MATEMATICKÁ LOGIKA

Předběžný studijní text

Petr Hájek a Vítězslav Švejdar

Praha, listopad 1994

(povrchní typografická revize v červnu 99)

Obsah

Úvod

Máte v rukou studijní materiál k semestrální tříhodinové přednášce Výrokový a predikátový počet pro studijní směr Informatika na MFF UK. Možná, že tento materiál bude také užitečný studentům Filosofické fakulty UK studujícím logiku. V tomto úvodu se dozvíte, jak je text zamýšlen a jak s ním máte pracovat.

Matematickou logiku chápeme především jako *metamatematiku,* to jest matematické (formální) studium vztahu důsledku mezi matematickými výroky (tvrzeními). Takto chápaná logika má velký význam pro informatiku; bude o tom řeč v závěru. V první polovině přednášky jde o obecnou metamatematiku matematických teorií (na dvou úrovních: v rámci výrokového a predikátového počtu), v druhé o metamatematiku teorií, kterým můžeme říkat axiomatické aritmetiky, tj. teorií, které tak či onak popisují přirozená čísla.

V češtině neexistuje monografie, která by pokrývala látku v přednášce probíranou jako celek; první polovina látky je však dobře zpracována v skriptu doc. Petra Štěpánka, DrSc "Matematická logika". První část textu, který máte v ruce, je vlastně obsáhlým komentářem k Štěpánkovým skriptům; něco se rozvádí, něco mírně modifikuje, něco jen zmiňuje. Navíc je zde řada úloh probíraných ve cvičeních k přednášce. V textu též naleznete řadu poznámek a fakt týkajících se teorie výpočtové složitosti; pokud tuto teorii ovládáte, bude Vám vše jasné. Jinak berte tato místa jen jako upozornění na zajímavé vazby mezi logikou a teoretickou informatikou. *Upozornění:* některé partie z přednášky se v této části textu nekomentují, přesto však jsou důležité (je třeba je znát), např: některé důkazy (věty o úplnosti aj.), resoluční výrokový počet, Skolemova a Herbrandova věta. Na druhé straně Štěpánkova skripta obsahují podrobný výklad některých partií (např. teorie modelů), které do této přednášky nezahrnujeme. První část textu sepsal V.Š.

Druhá část textu je výklad metamatematiky aritmetiky a obsahuje (jak doufáme) vše podstatné, co bude v této části přednášeno, a též řadu cvičení. Z této partie se najdou v Štěpánkových skriptech jen zlomky, protože se touto tématikou ve skriptech nezabýval. Tuto část textu sepsal P.H. kromě cvičení, která sepsal V.Š.

Úmyslně nazýváme tento text studijním textem, nejde o vypilovaná skripta. Jde o první pracovní versi; povšimnete si např. rozdílné grafické úpravy v obou částech. Doufáme však, že Vám tento materiál usnadní studium a přípravu ke zkoušce. Pokud najdete v textu chyby (tiskové i věcné), sdělte nám je; usnadníte tím práci dalším studentům.

Nakonec uvádíme vybranou literaturu pro vážnější zájemce o matematickou logiku.

Literatura

- P. Štěpánek: Matematická logika. Skripta MFF
- E. Mendelson: Introduction to Mathematical Logic, Van Nostrand Co. 1964 (existuje ruský překlad)
- J. R. Shoenfield: Mathematical Logic, Addison-Wesley 1967 (existuje ruský překlad)
- J. D. Monk: Mathematical Logic, Springer-Verlag 1976
- J. Barwise (editor): Handbook of Mathematical Logic, North-Holland Publ. Comp. 1977
- C. Smoryński: Logical Number Theory I, Springer-Verlag 1991
- P. Hájek, P. Pudlák: Metamathematics of first order arithmetic, Springer-Verlag 1993

1 Výroková a predikátová logika

V této části se pokusíme stručně navázat na skriptum P. Štěpánka [Š]. Odkazy tvaru [Š 41], které se v této kapitole hojně vyskytují, udávají stránky v onom skriptu, na kterých je příslušná problematika podrobněji vyložena.

1.1 Formule a sémantika výrokové logiky

Formule výrokového počtu (*výrokové formule*) jsou sestaveny z *výrokových atomů* (též jen *atomů*, nebo v [Š] *prvotních formulí*) pomocí *logických spojek* (a závorek); [Š 22–23]. K označování formulí užíváme buď velká latinská písmena jako v [Š], nebo (raději) malá řecká písmena.

Pravdivostní ohodnocení je libovolná funkce $v : P \to \{0, 1\}$, kde P je množina všech výrokových atomů. Pravdivostní tabulky logických spojek ([Š 24]) jednoznačně určují rozšíření $\bar{v}$ libovolného pravdivostního ohodnocení v, které je definované na množině všech výrokových formulí. V dalším nebudeme rozlišovat mezi pravdivostním ohodnocením v a jeho rozšířením $\bar{v}$ na všechny formule, tj. pruh nad označením pravdivostního ohodnocení budeme vypouštět. Místo $v(\varphi) = 1$ lze také psát $v \models \varphi$ a říkat, že φ *je splněna* pravdivostním ohodnocením v nebo že v *splňuje* φ.

Formule φ (množina formulí T) je *splnitelná*, jestliže existuje pravdivostní ohodnocení v takové, že $v(\varphi) = 1$ (resp. $v(\psi) = 1$ pro každou $\psi \in T$). Formule φ je *(výroková) tautologie*, jestliže $v(\varphi) = 1$ pro každé pravdivostní ohodnocení v. Formule φ je *(tautologickým) důsledkem* množiny formulí T, jestliže φ je splněna každým pravdivostním ohodnocením, které splňuje všechny formule z T. Vztah důsledku zapisujeme $T \models \varphi$, tedy

$$T \models \varphi \quad \text{iff} \quad \forall v (\forall \psi \in T (v(\psi) = 1) \Rightarrow v(\varphi) = 1).$$

Zápis $T \models \varphi$ lze také číst "φ *vyplývá* z T". O množině T v této souvislosti mluvíme jako o *množině předpokladů* nebo o *množině axiomů* nebo jako o *teorii*. V tomto odstavci jsme symbol $\models$ použili v jiném významu než v odstavci předcházejícím v zápisu $v \models \varphi$. Vlevo od $\models$ může opravdu stát buď pravdivostní ohodnocení nebo množina formulí. V prvním případě $\models$ označuje splněnost formule při daném ohodnocení, v druhém případě se jedná o vztah důsledku. Kolizi bychom se samozřejmě mohli vyhnout tak, že bychom symbol $\models$ vyhradili jen pro vztah důsledku. Bylo by to ale možné jen ve výrokovém počtu. V predikátovém počtu je použití symbolu $\models$ ve dvojím významu natolik rozšířené, že je asi měnit nelze.

Formule je tautologie, právě když je důsledkem prázdné množiny axiomů. Místo "φ je tautologie" můžeme tedy psát $\emptyset \models \varphi$, případně jen $\models \varphi$. Místo $T \cup \{\psi_1, .., \psi_n\} \models \varphi$ píšeme jen $T, \psi_1, .., \psi_n \models \varphi$. Zápisy $\{\psi\} \models \varphi$ i $\psi \models \varphi$

mají tedy stejný význam a čteme je "formule φ je důsledkem (resp. vyplývá z) formule ψ". Formule φ a ψ jsou *(výrokově) ekvivalentní*, jestliže každá z nich je důsledkem té druhé.

V některých případech je výhodné pracovat s menším počtem logických spojek než $\rightarrow, \neg, \&, \vee, \equiv$. V tom případě (viz cvičení) lze jen některé z nich prohlásit za základní (tj. za opravdové symboly) a formule obsahující ty ostatní považovat za zkratkovité zápisy formulí obsahujících jen ony základní. Někdy je naopak výhodné seznam logických symbolů ještě rozšířit, např. o tzv. *logické konstanty* $\top$ a $\bot$ (pravda a nepravda), které se syntakticky chovají jako atomy, ale při každém pravdivostním ohodnocení má $\top$ povinně hodnotu 1 a $\bot$ naopak 0.

Protože množinu P všech výrokových atomů si zpravidla představujeme jako nekonečnou, kvantifikátor "pro každé pravdivostní ohodnocení" v definici tautologie se vztahuje k nekonečnému oboru. Je ale zřejmé, že pravdivostní hodnota formule φ při nějakém pravdivostním ohodnocení závisí na ohodnocení jen těch atomů, které se ve φ skutečně vyskytují. A těch je jen konečně mnoho. Toto pozorování umožňuje sestrojit jednoduchý algoritmus pro rozhodování o tautologičnosti dané formule φ (nebo o splnitelnosti nebo o vyplývání z konečné množiny předpokladů). Stačí probrat všechny funkce $v : A \rightarrow \{0, 1\}$, kde A je množina všech atomů, které se ve φ skutečně vyskytují. Tomuto algoritmu se někdy říká *tabulková metoda*. Tabulková metoda ukazuje, že tautologičnost výrokových formulí, splnitelnost výrokových formulí a vyplývání z konečné množiny předpokladů jsou algoritmicky rozhodnutelné úlohy.

Věta 1.1 (o kompaktnosti) *(a) Množina T výrokových formulí je splnitelná, právě když každá konečná $F \subseteq T$ je splnitelná.*
(b) $T \models \varphi$, právě když existuje konečná $F \subseteq T$ taková, že $F \models \varphi$.

Důkaz (a) je uveden v [Š 26]. Čtenář by neměl mít potíže s ověřením, že implikace $\Rightarrow$ v (a) a $\Leftarrow$ v (b) jsou triviální a že obě formulace (a), (b) jsou ekvivalentní.

V našem textu se stejně jako v [Š] vyhýbáme tomu, abychom podali formálně přesnou definici formule. Kdybychom to chtěli napravit, dopadlo by to nějak tak, že formule jsou jisté konečné posloupnosti prvků množiny $P \cup \{(,), \neg, \rightarrow, \&, \vee, \equiv\}$, kde P je neprázdná množina a o symblech $\neg, \rightarrow$ atd. předpokládáme, že nejsou v P. Věta o kompaktnosti platí, i když P je třeba nespočetná. Totéž lze říci také o větách o úplnosti, o kterých bude řeč dále. I výrokový počet s nespočetnou množinou atomů má určité aplikace.

Uvažujeme-li ale o rozhodnutelnosti různých úloh vyskytujících se v logice, např. problému splnitelnosti, musíme mít možnost považovat formule nikoliv za posloupnosti abstraktních objektů, ale za slova v jisté konečné abecedě Σ. Pro tento účel se obvykle předpokládá, že množina P všech atomů je nekonečná spočetná, $P = \{p_0, p_1, p_2, ..\}$, a že atomy nejsou samostatnými znaky (těch má být jen konečně mnoho), nýbrž slovy sestavenými ze základnějších symbolů. Při binárním kódování se atomy p_0, p_1, p_2, … považují za zkratky slov `p`, `p1`, `p10`, `p11`, `p101`, … , při unárním za zkratky slov `p`, `p|`, `p||`, `p|||`, … , kde `0`, `1` resp. `|` jsou pomocné znaky přijaté do základní abecedy Σ právě pro kódování indexů. Někdy (zejména v příští kapitole v souvislosti s tzv. polskou notací) je užitečná úmluva, že indexy se zapisují dopředu (např. `101p`).

Vraťme se ještě k tabulkové metodě a k problému splnitelnosti výrokových formulí. Tento problém chápaný jako formální jazyk (tj. jako množina slov v nějaké konečné abecedě) se označuje SAT. Tabulková metoda není příliš efektivním algoritmem pro řešení úlohy SAT. K rozhodnutí o splnitelnosti formule s n atomy (jejíž délka může být řádově také jen n) je totiž třeba probrat 2^n pravdivostních ohodnocení. Je to tedy algoritmus, který pracuje v exponenciálním čase. Není známo, zda úloha SAT má účinnější algoritmus, který by například pracoval v polynomiálním čase. SAT je jednou z referenčních úloh v teorii výpočtové složitosti. Řečeno odbornými termíny, je to NP-úplná úloha. Existence efektivního algoritmu pro její řešení by znamenala existenci efektivního algoritmu pro řešení mnoha jiných úloh a otázka, zda takový algoritmus existuje, je jedním z důležitých otevřených problémů soudobé informatiky. Poznamenejme, že úloha SAT je NP-úplná jak při binárním tak při unárním zapisování výrokových atomů.

V celém textu se zabýváme jen klasickou logikou, přičemž tento a příští paragraf jsou věnovány jejímu výrokovému počtu. Sémantika klasické logiky je založena na pojmu (dvouhodnotového) pravdivostního ohodnocení. Jiné, *neklasické*, logiky zpravidla také mají nějakou sémantiku, která umožňuje odlišit logicky platné formule (tj. pravdivé jen díky svému syntaktickému tvaru) od těch ostatních. Ne vždy je to sémantika založená na dvou pravdivostních hodnotách. Jedno z cvičení příštího paragrafu naznačuje, jak může vypadat sémantika neklasických logik. Existují i rozumné a aplikovatelné neklasické logiky, pro které neplatí věta o kompaktnosti. Výrokové počty známých neklasických logik jsou zpravidla rozhodnutelné. Některé rozhodovací úlohy, které se vyskytují v neklasických logikách, jsou také, stejně jako úloha SAT, velmi zajímavé z hlediska výpočtové složitosti.

Cvičení

1. Určete, které z následujících výrokových formulí jsou splnitelné a které jsou tautologie:

   $((p \to q) \to q) \to q$ $\quad\quad$ $\neg p \to \neg(p \vee (p \,\&\, q))$

   $\neg p \to \neg(p \vee q)$ $\quad\quad$ $(p \to (q \vee r)) \to (q \vee (p \to r))$

   $\neg p \to \neg(p \,\&\, q)$ $\quad\quad$ $(p \to q) \to ((q \to r) \to (p \to q))$

   $p \to p \,\&\, (p \vee q)$ $\quad\quad$ $(p \to q) \,\&\, q \to p$

   $p \to p \vee (p \,\&\, q)$ $\quad\quad$ $\neg p \to (p \,\&\, q)$

   $(p \to q) \vee (q \to p)$ $\quad\quad$ $((p \to q) \to p) \to p$

2. Dokažte, že
   (a) $\varphi \models \psi$, právě když $\varphi \to \psi$ je tautologie. φ a ψ jsou ekvivalentní, právě když $\varphi \equiv \psi$ je tautologie.
   (b) φ je splnitelná, právě když $\neg\varphi$ není tautologie.
   (c) Když $\varphi \to \chi$ i $\chi \to \psi$ jsou tautologie, pak $\varphi \to \psi$ je tautologie.

3. Rozhodněte, zda platí
   (a) Když φ je výroková tautologie a ψ vznikne z φ nahrazením některých výskytů výrokového atomu p toutéž formulí χ, pak ψ je tautologie.
   (b) Když φ je tautologie a ψ vznikne z φ nahrazením všech výskytů atomu p toutéž formulí χ, pak ψ je tautologie.
   (c) Když ψ vznikne z φ nahrazením všech výskytů atomu p libovolnými (i různými) formulemi, pak ψ je tautologie.
   (d) Když ψ_1 resp. ψ_2 vznikne z φ nahrazením některých výskytů atomu p formulí χ_1 resp. χ_2 a χ_1 a χ_2 jsou ekvivalentní, pak ψ_1 a ψ_2 jsou ekvivalentní.

4. Dokažte, že jsou-li A, B libovolné výrokové formule, pak formule $A \,\&\, B$ a $\neg(A \to \neg B)$ jsou ekvivalentní. S použitím cvičení 3 zdůvodněte, že když ψ vznikne z φ nahrazením všech podformulí tvaru $A \,\&\, B$ formulí $\neg(A \to \neg B)$, pak φ a ψ jsou ekvivalentní. Navrhněte podobné záměny i pro ostatní logické spojky a zdůvodněte, že každá formule φ je ekvivalentní s formulí ψ, která neobsahuje jiné logické spojky než
   (a) $\to$ a $\neg$
   (b) $\&$ a $\neg$
   (c) $\vee$ a $\neg$
   Pro atomy a negované atomy se užívá společné označení *literály*. Dokažte dále, že každá formule φ je ekvivalentní s formulí ψ, která neobsahuje jiné spojky než $\&, \vee, \neg$ a negace se ve ψ vyskytuje jen v literálech.

5. Zdůvodněte, že pokud formule φ v cvičení 4 neobsahuje spojku $\equiv$, lze z ní formuli ψ získat algoritmem, který pracuje v polynomiálním čase, a že počet symbolů formule ψ je lineární v počtu symbolů původní φ. Proč je potíž se spojkou $\equiv$? Zdůvodněte, že také o pravdivostní hodnotě dané formule při daném pravdivostním ohodnocení a o splnitelnosti formule, která obsahuje atomy jen z předem dané konečné množiny, lze rozhodovat v polynomiálním čase.

6. *Boolovská funkce* n proměnných je libovolná funkce f z $\{0,1\}^n$ do $\{0,1\}$. Například rovnosti
   $$f(0,0) = 0,\ f(0,1) = 0,\ f(1,0) = 1,\ f(1,1) = 0$$
   určují jednu z boolovských funkcí dvou proměnných. Kolik je boolovských funkcí n proměnných? Řekneme, že výroková formule neobsahující jiné atomy než $p_0, \ldots, p_{n-1}$ *definuje* boolovskou funkci f, jestliže pro každé pravdivostní ohodnocení v je $v(\varphi) = f(v)$ (to je napsáno trochu nepřesně, ale

snad je tomu rozumět: formule $\neg(p_0 \to p_1)$ definuje funkci dvou proměnných zmíněnou výše). Dokažte, že každou boolovskou funkci definuje některá výroková formule.
Návod. Nejprve uvažujte funkce, které mají jen jednu hodnotu 1 a jinak samé 0. Pak uvažujte disjunkce formulí definujících takové funkce.

7. Disjunkce literálů se nazývá *klauzule*. Formule je v *disjunktivním normálním tvaru*, je-li disjunkcí (několika, případně jen jedné) konjunkcí literálů. Formule je v *konjunktivním normálním tvaru*, je-li konjunkcí disjunkcí literálů, tj. je konjunkcí klauzulí. Použijte cvičení 6 k důkazu, že každá výroková formule je ekvivalentní s formulí v disjunktivním normálním tvaru a také s formulí v konjunktivním normálním tvaru ([Š 42]). Zdůvodněte, že splnitelnost formulí v disjunktivním normálním tvaru je rozhodnutelná v polynomiálním čase.

8. Není pravda, že každou výrokovou formuli lze algoritmem pracujícím v polynominálním čase převést na ekvivalentní formuli v konjunktivním (nebo disjunktivním) normálním tvaru. Například o formuli
$$(p_1 \,\&\, q_1) \vee (p_2 \,\&\, q_2) \vee \,..\, \vee (p_n \,\&\, q_n)$$
lze dokázat, že každá s ní ekvivalentní formule v konjunktivním normálním tvaru má alespoň 2^n symbolů, takže každý algoritmus potřebuje na pouhý zápis výsledku větší než polynomiální počet kroků. Dokažte ale, že platí toto. Ke každé výrokové formuli φ lze v polynomiálním čase sestrojit formuli ψ, která je v konjunktivním normálním tvaru, a je splnitelná, právě když ψ je splnitelná (nelze samozřejmě požadovat, aby φ a ψ byly ekvivalentní). Navíc každá klauzule ve formuli ψ je nejvýše tříprvková.
Návod. Každé podformuli A původní formule φ, včetně atomů a φ samotné, přiřaďte atom p_A tak, že je-li A atomická, p_A je A, jinak p_A je nový atom (nevyskytující se ve φ a různý od ostatních p_B). Pro každou neatomickou podformuli A formule φ tvaru $B \,\&\, C$ utvořte tři klauzule $\neg p_B \vee \neg p_C \vee p_A$, $\neg p_A \vee p_B$, $\neg p_A \vee p_C$. Něco podobného navrhněte i pro ostatní možnosti, kterými může A být sestavena z B a C. Označte χ konjunkci všech takto utvořených klauzulí. Na formuli χ se můžeme dívat jako na popis výpočtu pravdivostní hodnoty formule φ. Ověřte, že φ je splnitelná, právě když $p_\varphi \,\&\, \chi$ je splnitelná. Toto cvičení ukazuje, že pokud je problém splnitelnosti výrokových formulí NP-úplný, pak i problém splnitelnosti formulí v konjunktivním normálním tvaru, v němž každá klauzule má nejvýše tři literály (tento problém se označuje 3SAT), je také NP-úplný.

