p}),$

VP2′ $\quad [\mathsf{p} \to (\mathsf{q} \to \mathsf{r})] \to [(\mathsf{p} \to \mathsf{q}) \to (\mathsf{p} \to \mathsf{r})],$

VP3′ $\quad (\neg\mathsf{p} \to \neg\mathsf{q}) \to (\mathsf{q} \to \mathsf{p})$

a pravidlo modus ponens a **pravidlo nahrazení ve výrokovém počtu** (čímž myslíme pochopitelně pravidlo popsané větou o nahrazení, tj. pravidlo dovolující z formule $\mathcal{P}$ vyvodit jakoukoli formuli, která vznikne z formule $\mathcal{P}$ nahrazením všech výskytů (od sebe různých) výrokových proměnných $\mathsf{p}_1, \ldots, \mathsf{p}_k$ po řadě formulemi $\mathcal{P}_1, \ldots, \mathcal{P}_k$). V takovémto systému evidentně dokážeme — v důsledku věty o nahrazení — právě tytéž formule jako v námi vybraném systému. Uvědomte si, že pokud používáte náš původní systém, smíte nahrazovat proměnné v axiomech **VP**1′–**VP**3′ pouze na začátku (a tak získáte naše axiomy **VP**1–**VP**3), naopak při použití pravidla nahrazení smíte nahrazovat v jakékoli již dokázané formuli. Tvrdíme, že „zvětšení“ možností při druhém přístupu je nepodstatné.

§3

ÚPLNOST VÝROKOVÉHO POČTU, NORMÁLNÍ TVAR FORMULE

strany 43–51

CVIČENÍ I

1) Ukažte, že $(\mathfrak{p} \to \mathfrak{q}) \to (\mathfrak{p} \to \neg\mathfrak{q})$ a $\neg(\mathfrak{p} \to \neg\mathfrak{q}) \to (\mathfrak{p} \to \mathfrak{q})$ jsou formule výrokového počtu, najděte všechny jejich podformule, určete všechny společné podformule. Je slovo $\mathfrak{q}) \to (\mathfrak{p}$ společným podslovem, či dokonce společnou podformulí? Prokažte. Sestrojte tabulky pravdivostních hodnot těchto formulí. Je některá z nich tautologií? Vyjádřete formule ekvivalentně jednoduššími formulemi výrokového počtu.

2) Prokažte větu z §1 tím, že pro každou formuli vzniklou nahrazením podformule přímo sestrojíte její vytvářející posloupnost na základě vytvářejících posloupností formule, ve které nahrazujeme, a formule, kterou dosazujeme.

3) Jsou formule $(\mathfrak{q} \to \mathfrak{r}) \to \big((\neg\mathfrak{p} \to \mathfrak{r}) \to [(\mathfrak{p} \to \mathfrak{q}) \to \mathfrak{r}]\big)$, $\neg(\mathfrak{p} \to \mathfrak{q}) \to \mathfrak{p}$ a $\mathfrak{p} \to (\neg\mathfrak{p} \to \mathfrak{q})$ tautologiemi? Sestrojte (podejte návod konstrukce) jejich důkazy (návod: pro prvou formuli použijte tranzitivitu implikace a větu o neutrální formuli, pro druhou tvrzení (3) ze třetího paragrafu a způsob zavedení konjunkce, pro třetí zákon Dunse Scota) a zkuste jim dát intuitivní význam (dokazatelnost uvedených formulí využijeme v následujícím textu).

Dále dokažte $(\mathfrak{p} \to \mathfrak{q}) \equiv (\neg\mathfrak{p} \vee \mathfrak{q})$ a prokázané využijte k dokázání $[(\mathfrak{p} \,\&\, \mathfrak{q}) \to \mathfrak{r}] \equiv [(\mathfrak{p} \to \mathfrak{r}) \vee (\mathfrak{q} \to \mathfrak{r})]$. Návod: Navíc užijte de Morganovo pravidlo, (25) §3, komutativitu a asociativitu disjunkce a větu o ekvivalenci.

4) Ukažte, že formule $(\mathfrak{q} \to \mathfrak{r}) \to [(\mathfrak{p} \to \mathfrak{q}) \to \mathfrak{r}]$ není tautologií. Srovnejte intuitivní význam této formule a tranzitivity implikace.

5) Popište tabulku pravdivostních hodnot pro vylučující disjunkci a srovnejte ji s tabulkou pro negaci ekvivalence. Dokažte $[(\mathfrak{p} \vee \mathfrak{q}) \,\&\, \neg(\mathfrak{p} \,\&\, \mathfrak{q})] \equiv \neg(\mathfrak{p} \equiv \mathfrak{q})$.

6) Při použití prvních čtyř tvrzení věty 3 §2 (a věty o ekvivalenci) ukažte $\mathcal{Q} \to \neg(\neg\mathcal{P} \,\&\, \mathcal{P})$.

7) V naší notaci je možno zapsat základní pravidla Stoiků (nazývaná „nedokazovaná“), z nichž první odpovídá modus ponens

(1) $[(\mathcal{P} \to \mathcal{Q}) \,\&\, \mathcal{P}] \to \mathcal{Q}$,
(2) $[(\mathcal{P} \to \mathcal{Q}) \,\&\, \neg\mathcal{Q}] \to \neg\mathcal{P}$,
(3) $[\neg(\mathcal{P} \,\&\, \mathcal{Q}) \,\&\, \mathcal{P}] \to \neg\mathcal{Q}$,
(4) $[(\mathcal{P} \oplus \mathcal{Q}) \,\&\, \mathcal{P}] \to \neg\mathcal{Q}$,
(5) $[(\mathcal{P} \oplus \mathcal{Q}) \,\&\, \neg\mathcal{P}] \to \mathcal{Q}$.

Ukažte jejich korektnost za předpokladu, že $\oplus$ je symbol pro vylučující disjunkci.

Uvažujte (4′) a (5′) vzniklé z (4) a (5) nahrazením vylučující disjunkce běžnou disjunkcí. Zvažte, zda takto vzniklá pravidla jsou korektní. Návod: pro jedno z pravidel nalezněte ohodnocení, při kterém neplatí.

Uvažte následující dedukční pravidla:

(a) $(\mathcal{P} \,\&\, \mathcal{Q}) \to \mathcal{R}, \neg\mathcal{R} \,\&\, \mathcal{Q} \vdash \neg\mathcal{P}$,
(b) $(\mathcal{P} \,\&\, \mathcal{Q}) \to \mathcal{R}, \mathcal{S} \to \mathcal{P} \vdash (\mathcal{S} \,\&\, \mathcal{Q}) \to \mathcal{R}$.

Ukažte jejich korektnost a rozmyslete si jejich intuitivní význam.

Stoikové uváděli čtyři dedukční pravidla. Pravidla (a) a (b) odpovídají prvnímu a třetímu pravidlu Stoiků, přičemž musíme připustit i symetrická pravidla $(\mathcal{P} \,\&\, \mathcal{Q}) \to \mathcal{R}, \mathcal{P} \,\&\, \neg\mathcal{R} \vdash \neg\mathcal{Q}$ a $(\mathcal{P} \,\&\, \mathcal{Q}) \to \mathcal{R}, \mathcal{S} \to \mathcal{Q} \vdash (\mathcal{P} \,\&\, \mathcal{S}) \to \mathcal{R}$. Druhé a čtvrté pravidlo je ztraceno. Stoickému vyjádření by přesněji odpovídalo formulovat (1)–(5) jako pravidla a (a), (b) jako „metapravidla“. U Stoiků se však nalezne i pravidlo odpovídající větě o dedukci (což by umožnilo jejich metapravidla chápat jako pravidla). Stoikové používali číslovky místo výrokových proměnných, tedy např. „Jestliže prvé, pak druhé. Avšak prvé. Tedy druhé.“