9. Nechť výroková formule D je v konjunktivním normálním tvaru (viz cvičení 7). Nechť p je libovolný výrokový atom formule D. Napišme D ve tvaru
$$C_1 \,\&\, .. \,\&\, C_k \,\&\, (A_1 \vee p) \,\&\, .. \,\&\, (A_n \vee p) \,\&\, (B_1 \vee \neg p) \,\&\, .. \,\&\, (B_m \vee \neg p)$$

kde formule A_i, B_j, C_l neobsahují p, a utvořme formuli D':

$$C_1 \;\&\; .. \;\&\; C_k \;\&\; \bigwedge_{i,j} (A_i \vee B_j)$$

Dokažte, že D' je splnitelná, právě když D je splnitelná. Jsou D a D' ekvivalentní? Dále vezměte v úvahu i mezní případy (např. že některé z čísel k, n, m je nula) a navrhněte algoritmus, který rozhodne o splnitelnosti formulí v konjunktivním normálním tvaru. Zdůvodněte, že jsou-li všechny klauzule v původní formuli nejvýše dvouprvkové, váš algoritmus pracuje v polynomiálním čase.

10. *Hornovská klauzule* je taková, která obsahuje nejvýše jeden literál bez negace. Definujme pro účely tohoto cvičení *hornovskou formuli* jako formuli v konjunktivním normálním tvaru, jejíž všechny klauzule jsou hornovské. Dokažte, že
(a) Postupem popsaným v cvičení 9 z hornovské formule vznikne opět hornovská formule.
(b) Je-li hornovská formule nesplnitelná, obsahuje klauzuli pozůstávající z jediného pozitivního literálu (tj. z literálu neobsahujícího negaci).
(c) Zvolíme-li k transformaci popsané v cvičení 9 takový atom p, že některá z klauzulí je p, tj. že některá z formulí A_i je prázdná, lze místo formule D' vzít jednodušší formuli

$$C_1 \;\&\; .. \;\&\; C_k \;\&\; B_1 \;\&\; .. \;\&\; B_m$$

Zdůvodněte, že i splnitelnost hornovských formulí je rozhodnutelná v polynomiálním čase.

11. Pro libovolnou množinu výrokových formulí A označme $\mathrm{Cl}(A)$ (od closure) množinu všech tautologických důsledků množiny A. Rozhodněte, zda pro každou množinu formulí A platí
(a) $A \subseteq \mathrm{Cl}(A)$
(b) $\mathrm{Cl}(\mathrm{Cl}(A)) = \mathrm{Cl}(A)$
(c) $\mathrm{Cl}(A \cup B) = \mathrm{Cl}(A) \cup \mathrm{Cl}(B)$
Pokud v (b) nebo v (c) je odpověď ne, rozhodněte, zda platí alespoň některá inkluze.

12. Zapomeňme na chvíli na platnost věty o kompaktnosti a nazvěme množinu T formulí *konečně splnitelnou*, jestliže každá její konečná část je splnitelná. Dokažte, že je-li φ formule a T konečně splnitelná množina formulí, pak jedna z množin T, φ (čímž myslíme $T \cup \{\varphi\}$) a $T, \neg\varphi$ je konečně splnitelná.

13. Předpokládejme, že množina všech výrokových atomů je spočetná, takže všechny výrokové formule lze seřadit do posloupnosti $\varphi_0, \varphi_1, \varphi_2, \ldots$. Nechť T jako v cvičení 12 je konečně splnitelná. Definujme posloupnost $\{S_i\}$

množin formulí takto: $S_0 = T$, S_{i+1} je $S_i \cup \{\varphi_i\}$ pokud $S_i \cup \{\varphi_i\}$ je konečně splnitelná a S_{i+1} je $S_i \cup \{\neg\varphi_i\}$ v opačném případě. Vezměte $S = \cup_i S_i$. Dokažte, že S je konečně splnitelná a $S \supseteq T$. Dále dokažte, že pro každou výrokovou formuli φ platí

$$\varphi \in S \iff \neg\varphi \notin S. \tag{$*$}$$

Z faktu $(*)$ a z konečné splnitelnosti množiny S dále dokažte:

$$\varphi \vee \psi \in S \iff \varphi \in S \text{ nebo } \psi \in S$$

$$\varphi \,\&\, \psi \in S \iff \varphi \in S \text{ a } \psi \in S$$

$$\varphi \to \psi \in S \iff \varphi \notin S \text{ nebo } \psi \in S.$$

Tyto vlastnosti dohromady s $(*)$ ukazují, že předpis

$$v(\varphi) = 1 \iff \varphi \in S$$

korektně definuje pravdivostní ohodnocení v. Ohodnocení v splňuje všechny formule v T. Dokázali jsme, že každá konečně splnitelná množina formulí je splnitelná. Toto je jiný důkaz věty o kompaktnosti, než je uveden v [Š].

1.2 Důkazový systém pro výrokovou logiku

Důkaz z množiny předpokladů T ([Š 27]) je konečná posloupnost formulí taková, že každý člen φ je výrokovým axiomem nebo prvkem množiny T nebo některé dva předchozí členy posloupnosti jsou tvaru ψ a $\psi \to \varphi$. V posledním případě řekneme, že φ je z ψ a $\psi \to \varphi$ odvozena pravidlem *modus ponens* (MP). Formule φ je *dokazatelná* z předpokladů T, symbolicky $T \vdash \varphi$, jestliže existuje důkaz z předpokladů T, který má φ jako poslední (nebo některý) člen. Za *výrokový axiom* považujme každou formuli, která má jeden z následujících tvarů:

A1: $\varphi \to (\psi \to \varphi)$
A2: $(\varphi \to (\psi \to \chi)) \to ((\varphi \to \psi) \to (\varphi \to \chi))$
A3*: $(\neg\varphi \to \neg\psi) \to ((\neg\varphi \to \psi) \to \varphi)$

Za φ, ψ, χ mohou být voleny libovolné výrokové formule. Výrokových axiomů a tedy i dokazatelných formulí je tedy nekonečně mnoho. Hvězdička v A3* upozorňuje, že jsme přijali jiné schema než v [Š]. Je dobré si uvědomit, že táž logika (v našem případě klasická logika) může mít více důkazových systémů (též *kalkulů*), které se od sebe mohou lišit mnohem podstatněji, než jen záměnou jednoho schematu. Užitečný důkazový systém může být například založen na pravidle rezoluce, které vlastně bylo použito v cvičení 9 předchozího paragrafu. Náš A3* je v [Š] (viz [Š 47]) označen A4. Výrokovým systémům založeným na pravidle MP se říká *fregovské*. Kdybychom kromě implikace a negace považovali za základní symboly i konjunkci a disjunkci, přijali bychom ještě tato schemata:

A4: $\varphi \to (\psi \to \varphi \,\&\, \psi)$
A5: $\varphi \,\&\, \psi \to \varphi, \quad \varphi \,\&\, \psi \to \psi$
A6: $\varphi \to \varphi \vee \psi, \quad \psi \to \varphi \vee \psi$
A7: $(\varphi \to \chi) \to ((\psi \to \chi) \to (\varphi \vee \psi \to \chi))$

Pro zpřehlednění zápisů užíváme standardní konvenci pro vypouštění závorek, tj. negace má vyšší prioritu než ostatní spojky (tomu odpovídá i formální definice v [Š 22], která při negování nepředepisuje závorky) a implikace má nižší prioritu než všechny ostatní spojky.

Slovo důkaz tedy užíváme ve dvojím smyslu: (formální) důkaz jako odborný termín (posloupnost formulí taková a taková) a důkaz (neformální) nějakého tvrzení (o formulích, formálních důkazech, ...).

V [Š 28] je uveden důkaz schematu $\varphi \to \varphi$. Ve fregovském systému je to jeden z mála důkazů z prázdné množiny předpokladů, který může čtenář vidět zapsaný celý. K důkazům o dokazatelnosti ostatních formulí je zpravidla velice výhodné užít větu o dedukci, [Š 29]. Doporučujeme čtenáři, aby při jejím studiu ověřil, že schema A3 je pro důkaz nepodstatné (takže věta platí i pro náš systém s A3*), ale je potřeba vědět, že každá formule tvaru $\varphi \to \varphi$ je dokazatelná.

Ukažme si použití věty o dedukci na tomto příkladě: každá formule tvaru $\psi \to (\neg\psi \to \varphi)$ je dokazatelná z prázdné množiny předpokladů. Nechť φ a ψ jsou dány. Podle věty o dedukci stačí ukázat, že φ je dokazatelná z množiny předpokladů $\{\psi, \neg\psi\}$. Schema A3* lze číst zhruba tak, že pokud $\neg\varphi$ vede ke sporu, platí φ. A vede $\neg\varphi$ ke sporu? Ano, předpoklady ψ a $\neg\psi$ tvoří dohromady spor a nevadí, že při jeho odvození se $\neg\varphi$ neuplatnila. Takováto hrubá úvaha plus možná několik pokusů zpravidla umožňují sestrojit hledaný důkaz:

1:	$\psi, \neg\psi \vdash (\neg\varphi \to \neg\psi) \to ((\neg\varphi \to \psi) \to \varphi)$	; A3*
2:	$\psi, \neg\psi \vdash \neg\psi \to (\neg\varphi \to \neg\psi)$	; A1
3:	$\psi, \neg\psi \vdash \neg\psi$	
4:	$\psi, \neg\psi \vdash \neg\varphi \to \neg\psi$	; MP na 2,3
	$\psi, \neg\psi \vdash \psi \to (\neg\varphi \to \psi)$	; A1
5:	$\psi, \neg\psi \vdash \neg\varphi \to \psi$	; podobně jako 2,3,4
6:	$\psi, \neg\psi \vdash (\neg\varphi \to \psi) \to \varphi$	; MP na 1,4
	$\psi, \neg\psi \vdash \varphi$	; MP na 5,6
	$\psi \quad\;\; \vdash \neg\psi \to \varphi$	; V o dedukci
	$\vdash \psi \to (\neg\psi \to \varphi)$	; ...

V zápisu důkazu a i nadále pokračujeme v praxi vypouštění symbolů množinových operací $\{\}$ a případně $\cup$, jde-li o množiny formulí. Další použití věty o dedukci nabízíme ve cvičení 1.

Množina předpokladů T je *sporná*, jestliže z ní lze dokázat nějakou formuli a zároveň její negaci. Jinak je T *bezesporná* (*konzistentní*). Z dokazatelnosti schematu $\psi \to (\neg\psi \to \varphi)$ plyne, že T je sporná, právě když každá formule je v T dokazatelná, [Š 36].

Abychom zdůvodnili důležitost toho, co přijde dále, uveďme dvě otázky, na které by nebylo snadné odpovědět bez vět o korektnosti a úplnosti.
1. Je prázdná množina bezesporná?
2. Je množina všech formulí dokazatelných z prázdné množiny předpokladů algoritmicky rozhodnutelná?

Věta 1.2 (o úplnosti, [Š 34]) *Formule φ je dokazatelná z prázdné množiny předpokladů, právě když je tautologií.*

Věta 1.3 (o silné úplnosti, [Š 37]) *(a) Je-li T libovolná množina formulí, pak T je splnitelná, právě když T je bezesporná.*
(b) Je-li φ libovolná formule a T množina předpokladů, pak

$$T \vdash \varphi, \quad \textit{právě když} \quad T \models \varphi.$$

Implikacím $\Rightarrow$ v obou větách se říká věty o korektnosti. Zdůrazněme, že právě věty o korektnosti jsou důležitým nástrojem, chceme-li dokázat, že nějaká formule **není** dokazatelná nebo že nějaká množina je bezesporná. Cvičení 4 ukazuje použití věty o korektnosti na kalkulus, o kterém nevíme, jestli je úplný vůči dané sémantice. Čtenář by neměl mít problémy s ověřením následujících faktů:

- $T \vdash \varphi$, právě když $T, \neg\varphi$ je sporná
- obě formulace (a), (b) ve větě o silné úplnosti jsou ekvivalentní
- z úplnosti vyplývá "silná úplnost" pro konečnou množinu T (protože místo $T \vdash \varphi$ a $T \models \varphi$ lze psát $\vdash \&T \to \varphi$ resp. $\models \&T \to \varphi$, kde $\&T$ je konjunkce všech formulí v T)
- z korektnosti vyplývá silná korektnost (protože v důkazu φ z T se beztak uplatní jen konečně mnoho prvků z T)
- ze silné úplnosti vyplývá kompaktnost (ze stejného důvodu)
- z úplnosti a kompaktnosti vyplývá silná úplnost .

Obtížnější důkaz má jen implikace $\Leftarrow$ ve větě o úplnosti. Tuto implikaci lze pro náš kalkulus dokázat stejným postupem, který je v [Š] na stranách 33–35 pro kalkulus se schematy A1–A3. Formule v cvičení 1 nejsou vybrány náhodně. Formule v (i) je jen jinou formulací lemmatu 2, [Š 33], a ostatní formule postačují k důkazu lemmatu 3.

Samotná definice důkazu nedává žádný návod k sestrojení algoritmu, který by rozhodoval, zda daná formule je dokazatelná. Pravidlo modus ponens má totiž nevýhodnou vlastnost, že neumožňuje určit, z kterých dvou formulí je daná formule odvozena. Dvojic ψ_1, ψ_2, ze kterých lze jedním použitím pravidla MP odvodit danou formuli φ, je nekonečně mnoho. Některé důkazové systémy tuto nevýhodnou vlastnost nemají. I pro fregovský systém ale platí, že důkazů, které mají nejvýše daný počet symbolů, je jen konečně mnoho. Na základě tohoto pozorování by bylo možné sestrojit mechanickou proceduru (tj. program, ale poněkud netypický: nepožaduje žádný vstup a je-li jednou spuštěn, nikdy se nezastaví), která postupně probírá všechny důkazy a tiskne jejich poslední členy. Množiny, které lze tímto způsobem *vygenerovat*, se v teorii rekurzivních funkcí nebo v teorii formálních jazyků nazývají *rekurzivně spočetné*. Jiný termín pro algoritmicky rozhodnutelné množiny je *rekurzivní množiny*. Je známo, že každá rekurzivní množina je rekurzivně spočetná, ale opačná inkluze neplatí. Úvahy o algoritmické rozhodnutelnosti uvedené v tomto a v předchozím paragrafu lze tedy shrnout takto. Z definice důkazu je zřejmé, že množina všech dokazatelných formulí je rekurzivně spočetná. Z věty o úplnosti a z existence tabulkové metody pro rozpoznávání tautologií vyplývá, že je dokonce rekurzivní.

Uveďme na závěr poznámku, která může být zajímavá pro příznivce výpočtové složitosti, ale která je nepodstatná pro pochopení dalšího textu a čtenář ji může klidně přeskočit, zejména pokud neví, co je třída coNP a coNP-úplnost.

V předcházejícím odstavci jsme se dotkli otázky, zda nalezení důkazu formule není rychlejší cestou k ověření, že je tautologií, než probrání všech příslušných pravdivostních ohodnocení. V jednotlivých případech tomu tak může být. Kdyby ale platilo, že každá tautologie s n symboly má důkaz s nejvýše $p(n)$ symboly, kde p je nějaký polynom, znamenalo by to, že množina TAUT všech tautologií je v NP. O množině TAUT je ale známo, že je coNP-úplná, a její současná příslušnost do NP by znamenala rovnost NP=coNP. Není známo, zda tato rovnost platí, ale odborníci považují za pravděpodobné spíš to, že neplatí. Pokud je tomu tak, znamená to, že některé krátké tautologie mají jen velmi dlouhé důkazy. Analýzou důkazu věty o úplnosti lze ale ověřit, že každá tautologie délky nejvýše n má důkaz délky $O(n \cdot 2^n)$, kde délka znamená počet symbolů.

Cvičení

1. Dokažte (s použitím věty o dedukci, ale bez použití věty o úplnosti), že následující schemata jsou dokazatelná v systému s A3*.

   (a) $\neg\neg\varphi \to \varphi$
   (b) $\neg\neg\neg\varphi \to \neg\varphi$
   (c) $\varphi \to \neg\neg\varphi$
   (d) $(\neg\psi \to \neg\varphi) \to (\varphi \to \psi)$
   (e) $(\varphi \to \psi) \to (\neg\neg\varphi \to \neg\neg\psi)$
   (f) $(\varphi \to \psi) \to (\neg\psi \to \neg\varphi)$
   (g) $\varphi \to (\neg\psi \to \neg(\varphi \to \psi))$
   (h) $\neg\varphi \to (\varphi \to \psi)$
   (i) $(\neg\psi \to \varphi) \to ((\psi \to \varphi) \to \varphi)$

2. Je-li v libovolné pravdivostní ohodnocení, pak φ^v je φ pokud $v(\varphi) = 1$ a φ^v je $\neg\varphi$ v opačném případě. Schemata (c), (g), (h) cvičení 1 jsou dostatečná k důkazu tvrzení, že pro každou formuli φ neobsahující jiné atomy než $p_1, \ldots, p_n$ a pro každé pravdivostní ohodnocení v platí

$$p_1^v, \ldots, p_n^v \vdash \varphi^v$$

Najděte podobná schemata i pro případ, že se za základní považují i spojky & a $\vee$ a dokažte je z axiomů A4–A7.

3. *Pravidlo substituce* φ / $\varphi_p(\chi)$ umožňuje z libovolné formule φ odvodit formuli, která z ní vznikne nahrazením všech výskytů některého atomu toutéž (libovolnou) formulí. Rozhodněte, zda pro kalkulus, který vznikne přidáním pravidla substituce ke kalkulu z tohoto paragrafu, platí věta o korektnosti a věta o silné korektnosti.

4. Dokažte, že množina všech tautologií je maximální bezesporná množina formulí, která je uzavřená na pravidlo substituce.

5. Představte si modifikovanou sémantiku výrokové logiky, ve které logické spojky nemají dvouhodnotové, ale následující tříhodnotové tabulky:

$\neg$	
0	2
1	0
2	0

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

Uvažujte výrokový logický systém s jediným pravidlem modus ponens a s následujícími schematy axiomů:

$$\varphi \to (\psi \to \varphi)$$
$$(\varphi \to (\psi \to \chi)) \to ((\varphi \to \psi) \to (\varphi \to \chi))$$
$$(\varphi \to \psi) \to ((\varphi \to \neg\psi) \to \neg\varphi)$$
$$\varphi \to (\neg\varphi \to \psi)$$

Dokažte, že tento systém je korektní vůči uvedené sémantice v tom smyslu, že každá dokazatelná formule má při každém pravdivostním ohodnocení hodnotu 2. Dokažte, že formule $\neg\neg p \to p$, $(\neg p \to \neg q) \to ((\neg p \to q) \to p)$ a $(\neg p \to \neg q) \to (q \to p)$ nejsou v tomto systému dokazatelné (protože existuje pravdivostní ohodnocení, které jim dává jinou hodnotu než 2).

6. Rozhodněte, které formule z cvičení 1 jsou dokazatelné v kalkulu z cvičení 5. Návod. Narozdíl od cvičení 1 je tentokrát asi výhodnější dokázat dřív (c) než (b) a dřív (f) než (e).

1.3 Predikátová logika

Formule predikátové logiky ([Š 51–53]) jsou sestaveny z atomických formulí pomocí logických spojek a *kvantifikátorů* $\forall$ a $\exists$. *Atomická formule* se vždy skládá z jednoho *predikátového symbolu* (též *relačního symbolu*) nějaké četnosti n a z n termů. *Termy* jsou sestaveny z *proměnných* (a konstant) pomocí *funkčních symbolů*. Funkční symboly četnosti nula se nazývají *konstanty*. Funkční a predikátové symboly jsou prvky předem zvolené množiny nazývané *jazyk*. Prvkům jazyka se někdy říká *mimologické symboly*.

V [Š 51–52] jsou uvedeny příklady jazyků. Jazyk teorie grup má dva funkční symboly (jeden binární a jednu konstantu). Teorie uspořádání a teorie množin mají shodně jeden binární predikátový symbol. Za *jazyk aritmetiky* považujeme množinu $\{+, \cdot, \overline{0}, S, \leq\}$, kde $+$, $\cdot$, S, $\overline{0}$ jsou dva binární, jeden unární funkční symbol a konstanta, $\leq$ je binární predikát. Symbol $=$ pro rovnost může nebo nemusí být pokládán za automatickou součást jazyka. V teorii grup ale musí; bez alespoň jednoho predikátového symbolu bychom nemohli napsat ani jednu formuli.

Příklad 1 $\neg(x = 0) \to \exists v(v \cdot x = y)$ a $\forall x \forall y(S(S(\overline{0})) \cdot (y \cdot y) = x \cdot x) \to y = \overline{0})$ jsou aritmetické formule.

Výskyty proměnných ve formulích se dělí na *volné* a *vázané* [Š 55]. Formule bez vázaných výskytů proměnných (tj. bez kvantifikátorů) se nazývá *otevřenou*. *Uzavřená formule* nebo též *sentence* je formule bez volných proměnných.

Příklad 2 Druhá formule předcházejícího příkladu je sentence. Formule $S(\overline{0}) \leq \overline{0} \vee S(\overline{0}) + S(S(\overline{0})) = S(S(S(\overline{0})))$ je dokonce otevřená sentence.

Struktura $\mathbf{M}$ *pro* daný *jazyk* L má neprázdnou *nosnou množinu* (*universum*) M a *realizaci* $s^{\mathbf{M}}$ každého symbolu $s \in L$. Realizací n-árního predikátového symbolu je (libovolná) n-ární relace na množině M, realizací n-árního funkčního symbolu je n-ární operace na M, tj. funkce z M^n do M. V predikátovém počtu s rovností se rovnítko pokládá za vždy přítomný logický symbol. Jeho realizací je vždy rovnost (tj. diagonála) na M. To samozřejmě neznamená, že v predikátovém počtu bez rovnosti nesmíme některému binárnímu predikátu říkat rovnítko. Odpadá jen povinnost je určitým způsobem realizovat.

Příklad 3 Každá množina s jednou binární operací a s jednou konstantou (bez ohledu na to, je-li grupou) je příkladem struktury pro jazyk teorie grup. Struktura $\mathbf{R} = \langle R, +^{\mathbf{R}}, \cdot^{\mathbf{R}}, 0, .+1, \leq^{\mathbf{R}} \rangle$, tj. množina všech reálných čísel s obvyklými operacemi a uspořádáním (zápis ".+1" označuje přičítání jedničky chápané jako unární funkce), je strukturou pro aritmetický jazyk. Horní indexy u funkcí a relací budeme pokud možno pomíjet. Takže strukturu přirozených čísel s obvyklými operacemi (která je strukturou pro týž aritmetický jazyk) budeme zapisovat $\mathbf{N} = \langle N, +, \cdot, 0, .+1, \leq \rangle$ a strukturu reálných čísel budeme zapisovat $\mathbf{R} = \langle R, +, \ldots \rangle$.

Tarského definice pravdy [Š 58] určuje pravdivostní hodnotu dané formule v dané struktuře při daném ohodnocení, tj. určuje, zda daná formule je nebo není *splněna* v dané struktuře při daném ohodnocení proměnných. Splněnost formule φ v $\mathbf{M}$ daným ohodnocením e se značí $M \models \varphi[e]$. Je-li φ splněna každým e, řekneme, že φ *platí* v $\mathbf{M}$ a píšeme $M \models \varphi$. V terminologii "platí–splněna" (ale nikoliv ve značení) jsme se poněkud odchýlili od skripta [Š 59]. Učinili jsme to ve snaze uvést do souladu obraty "splněná formule" a "splnitelná formule", a to ve výrokovém i v predikátovém počtu. Pravdivostní hodnota formule φ při ohodnocení e závisí jen na ohodnocení těch proměnných, které se ve φ vyskytují volně. Tedy sentence je v nějaké struktuře splněna, právě když tam platí, a to je právě když její negace neplatí.

Příklad 4 První formule z příkladu 1 je ve struktuře $\mathbf{N}$ splněna např. dvojicí $[3, 15]$ (tj. ohodnocením proměnných, které proměnné x přiřazuje hodnotu 3 a y hodnotu 15). Ve struktuře $\mathbf{R}$ tato formule dokonce platí. Druhá formule platí ve struktuře $\mathbf{R}$, v $\mathbf{N}$ platí její negace. Je-li φ libovolná formule v nějakém jazyce L, pak formule $\exists y \forall x \varphi \to \forall x \exists y \varphi$ platí v každé struktuře pro jazyk L.

Se strukturou $\mathbf{N}$ přirozených čísel s obvyklými operacemi a relacemi se v našem textu ještě mnohokrát setkáme. Nazýváme ji *standardním modelem aritmetiky*. Formule aritmetického jazyka umožňuje vyjádřit nejen obecná fakta o číslech, jako třeba formule $\forall x \forall y (x + y = y + x)$, ale i fakta o konkrétních přirozených číslech, jako třeba formule

$$\forall x \forall y (x \cdot y = S(S(S(\overline{0}))) \to x = S(\overline{0}) \vee x = S(S(S(\overline{0})))) \ ,$$

která vyjadřuje, že číslo tři je prvočíslo. Termům $\overline{0}$, $S(\overline{0})$, $S(S(\overline{0}))$, ... říkáme *numerály* (někdy též *cifry*) a značíme je $\overline{0}$, $\overline{1}$, $\overline{2}$, ... Součástí Tarského definice pravdy je i definice hodnoty (realizace) $t^{\mathbf{M}}[e]$ termu t ve struktuře $\mathbf{M}$ při ohodnocení proměnných e. Numerály neobsahují proměnné (jsou to *uzavřené termy*) a jejich realizace nezávisejí na ohodnocení proměnných: realizací numerálu $\overline{m}$ ve standardním modelu je číslo m, tedy $\overline{m}^{\mathbf{N}} = m$. Každý prvek standardního modelu je realizací některého numerálu. Je důležité odlišit numerály od proměnných. Například $x + y = z$ je **jedna** formule, která je nebo není splněna podle toho, jaké hodnoty přiřadí ohodnocení proměnných proměnným x, y, z. Naproti tomu $\overline{n} + \overline{m} = \overline{k}$ je **schema**, které zastupuje různé formule, jinou pro každou trojici n, m, k. Každá z nich je ale sentencí a její pravdivost tedy nezávisí na ohodnocení proměnných.

Formule φ jazyka L je *(logickým) důsledkem* množiny formulí Δ (φ *vyplývá* z Δ), jestliže v každé struktuře $\mathbf{M}$ pro jazyk L je φ splněna každým ohodnocením proměnných, které v $\mathbf{M}$ splňuje všechny formule z Δ. Symbolicky:

$$\Delta \models \varphi \quad \text{iff} \quad \forall \mathbf{M} \forall e (\mathbf{M} \models \Delta[e] \ \Rightarrow \ M \models \varphi[e]).$$

Jako ve výrokovém počtu, *důsledek formule* ψ je totéž, co důsledek množiny $\{\psi\}$, a formule jsou *(logicky) ekvivalentní*, jestliže každá je důsledkem té druhé. Formule, která je důsledkem prázdné množiny (tj. platí v každé struktuře pro svůj jazyk), se nazývá *logicky platnou formulí* nebo též *predikátovou tautologií*. Podobně jako ve výrokovém počtu symbol $\models$ užíváme ve dvojím významu. Vlevo od něj může stát buď struktura nebo množina formulí.

Příklad 5 Mějme jazyk s jediným unárním predikátem P. Uvažujme dvouprvkovou strukturu $\mathbf{M}$, kde $M = \{a, b\}$ a $P^{\mathbf{M}} = \{a\}$. Pak $\mathbf{M} \models P(x)[a]$, $\mathbf{M} \not\models P(x)[b]$, $\mathbf{M} \not\models \forall x P(x)$. Tedy formule $\forall x P(x)$ není důsledkem množiny $\{P(x)\}$.

Příklad 6 Mějme jazyk $L = \{+, \overline{0}, S\}$. Uvažujme strukturu $\mathbf{M} = \langle \{a, b\}, +^{\mathbf{M}}, S^{\mathbf{M}}, \overline{0}^{\mathbf{M}} \rangle$, kde $\overline{0}^{\mathbf{M}} = a$ a operace $+^{\mathbf{M}}, S^{\mathbf{M}}$ jsou definovány takto:

$S^{\mathbf{M}}$	
a	b
b	b

$+^{\mathbf{M}}$	a	b
a	a	b
b	b	a

Díky přítomnosti symbolů $\overline{0}$ a S lze užívat numerály. Můžeme se tedy ptát, zda formule $\overline{1} + \overline{1} = \overline{2}$ platí v $\mathbf{M}$. Lehce lze ověřit, že neplatí. Není to tedy logicky platná formule. Snadno bychom ověřili, že také formule $\overline{2} \cdot \overline{2} = \overline{3}$ (ani její negace) není logicky platnou formulí. Nicméně obě formule $\exists x(\overline{2} \cdot x = \overline{3})$ a $\exists x(x \cdot x = \overline{3})$ jsou důsledkem formule $\overline{2} \cdot \overline{2} = \overline{3}$.

Příklad 7 Každé dvě formule tvaru $\neg\forall x\varphi$ a $\exists x\neg\varphi$ jsou spolu ekvivalentní. Každá formule tvaru $\exists y \forall x \varphi \to \forall x \exists y \varphi$ je logicky platnou formulí. Totéž platí pro každou formuli tvaru $\varphi \to (\exists v \psi \to \varphi)$. Obecně každá výroková tautologie je zároveň logicky platnou formulí. Každá formule je ekvivalentní formuli v *prenexním normálním tvaru*, tj. formuli, v níž všechny kvantifikátory předcházejí všechny logické spojky. Pro převedení formule na prenexní normální tvar existuje efektivní algoritmus, který je založen na tzv. *prenexních operacích*, viz [Š 79 (a)–(e)].

Chceme-li ukázat, že nějaká formule φ nevyplývá z nějaké množiny předpokladů Δ, podle definice máme najít strukturu $\mathbf{M}$ (a ohodnocení proměnných, jsou-li v Δ nebo φ volné proměnné) takovou, že $\mathbf{M} \models \Delta$ a $\mathbf{M} \not\models \varphi$. To jsme také udělali v příkladu 5. Přitom by nás mohly napadnout tyto otázky:
1. Je někdy nutné volit strukturu $\mathbf{M}$ *nekonečnou?*
2. Je někdy nutné volit strukturu $\mathbf{M}$ *dokonce nespočetnou?*
Odpověď na druhou otázku dává Löwenheim-Skolemova věta v následujícím paragrafu. Rovněž odpověď na první otázku se vyjasní nejpozději v příštím paragrafu.

Věta 1.4 (o kompaktnosti) *(a) Množina Δ predikátových formulí je splnitelná, právě když každá konečná $F \subseteq \Delta$ je splnitelná.*
(b) $\Delta \models \varphi$, právě když existuje konečná $F \subseteq \Delta$ taková, že $F \models \varphi$.

Věta o kompaktnosti je v [Š 112 a 114] odvozena z věty o silné úplnosti. Uvádíme ji už v tomto místě proto, abychom zachovali podobnost textu o predikátové logice s textem v 1.1 a 1.2 o výrokové logice, a také abychom zdůraznili, že kompaktnost považujeme za sémantický princip. Sémantický v tom smyslu, že znění se netýká pojmu formální důkaz.

Obraťme se nyní k úkolu charakterizovat logickou platnost a vyplývání pomocí vhodného důkazového kalkulu. V jeho konstrukci se uplatňuje substituce termů za proměnné. *Současnou substituci* termů $t_1, .., t_n$ za proměnné $x_1, .., x_n$ do termu s nebo do formule φ značíme $s_{x_1,..,x_n}(t_1, .., t_n)$ resp. $\varphi_{x_1,..,x_n}(t_1, .., t_n)$. Substituuje se jen za volné proměnné a to vždy za všechny výskyty. Ne každý term je *substituovatelný* za libovolnou proměnnou do libovolné formule, viz [Š 60–61]. Za ilustrativní považujeme také příklad [Š 69], který ukazuje, že $\varphi_{x,y}(t, s)$ nemusí být totéž, co $(\varphi_x(t))_y(s)$.

Důkazový systém pro predikátovou logiku je dán logickými axiomy a odvozovacími pravidly. My se zabýváme důkazovým systémem, který vznikne přidáním axiomů a pravidel o kvantifikátorech k výrokovému systému se schematy A1–A3 resp. A1–A7 a s pravidlem modus ponens $\varphi,\ \varphi \to \psi \ /\ \psi$, viz par. 1.2. Všechna schemata z par. 1.2 ovšem chápeme tak, že za φ, ψ resp. χ lze dosadit libovolné **predikátové** formule. *Dokazatelnost z* množiny *předpokladů* je definována stejně jako v 1.2. Jako kvantifikátorová pravidla a axiomy přijměme následující dvojici

B1:	$\forall x\varphi \to \varphi_x(t)$	, pokud t je substituovatelný za x ve φ
GEN:	$\psi \to \varphi \ /\ \psi \to \forall x\varphi$	, pokud x není volná ve ψ

Této dvojici říkáme *axiom specifikace* (nebo *konkretizace*) a *pravidlo generalizace*. Místo nich by také šlo přijmout následující trojici s jednodušším pravidlem generalizace

B1:	$\forall x\varphi \to \varphi_x(t)$	, pokud t ... (jako výše) ...
B2:	$\forall x(\psi \to \varphi) \to (\psi \to \forall x\varphi)$	, pokud x není volná ve ψ
GEN*:	$\varphi \ /\ \forall x\varphi$	

Snadno lze ukázat, že obě verze jsou ekvivalentní v tom smyslu, že z nich lze dokázat stejné formule. Zdůvodněme na ukázku, že schema B2 lze dokázat v systému s B1 a GEN. Podle věty o dedukci stačí dokázat formuli $\psi \to \forall x\varphi$ z předpokladu $\forall x(\psi \to \varphi)$, pokud se podaří splnit podmínku (viz [Š 73–74]), že v důkazu nepoužijeme generalizaci na žádnou proměnnou volnou v předpokladu $\forall x(\psi \to \varphi)$. Nevadí ale použít generalizaci na proměnnou x. Takže pojďme na to:

$\forall x(\psi \to \varphi) \vdash \forall x(\psi \to \varphi) \to (\psi \to \varphi)$	; B1. x je totiž substituo-
	; vatelná sama za sebe
$\forall x(\psi \to \varphi) \vdash \psi \to \varphi$	; MP
$\forall x(\psi \to \varphi) \vdash \psi \to \forall x\varphi$	; GEN, x není volná v ψ

Kvantifikátor $\exists x$ můžeme považovat za zkratku zápisu $\neg\forall x\neg$. Kdybychom to udělat nechtěli, přijali bychom axiom

B3: $\exists x\varphi \equiv \neg\forall x\neg\varphi$

nebo dvojici

$\exists$-B1: $\varphi_x(t) \to \exists x\varphi$
$\exists$-GEN: $\varphi \to \psi \ / \ \exists x\varphi \to \psi$

s podmínkami pro x, t stejnými jako u B1 a GEN.

V predikátovém počtu s rovností musíme samozřejmě přijmout také axiomy nebo pravidla o rovnítku. Ty mohou vypadat např. takto

E1: $x = x$
E2: $x = y \ \to \ y = x$
E3: $x = y \ \& \ y = z \ \to \ x = z$
E4: $x_1 = y_1 \ \& \ .. \ \& \ x_n = y_n \ \to \ F(x_1, .., x_n) = F(y_1, .., y_n)$
E5: $x_1 = y_1 \ \& \ .. \ \& \ x_n = y_n \ \to \ (P(x_1, .., x_n) \ \equiv \ P(y_1, .., y_n))$

kde E1–E3 jsou jednotlivé axiomy a E4, E5 jsou schemata; každý funkční a predikátový symbol má jeden axiom tvaru E4 resp. E5. O predikátovém počtu s rovností je v [Š] řeč na straně 84–87.

Důkazovým systémům jako je výše popsaný, které mají jen málo jednoduchých pravidel a k tomu větší počet logických axiomů, se říká *hilbertovské*. Vidíme, že i hilbertovských systémů je přinejmenším několik. Vnucuje se otázka, které vlastnosti musí logický kalkulus mít, abychom jej uznali za přípustný nebo dokonce ten pravý. Tak tedy: axiomy a pravidla důkazového systému by měly být definovány čistě syntakticky, bez odvolání se k sémantice. Tato vlastnost umožňuje sestrojit algoritmus, který rozhoduje, zda daná formule je nebo není logickým axiomem nebo zda je nebo není odvozena **jedním krokem** z daných předpokladů. A dále, pro důkazový systém by měla platit věta o úplnosti, která říká, že dokazatelné jsou přesně ty formule, které **mají** být dokazatelné (z hlediska sémantiky). Popsaný kalkulus obě podmínky splňuje.

Věta 1.5 (o úplnosti, Gödel 1930) *Formule φ je dokazatelná z prázdné množiny předpokladů, právě když φ je logicky platnou formulí.*

Věta 1.6 (o silné úplnosti, [Š 99–100]) *(a) Množina* sentencí *Δ je splnitelná, právě když je bezesporná.*
(b) Je-li φ formule a Δ množina sentencí*, pak*

$$\Delta \vdash \varphi, \quad \textit{právě když} \quad \Delta \models \varphi.$$

Pojem *bezesporné množiny* je ovšem definován stejně jako ve výrokovém počtu. Předpoklad, že ve formulích z Δ nejsou volné proměnné, je v (b) podstatný.

Formule $\forall x P(x)$, kde P je unární predikátový symbol, je dokazatelná z předpokladu $P(x)$. V příkladu 5 jsme ale viděli, že není jeho důsledkem. Tento příklad zároveň ukazuje, proč je ve větě o dedukci nutný předpoklad o (neexistenci) volných proměnných, viz [Š 73].