8) Kromě pravidla *modus ponendo ponens* (obvykle prostě modus ponens) („tvrdící tvrzením“) $\mathcal{P}, \mathcal{P} \to \mathcal{Q} \vdash \mathcal{Q}$ byla pokládána za podstatná také pravidla *modus tollendo tollens* (často prostě modus tollens; „popírající popíráním“) $\neg\mathcal{Q}, \mathcal{P} \to \mathcal{Q} \vdash \neg\mathcal{P}$ (viz rovněž bod (2) předchozího cvičení), *modus tollendo ponens* $\neg\mathcal{P}, \mathcal{P} \vee \mathcal{Q} \vdash \mathcal{Q}$ a *modus ponendo tollens* $\mathcal{P}, \neg(\mathcal{P} \mathbin{\&} \mathcal{Q}) \vdash \neg\mathcal{Q}$ (viz také bod (3) předchozího cvičení). Odvozovací princip odpovídající větě o rozboru případů býval nazýván *konstruktivní dilema* a za důležité bylo pokládáno i *destruktivní dilema* $\neg\mathcal{Q} \vee \neg\mathcal{R}, \mathcal{P} \to (\mathcal{Q} \mathbin{\&} \mathcal{R}) \vdash \neg\mathcal{P}$. Prokažte korektnost těchto pravidel, příp. dokažte odpovídající formule (tj. formule vzniklé užitím věty o dedukci) ve výrokovém počtu.

9) Ukažte, že formule vzniklá jen (jakkoli iterovaným) použitím konjunkcí a disjunkcí (bez negace!) není nikdy tautologií ani kontradikcí. Není tedy možné použít pro výstavbu formulí pouze tuto dvojici operací. Dále ukažte, že pomocí negace a ekvivalence nevyjádříme implikaci (návod: počet ohodnocení, při kterých je implikace pravdivá, je lichý). Naproti tomu vyjádřete implikaci pomocí negace a konjunkce a také pomocí negace a disjunkce, z čehož vyvoďte, že pro výstavbu formulí můžeme používat tyto dvojice místo dvojice negace a implikace.

10) Ukažte, že pro každou funkci F zobrazující $\{0,1\}^n$ do $\{0,1\}$ (tak zvanou **booleovskou funkci**) existuje formule $\mathcal{A}$ výrokového počtu, ve které se vyskytují pouze výrokové proměnné $\mathtt{p}_1, \ldots, \mathtt{p}_n$ a taková, že pro každé ohodnocení $\mathbb{v}$ těchto proměnných platí $\mathcal{A}[\mathbb{v}] = F(\mathbb{v}(\mathtt{p}_1), \ldots, \mathbb{v}(\mathtt{p}_n))$. Návod: Uvažte demonstraci věty o normálním tvaru.

11) Nechť formule $\mathcal{A}|\mathcal{B}$ (**Shefferova operace**, méně často nazývaná *exkluzí*) je vyjádřitelná formulí $\neg(\mathcal{A} \mathbin{\&} \mathcal{B})$ (tj. obratem „neplatí současně ... a ... “)[1]. Ukažte, že pro libovolné ohodnocení $\mathbb{v}$ výrokových proměnných $\mathtt{p}, \mathtt{q}$ je $(\neg\mathtt{p})[\mathbb{v}] = (\mathtt{p}|\mathtt{p})[\mathbb{v}]$ a $(\mathtt{p} \mathbin{\&} \mathtt{q})[\mathbb{v}] = ((p|q)|(p|q))[\mathbb{v}]$; vyjádřete implikaci pomocí Shefferovy operace. Při budování formulí je tedy možno používat pouze samotnou Shefferovu operaci.

Zjistěte zda existují i jiné (a které) binární operace na formulích, jež mají stejnou vlastnost. Návod: Všech možných (booleovských) funkcí zobrazujících $\{0,1\}^2$ do $\{0,1\}$ je sice 16, ale okamžitě můžeme vyřadit ty operace F, pro které $F(1,1) = 1$, protože pak nikdy nemůžeme pomocí F vyjádřit formuli $\neg\mathtt{p}$, a analogicky vyřadíme ty operace F, pro které $F(0,0) = 0$. Zbudou jen čtyři možnosti, ale z nich dvě operace jsou ve skutečnosti unární; operace, která je vyjádřitelná formulí $\neg\mathcal{A} \mathbin{\&} \neg\mathcal{B}$ se nazývá *Peirceova* (také *Nicodova*).

Srovnejte obrat běžného jazyka „ani ... ani ... “ s Peirceovou operací.

12) Vyjádřete formule $\mathtt{p} \mathbin{\&} (\mathtt{q} \equiv \neg\mathtt{p})$, $(\mathtt{p} \to \mathtt{q}) \mathbin{\&} (\mathtt{q} \to \mathtt{p}) \mathbin{\&} (\neg\mathtt{p} \mathbin{\&} \mathtt{q})$ a $[\mathtt{p} \to (\mathtt{q} \mathbin{\&} \mathtt{r})] \vee \mathtt{q}$ v normálním tvaru.

Ukažte větu o normální formě bez použití věty o úplnosti. Návod: Podle složitosti formule výrokového počtu ukazujte existenci obou tvarů současně; při kroku pro negaci využijete existenci druhého tvaru a de Morganových pravidel, při kroku pro implikaci využijete $\vdash (\mathcal{A} \to \mathcal{B}) \equiv (\neg\mathcal{A} \vee \mathcal{B})$, předpokládanou existenci obou tvarů a opět de Morganova pravidla.

[1] Existují i (nepřevažující) texty připisující Stoikům chápání disjunkce ve významu uvedené formule.

13) **Polská** (*bezzávorková*, též *prefixní*) **notace.** Definujeme formule tak, že:

(a) každá výroková proměnná je formulí,

(b) je-li $\mathcal{A}$ formulí, je $\neg\mathcal{A}$ formulí a je-li i $\mathcal{B}$ formulí, jsou formulemi i $\rightarrow\mathcal{A}\mathcal{B}$, $\vee\mathcal{A}\mathcal{B}$, $\&\mathcal{A}\mathcal{B}$, $\equiv\mathcal{A}\mathcal{B}$,

(c) všechny formule dostaneme postupnou aplikací pravidel (a) a (b).

Ukažte vzájemně jednoznačnou korespondenci formulí podle této definice a dle definice dříve zavedené a uvědomte si, že v polské notaci jsou k formuli $\mathcal{A}$ jednoznačně určeny jak formule, tak i operace, jimiž formule $\mathcal{A}$ vznikne, a to vše bez použití závorek (za cenu snížení přehlednosti textu). Název prefixní vyjadřuje, že logická spojka předchází formule, na které je operace aplikována.

14) Ukažte, že systém formulí $\mathcal{T}$ výrokového počtu je sporný, právě když existuje formule $\mathcal{A}$ výrokového počtu tak, že $\mathcal{T} \vdash (\mathcal{A} \ \& \ \neg\mathcal{A})$, a to je, právě když existuje formule $\mathcal{B}$ tak, že $\mathcal{T} \vdash \mathcal{B}$ a současně $\mathcal{T} \vdash \neg\mathcal{B}$. Prokažte, že formule výrokového počtu je splnitelná, právě když není kontradikcí.

15) Formule $\mathcal{A}, \mathcal{B}$ výrokového počtu se nazývají **(výrokově) ekvivalentní,** jestliže $\mathcal{A} \models \mathcal{B}$ a současně $\mathcal{B} \models \mathcal{A}$. Ukažte, že $\mathcal{A} \models \mathcal{B}$, právě když $\vdash \mathcal{A} \rightarrow \mathcal{B}$, a že $\mathcal{A}$ a $\mathcal{B}$ jsou výrokově ekvivalentní, právě když $\vdash \mathcal{A} \equiv \mathcal{B}$, tzn. právě když $\models \mathcal{A} \equiv \mathcal{B}$.

16) Platí, že $\mathcal{T} \vdash \mathcal{A}$ a současně $\mathcal{S} \vdash \mathcal{A}$, právě když $\mathcal{T} \cap \mathcal{S} \vdash \mathcal{A}$? Platí, že $\mathcal{T} \vdash \mathcal{A}$ nebo $\mathcal{S} \vdash \mathcal{A}$, právě když $\mathcal{T} \cup \mathcal{S} \vdash \mathcal{A}$? Prokažte nebo najděte protipříklady. Zaručuje v předchozích případech alespoň jedna podmínka druhou?

17) (Věta o dualitě) Nechť ve formuli $\mathcal{A}$ výrokového počtu se vyskytují jenom spojky $\neg, \&, \vee$ a nechť formule $\mathcal{B}$ vznikne z $\mathcal{A}$ záměnou znaku $\&$ znakem $\vee$ a znaku $\vee$ znakem $\&$ a záměnou výrokové proměnné její negací. Ukažte $\vdash \neg\mathcal{A} \equiv \mathcal{B}$. Návod: Prokazujte postupně podle složitosti formule při použití de Morganových pravidel.