Větami o korektnosti se opět míní všechny tři implikace $\Rightarrow$ v obou větách. Zmiňme se o implikaci $\Rightarrow$ v (b). Když $\Delta \vdash \varphi$, pak existuje důkaz $\varphi_1, .., \varphi_m$ $(= \varphi)$ formule φ z předpokladů Δ. Dále se postupuje indukcí podle $i \leq m$. Je ale nutné si uvědomit, jak přesně zní tvrzení, které dokazujeme indukcí. *Každá φ_i platí v každé (nebo v dané) struktuře, v které platí všechny formule z Δ.* Nepodařilo by se dokázat, že každá φ_i je v dané struktuře splněna daným ohodnocením proměnných (které splňuje všechny formule z Δ). To souvisí s rozdílem mezi pravidly MP a GEN. Když φ i $\varphi \rightarrow \psi$ jsou splněny v $\mathbf{M}$ nějakým ohodnocením proměnných e, pak i ψ je splněna tímtéž ohodnocením e. O pravidlu generalizace lze ale říci pouze, že když ψ je odvozena pravidlem GEN z φ a φ je v $\mathbf{M}$ splněna **každým** ohodnocením, pak i ψ je v $\mathbf{M}$ splněna každým ohodnocením proměnných.

Doporučujeme čtenáři, aby si na tomto místě rozmyslel, že všechny vztahy mezi podmínkami vět o kompaktnosti a úplnosti zmíněné v par. 1.2 platí i v predikátovém počtu. To je samozřejmě něco jiného než vlastní důkaz věty o úplnosti. Ten je v [Š] na stranách 101–112.

Podobně jako ve výrokovém počtu věty o kompaktnosti a úplnosti platí bez ohledu na mohutnost jazyka. Chceme-li ale uvažovat o algoritmické rozhodnutelnosti, předpokládáme, že jazyk je nejvýše spočetný a že jsme přijali nějakou dohodu na téma nekonečná množina symbolů je vlastně nekonečnou množinou jednoduchých slov sestavených z konečně mnoha elementárnějších symbolů. Teorie "ze života" mají dost často dokonce konečný jazyk. Ale i v tom případě máme co dělat s nekonečně mnoha symboly: už proměnných je nekonečně mnoho.

V tomto paragrafu jsme viděli, že pojem struktura pro daný jazyk spolu s ohodnocením proměnných hrají v sémantice predikátové logiky podobnou úlohu jako pravdivostní ohodnocení ve výrokové logice. Rozdíl je v tom, že sémantika predikátové logiky nedává žádný návod, jak sestrojit algoritmus, který by rozhodoval, zda formule je logicky platná nebo zda vyplývá z daných předpokladů. Bylo by třeba ověřit, že něco platí o **všech** strukturách, ale struktur je nekonečně mnoho a některé z nich mohou být nekonečné. Přesto takový algoritmus v některých případech, tj. pro některé jazyky nebo některé množiny předpokladů, (kupodivu) sestrojit lze. V jiných případech lze naopak dokázat, že takový algoritmus neexistuje. S ukázkami obojího se ještě setkáme.

Máme-li konečnou strukturu $\mathbf{M}$ pro konečný jazyk, jejíž predikáty a operace jsou zadány tabulkami, pak ovšem lze snadno sestrojit algoritmus pro rozhodování, zda daná formule v $\mathbf{M}$ platí. Nebude to ale příliš efektivní algoritmus. Množina všech formulí platných v předem dané konečné struktuře $\mathbf{M}$ je totiž skoro vždy (tj. za slabých předpokladů o struktuře $\mathbf{M}$) PSPACE-úplným jazykem.

Jedna věc ale je stejná jako ve výrokovém počtu. Lze sestrojit mechanickou proceduru, která postupně generuje všechny důkazy (v daném jazyce a z prázdné množiny předpokladů) nebo všechny dokazatelné formule. Tato úvaha spolu s větou o úplnosti ukazuje, že všechny logicky platné formule v daném například konečném jazyce tvoří rekurzivně spočetnou množinu.

Cvičení

1. Převeďte následující formule na prenexní normální tvar

   $\forall x(P(x) \to \forall y(Q(x,y) \to \neg\forall z R(y,z)))$
   $\exists x A(x,y) \to (B(x) \to \neg\exists u A(x,u))$
   $P(x,y) \to \exists y(Q(y) \to (\exists x Q(x) \to R(y)))$

   Stanovte, zda a jak moc se formule převedením na prenexní tvar prodlouží.

2. Nechť P, Q jsou unární a R binární predikát. Dokažte, že následující formule jsou logicky platné, ale obrátíme-li (vnější) implikaci, ve všech případech vznikne formule, která není logicky platná.

   $\exists x(P(x)\ \&\ Q(x)) \to \exists x P(x)\ \&\ \exists x Q(x)$
   $\forall x P(x) \vee \forall x Q(x) \to \forall x(P(x) \vee Q(x))$
   $\exists x \forall y R(x,y) \to \forall y \exists x R(x,y)$
   $\forall x(P(x) \to Q(x)) \to (\forall x P(x) \to \forall x Q(x))$
   $\forall x(P(x) \to Q(x)) \to (\exists x P(x) \to \exists x Q(x))$

3. Najděte formuli φ a množinu formulí Δ takovou, že φ platí ve všech *konečných* strukturách, ve kterých platí všechny formule z Δ, ale φ nevyplývá z Δ. Lze množinu Δ volit konečnou?

4. Najděte sentenci v příslušném jazyce, která platí jen v jedné resp. jen v jedné ze tří struktur
   (a) $\langle R, +, \cdot, 0, 1\rangle$, $\langle Q, +, \cdot, 0, 1\rangle$
   (b) $\langle N, <\rangle$, $\langle Z, <\rangle$, $\langle Q, <\rangle$
   Příslušným jazykem se myslí jazyk se dvěma binárními funkčními symboly a se dvěma konstantami v (a) a jazyk s jedním binárním predikátovým symbolem v (b). Všechny formule myslíme v predikátovém počtu s rovností. N, Z, Q a R značí množiny všech přirozených (s nulou), celých, racionálních a reálných čísel.

5. Nechť T je teorie s jazykem $\{\in\}$ s jediným binárním predikátem a s axiomy

   $\forall x \forall y(\forall v(v \in x \equiv v \in y) \to x = y)$
   $\exists x \forall v \neg(v \in x)$
   $\forall x \forall y \exists z \forall v(v \in x \vee v = y \to v \in z)$

(a) Dokažte pomocí konečných modelů, že v T nelze dokázat žádnou z formulí $\forall x(x \notin x)$ ani $\neg\exists x\forall v(v \in x)$.
(b) Dokažte, že žádný ze tří axiomů teorie T není dokazatelný z ostatních dvou.

6. Nechť Σ je množina formulí, která je ekvivalentní s nějakou konečnou množinou formulí Δ (v tom smyslu, že každý prvek kterékoliv množiny vyplývá z druhé množiny). Dokažte, že v tom případě je Σ ekvivalentní i s jistou konečnou množinou Δ' takovou, že $\Delta' \subseteq \Sigma$.

7. Dokažte, že pokud existenční kvantifikátor $\exists x$ považujeme za zkratku pro $\neg\forall x\neg$, pak $\exists$-B1 je dokazatelné schema a $\exists$-GEN je korektní v systému s B1 a GEN. Pokud bychom naopak univerzální kvantifikátor považovali za zkratku, pak B1 a GEN jsou dokazatelné z $\exists$-B1 a $\exists$-GEN.

8. Dokažte bez užití věty o úplnosti, že formule v cvičení 2 jsou v predikátovém počtu dokazatelné.

9. Představte si, že bychom sémantiku predikátové logiky modifikovali tak, že by se připouštěly jen všechny neprázdné *konečné* struktury. Dokažte, že pro "logiku" s takto definovanou sémantikou (tj. pro množinu všech formulí platných ve všech konečných neprázdných strukturách) by neplatila věta o úplnosti ani věta o kompaktnosti.
Návod. Použijte cvičení 3. Dále najděte množinu sentencí, jejíž každá konečná část je, ale celá není splnitelná v konečné struktuře.

1.4 Teorie, vlastnosti teorií, příklady

Axiomatická teorie je dána volbou jazyka L a množiny T sentencí v L. Prvkům množiny T říkáme *axiomy* teorie $\langle L, T\rangle$. Místo $\langle L, T\rangle$ budeme ale psát jen T, jako kdyby na volbě jazyka nezáleželo. A ono opravdu moc nezáleží. Za jazyk totiž vždy můžeme vzít seznam těch symbolů, které se vyskytují v axiomech.

Narozdíl od [Š] požadujeme, aby axiomy neměly volné proměnné. Kdybychom to snad někdy nedodrželi a řekli třeba, že axiom je $x + y = y + x$, myslíme samozřejmě, že axiom je formule $\forall x\forall y(x + y = y + x)$, tj. za skutečný axiom považujeme *univerzální uzávěr* dané formule. Požadavek, aby předpoklady neobsahovaly volné proměnné, se vyskytuje (mimo jiné) ve větě o úplnosti a viděli jsme, že tam má dobrý smysl. Jak to, že se ale takový požadavek nevyskytuje ve větě o úplnosti uvedené v [Š]? Je to proto, že jsme se od [Š] odchýlili už v definici důsledku. Definice v [Š 93]

$$T \models \varphi \quad \text{iff} \quad \forall \mathbf{M}(\forall e\forall\psi \in T(\mathbf{M} \models \psi[e]) \Rightarrow \forall e(\mathbf{M} \models \varphi[e]))$$

splývá s naší definicí v případě, že T je množina sentencí, a umožňuje opticky obecnější formulaci věty o úplnosti. Neumožňuje ale definovat, co jsou ekvivalentní formule. A to jsme v minulém paragrafu potřebovali.

Umluvme se, že odtud dále všechny teorie a jazyky myslíme v predikátovém počtu s rovností.

Příklad 1 *Teorie grup* má jazyk s jednou binární operací a s jednou konstantou a známou trojici axiomů, viz [Š 165]. Modely teorie grup jsou právě všechny grupy. *Teorie* DNO (DeNse Order) *lineárního hustého uspořádání* má jeden binární predikát $<$ a axiomy

$$\forall x \forall y \forall z (x < y \ \& \ y < z \rightarrow x < z)$$
$$\forall x \forall y (x < y \rightarrow \neg (y < x))$$
$$\forall x \forall y (x < y \vee x = y \vee y < x)$$
$$\forall x \forall y (x < y \rightarrow \exists z (x < z \ \& \ z < y))$$
$$\forall x \exists z_1 \exists z_2 (z_1 < x \ \& \ x < z_2)$$

Modely teorie DNO jsou právě všechny lineárně hustě uspořádané množiny bez koncových bodů. Kdybychom přijali jen první dva nebo jen první tři axiomy, dostali bychom teorii *(ostrého) uspořádání* resp. teorii LO *(ostrého) lineárního uspořádání*.

Příklad 2 Existují různé verze *teorie množin* formulované v jazyce $\{\in\}$ s jediným binárním predikátem. Nejběžnější jsou Gödel-Bernaysova teorie množin s konečným počtem (asi čtrnácti) axiomů a Zermelo-Fraenkelova teorie množin s konečně mnoha axiomy a několika axiomatickými schematy. Modelem teorie množin je samozřejmě každá množina s jednou binární relací, ve které platí všechny axiomy. Potíž je ale v tom, že není známa žádná "přímá" konstrukce modelu (některé) teorie množin. Podle věty o úplnosti takový model samozřejmě existuje, pokud je teorie množin bezesporná. Ale ani žádné důkazy bezespornosti teorie množin, které by nepoužily nějaké diskutabilní předpoklady (např. že existují nedosažitelné kardinály), nejsou známy. Druhá Gödelova věta o neúplnosti, s kterou se setkáme dále, ukazuje, že je to zákonité.

Příklad 3 Je-li $\mathbf{M}$ nějaká struktura pro nějaký jazyk L, pak $\mathrm{Th}(\mathbf{M})$ je množina

$$\{ \varphi \ ; \ \varphi \text{ je sentence v } L \text{ a } \mathbf{M} \models \varphi \}.$$

Množinu $\mathrm{Th}(\mathbf{M})$ nazýváme *teorií struktury* $\mathbf{M}$. Tento příklad má zdůraznit, že v definici teorie skutečně stojí "množina" a že množina axiomů nemusí být totéž co "úhledný seznam". Věty o kompaktnosti a úplnosti se vztahují i na teorie, u kterých není zřejmé, zda množina axiomů je algoritmicky rozhodnutelná. Teorii $\mathrm{Th}(\mathbf{R})$ nazýváme *teorií reálných čísel* a $\mathrm{Th}(\mathbf{N})$ nazýváme *úplnou aritmetikou*.

Vidíme, že některé vlastnosti struktur jsou *vyjádřitelné* formulí nebo množinou formulí v tom smyslu, v jakém je vlastnost "býti lineárně uspořádanou množinou" vyjádřitelná axiomy teorie LO. Jsou všechny vlastnosti struktur takto vyjádřitelné? Rozhodně ne. Například "míti určitou mohutnost" je příklad vlastnosti, která vyjádřitelná není. Podle Löwenheim-Skolemovy věty [Š 173] každá teorie, která má nejvýše spočetný jazyk a alespoň jeden nekonečný model, má modely všech nekonečných mohutností. Pro teorii Th($\mathbf{R}$) tento fakt znamená, že existuje spočetné uspořádané těleso, ve kterém platí přesně tytéž sentence v aritmetickém jazyce, jako platí v tělese $\mathbf{R}$ všech reálných čísel. To se může zdát překvapivé, protože z analýzy víme, že určitá vlastnost určuje uspořádání reálných čísel až na izomorfismus. Máme na mysli toto tvrzení. Když $\langle A, <_A\rangle$ je *lineárně hustě uspořádaná množina bez minima a maxima, která obsahuje spočetnou hustou podmnožinu a ve které každá neprázdná shora omezená část má suprémum,* pak $\langle A, <_A\rangle$ je izomorfní s uspořádáním reálných čísel$\langle R, <\rangle$. Toto tvrzení ale není ve sporu s existencí spočetného modelu teorie Th($\mathbf{R}$). Existence takového modelu je ale důkazem, že výše zmíněná vlastnost (zvýrazněná odlišným typem písma) není vyjádřitelná formulí ani množinou formulí v aritmetickém jazyce.

U příkladu 2 jsme poznamenali, že vlastně není znám žádný důkaz existence modelu teorie množin. Pokud ale takový model existuje, pak podle Löwenheim-Skolemovy věty existuje i spočetný model teorie množin. Tento fakt se rovněž může na první pohled zdát paradoxní.

Nespočetný model úplné aritmetiky Th($\mathbf{N}$) a obecně každý model teorie Th($\mathbf{N}$), který není izomorfní s $\mathbf{N}$, nazýváme *nestandardní*. Vidíme, že ani vlastnost "každý prvek má jen konečně mnoho předchůdců" není vyjádřitelná v aritmetickém jazyce a to ať předchůdce myslíme ve smyslu uspořádání nebo ve smyslu následnické funkce S. Není náhodou existence nestandardních modelů Th($\mathbf{N}$) možná jen díky tomu, že se připouštějí i nespočetné modely? Ne, s užitím věty o kompaktnosti lze dokázat, viz [Š 115], že Th($\mathbf{N}$) má i spočetné nestandardní modely. Jiný školní příklad na užití věty o kompaktnosti je příklad 11 v [Š 119]. Dobře, není to tedy potom tak, že každá teorie má různé modely každé dané mohutnosti? Hned uvidíme, že ani to není pravda.

Nechť κ je nekonečný kardinál. Řekneme, že teorie T je *κ-kategorická*, jestliže každé dva modely teorie T mohutnosti κ jsou spolu izomorfní.

Příklad 4 Krajní teorie, která nemá žádné mimologické symboly (má ovšem rovnítko) a žádné axiomy, je κ-kategorická pro každé nekonečné κ. Uvažujme teorii SUCC, která má jazyk $\{\overline{0}, S\}$ a axiomy

Q1:	$S(x) \neq \overline{0}$
Q2:	$S(x) = S(y) \rightarrow x = y$
Q3:	$x \neq \overline{0} \rightarrow \exists y(x = S(y))$
Ln:	$S^{(n)}(x) \neq x$, pro $n \neq 0$

V zápisu axiomů jsme vynechali úvodní univerzální kvantifikátory. $S^{(n)}(x)$ pochopitelně znamená term $S(S \ldots S(x) \ldots)$ s n výskyty symbolu S. A poslední řádek označený Ln myslíme jako nekonečně mnoho axiomů, jeden pro každé $n \neq 0$. Teorie SUCC **není** $\aleph_0$-kategorická, protože kromě $\mathbf{N}^- = \langle N, 0, .+1\rangle$

má ještě například model $\mathbf{N}^- + \mathbf{Z}^-$, jehož nosná množina je disjunktním sjednocením množiny přirozených čísel N a množiny celých čísel Z, funkce S je realizována "normálně" přičítáním jedničky v obou množinách a $\overline{0}$ je realizována přirozenou — nikoliv celočíselnou — nulou. Minus v horním indexu znamená, že uvažujeme strukturu pro jazyk jen se dvěma symboly, neuvažujeme sčítání a násobení jako v příkladu 3. Naproti tomu o teorii DNO lineárního hustého uspořádání z příkladu 1 můžeme dokázat, že **je** $\aleph_0$-kategorická. Nechť $\langle A, <_1\rangle$ a $\langle B, <_2\rangle$ jsou libovolné dva její spočetné modely. Nechť $A = \{a_0, a_1, a_2, \ldots\}$, $B = \{b_0, b_1, b_2, \ldots\}$. Izomorfismus $f : A \to B$ obou struktur se sestrojí rekurzí tak, že v kroku $2n$ určíme $f(a_n) \in B$ a v kroku $2n + 1$ určíme $x \in A$ takové, že $f(x) = b_n$, a to vždy tak, že dosud sestrojený konečný fragment funkce f zachovává uspořádání obou množin.

Dejme tomu, že existenci nestandardních (tj. neizomorfních s $\langle N, 0, .+1\rangle$) modelů teorie SUCC budeme na chvíli považovat za nežádoucí. Nešlo by je zakázat přidáním dalších axiomů k teorii SUCC, které by třeba v $\mathbf{N}^- + \mathbf{Z}^-$ neplatily? I u jiných teorií můžeme uvažovat o možnosti přidat nějaké axiomy. Aby to mělo smysl, přidané axiomy nesmějí porušit bezespornost teorie a neměly by vyplývat z dosavadních axiomů. Například všechny formule tvaru

$$\text{IND}^-:\quad \varphi_x(\overline{0})\ \&\ \forall x(\varphi \to \varphi_x(S(x))) \to \forall x\varphi$$

kde minus v indexu opět upozorňuje na nepřítomnost sčítání a násobení, platí v $\langle N, 0, .+1\rangle$ a jejich přidání tedy neporuší bezespornost. Je mezi nimi některá , která není dokazatelná v teorii SUCC? Je mezi nimi některá, která neplatí v $\mathbf{N}^- + \mathbf{Z}^-$?

Nechť T je teorie v jazyce L. Řekneme, že T je *úplná*, jestliže T je bezesporná a pro každou sentenci φ platí $T \vdash \varphi$ nebo $T \vdash \neg\varphi$. Řekneme, že sentence φ v L je *nezávislá* na T, jestliže φ ani $\neg\varphi$ není v T dokazatelná.

Příklad 5 *Robinsonova aritmetika* Q má aritmetický jazyk $\{+, \cdot, \overline{0}, S, \leq\}$, axiomy Q1–Q3 z příkladu 4 a dále axiomy

Q4: $x + \overline{0} = x$
Q5: $x + S(y) = S(x + y)$
Q6: $x \cdot \overline{0} = \overline{0}$
Q7: $x \cdot S(y) = x \cdot y + x$
Q8: $x \leq y \equiv \exists v(v + x = y)$

Robinsonova aritmetika je neúplná teorie. Cvičení 12 ukazuje několik sentencí — mezi nimi $\forall x(\overline{0}+x = x)$ —, které platí v $\mathbf{N}$ a jsou nedokazatelné v Q. Rovněž schema Ln je v Q nedokazatelné. Naproti tomu Th($\mathbf{N}$) a také každá jiná teorie tvaru Th(...) je úplná.

Mějme nějakou teorii T, která je neúplná. Nechť φ je některá sentence nezávislá na T. To znamená, že obě teorie T, φ i $T, \neg\varphi$ jsou bezesporné a mají tedy nějaké modely $\mathbf{M_1}$ a $\mathbf{M_2}$. Kdyby $\mathbf{M_1}$ a $\mathbf{M_2}$ byly izomorfní, musely by v nich platit stejné sentence, viz cvičení 9. Tedy $\mathbf{M_1}$ a $\mathbf{M_2}$ **nejsou** izomorfní. Přidáme-li navíc podmínku, že T nemá žádné konečné modely, můžeme díky Löwenheim-Skolemově větě požadovat, aby $\mathbf{M_1}$ a $\mathbf{M_2}$ měly stejnou mohutnost. Tím jsme dokázali následující větu.

Věta 1.7 (Vaughtův test) *Nechť T má nejvýše spočetný jazyk, nemá žádné konečné modely a je κ-kategorická pro některý nekonečný kardinál κ. Pak T je úplná.*

Příklad 6 Teorie DNO nemá žádné konečné modely a je $\aleph_0$-kategorická. Tedy je úplná. Obraťme se nyní k teorii SUCC. Nechť $\langle M, a, f\rangle$ je libovolný model teorie SUCC. Tedy $a \in M$ a $f : M \to M$. Z platnosti axiomů plyne, že f je prostá funkce a že pro její obor hodnot platí $\mathrm{Rng}(f) = M - \{a\}$. Definujme na M relaci $\sim$ takto: $x \sim y$, právě když některý prvek dvojice $\{x,y\}$ je z druhého dosažitelný konečně mnoha skoky funkce f. Relace $\sim$ je ekvivalence (cvičení: z platnosti kterého axiomu to plyne?) a každá třída rozkladu je nekonečná (cvičení: z platnosti kterého axiomu ... ?). Třída rozkladu obsahující a je izomorfní s $\langle N, 0, .{+}1\rangle$, každá jiná třída je izomorfní se $\langle Z, 0, .{+}1\rangle$. Jiné třídy ovšem nemusí existovat. Pokud ale celá množina M má nespočetnou mohutnost κ, existovat musí a musí jich být κ. Rovnice $\aleph_0 \cdot x = \kappa$ má totiž v kardinální aritmetice pro nespočetné κ jediné řešení $x = \kappa$. Model $\mathbf{M}$ má tedy jedinou možnou strukturu: κ na obě strany neomezených "řetízků" plus jeden "půlřetízek" obsahující prvek a. Z toho plyne, že každé dva modely teorie SUCC mohutnosti κ jsou spolu izomorfní. Dokázali jsme, že teorie SUCC je κ-kategorická pro každé nespočetné κ. Dle Vaughtova testu je úplná. To například znamená, že modely $\langle N, 0, .{+}1\rangle$ a $\mathbf{N}^- + \mathbf{Z}^-$ se neliší platností žádné sentence a také, že schema IND^- je v SUCC dokazatelné.

Řekneme, že teorie T je *rozhodnutelná*, jestliže existuje algoritmus rozhodující o dokazatelnosti formulí v T, tj. jestliže množina všech vět teorie T je rekurzivní.

Příklad 7 Je-li $\mathbf{M}$ konečná struktura pro konečný jazyk, pak $\mathrm{Th}(\mathbf{M})$ je rozhodnutelná teorie.

Věta 1.8 *Má-li teorie T rekurzivní množinu axiomů a je úplná, pak T je rozhodnutelná.*

Důkaz. Algoritmus P přijme vstupní sentenci φ a pak postupně probírá všechna slova v příslušném abecedě a blíže se věnuje těm, která jsou důkazy v teorii T. K rozhodnutí, zda slovo je nebo není důkazem, potřebuje podprogram, který rozhoduje, zda daná formule je axiomem teorie T. Takový podprogram existuje díky podmínce, že T má rekurzivní množinu axiomů. Narazí-li P na důkaz formule φ, řekne ANO, φ je dokazatelná. Narazí-li na důkaz formule $\neg\varphi$, řekne NE, φ není dokazatelná. V obou případech skončí.

Příklad 8 Teorie DNO i SUCC jsou rozhodnutelné.

Naše úvaha o teorii SUCC je zajímavá tím, že se v ní spojily možná dost vzdálené oblasti matematiky: fakt o nespočetných modelech měl za následek existenci nějakého algoritmu. Řekněme to přesněji. Algoritmus si můžeme představit napsaný v nějakém programovacím jazyce a o jeho existenci pochybovat nelze. Fakt o nespočetných modelech se ale uplatnil v důkazu jeho **korektnosti**.

V tomto místě můžeme prozradit něco, co jsme odkládali ve snaze přesvědčit čtenáře o užitečnosti úvah o modelech. Existuje i jiná metoda pro důkazy úplnosti a rozhodnutelnosti teorií, která se jmenuje *eliminace kvantifikátorů*. Její použití na teorii SUCC ukazují cvičení 14, 15, 16. S použitím eliminace kvantifikátorů lze dokázat i rozhodnutelnost teorií

$$\mathrm{Th}(\langle N, 0, .{+}1, \leq, < \rangle) \ \text{ a } \ \mathrm{Th}(\langle N, +, 0, .{+}1, \leq, < \rangle)\ .$$

Postup je jen (v druhém případě o hodně) pracnější.

Také teorie $\mathrm{Th}(\mathbf{R})$ je rozhodnutelná. Ale pozor: z rozhodnutelnosti $\mathrm{Th}(\mathbf{R})$ nijak nevyplývá rozhodnutelnost teorie $\mathrm{Th}(\mathbf{N})$, kde $\mathbf{N}$ je standardní model aritmetiky — se sčítáním i násobením — z příkladu 3.

Peanova aritmetika PA vznikne přidáním *schematu indukce*

$$\text{IND:} \qquad \varphi_x(\overline{0}) \ \& \ \forall x(\varphi \rightarrow \varphi_x(S(x))) \rightarrow \forall x \varphi$$

k Robinsonově aritmetice Q. Na rozdíl od případu, kdy jsme se schema indukce pokusili přidat k teorii SUCC, tentokrát φ může obsahovat všechny aritmetické symboly. A tentokrát přidání má cenu: formule ve cvičení 12, o kterých zjistíte, že jsou platné v $\mathbf{N}$ a nedokazatelné v Q, jsou všechny dokazatelné v PA. Schema IND platí v $\mathbf{N}$, tedy $\mathbf{N}$ je jedním z modelů PA. Obecně každý model teorie $\mathrm{Th}(\mathbf{N})$ je zároveň modelem PA. Tedy PA má i nestandardní modely. Bohužel tak jednoduchým postupem, jakým je ve cvičení 11 sestrojen nestandardní model Robinsonovy aritmetiky — zvolit spočetnou množinu a definovat na ní sčítání a násobení větvením na konečně mnoho případů —, nelze sestrojit nestandardní model Peanovy aritmetiky. To je důvod, proč není tak snadné rozhodnout, zda PA je úplná teorie.

Vyjmenujme na závěr několik otázek, na které jsme neodpověděli a ke kterým se vrátíme v dalším textu.

1. Je PA úplná? Pokud ne, nešlo by ji zúplnit předáním několika axiomů nebo schemat?

2. Je PA rozhodnutelná?

3. Je $\mathrm{Th}(\mathbf{N})$ *rozhodnutelná? Pokud ne, je množina všech sentencí platných v* $\mathbf{N}$ *alespoň rekurzivně spočetná?*

4. Je Q rozhodnutelná?

Cvičení

1. (a) Nechť T je teorie s jedním binárním predikátem R a s axiomy

$$R(x,x), \quad R(x,y) \rightarrow R(y,x), \quad R(x,y) \;\&\; R(y,z) \rightarrow R(x,z)$$

Kolik má T navzájem neizomorfních například pětiprvkových modelů?
(b) Formulujte ve vhodném jazyce teorii, která má konečné modely všech možných sudých mohutností a nemá žádný model liché mohutnosti. Návod. Lze přidat vhodné axiomy k teorii z (a).

2. Nechť T je teorie v jazyce $\{<\}$ taková, že každá dobře uspořádaná množina je jejím modelem. Dokažte, že T musí mít i modely, které nejsou dobře uspořádané. Použijte návod k cv. 11 v [Š 119].

3. V jazyce bez mimologických symbolů (tj. jen s predikátem rovnosti) formulujte bezespornou teorii, která nemá žádné konečné modely.

4. Dokažte, že teorie z cvičení 3 není konečně axiomatizovatelná (tj. není ekvivalentní s žádnou konečnou množinou axiomů). Dokažte, že ani teorie SUCC není konečně axiomatizovatelná.
Návod. Použijte cvičení 6 z předcházejícího paragrafu.

5. Rozhodněte, zda teorie DNO je κ-kategorická pro každé nekonečné κ.

6. Dokažte, že platí. Teorie T je úplná, právě když je bezesporná a pro každou sentenci φ a pro každé dva modely $\mathbf{M_1}, \mathbf{M_2}$ platí $\mathbf{M_1} \models \varphi \Leftrightarrow \mathbf{M_2} \models \varphi$.

7. Dokažte, že teorie z cvičení 3 je úplná.

8. Rozhodněte, zda platí: je-li T bezesporná teorie a každé dva její nekonečné spočetné modely jsou spolu izomorfní, pak T je úplná.

9. Nechť $\mathbf{M_1}, \mathbf{M_2}$ jsou dvě struktury pro týž jazyk L a nechť $F : M_1 \rightarrow M_2$ je izomorfismus obou struktur. Je-li e ohodnocení proměnných v M_1, označme $F(e)$ ohodnocení v M_2, které každé proměnné x přiřazuje F onoho prvku z M_1, který je proměnné x přiřazen ohodnocením e. Dokažte, že pro každou formuli φ a každé ohodnocení e platí

$$\mathbf{M_1} \models \varphi[e] \Leftrightarrow \mathbf{M_2} \models \varphi[F(e)]$$

Ukažte na příkladě, že požadavek, aby F byl izomorfismus, nelze nahradit požadavkem, že F je prostá funkce.

10. Nechť T je teorie, která má neomezeně velké konečné modely. Užijte větu o kompaktnosti k důkazu, že T musí mít i nekonečné modely.

11. Přidejme ke struktuře **N** přirozených čísel dva nové prvky a, b a rozšiřme následnickou funkci na množinu $M = N \cup \{a, b\}$ předpisem $S(a) = b$, $S(b) = a$. Dokažte, že sčítání a násobení je možno rozšířit na celou množinu M tak, aby v M platily všechny axiomy Robinsonovy aritmetiky Q.

12. Rozhodněte, zda následující formule jsou dokazatelné v Robinsonově aritmetice Q:

$\forall x(x \leq x)$	$\forall x \forall y(x + y = \overline{0} \rightarrow x = \overline{0} \ \& \ y = \overline{0})$
$\forall x(x \leq \overline{0} \rightarrow x = \overline{0})$	$\forall x \forall y(x \leq y \equiv S(x) \leq S(y))$
$\forall x(\overline{0} \leq x)$	$\forall x \forall y(x \cdot y = \overline{0} \rightarrow x = \overline{0} \vee y = \overline{0})$
$\forall x(\overline{0} \cdot x = \overline{0})$	$\forall x(\overline{n} \leq x \rightarrow x = \overline{n} \vee \overline{n+1} \leq x)$
$\forall x(x \cdot \overline{1} = x)$	$\forall x \forall y \forall z((z + y) + x = z + (y + x))$
$\forall x \forall y \exists z(x \leq z \ \& \ y \leq z)$	

Návod. NE lze dokázat vhodnou volbou operací v cvičení 11. Pro všechna NE lze vystačit s jediným modelem.

13. Je-li teorie T rozhodnutelná, pak i každé rozšíření T, φ teorie T o jeden axiom φ je rozhodnutelné. Dokažte.

14. Každá formule v jazyce $\{\overline{0}, S\}$, která je zároveň otevřená i uzavřená, je v teorii SUCC dokazatelná nebo vyvratitelná, a to podle toho, zda platí nebo neplatí v $\langle N, 0, .+1\rangle$. Dokažte.
Návod. Každá taková formule musí být boolovskou kombinací formulí tvaru $\overline{n} = \overline{m}$.

15. Nechť A je formule v jazyce $\{\overline{0}, S\}$, která je konjunkcí literálů (literály jsou atomické formule a negace atomických formulí). Dokažte, že formule $\exists x A$ je v teorii SUCC ekvivalentní s nějakou otevřenou formulí.
Návod. Nejprve uvažte, že každý literál v A je tvaru $t = s$ nebo $t \neq s$, a termy t, s musí mít tvar $\overline{n}$ nebo $S^{(n)}(v)$, kde v může ale nemusí být x. Dále postupujte v těchto krocích
(a) Lze předpokládat,že x se v žádném literálu nevyskytuje na obou stranách (rovnítka nebo nerovnítka).
(b) Lze předpokládat, že x se vyskytuje jen v kontextu $S^{(m)}(x)$, kde m je jedno stejné pro všechny výskyty.
(c) V tom případě má formule $\exists x A$ jeden z tvarů
$$\exists x(S^{(m)}(x) = t \ \& \ B(S^{(m)}(x))) \quad \text{, nebo}$$
$$\exists x(S^{(m)}(x) \neq t_1 \ \& \ .. \ \& \ S^{(m)}(x) \neq t_n \ \& \ B) \quad ,$$
kde v prvním případě t a v druhé případě B a termy t_i neobsahují x.

16. Dokažte, že vůbec každá formule v jazyce $\{\overline{0}, S\}$ je v teorii SUCC ekvivalentní s otevřenou formulí.

2 Metamatematika aritmetiky

Úvod V první části jsme se seznámili s pojmem jazyka, pojmem axiomatické teorie (s rovností), pojmem modelu takové teorie a s Gödelovou větou o úplnosti. Mezi příklady se vyskytl jazyk aritmetiky obsahující predikát = rovnosti, predikát $\leq$ neostré nerovnosti (oba četnosti 2), unární funkční symbol S následníka, binární funkční symboly $+, *$ sčítání a násobení a konstantu $\bar{0}$; mezi termy tohoto jazyka máme *numerály* $\bar{n}$ (t.j. term $S \dots S\bar{0}$ s n exempláři symbolu S). Známe *standardní model* $\mathbf{N}$ jazyka aritmetiky (to je struktura přirozených čísel) a dvě teorie mající $\mathbf{N}$ za model: Robinsonovu aritmetiku Q a Peanovu aritmetiku PA. Víme, že obě mají také *nestandardní modely*, t.j. modely neisomorfní s $\mathbf{N}$.

V této části se budeme aritmetikou intensivně zabývat; jednak budeme studovat množiny čísel (části N) a funkce zobrazující N do N, které jsou *definovatelné* v $\mathbf{N}$ pomocí jazyka aritmetiky, jednak budeme studovat axiomatické teorie T v jazyce aritmetiky obsahující Q. Základní otázka zní takto: existuje taková rozumná teorie T, v níž by byly dokazatelné *právě všechny* sentence pravdivé v $\mathbf{N}$? Lze nabídnout triviální odpověď: jestliže $T = Th(\mathbf{N})$ je množina všech formulí pravdivých v $\mathbf{N}$, pak tato teorie triviálně dokazuje právě všechny formule pravdivé v $\mathbf{N}$. To je ovšem příliš laciné a nevíme, jak algoritmicky rozhodovat, zda nějaká formule je či není pravdivá v $\mathbf{N}$ (a uvidíme, že to nejde). Upřesníme tedy otázku takto: chceme, aby množina axiomů teorie T byla navíc algoritmicky rozhodnutelná (rozpoznatelná), t.j. aby existoval algoritmus, který pro každou formuli rozhodne, zda je nebo není axiomem. (Řekneme, že taková teorie je *rekursivně axiomatizovaná.*) *Gödelova první věta o neúplnosti* říká, že taková teorie neexistuje. Každá rekursivně axiomatizovaná teorie T v jazyce aritmetiky, která má za model $\mathbf{N}$, je neúplná, t.j. existuje sentence φ pravdivá v $\mathbf{N}$ a nedokazatelná v T. (Gödelova věta říká více, jak uvidíme.)

Dvě Gödelovy věty o neúplnosti aritmetiky jsou hlavním cílem, k němuž směřujeme. Poznáme přitom Gödelovu metodu *aritmetizace metamatematiky* (definujeme uvnitř aritmetiky její vlastní syntax - poznáte, co to přesně znamená) a *autoreference*, t.j. možnosti sestrojit v jazyce aritmetiky sentenci, která jistým způsobem "mluví sama o sobě", totiž např. vyjadřuje svoji vlastní nedokazatelnost.

Výklad je rozvržen do deseti paragrafů 2.1 - 2.10. První je pomocný a vlastně se aritmetiky netýká, jde o vlastnosti výrazů, užitečné v dalším. Paragrafy 2.2 - 2.4 se zabývají definovatelností v $\mathbf{N}$ (aritmetickou hierarchií formulí, kódováním posloupností čísel čísly a aritmetizací syntaxe.) Paragraf 2.5 je vlastně také pomocný a uvádí do souvislosti pojem rekursivnosti a pojem Δ_1 - definovatelnosti. Paragrafy 2.6 - 2.9 jsou věnovány aritmetice Q a pojem rozšířením: dokážeme základní věci v Q, ukážeme, že φ je Σ_1 - úplná, dokážeme diagonální lemma (o autoreferenci) a Gödelovy věty o neúplnosti, včetně variant a důsledků. Paragraf 2.10 je epilog; tam se ohlédneme po tom, co jsme dokázali a zvážíme, jak a proč je to důležité.

2.1 Struktura výrazů

Formule výrokového počtu, termy jazyka predikátového počtu a formule takového jazyka jsou příklady výrazů: vždy jsou nějaké atomické výrazy a nějaké operace, pomocí nichž vznikají z jedněch výrazů jiné. Přitom atomický výraz v jednom smyslu může obsahovat neatomické výrazy jiné třídy výrazů (atomické formule obsahují termy). Bude se nám hodit přesně formulovat a dokázat vlastnosti, které výrazy mají mít.

2.1.1. Definice *Typ struktury výrazů* je dán neprázdnou množinou At atomů, neprázdnou množinou Op operací a funkcí Ar (arity, četnosti) přiřazující každé operaci o její četnost $Ar(o)$. Přitom At a Op jsou nejvýše spočetné a navzájem disjunktní a $Ar(o)$ je přirozené číslo.

2.1.2.Definice *Struktura výrazů* (At, Op, Ar)je dána množinou $E \supseteq At$ výrazů (expressions) a funkcí A (aplikace) přiřazující každé operaci o četnosti n a každé posloupnosti $\langle e_o, \ldots e_{n-1}\rangle$ výrazů složený výraz $A(o, \langle s_0, \ldots s_{n-1}\rangle)$ vznikající z výrazů $e_0, \ldots, e_{n-1}$ pomocí operace o, přičemž jsou splněny tyto podmínky:

(1) Každý atom $e \in At$ je různý od každého složeného výrazu.