Formulujte rovněž pro formule obsahující další spojky. Návod: Užijte $(\mathsf{p} \rightarrow \mathsf{q}) \equiv (\neg\mathsf{q} \rightarrow \neg\mathsf{p})$ a $(\mathsf{p} \equiv \mathsf{q}) \equiv (\neg\mathsf{p} \equiv \neg\mathsf{q})$.

18) Ukažte, že schéma **VP**3 lze nahradit schématem

$$(\neg\mathcal{Q} \rightarrow \neg\mathcal{P}) \rightarrow [(\neg\mathcal{Q} \rightarrow \mathcal{P}) \rightarrow \mathcal{Q}].$$

Návod: Nejprve ukažte, že $\neg\mathcal{Q} \rightarrow \neg\mathcal{P}, \neg\mathcal{Q} \rightarrow \mathcal{P}, \neg\mathcal{Q}$ je sporná, naproti tomu k prokázání

$$\big((\neg\mathcal{Q} \rightarrow \neg\mathcal{P}) \rightarrow [(\neg\mathcal{Q} \rightarrow \mathcal{P}) \rightarrow \mathcal{Q}]\big) \rightarrow [(\neg\mathcal{Q} \rightarrow \neg\mathcal{P}) \rightarrow (\mathcal{P} \rightarrow \mathcal{Q})]$$

v systému bez **VP**3 uvažte, že demonstrace věty o dedukci nevyužívá **VP**3, a prokažte, že z předpokladů

$$\mathcal{P}, \neg\mathcal{Q} \rightarrow \neg\mathcal{P}, (\neg\mathcal{Q} \rightarrow \neg\mathcal{P}) \rightarrow [(\neg\mathcal{Q} \rightarrow \mathcal{P}) \rightarrow \mathcal{Q}]$$

existuje důkaz formule $\mathcal{Q}$ využívající pouze **VP**1, **VP**2 a modus ponens (k čemuž využijte formuli $\mathcal{P} \rightarrow (\neg\mathcal{Q} \rightarrow \mathcal{P})$ a tranzitivitu implikace).

19) *Pravidlem řezu* se nazývá dedukční pravidlo dovolující z formulí $\neg\mathcal{P} \vee \mathcal{Q}$ a $\mathcal{P} \vee \mathcal{R}$ odvodit formuli $\mathcal{Q} \vee \mathcal{R}$. Je často používáno (případně jeho obměny) v gentzenovských systémech. Ukažte korektnost tohoto pravidla. (Pro pravidlo řezu aplikované na literály se užívá název *pravidlo rezoluce*.)

Ukažte, že pravidlo řezu je vzájemně nahraditelné s pravidlem modus ponens za předpokladu, že ve zkoumaném gentzenovském systému smíme využívat záměny popsané formulí (23) §4 (tedy za předpokladu vhodné volby použitého gentzenovského systému). Návod: V systému popsaném v předchozím textu ukažte

$\neg\mathcal{P} \vee \mathcal{Q}, \mathcal{P} \vee \mathcal{R} \vdash \mathcal{Q} \vee \mathcal{R}$; naopak v gentzenovském systému (tzn. bez modus ponens!) ukažte, že $\mathcal{P} \to \mathcal{Q}, \mathcal{P} \vdash \mathcal{Q}$ využívajíce záměn popsaných formulí (23) a používajíce vyjádření formule $\mathcal{P} \to \mathcal{Q}$ formulí $\neg\mathcal{P} \vee \mathcal{Q}$.

20) Uvažte dokazovací systém sestávající z jediného axiomu $\neg\mathcal{P} \vee \mathcal{P}$ a z dedukčních pravidel: z $\mathcal{P}$ odvoď $\mathcal{Q} \vee \mathcal{P}$ (prodloužení), z $\mathcal{P} \vee \mathcal{P}$ odvoď $\mathcal{P}$ (stažení či zjednodušení pro disjunkci), z $\mathcal{P} \vee (\mathcal{Q} \vee \mathcal{R})$ odvoď $(\mathcal{P} \vee \mathcal{Q}) \vee \mathcal{R}$ (asociativita), z $\mathcal{P} \vee \mathcal{Q}$ a $\neg\mathcal{P} \vee \mathcal{R}$ odvoď $\mathcal{Q} \vee \mathcal{R}$ (řez). Ukažte, že uvedený systém je korektní (nebo přímo prokažte uvedená dedukční pravidla v systému uvedeném v textu). Systém z tohoto cvičení je také úplný (viz např. [Sh1]), a tudíž stejně silný jako námi vyšetřovaný.

21) Uvažte dokazovací systém z dedukčních pravidel:

(1) $\mathcal{P} \vdash \mathcal{P}$,
(2) jestliže $\mathfrak{T} \vdash \mathcal{Q}$, pak $\mathfrak{T} - \{\mathcal{P}\} \vdash \mathcal{P} \to \mathcal{Q}$ (srovnej s větou o dedukci),
(3) jestliže $\mathfrak{T} \vdash \mathcal{Q}$ a $\mathfrak{S} \vdash \neg\mathcal{Q}$, pak $(\mathfrak{T} \cup \mathfrak{S}) - \{\neg\mathcal{P}\} \vdash \mathcal{P}$ (srovnej s větou o důkazu sporem),
(4) jestliže $\mathfrak{T} \vdash \mathcal{P} \to \mathcal{Q}$ a $\mathfrak{S} \vdash \mathcal{P}$ pak $\mathfrak{T} \cup \mathfrak{S} \vdash \mathcal{Q}$ (srovnej s principem modus ponens).

Dedukcí rozumíme posloupnost vztahů typu $\mathfrak{T} \vdash \mathcal{P}$, při jejíž konstrukci můžeme používat pravidla (1)–(4), případně aplikovaná na předchozí členy posloupnosti. Ukažte, že pro každý axiom výrokového počtu $\mathcal{P}$ existuje dedukce obsahující $\emptyset \vdash \mathcal{P}$. Návod:

(a) Pro **VP**1 zkoumejte (a doplňte) posloupnost $\mathcal{P} \vdash \mathcal{P}$; $\mathcal{P} \vdash \mathcal{Q} \to \mathcal{P}$ (pravidlo (2), kde vynecháváme z jednoprvkového systému obsahujícího $\mathcal{P}$ formuli $\mathcal{Q}$, přestože tam není),
(b) pro **VP**2 použijte posloupnost $\mathcal{P} \to (\mathcal{Q} \to \mathcal{R}) \vdash \mathcal{P} \to (\mathcal{Q} \to \mathcal{R})$; $\mathcal{P} \to \mathcal{Q} \vdash \mathcal{P} \to \mathcal{Q}$; $\mathcal{P} \vdash \mathcal{P}$; $\mathcal{P} \to (\mathcal{Q} \to \mathcal{R}), \mathcal{P} \vdash \mathcal{Q} \to \mathcal{R}$; $\mathcal{P} \to \mathcal{Q}, \mathcal{P} \vdash \mathcal{Q}$; $\mathcal{P} \to (\mathcal{Q} \to \mathcal{R}), \mathcal{P} \to \mathcal{Q}, \mathcal{P} \vdash \mathcal{R}$ a dále užijte třikrát pravidlo (2),
(c) pro **VP**3 užijte $\neg\mathcal{Q}, \neg\mathcal{Q} \to \neg\mathcal{P} \vdash \neg\mathcal{P}$; $\mathcal{P} \vdash \mathcal{P}$; $\neg\mathcal{Q} \to \neg\mathcal{P}, \mathcal{P} \vdash \mathcal{Q}$ (pravidlo (3)) a dvakrát použijte pravidlo (2).