(2) Jestliže $A(o_1, \langle s_0, \ldots s_{m-1}\rangle) = A(o_2, \langle t_0, \ldots, t_{n-1}\rangle)$, pak $o_1 = o_2, m = n$ a $s_i = t_i$ pro $i = 0, \ldots, m-1$, t.j. složený výraz jednoznačně určuje operaci a výrazy, z nichž vznikl.

(3) $\mathbf{E}$ je nejmenší množina obsahující At a uzavřená na O_p, t.j. jestliže $X \subseteq \mathbf{E}, X \supseteq At$ a pro každé $o \in Op$ a $s_0, \ldots, s_{m-1} \in X$ je $A(o, \langle s_0, \ldots, s_{m-1}\rangle) \in X$, pak $X = \mathbf{E}$.

2.1.3. Věta o existenci struktury výrazů. Pro každý typ (At, Op, Ar) existuje struktura (E, A) výrazů tohoto typu.

Důkaz. Jde vlastně o konstrukci volné algebry s danou množinou generátorů a operací. To lze dělat různými způsoby; užijeme tzv. *polské notace* (prefixové, bezzávorkové) pro její eleganci a zajímavost. Zdůrazněme, že jde o existenční důkaz, nikoliv o to, že bychom chtěli výrazy vskutku níže popsaným způsobem zapisovat. Zvolme nějakou konečnou abecedu Λ a vhodným způsobem ztotožněme prvky množiny $At \cup Op$ s jistými slovy v abecedě Λ (t.j. $At \subseteq \Lambda^*$) tak, že žádný $e \in At \cup Op$ není vlastním počátečním úsekem jiného $e' \in At \cup Op$. (Pišme $e \subseteq_p$, je-li e počátečním úsekem e'.) Je-li atomů konečně mnoho a Λ má dost prvků, můžeme ztotožnit atomy s jednoprvkovými slovy; jinak např. ve výrokovém počtu nechť $\Lambda = \{\mathtt{p}, \mathtt{1}, \mathtt{0}, \neg, \rightarrow\}$ a ztotožněme n-tou výrokovou proměnnou s posloupností, která sestává z cifer dyadického zápisu čísla n, za nimiž následuje $\mathtt{p}$, t.j. např. p_5 bude representováno jako $\mathtt{101p}$. Všimněte si, že při opačném pořadí, t.j. kdyby $\mathtt{p}$ předcházalo index, neplatilo by následující lemma. Nechť $\frown$ značí operaci juxtapozice (slepení) posloupností, t.j. např. $\mathtt{101}^\frown\mathtt{110}$ je $\mathtt{101110}$. Zřejmě $\frown$ je asociativní; definujme $A(o, \langle s_0, \ldots, s_{n-1}\rangle) = o^\frown s_0^\frown \ldots^\frown s_{n-1}$, t.j.

složený výraz vznikne slepením operace o (což je slovo) s $s_0, s_1 \ldots s_{n-1}$. (Např. $A(\rightarrow, \mathtt{1p}, \mathtt{10p}) = \rightarrow \mathtt{1p10p}$ atd.) **E** nechť je nejmenší část Λ^* obsahující At a uzavřená na A; zbývá ověřit jednoznačnost rozkladu složených výrazů. K tomu dvě lemmata.

Lemma A. Žádný výraz není vlastním počátečním úsekem jiného výrazu.

Důkaz. Nechť e' je nejkratší výraz, pro nějž existuje výraz e, který je jeho vlastním počátečním úsekem. Zřejmě e' není atom, jinak by e měl za počáteční úsek jiný atom nebo operaci, což nelze; tedy e i e' začínají operací, a to nutně stejnou (jinak by jedna operace byla počátečním úsekem jiné operace.) Je tedy $e = o^\frown s_0^\frown \ldots ^\frown s_{m-1}, e' = o^\frown t_0^\frown \ldots t_{m-1}$; nechť j je první index takový, že $s_j \neq t_j$. Pak $s_j^\frown \ldots ^\frown s_{m-1} \subseteq_p t_j^\frown \ldots ^\frown t_{m-1}$ a buďto $s_j \subseteq_p t_j$ nebo $t_j \subseteq_p s_j$; což je spor, neboť s_j i t_j jsou slova kratší než e a jedno je vlastním počátečním úsekem druhého.

Lemma B. Jestliže výrazy $e = A(o_1, \langle s_0, \ldots s_{m-1}\rangle), e' = A(o_2, \langle t_0, \ldots, t_{n-1}\rangle)$ se rovnají, pak $o_1 = o_2$, $m = n$ a $s_i = t_i$ pro $i = 0, \ldots, m-1$.

Důkaz. Zřejmě $o_1 = o_2$, nechť jsou to počáteční úseky slova $e = e'$, tedy $o_1 \subseteq_p o_2$ nebo $o_2 \subseteq_p o_1$, čili $o_1 = o_2$ (z podmínky na operace jako slova). Tedy $m = n = Ar(o_1) = Ar(o_2)$ a $s_0^\frown \ldots ^\frown s_{m-1} = t_0^\frown \ldots ^\frown t_{m-1}$. Buď j první takové, že $s_j \neq t_j$; pak buď s_j je vlastní počáteční úsek t_j nebo naopak, což je spor s Lemmatem A. Tedy odpovídající slova s_j, t_j jsou si rovna.

Poznámka. (1) Zcela stejně se ukáže, že je-li s slovo vzniklé slepením výrazů $e_0, \ldots, e_{m-1}$, pak s jednoznačně určuje m a $e_0, \ldots, e_{m-1}$.
(2) Zajisté popsaná konstrukce není jediná možná; brzy popíšeme strukturu výrazů vyrobenou z přirozených čísel. Ovšem každé dvě struktury výrazů téhož typu jsou ve zřejmém smyslu izomorfní.
(3) Termy a formule jazyka aritmetiky můžeme tedy chápat stejně jako slova v abecedě $=, \leq, +, *, S, \bar{0}, \rightarrow, \forall, \mathtt{x}, \mathtt{0}, \mathtt{1}$; proměnné x_n se representují pomocí `x`, `0`, `1` podobně jako výrokové proměnné výše. (Pozor: $\bar{0}$ je konstanta jazyka, `0` a `1` jsou pomocné symboly.) Máme-li už definovány termy a atomické formule, definujeme formule užitím operací $\rightarrow, \neg$ a nekonečně mnoho unárních operací odpovídajících kvantifikaci proměnné x_n.)

2.2 Aritmetická hierarchie formulí

Zahajujeme systematické studium formulí jazyka aritmetiky a množin, relací a funkcí definovaných těmito formulemi ve standardním modelu **N**. Výklad se opírá o úvodní kapitolu monografie P.Hájek - P.Pudlák: Metamathematics of first-order aritmetic. Nejprve vybudujeme jistou hierarchii formulí (a jimi definovaných množin); později uvidíme, že tato hierarchie je úzce svázána s teorií rekurse. Vyjdeme z formulí, kterým budeme říkat *omezené*.

2.2.1 Definice Buď φ formule, x, y dvě různé proměnné. $(\forall x \leq y)\varphi$ je zkratka za formuli $(\forall x)(x \leq y \rightarrow \varphi)$, $(\exists x \leq y)\varphi$ je zkratka za $(\exists x)(x \leq y \ \& \ \varphi)$.

$(\forall x \leq y)$, $(\exists x \leq y)$ se nazývají *omezené kvantifikátory*. Formule aritmetiky je *omezená*, jestliže neobsahuje jiné kvantifikátory než omezené. Podrobněji: atomické formule jsou omezené; jsou-li φ, ψ omezené a jsou-li x, y různé proměnné, jsou formule $\neg\varphi$, $\varphi \rightarrow \psi$, $(\forall x \leq y)\varphi$ omezené. Jiné omezené formule nejsou. (Pozor: formule $\varphi \,\&\, \psi$, $\varphi \vee \psi$, $\varphi \equiv \psi$ považujeme za zkratky za příslušné formule vybudované pomocí $\neg, \rightarrow$; tedy jsou-li φ, ψ omezené, jsou i $(\varphi \,\&\, \psi)$ atd. omezené podle naší definice.) Omezeným formulím říkáme také Σ_0-formule a také Π_0-formule.

Příklad. $(\exists x \leq y)(y = \bar{2} * x)$ je omezená formule ($\bar{2}$ je numerál $SS\bar{0}$); zřejmě definuje množinu všech sudých čísel v $\mathbf{N}$.

2.2.2 Definice Pro každé přirozené n definujeme: Σ_{n+1}-*formule* jsou formule tvaru $(\exists x)\varphi$, kde φ je Π_n-formule; Π_{n+1} - *formule* jsou formule tvaru $(\forall x)\varphi$, kde φ je Σ_n- formule.

Tedy Σ_3 formule mají tvar $(\exists x)(\forall y)(\exists_2)\varphi$, kde φ je omezená; Π_3 formule podobně $(\forall x)(\exists y)(\forall_2)\varphi$.

2.2.3 Definice Množina $A \subseteq N$ je Σ_n-*množina*, jestliže existuje Σ_n-formule $\varphi(x)$ s jednou volnou proměnnou x definující A v $\mathbf{N}$, t.j. $A = \{n \mid \mathbf{N} \models \varphi[x/n]\}$. (Zde x/n značí libovolné ohodnocení e proměnných takové, že $e(x) = n$). Podobně relace $R \subseteq N^k$ je Σ_n - *relace* jestliže existuje Σ_n - formule $\varphi(x_1, \ldots, x_n)$ definující R v $\mathbf{N}$. Analogicky se definují Π_n množiny a relace.

Množina $A \subseteq N$ je Δ_n - *množina*, je-li současně Σ_n - množinou a Π_n - množinou, t.j. má jak Σ_n - definici tak (jinou) Π_n - definici v $\mathbf{N}$. Podobně pro relace $R \subseteq N^k$. Nemá smysl říci, že φ je Δ_n - formule (s jedinou výjimkou: Σ_0 - formulím neboli Π_0 - formulím se též říká Δ_0 - formule); ale budeme říkat, že $\varphi(x_1, \ldots x_k)$ je Δ_n - *formule v* $\mathbf{N}$, jestliže φ definuje Δ_n - množinu, t.j. existuje Σ_n - formule $\sigma(x_1 \ldots x_n)$ a Π_n - formule $\pi(x_1 \ldots x_n)$, které jsou ekvivalentní ekvivalentní formuli φ v $\mathbf{N}$ (ekvivalence $\varphi \equiv \sigma$, $\varphi \equiv \pi$ jsou pravdivé v $\mathbf{N}$).

Funkce $F : N^k \rightarrow N$ je $\Sigma_n(\Pi_n, \Delta_n)$, je-li takový její graf, t.j. relace

$$\{\langle m_1, \ldots, m_k, p\rangle \in N^{k+1} \mid p = F(m_1, \ldots, m_k)\}$$

2.2.4 Příklad. Existuje Σ_0 - *párovací funkce*, t.j. funkce $F : N^2 \rightarrow N$, která prostě zobrazuje N^2 na N a je Σ_0 (omezeně definovaná).

Vskutku, ověřte, že funkce

$$F(m, n) = \frac{1}{2}(m + n + 1)(m + n) + m$$

má požadované vlastnosti: je je definována Σ_0 - formulí

$$\overline{2} * z = (x + y + \overline{1}) * (x + y) + \overline{2} * x$$

a definuje diagonální číslování uspořádaných dvojic přirozených čísel:

	0	1	2	3	4
0	0	1	3	6	10
1	2	4	7	11	
2	5	8	12		
3	9	13			
4	14	...			

Píšeme $(m, n)_N$ místo $F(m, n)$ (také jen (m, n)).

2.2.5 Věta. Pro libovolné přirozené n platí:
(1) Σ_n, Π_n, Δ_n relace jsou uzavřeny na průnik a sjednocení;
(2) Δ_n relace jsou uzavřeny na komplement (v N^n);
(3) pro $n > 0$ jsou Σ_n - relace uzavřeny na existenční projekci a Π_n - relace na universální projekci.

Jinými slovy: nechť R, s jsou k-ární relace definované formulemi $\varphi(\mathbf{x})$, $\psi(\mathbf{x})$ ($\mathbf{x}$ je $x_1, \ldots, x_k$); (1) jsou-li φ, ψ, Σ_n, pak formule φ & ψ je Σ_n v $\mathbf{N}$ (podobně Π_n, Δ_n); (2) je-li φ Δ_n v $\mathbf{N}$ pak $\neg\varphi$ je Δ_n v $\mathbf{N}$; (3) je-li φ Σ_n, pak formule $(\exists x_1)\varphi$ je Σ_n v $\mathbf{N}$, podobně pro Π_n a $(\forall x_1)\varphi$.

Důkaz. Dokážeme všechna tři tvrzení najednou indukcí dle n. Pro $n = 0$ odpadá (3) a (1), (2) jsou zřejmé, neboť omezené formule jsou uzavřeny na konjunkci a negaci. Předpokládejme (1)-(3) pro n a dokazujme pro $(n + 1)$. Tvrzení (2) je zřejmé; dokazujme nejprve (3) pro Σ_{n+1} (důkaz pro Π_{n+1}, je analogický). Buď R definována formulí $(\exists z)\varphi(x, y, z)$, kde φ je Π_n - formule, buď R' definována formulí $(\exists y)(\exists z)\varphi(x, y, z)$; chceme dokázat, že poslední formule je Σ_{n+1} v $\mathbf{N}$. Vskutku použitím párovací funkce (a faktu, že tato funkce roste v obou argumentech) můžeme R' definovat formulí

$$(\exists u)(u = (y, z) \ \& \ (\forall y)(\forall z)(u = (y, z) \rightarrow \varphi(x, y, z)), \qquad (*)$$

a také formulí

$$(\exists u)(a = (y, z) \ \& \ (\forall y \leq u)(\forall z \leq u)(u = (y, z) \rightarrow \varphi(x, y, z)). \qquad (**)$$

Zde $u = (y, z)$ znamená Σ_0 formuli definující párovací funkci. Je-li $n = 0$, je formule (**) evidentně Σ_1; pro $n > 0$ nejprve užijme tvrzení (1) pro n a pro formuli $(\forall y)(\forall z)(u = (y, z) \rightarrow \varphi(x, y, z))$, která tedy je Π_n v $\mathbf{N}$ a proto (*) je Σ_{n+1} v $\mathbf{N}$.

Pro Π_{n+1} použijeme anologie formulí (*), (**) tvaru

$$(\exists u)(u < (y, z) \ \& \ (\exists y)(\exists z)(u = (y, z) \ \& \ \varphi(x, y, z))$$

a podobně s omezenými kvantifikátory.

Zbývá dokázat (1) pro $n + 1$. Nechť $(\exists y)\varphi(y, \mathbf{x})$ a $(\exists z)\psi(z, \mathbf{x})$ jsou Σ_{n+1} - formule v $\mathbf{N}$ a nechť y, z jsou různé proměnné; pak i jejich konjunkce je Σ_{n+1}

v **N**, neboť je v **N** ekvivalentní formuli

$$(\exists y)(\exists z)(\varphi(y,\mathbf{x}) \ \& \ \psi(z,\mathbf{x})),$$

která je Σ_{n+1} v **N** díky tvrzení (1) pro n a (3) pro $(n+1)$. Podobně pro disjunkci, Π_{n+1}.

Poznámka. Budeme se zabývat jen $\Sigma_0, \Sigma_1, \Pi_1, \Delta_1$ množinami; v paragrafu 2.5 ukážeme, že Δ_1 množiny jsou v podstatě rekursivní množiny a Σ_1 jsou v podstatě rekursivně spočetné množiny. (Co znamenají slova "v podstatě", se tam dozvíme přesně).

2.2.6 Věta. Σ_1 relace jsou uzavřeny na omezenou universální projekci, t.j. je-li $(\exists y)\varphi(\mathbf{x},y,z)$ Σ_1, je $(\forall z \leq x)(\exists y)\varphi(\mathbf{x},y,z)$ Σ_1 v **N**.

Důkaz. Pro jednoduchost nahradíme posloupnost proměnných $\mathbf{x}$ jedinou proměnnou x (obecný důkaz je zcela analogický). Ukážeme, že formule $(\forall z \leq x)\exists y)\varphi(x,y,z)$ je v **N** ekvivalentní formuli $(\exists u)(\forall z \leq x)(\exists y \leq u)\varphi(x,y,z)$, která je zřejmě Σ_1 v **N**. Zřejmě druhá formule implikuje první, t.j.

$$N \models (\exists u)(\forall z \leq x)(\exists y \leq u)\varphi(x,y,z) \ \rightarrow \ (\forall z \leq x)(\exists y)\varphi(x,y,z);$$

Ukážeme pravdivost obrácené implikace. Nechť $N \models (\forall z \leq \bar{k})(\exists y)\varphi(\bar{k},y,z)$ (t.j. $\bar{k}$ splňuje formuli $(\forall z \leq x)(\exists y)\varphi(x,y,z)$): najdeme q takové, že $N \models (\forall z \leq \bar{k})(\exists y \leq \bar{q})\varphi(\bar{k},y,z)$. Pro každé $i = 0,1,\ldots k$ najdeme q_i tak, že $N \models (\forall z \leq \bar{i})(\exists y \leq \bar{q_i})\varphi(\bar{k},y,z)$. To je zřejmé pro $i = 0$, máme-li q_i dáno $(i < k)$ a p je takové, že $N \models \varphi(\bar{k},\bar{p},\overline{i+1})$ (takové p existuje, protože $i+1 \leq k$ a tedy $N \models (\exists y)\varphi(\bar{k},y,i \bar{+} 1))$, stačí vzít $q_{i+1} = max(q_i,p)$. Nyní stačí vzít $q = q_t$.

2.2.7 Věta. (1) Je-li $F : N^k \rightarrow N$ Σ_1 funkce, pak F je Δ_1. (2) Δ_1 funkce jsou uzavřeny vůči skládání, např. je-li $F : N^2 \rightarrow N, G : N^2 \rightarrow N$, $H : N \rightarrow N$ a $K(m,n,p) = F(G(m,n),H(p))$, kde F,G,H jsou Δ_1 funkce, pak K je Δ_1 funkce.

Důkaz. (2) Nechť $i = F(j,k)$, právě když $N \models \varphi(\bar{i},\bar{j},\bar{k})$, dále $i = G(j,k)$, právě když $N \models \psi(\bar{i},\bar{j},\bar{k})$ a konečně $i = H(j)$ právě když $N \models \chi(i,j)$, nechť φ,ψ,χ jsou Σ_1. Pak $i = K(m,n,p)$, právě když

$$N \models (\exists x)(\exists y)(\psi(x,\bar{m},\bar{n}) \ \& \ \chi(y,\bar{p}) \ \& \ \varphi(\bar{i},x,y));$$

poslední formule je Σ_1 v **N** dle předchozí věty.

(1) Ať $i = F(m,\ldots,n)$, právě když $N \models (\exists y)\psi(\bar{i})\bar{m_1},\ldots,\bar{m_n}y)$, kde ψ je omezené; pak $i \neq F(m,\ldots,n)$, právě když existuje $j \neq i$ takové, že $j = F(m,\ldots,n)$, t.j.

$$N \models (\exists z)(z \neq \bar{i} \ \& \ (\exists y)\psi(z,\bar{m_1},\ldots \bar{m_n},y));$$

poslední formule je Σ_1 v **N**. Tedy $i \neq F(m,\ldots,n)$ je Σ_1 relace,tedy $i = F(m,\ldots,n)$ je Π_1 relace (a též Σ_1 relace, je tedy Δ_1). Zde bylo důležité, že F je definováno pro *každé* $m,\ldots,n \in N$ (je totální); pro parciální funkce věta neplatí.