Ukažte naopak korektnost uvedených pravidel a dále pravidel (5) jestliže $\mathfrak{T} \vdash \mathcal{P}$ a $\mathfrak{S} \vdash \mathcal{Q}$, pak $\mathfrak{T} \cup \mathfrak{S} \vdash \mathcal{P} \,\&\, \mathcal{Q}$, (6) jestliže $\mathfrak{T} \vdash \mathcal{P}$, pak $\mathfrak{T} \vdash \mathcal{P} \vee \mathcal{Q}$ a také $\mathfrak{T} \vdash \mathcal{Q} \vee \mathcal{P}$, (7) jestliže $\mathfrak{T} \vdash \mathcal{P} \,\&\, \mathcal{Q}$, pak $\mathfrak{T} \vdash \mathcal{P}$ a také $\mathfrak{T} \vdash \mathcal{P} \,\&\, (\mathcal{Q} \vee \mathcal{Q})$, (8) jestliže $\mathfrak{T} \vdash \mathcal{P} \vee \mathcal{Q}$, jestliže $\mathfrak{S} \vdash \mathcal{P} \to \mathcal{R}$ a jestliže $\mathfrak{R} \vdash \mathcal{Q} \to \mathcal{R}$, pak $\mathfrak{T} \cup \mathfrak{S} \cup \mathfrak{R} \vdash \mathcal{R}$.

22) Ukažte, že vztah $\vdash \mathcal{A} \equiv \mathcal{B}$ vytváří ekvivalenci na množině všech formulí výrokového počtu. Nechť $\mathfrak{S}$ je „výběrová“ množina příslušející této ekvivalenci (tj. pro každou formuli $\mathcal{A}$ existuje právě jedna formule $\mathcal{B}$ z množiny $\mathfrak{S}$ tak, že $\vdash \mathcal{A} \equiv \mathcal{B}$). Pro prvky $\mathfrak{S}$ definujme $\mathcal{A} \leqq \mathcal{B}$, právě když $\vdash \mathcal{B} \to \mathcal{A}$. Ukažte, že relace $\leqq$ je uspořádání, popište největší a nejmenší prvek. Zjistěte, zda se jedná o svaz či dokonce úplný svaz, pokuste se popsat suprema a infima — pokud existují. Jsou odpovědi v případě konečné množiny a nekonečné množiny výrokových proměnných tytéž?

23) Nezávislost jednotlivých syntaktických zákonů (**VP**1–**VP**3 a modus ponens) je možno ukazovat pomocí trojhodnotové sémantiky. Uvažme např. modifikovanou sémantiku výrokové logiky, ve které logické spojky nemají dvouhodnotové, ale následující trojhodnotové tabulky:

$\neg$	
0	1
1/2	0
1	0

$\to$	0	1/2	1
0	1	1	1
1/2	0	1	1
1	0	1/2	1

Systém obsahující **VP**1, **VP**2 a modus ponens je korektní vůči uvedené sémantice v tom smyslu, že každý uvedený axiom má při každém pravdivostním ohodnocení hodnotu 1 a nadto nabývají-li formule $\mathcal{P}$ a $\mathcal{P} \to \mathcal{Q}$ při nějakém ohodnocení hodnoty 1, musí pro toto ohodnocení nabývat hodnotu 1 rovněž formule $\mathcal{Q}$. Navíc totéž platí i pro formule $(\mathsf{p} \to \mathsf{q}) \to [(\mathsf{p} \to \neg\mathsf{q}) \to \neg\mathsf{p}]$ a $\mathsf{p} \to (\neg\mathsf{p} \to \mathsf{q})$. Naproti tomu pro

VP3 existuje pravdivostní ohodnocení, které dává jinou hodnotu než 1. Totéž platí i o formulích $\neg\neg p \to p$ a $(\neg p \to \neg q) \to [(\neg p \to q) \to p]$. Prokažte.

Uvažte následující ohodnocení implikace

$\to$	0	1/2	1
0	1	1	1
1/2	0	1	1
1	0	1	1

Nezávislost kterého syntaktického zákona výrokového počtu na ostatních týkajících se pouze implikace prokazuje takováto sémantika? Zvolte ohodnocení negace, aby **VP**3 bylo korektní.

Pokuste se využít zmíněnou metodu k prokázání dalších nezávislostí.

24) Přeformulujte sémantické podmínky Tarského (a)–(c) z konce §1 do syntaktické verze. Jsou tyto syntaktické podmínky prokazatelné?

25) Za cenu přímého důkazu několika formulí není potřeba při demonstraci věty o úplnosti užít větu o ekvivalenci. Prokažte větu o ekvivalenci na základě věty o úplnosti. Analogicky prokažte větu o nahrazení na základě věty o úplnosti. Formulujte důvod nepřijatelnost nahrazení jakékoli podformule jinou formulí ve větě o nahrazení využívajíce pojmů sémantiky.