2.3 Kódování posloupností čísel

Základní operace v **N** jsou následník, sčítání a násobení. Tyto operace jsou triviálně Δ_0 (tedy i Δ_1), neboť jsou definovány atomickými formulemi $z = Sx$, $z = x + y$, $z = x * y$. Je *mocnina* (třeba mocnina dvojky 2^x) Δ_1? Obecněji, jsou Δ_1 funkce uzavřeny na primitivní rekursi? T.j. např. je-li $H(0) = 1$, $H(n+1) = F(n, H(n))$ kde F je Δ_1, je H Δ_1? Odpověď je ANO; ale dokázat to dá jistou práci. Například: $m = 2^n$, jestliže existuje posloupnost $\langle s_0, s_1, \ldots, s_n\rangle$ taková, že $s_0 = 1$, pro $i < n$ je $s_{i+1} = 2 * s_i$ a $s_n = m$. Zde však kvantifikujeme přes libovolné konečné *posloupnosti přirozených čísel*; lze je nějak rozumně kódovat čísly? Odpověď je opět ANO, ale opět to dá práci (za to však druhá odpověď dává první odpověď už lehko). Hlavním cílem této sekce je dokázat následující větu:

2.3.1 Věta. Existuje Δ_0 množina $Seq \subseteq N$ (její prvky nazýváme *posloupnosti* nebo podrobněji *kódy posloupností*, unární Δ_0 operace $lh(s)$ (pro $s \in Seq$ nazýváme $lh(s)$ *délkou* posloupnosti s), binární Δ_0 operace $(s)_n$ argumentů s, n (pro $s \in Seq$ a $n < lh(s)$ nazýváme číslo $(s)_n$ *n-tým prvkem* posloupnosti s) a binární Δ_0 operace $s^\frown t$ (pro $s, t \in Seq$ nazýváme $s^\frown t$ *slepením* nebo juxtapozicí posloupností s, t) tak, že platí:

- existuje $s \in Seq$ takže $lh(s) = 0$ (značení: $s = \emptyset$)
- pro $n > lh(s)$ je $(s)_n = 0$
- pro každé $k \in N$ existuje s tak, že $lh(s) = 1$ a $(s)_0 = k$
- pro každé $s, t \in Seq$ je $s^\frown t \in Seq$, $lh(s^\frown t) = lh(s) + lh(t)$, pro $i = 0, \ldots, lh(s) - 1$ je $(s^\frown t)_i = s_i$, pro $i = 0, \ldots, lh(t) - 1$ je $(s^\frown t)_{lh(s)+i} = (t)_i$;
- pro $s, t \in Seq$ je $s = t$ právě když $lh(s) = lh(t)$ a pro každé $i = 0, \ldots, lh(s) - 1$ je $(s)_i = (t)_i$;
- $s \leq s^\frown t, t \leq s^\frown t$.

Označení Seq, lh je z anglického sequence=posloupnost a length=délka (bude dobře, když si čtenář tato slova zapamatuje). Řekneme, že s kóduje posloupnost $k_0, \ldots k_{k-1}$, jestliže $s \in Seq$, $lh(s) = m$, $(s)_0 = k_0, \ldots, (s)_{m-1} = k_{m-1}$. Požadujeme, že kóduje-li s posloupnost $k_0, \ldots, k_{m-1}$ a t posloupnost $h_0, \ldots, h_{n-1}$, pak $s^\frown t$ kóduje $k_0, \ldots, k_{m-1}, h_0, \ldots, h_{n-1}$. Poslední požadavek říká, že posloupnost je jednoznačně určena svou délkou a svými členy (nultým až $(lh(s) - 1)$-tým). Zbývají dva požadavky: požadavek existence prázdné posloupnosti (délky t) a pro každé $k \in n$ posloupnost délky 1 s nultým prvkem k.

Máme za úkol sestrojit kódování konečných posloupností čísel čísly, které má uvedené vlastnosti a je Δ_0, to znamená, že všechny uvedené pojmy jsou definovatelné omezenými formulemi (bude pro nás vlastně důležité jen to, že množina Seq a tři uvedené funkce jsou Δ_1; ale dostaneme Δ_0 se stejným úsilím). To mimo jiné znamená, že máme definovat kódování jen pomocí sčítání a násobení (formulemi aritmetiky), což je poněkud obtížný úkol. Je mu věnován zbytek tohoto odstavce. Prosím čtenáře o trpělivost; vyplatí se nám, neboť jednak uvidíme, že mocnina a spousta jejich funkcí je definovatelná v aritmetice (zvolili jsme jazyk aritmetiky dost bohatý), jednak toto (nebo nějaké podobné) kódování je nezbytné pro aritmetizaci metamatematiky a tak pro důkaz Gödelových vět. Nejprve ukážeme, jak kódovat konečné množiny čísel $A \subseteq N$ pomocí čísel. Využijeme k tomu pojmu dělitelnosti.

2.3.2 Definice. Číslo k *dělí* číslo m (symbolicky $k \mid m$), jestliže existuje $n \leq m$ tak, že $m = k * n$. Číslo m *obaluje* číslo k, jestliže každé číslo p splňující $1 \leq p \leq k$ dělí m. Číslo m je *slupkou* k ($m = hull(k)$), jestliže m je nejmenší číslo obsahující k.

Poznámka. Zřejmě každé $k \geq 1$ má slupku (neboť má aspoň jedno obalující číslo, např. $k!$). Zřejmě relace dělitelnosti je Δ_0. Funkce $hull$ je Δ_0 funkce; následující formule definuje relaci $m = hull(k)$:

$$x \geq 1 \ \& \ (\forall z \leq x)(z \mid y)) \ \& \ (\forall y' \leq y)(y' \neq y \rightarrow \neg(\forall z \leq x)(z \mid y'))$$

2.3.3 Lemma. Nechť $m = hull(k)$; pak pro každé dvě různá čísla $p, q \leq k$ jsou čísla $1 + (1 + p)m,\ 1 + (1 + q)m$ nesoudělná.

Důkaz. Buď $P = 1 + (1 + p)m,\ Q = 1 + (1 + q)m$, nechť c dělí P i Q, t.j. $P = ac,\ Q = bc$. Pak P dělí $abc = aQ = a(1 + (1 + q)m)$ a ovšem P dělí $aP = a(1+(1+p)m)$. Nechť $P < Q$, t.j. P dělí $a(Q - P) = a(q - p)m$. Zřejmě P a m jsou nesoudělná čísla (neboť $P = 1 + (1 + p)m$), t.j. P dělí $a(q - p)$. Ovšem $q - p$ dělí m (protože $m = hull(k)$), t.j. P a $(q - p)$ jsou opět nesoudělná, tedy P musí dělit a. Protože $P = ac$, musí nutně být $c = 1$; t.j. P, Q jsou nesoudělná.

Toto lemma umožňuje následující kódování konečných množin čísel čísly.

2.3.4 Definice. (1) $code(\emptyset) = 0$ (kód prázdné množiny je nula); je-li $A = \{a_0, \ldots, a_n\}$ konečná neprázdná množina přirozených čísel, pak

$$code(A) = (m_1, m_2),$$

kde $m_1 = hull(max(A)), m_2 = \Pi_{i=0}^{n}(1 + (1 + a_i)m_1)$. (2) Číslo m je kódem konečné množiny (symbol: $Set(m)$), jestliže existuje konečná množina $A \subseteq N$ taková, že $m = code(A)$ t.j. buď $A = \emptyset$ a $m = 0$ nebo $m = (m_1, m_2) = code(A)$ pro nějakou neprázdnou A). (3) Buď $m_1 = hull(k)$, $m = (m_1, m_2)$; definujeme $a \in_0 m$, jestliže $a \leq k$ a $1 + (1 + a)m_1$ dělí m_2. Dále buď $m \subseteq_0 m'$, jestliže pro každé $a < m$ z $a \in_0 m$ plyne $a \in_0 m'$.

2.3.5 Lemma. (1) Je-li $m = code(A)$, pak $a \in A$ právě když $a \in_0 m$. Tedy: $code(A) = code(B)$, právě když $A = B$.
(2) Je-li $A \subseteq B$, pak $code(A) \leq code(B)$
(3) Je-li $F : N \rightarrow N$ rostoucí a B je obraz množiny A v zobrazení F (t.j. $B = F''A$), pak $code(A) \leq code(B)$.

(4) $Set(m)$, právě když buď $m = 0$ nebo existují $m_1, m_2, k \leq m$ taková, že $m = (m_1, m_2)$, $m_1 = hull(k)$, k je největší číslo (pod m) takové, že $k \in_0 m$, a neexistuje $m' < m$ takové, že $(m_1, m_2) \subseteq_0 (m_1, m_2')$.
(5) Množina všech kódů konečných množin a relace $a \in_0 m$ jsou Δ_0 definovatelné v N.

Důkaz. (1) Zajisté když $a \in A$ pak $1 + (1 + a)m_1$ dělí m_2, kde $code(A) = (m_1, m_2)$, tedy $a \in_0 code(A)$. Obráceně, když $a \in_0 code(A)$, tedy $a \leq k$ a $1 + (1 + a)m_1$ dělí m_2, pak existuje $a_i \in A$ takové, že $1 + (1 + a)m_1$ je soudělné s $1 + (1 + a_i)m_1$ a tedy nutně $a = a_i$ díky lemmatu o nesoudělnosti.
(2) Nechť $code(A) = (m_1, m_2)$, $code(B) = (m_3, m_4)$. Platí $m_1 \leq m_3$ a $m_2 \leq m_4$ (přímo z definice $code(A)$) tedy $(m_1, m_2) \leq (m_3, m_4)$ (z definice párovací funkce).
(3) podobně.
(4) Je-li $m = code(A)$, $m = (m_1, m_2)$, pak jsou zřejmě splněny uvedené podmínky. Obráceně, jsou-li $m_1, m_2, k \leq m$ čísla splňující ony podmínky a A je množina všech čísel $j \leq k$ takových, že $j \in_0 m$, pak $code(A) = (m_1, m_2')$, kde $m_2 = \prod_{j \in A} = (1 + (1 + j)m_1)$; tedy $m_2' \leq m_2$ a $(m_1, m_2) \subseteq_0 (m_1, m_2')$, takže $m_2 = m_2'$.
(5) Víme již, že funkce $hull$ je Δ_0. Ukázat, že $\in_0$ je Δ_0, je lehké:

$$x \in_0 y \equiv Set(y) \ \& \ (\exists y_1, y_2, z \leq y)(y = (y_1, y_2) \ \& \ y_1 = hull(z) \ \&$$

$$\& \ x \leq z \ \& \ (1 + (1 + x)y_1) \mid y_2).$$

Fakt, že $Set(x)$ je Δ_0, plyne bezprostředně z předchozího bodu (4).

Nyní už je lehké zakódovat posloupnosti: posloupnost prvků $a_0, \ldots, a_{n-1}$ zakódujeme jako množinu dvojic $(0, a_0), \ldots, (n-1, a_{n-1})$. Tedy:

2.3.6 Definice. Seq je množina všech *kódů konečných posloupností* přirozených čísel, t.j. čísel tvaru $code(\{(0, a_0), \ldots, (n-1, a_{n-1})\})$ pro nějaké n a nějakou posloupnost $a_0, \ldots, a_{n-1}$. n je *délka* (kódu) posloupnosti $\{(0, a_0), \ldots, (n-1, a_{n-1})\}$; a_i je její i-tý člen. Funkce $lh(s)$, $s^\frown t, (s)_i$ pro kódy posloupností definujeme zřejmým apůsobem.

2.3.7 Lemma. Množina Seq a funkce $lh, s^\frown t, (s)_i$ jsou Δ_0 definovatelné v **N**.

Důkaz. $s \in Seq$ znamená, že s je kód množiny a pro jisté n (které je $\leq s$) každý prvek s je dvojice s prvním členem $< n$ a pro každé $i < n$ má s za prvek právě jednu dvojici s druhým členem i:
$Seq(s) \equiv Set(s) \ \& \ (\exists x \leq s)(\forall y \in_0 s)(\exists u < x)(\exists v < y)(y = (u, v)) \ \& \ (\forall u < x)(\exists! v \leq s)((u, v) \in_0 s)$.
$lh(s) = x \equiv Seq(s) \ \& \ (\forall u < x)(\exists v < s)((u, v) \in_0 s) \ \& \ \neg(\exists v < s)((x, v) \in_0 s)$.
(Délka posloupnosti je první x, pro které žádná dvojice (x, v) není v s).

Δ_0 definice ostatních funkcí napíše čtenář snadno za cvičení. Také vlastnosti z věty 2.3.1 jsou pro naši definici zřejmé. (Ověřte.)

Nyní můžeme zodpovědět otázku, položenou na začátku této sekce 2.3, zda Δ_1 funkce jsou uzavřeny vůči primitivní rekursi.

2.3.8 Věta. Nechť $F : N^2 \rightarrow N$ je Δ_1 v $\mathbf{N}$ a nechť $H : N \rightarrow N$ splňuje $H(0) = 1$, $H(n+1) = F(n, H(n))$ pro každé n. Pak H je Δ_1 v $\mathbf{N}$.

Důkaz. $H(k) = m$, právě když $\mathbf{N} \models \varphi(\bar{k}, \bar{m})$, kde $\varphi(x, y)$ je formule

$$(\exists s)(Seq(s) \ \& \ lh(s) = x + \bar{1} \ \& \ (s)_o = \bar{1} \ \&$$

$$\& \ (\forall z < x)\psi(z, (s)_z, (s)_{z+\bar{1}}) \ \& \ (s)_x = y),$$

kde ψ Δ_1 definuje F v $\mathbf{N}$, t.j.

$$F(p, q) = r, \text{ právě když } \mathbf{N} \vdash \psi(\bar{p}, \bar{q}, \bar{r}).$$

Jelikož ψ je Δ_1 v $\mathbf{N}$, t.j. lze ji ekvivalentně psát jako Σ_1 i Π_1 formuli, je formule $\varphi(x, y)$ zajisté Σ_1; přímo se lehko ukáže, že $\varphi(x, y)$ je v $\mathbf{N}$ ekvivalentní následující formuli $\varphi'(x, y)$, která je Π_1 v $\mathbf{N}$:

$$(\forall s)(Seq(s) \ \& \ lh(s) = x + \bar{1} \ \& \ (s)_{\bar{0}} = \bar{1} \ \&$$

$$\& \ (\forall z < x)\psi(z, (s)_z, (s)_{z+\bar{1}}). \rightarrow (s)_x = y).$$

Ověřte; užijte fakt, že pro každé n existuje zřejmě *jediná* posloupnost s délky n taková, že $(s)_0 = 1$ a pro každé $k < n$ platí $(s)_{k+1} = F(k, (s)_k)$.

Dokažte dále analogickou variantu, kdy funkce F a H závisejí na dalších parametrech:

$H(0, p_1, \ldots, p_i) = G(p_1, \ldots, p_i)$
$H(n + 1, p_1, \ldots, p_i) = F(n, H(n, p_1, \ldots, p_i), p_n, \ldots, p_i)$.

2.3.9 Příklad. Funkce $E(m, n) = m^n$ (mocnina) je Δ_1 v $\mathbf{N}$; podobně faktoriál a pod. Vidíme tedy, že jsme jazyk aritmetiky zvolili dodatečně bohatý.

2.3.10 Označení. V dalším značí $\langle a_o, \ldots, a_n \rangle$ prvek i splňující $Seq(s)$ a pro každé $i < n$ $(s)_i = a_i$ (posloupnost prvků $a_o, \ldots, a_n$ v novém smyslu; s je prvek N).

2.4 Aritmetizace syntaxe

V tomto paragrafu ukážeme, že uvnitř aritmetiky lze definovat její vlastní syntax. Podrobněji řečeno, ukážeme, že termy a formule aritmetiky lze ztotožnit s jistými přirozenými čísly (nebo že termy a formule lze *kódovat* jistými přirozenými čísly) tak, že všechny důležité pojmy o nich až po pojem důkazu (včetně) se stanou Δ_1 definovatelnými v $\mathbf{N}$. (Pozor! Nic zatím netvrdíme o pojmu *dokazatelnosti.*) Tato technika bude podstatná v paragrafu 2.7 pro konstrukci autoreferenčních formulí (mluvících v jistém smyslu o sobě samých). Protože se většina úvah o termech opakuje pro formule, vyplatí se nám popsat situaci obecněji pro *výrazy*. Jde nám tedy o dvojí: (1) ukázat, jak se Δ_1 kódují výrazy a (2) použít vypracovanou techniku na Δ_1 kódování termů a formulí aritmetiky.

2.4.1 Definice. Nechť $\Lambda \subseteq N$ je množina (kódů) písmen (abeceda). V dalším značí Λ^* množinu kódů slov v abecedě Λ, tedy posloupností $s \in Seq$ takových, že každý prvek $(s)_i$ je v Λ.

2.4.2 Lemma. Je-li Λ Δ_1-definovatelná v $\mathbf{N}$, pak i Λ^* je Δ_1 definovatelná v $\mathbf{N}$.

Důkaz. Je-li Λ definována formulí $\varphi(x)$, pak Λ^* je definována následující formulí $\psi(x)$:

$$Seq(s)\ \&\ (\forall x < lh(s))\varphi((s)_x);\ \text{podrobněji}$$

$$Seq(s)\ \&\ (\forall x < s)(x < lh(s)) \rightarrow (\exists y \leq s)(y = (s)_x\ \&\ \varphi(y)).$$

Zřejmě tato formule je Δ_1 v $\mathbf{N}$.

2.4.3 Označení. V dalším použijeme označení $\subseteq_p$ pro prvky Λ^*, t.j. $s \subseteq_p t$, právě když $s, t \in Seq$ a s je počáteční úsek t, t.j. $lh(s) \leq lh(t)\ \&\ (\forall i < lh(s))((s)_i = (t)_i)$. Zřejmě relace $\subseteq_p$ je Δ_0 v $\mathbf{N}$ (ověřte!).

2.4.4 Definice. Nechť $\Lambda \subseteq N$ je abeceda; nechť $At \subseteq \Lambda^*$ je množina atomů, $Op \subseteq \Lambda^*$ je množina operací, $At \cap Op = \emptyset$, nechť neexistují žádné dva různé prvky $u, v \in At \cup Op$ tak, že $u \subseteq_p v$. Buď $Ar : Op \rightarrow (N - \{0\})$ funkce přiřazující každé operaci její četnost (aritu). Definujeme funkci A (aplikace) pro $o \in Op$, $s \in Seq$, $lh(s) = Ar(o)$; pro $i = 0, \ldots, lh(s) - 1$ nechť $(s)_i \in \Lambda^*$: $A(o, s) = o^\frown(s)_0^\frown \ldots ^\frown(s)_{lh(s)-1}$. E nechť je nejmenší část N taková, že $At \subseteq E$ a E je uzavřená ve A, t.j. je-li pro s jako nahoře $(\forall i < lh(s))((s)_i \in E)$, a je-li $o \in Op$, pak $A(o, s) \in E$.

(Tedy vše je jako v 2.1, jen s tím rozdílem, že nyní je vše tvořeno přirozenými čísly.)

2.4.5 Věta. Jsou-li za označení definice 2.4.4 množiny At, Op a funkce Ar Δ_1 v $\mathbf{N}$, pak i struktura výrazů (E, A) je Δ_1 v $\mathbf{N}$ (t.j. E je Δ_1 množina v $\mathbf{N}$, A je Δ_1 funkce v $\mathbf{N}$).

Důkaz. K ověření Δ_1-definovatelnosti funkce A stačí ukázat, že funkce $J(s)$ přiřazující argumentu s, který je posloupnost posloupností ($s \in Seq\ \&\ (\forall i < lh(s))((s)_i \in Seq)$ juxtapozici $(s)_0{}^\frown \ldots {}^\frown (s)_{lh(s)-1}$ (a rovná 0 pro jiné argumenty) je Δ_1 v $\mathbf{N}$. Protože juxtapozice $s^\frown t$ je Δ_1 v $\mathbf{N}$, stačí použít variantu věty 2.3.8 o primitivní rekursi.

Vyšetřeme množinu E výrazů. Odvození výrazu e je posloupnost posloupností s, jejíž každý člen $(s)_i$ je buď atom nebo vzniká aplikací A na nějakou operaci o a na posloupnost (patřičné délky) posloupností stojících v s před $(s)_i$

a přitom poslední člen $(s)_{lh(s)-1}$ je e. E je množina všech posloupností majících odvození; to dává Σ_1-definici množiny E v $\mathbf{N}$: definující formule má tvar

$$(\exists s)(s \text{ je odvození posloupnosti } x).$$

(Ověřte, že relace "s je odvození x" je Δ_1 v $\mathbf{N}$.)

Abychom dokázali, že E je Δ_1, potřebujeme vhodný odhad pro odvození výrazu e, t.j. takovou totální Δ_1 funkci F, že pro libovolné e platí: má-li e odvození, pak existuje odvození s výrazu e takové, že $s < F(e)$. Protože lze předpokládat, že všechny členy odvození výrazu e jsou podslova slova e (t.j. $e = u^\frown (s)_i^\frown v$ pro nějaké u, v), a že pro $i \neq j < lh(s)$ je $(s)_i \neq (s)_j$, vidíme, že existuje-li odvození s výrazu e, pak lze předpokládat, že má nejvýše $lh(e)$ členů, každý $\leq e$. Tedy za $F(e)$ lze vzít $e^\frown e^\frown \ldots ^\frown e$ ($lh(e)$ exemplářů posloupnosti e, slepených do jedné posloupnosti); tato funkce je zajisté Δ_1 definovatelná v $\mathbf{N}$.

Lze tedy definovat E formulí

$$(\exists s \leq F(e))\ (s \text{ je odvození výrazu } e),$$

t.j.

$$(\exists y)(y = F(e)\ \&\ (\exists s \leq y)(s \text{ je odvození výrazu } e))$$

a také ovšem (díky totálnosti funkce F) formulí

$$(\forall y)(y = F(e) \rightarrow (\exists s \leq y)(s \text{ je odvození výrazu } e).$$

Tím máme jak Σ_1-definici, tak Π_1-definici. Tedy E je Δ_1 v $\mathbf{N}$. Tím jsme dokončili první úkol tohoto paragrafu.

Nyní už rychle dostaneme aritmetizaci syntaxe aritmetiky.

2.4.6 Definice. *Abeceda* Λ_{Ar} *aritmetiky* sestává z těchto symbolů:

$$\mathtt{x}, =, \leq, S, +, *, \bar{0}, \rightarrow, \neg, \forall, \mathtt{1}, \mathtt{0}$$

očíslovaných (řekněme) sestupně čísly 11,10,9,8,7,6,5,4,3,2,1,0 (např. $\bar{0}$ je 5, $+$ je 7). Čísla kódující symboly nějaké abecedy a slova z nich vytvořená se někdy nazývají *Gödelova čísla* těchto symbolů a slov. My se na to díváme tak, že *ztotožníme* symboly a slova s jistými čísly. Proměnné jsou prvky v množiny Seq takové, že $(v)_{lh(v)-1} = 11$, $(v)_0 = 1$, a pro $0 < i < lh(v) - 1$ $(v)_i = 0$ nebo $(v)_i = 1$ (Např. `101x` a pod.).

Termy jsou prvky struktury výrazů, jejíž atomy jsou proměnné a dále posloupnost $\langle \bar{0} \rangle$ délky 1, a jejíž operace jsou $\langle S \rangle$ (unární), $\langle + \rangle$, $\langle * \rangle$ (binární).

Atomické formule mají následující možné tvary,

$$\langle =, t, s \rangle,\ \langle \leq, t, s \rangle,$$

kde t, s jsou termy. *Formule* jsou prvky struktury výrazů, jejíž atomy jsou atomické formule a operace jsou $\langle \rightarrow \rangle$, (binární), $\langle \neg \rangle$ (unární) a $\langle \forall \rangle^\frown v$, kde v je proměnná (unární).

Pozor: Je jasné, jak se tvoří formule; znovu upozorňuji čtenáře, že nyní vše jsou přirozená čísla (jako kódy všeho).

2.4.7 Věta. Následující množiny, relace, funkce jsou Δ_1 v $\mathbf{N}$:
(1) Množina *Atterm* všech atomických termů, množina *Term* všech termů.
(2) Množina *Atfl* všech atomických formulí, množina *Fl* všech formulí.
(3) Relace “proměnná u se vyskytuje v termu t”.
(4) Relace “proměnná u se vyskytuje volně (vázaně) ve formuli φ”.
(5) Relace “term t je substituovatelný za proměnnou u ve formuli φ”.
(6) Funkce $Subst_o(t,u,t')$ přiřazující každému termu t, proměnné u a termu t' výsledky substituce termu t' za proměnnou u v t.
(7) Funkce $Subst(\varphi,u,t)$ přiřazující každé formuli φ, proměnné u a termu t výsledek substituce termu t za volné výskyty proměnné u.
(8) Množina logických axiomů v jazyce aritmetiky.
(9) Množina důkazů v predikátovém počtu (v jazyce aritmetiky).
(10) Je-li T axiomatika v jazyce aritmetiky (množina formulí) a je-li T Δ_1 v $\mathbf{N}$, pak i množina důkazů v teorii T je Δ_1 v $\mathbf{N}$.

Důkaz. (1)-(2) jsou zřejmé z předchozího; (3) je lehké: proměnná u se vyskytuje v t, jestliže t se dá pro jistá slova v,w psát jako $v^\frown u^\frown w$), kde $\frown$ je operace juxtapozice, přičemž v nekončí žádným ze symbolů 0,1 (tj. u není koncovým úsekem jiné proměnné, která je podslovem t ve stejném kontextu). Rozebereme (6); (4)-(5),(7) se dokazuje podobně. Užijeme pojmu odvození formule (jakožto výrazu); zřejmě “být odvozením formule φ” je Δ_1 v $\mathbf{N}$. Ukážeme, že funkce $Subst_0(t,u,t')$ je Σ_1 v $\mathbf{N}$: $t''=Subst_0(t,u,t')$, právě když existuje odvození s termu t a posloupnost $\hat{s}$ téže délky jako s taková, že pro $i=0,\dots,lh(s)-1$ [je $(\hat{s})_i=Subst_o((s)_i,u,t')$, t.j.]: je-li $(s)_i$ proměnná u, je $(\hat{s})_i=t'$; je-li $(s)_i$ jiná proměnná, je $(\hat{s})_i=(s)_i$; je-li $(s)_i$ term vznikající aplikací funkčního symbolu $+$ na $(s)_j,(s)_k$ pro nějaké $j,k<i$ (t.j. $(\hat{s})_i=\langle 7\rangle\frown(s)_j^\frown(s)_k$, neboť 7 kóduje $+$), pak $(\hat{s})_i=\langle 7\rangle\frown(\hat{s})_i;\ \frown(\hat{s})_k$, t.j. $(\hat{s})_i$ vzniká aplikací symbolu $+$ na $(\hat{s})_j,(\hat{s})_k$. Podobně pro funkční symboly $S,*$. Když napíšete formální definici, bude mít tvar

$$(\exists s,\hat{s})[(s \text{ odvození } \bar{t}, lh(\hat{s})=lh(s)),$$

$$(\forall z<lh(s))(\text{podmínka na}\,(\hat{s})_z,(s)_z)\ \&\ (\hat{s})_{lh(s)-1}=\bar{t})$$

kde formule za $(\exists s,\hat{s})$ je Δ_1, t.j. celá formule je Σ_1 v $\mathbf{N}$. Zbytek plyne z 2.2.7(1). Zmiňme ještě (9). Posloupnost $s\in Seq$ je důkazem (v predikátovém počtu), právě když

$$N\models Seq(\bar{s})\ \&\ (\forall z<lh(\bar{s}))(LogAx((\bar{s}_z)\ \vee$$

$$\vee\ (\exists z_1,z_2<z)(DED((s)_{z_1},(s)_{z_2},(s)_z)),$$

kde $LogAx$ je formule (Δ_1 v $\mathbf{N}$) definující logické axiomy a $DED(u,v,w)$ říká, že w vzniká z u,v podle pravidla modus ponens, t.j. v je implikace s levým členem u a pravým členem w, t.j. $v=A(\langle 4\rangle,\langle u,v\rangle)$ (4 kóduje implikaci), nebo podobně pro generalizaci.

Podrobné dokončení celého důkazu věty je rutinní záležitostí (vyžaduje však jistou zběhlost v práci s formulemi, které jsou $\Sigma_1, \Delta_1, \Pi_1$ v $\mathbf{N}$). Zájemce najde detailněji informaci v knize Hájek-Pudlák.

Zdůrazněme na konec tohoto paragrafu, čeho jsme dosáhli: podařilo se nám zakódovat formule, termy jazyka aritmetiky přirozenými čísly, a to tak, že důležité symbolické pojmy (zejména pojmy z předchozí věty) jsou Δ_1 v $\mathbf{N}$. (Místo jazyka aritmetiky by šlo vzít pochopitelně jiný jazyk splňující některé minimální předpoklady; to však nebudeme potřebovat).

Vědět, že syntaktické pojmy uvedené v předchozí větě jsou Δ_1 v $\mathbf{N}$, je pro nás dobré ze dvou důvodů: z *technického* - budeme to potřebovat v důkazech Gödelových vět, a z důvodů *intuitivní adekvátnosti*: pojmy, které jsou Δ_1 (v $\mathbf{N}$), jsou intuitivně jednoduché. V následujícím paragrafu uvidíme, že Δ_1 definovatelná je v úzkém vztahu k rekursivnosti, tedy k algoritmické rozhodnutelnosti.

2.5 Δ_1-definovatelnost a rekursivnost

V tomto paragrafu seznámíme čtenáře s následující větou 2.5.1 a pohovoříme s jejím významu, důkazu a důsledcích. Podrobnosti důkazxu jsou mimo rámec tohoto textu.

2.5.1 Věta. Buď $A \subseteq N$.
(1) A je Δ_1, právě když A je rekursivní.
(2) A je Σ_1, právě když A je rekursivně spočetná.

Věta ukazuje, že definovatelnost v $\mathbf{N}$ je v úzkém vztahu k algoritmické rozhodnutelnosti: Δ_1 množiny jsou právě všechny algoritmicky rozhodnutelné množiny.

Rekursivnost a rekursivní spočetnost se definuje jednak pro množiny čísel, jednak pro množiny slov nějaké abecedy (obě definice jsou v jistém smyslu ekvivalentní). Vyjdeme-li z množin slov nějaké abecedy Λ, bude naše definice patrně užívat pojmu Turingova stroje; množina $X \subseteq \Lambda^*$ je rekursivně spočetná, existuje-li Turingův stroj M, který má za vstup slova S z Λ^* a zastaví se právě tehdy, když $s \in X$. Množina X je rekursivní, existuje-li Turingův stroj, který má za vstup slova S z Λ^*, vždy se zastaví a při zastavení je v přijímajícím stavu, právě když $s \in X$.

Tato definice se přenese na množiny $A \subseteq N$ tak, že se každé množině $A \subseteq N$ přiřadí jistá množina slov, např. množina všech numerálů prvků z A; $\Pi = \{\overline{n} \mid n \in A\}$. A je rekursivní (rekursivně spočetná), má-li tuto vlastnost množina $\overline{A}$. Stačí diskutovat důkaz tvrzení (2), neboť dle Postovy věty je A rekursivní, právě když A i $N - A$ jsou rekursivně spočetné (a ovšem A je Δ_1, právě když A i $N - A$ jsou Σ_1).

Implikace [A rekursivně spočetná $\Rightarrow A$ je Σ_1] se ukazuje tak, že se analyzuje pojem ***výpočtu*** Turingova stroje a ukáže se, že relace
"c je končící výpočet na stroji T se vstupem $\overline{n}$" je Δ_1 definovatelná v $\mathbf{N}$ (za

použití kódování posloupností z předchozích paragrafů; výpočet je posloupnost *stavů* Turingova stroje, každý stav je dán jistou konečnou posloupností a každý stav, který není poslední, přechází do následujících tak, jak přikazuje stroj).

Tedy $n \in A$, právě když existuje c, které je končícím výpočtem se vstupem $\overline{n}$; to dává Σ_1 definici.

Obráceně je třeba nejprve ukázat, že pro každou omezenou formuli $\varphi(x_1, \ldots x_k)$ existuje Turingův stroj T pracující s k-ticemi vstupních slov, který je totální (vždy se zastaví) a se vstupem $\overline{m}_1, \ldots \overline{m}_k$ se zastaví v přijímajícím stavu, právě když $\mathbf{N} \models \varphi(\overline{m}_1, \ldots, \overline{m}_k)$ (konstrukce stroje indukcí podle odvození formule φ). Je-li A definováno Σ_1-formulí $(\exists x_2)\varphi(x, x_2)$, kde φ je omezená, a je-li T stroj pro φ, pak z něj lze lehko sestrojit stroj T', který pro vstup $\overline{m}_1$ postupně generuje $\overline{m}_2 = \overline{0}, \overline{1}, \overline{2}, \ldots$, pro každé $\overline{m}_2$ ověří, zda platí $\varphi(\overline{m}_1, \overline{m}_2)$ (užitím stroje T); jakmile první takové $\overline{m}_2$ najde, zastaví se.

Tím jsme naskicovali důkaz věty 2.5.1. Nakonec uvedeme ještě jeden důsledek naší věty. Připomeňme si abecedu Λ_{Ar} jazyka aritmetiky; slova z Λ_{ar}^* jsme ztotožnili s jistými čísly z množiny $Seq \subseteq N$. Chápeme-li $X \subseteq \Lambda_{Ar}^*$ jako množinu slov, je její rekursivní spočetnost (rekursivnost) definována pomocí Turingových strojů, které pracují se slovy z Λ_{Ar}^*. (Není nutné napřed zakódovat slovo z Λ_{Ar}^* jako číslo a pak toto číslo kódovat jako slovo numerál.) Dostáváme toto:

2.5.2 Věta. Nechť $X \subseteq \Lambda_{Ar}^* \subseteq N$.

(1) X je Σ_1 množina čísel, právě když X je rekursivně spočetná jakožto množina slov v abecedě Λ_{Ar}.

(2) X je Δ_1 množina čísel, právě když X je rekursivní jakožto množina slov v abecedě Λ_{Ar}.

Stačí dokazovat (1) a implikace $\Leftarrow$ se dokazuje analogicky jako ve větě 2.5.1 (kódováním výpočtů). Obráceně je-li X Σ_1 množina čísel, víme, že $\overline{X} = \{\overline{n} \mid n \in X\}$ je rekursivně spočetná, t.j. máme stroj, který pro vstup $\overline{n}$ zastaví, právě když $n \in X$. Lze sestrojit jiný stroj T_0, který pro vstup $\langle s_0, \ldots, s_k \rangle \in \Lambda_{Ar}^*$ (chápaný jako slovo v abecedě Λ_{Ar}) sestrojí $\overline{n}$ takové, že n je kód posloupnosti $\langle s_0, \ldots, s_k \rangle$; s tímto $\overline{n}$ pak zachází přesně stejně jako stroj T. Stroj T_0 prokazuje, že X jakožto množina slov v abecedě Λ_{Ar} je rekursivně spočetná.

Od čtenáře se tedy očekává porozumění větám 2.5.1, 2.5.2; důkazy jsme jen naskicovali. Pokud však jste již absolvoval(a) přednášku z teorie rekurse, bude pro Vás hračkou důkazy vypracovat.

Tímto paragrafem končí studium definovatelnosti aritmetickými formulemi v N; v dalších paragrafech se budeme zabývat teoriemi v jazyce aritmetiky (obsahujícími Robinsonovu aritmetiku Q).

2.6 Σ_1-úplnost Robinsonovy aritmetiky

V tomto a následujících paragrafech se budeme zabývat Robinsonovou aritmetikou Q a jejími rozšířeními. Připomeňme axiomy:

2.6.1 Definice. Q je teorie v jazyce aritmetiky s následujícími axiomy:

Q1: $S(x) \neq \overline{0}$
Q2: $S(x) = S(y) \rightarrow x = y$
Q3: $x \neq \overline{0} \rightarrow (\exists y)(x = S(y))$
Q4: $x + \overline{0} = x$
Q5: $x + S(y) = S(x + y)$
Q6: $x * \overline{0} = \overline{0}$
Q7: $x * S(y) = (x * y) + x$
Q8: $x \leq y \equiv (\exists z)(z + x = y)$

2.6.2 Lemma. Následující formule jsou dokazatelné v Q:

(1) $x + y = \overline{0} \rightarrow .x = \overline{0} \; \& \; y = \overline{0},$
(2) $x * y = \overline{0} \rightarrow .x = \overline{0} \vee y = \overline{0},$
(3) $x + \overline{1} = S(x),$
(4) $\overline{0} \leq x,$
(5) $S(x) \leq \overline{n+1} \rightarrow x \leq \overline{n},$
(6) $S(x) + \overline{n} = x + \overline{n+1},$
(7) $\overline{n} \leq x \rightarrow .x = \overline{n} \vee \overline{n+1} \leq x.$

Důkaz. (1) Jestliže $y \neq \overline{0}$, pak $y = S(z)$ pro nějaké z, tedy $x+y = S(x+z) \neq \overline{0}$. Jestliže $x \neq \overline{0} \; \& \; y = \overline{0}$ pak $x + y = x \neq \overline{0}$. Tím je (1) dokázáno. (2) Nechť $x, y \neq \overline{0}, x = S(u), y = S(v)$. Pak $x * y = S(u) * S(v) = (S(u) * v) + S(u) = S(S(u) + v) \neq \overline{0}$. (3) je zřejmé. (4) plyne dle (Q4). (5) Jestliže $z + S(x) = \overline{n+1}$, pak $S(z + x) = S(\overline{n})$, tedy $z + x = \overline{n}$. Všimněte si, že (5) je schema; pro každé n máme jiný důkaz. Také (6) je schema; sestrojíme požadované důkazy indukcí. Přitom je důležité, že *nebudeme* používat idukci *uvnitř* důkazů (protože v Q nemáme žádný axiom indukce); sestrojíme $(n+1)$-tý důkaz z n-tého. (Srovnejte s 2.6.6.) Pro $n = 0$ Q dokazuje $S(x) + \overline{0} = S(x) = x + \overline{1}$. Předpokládejme (6) pro n; dostaneme Q$\vdash S(x) + \overline{n+1} = S(x) + S(\overline{n}) = S(S(x) + \overline{n})) = S(x + \overline{n+1}) = x + S(\overline{n+1}) = x + \overline{n+2}$. (7) Předpokládejme $\overline{n} \leq x \; \& \; x \neq \overline{n}$; pak pro jisté $z \neq \overline{0}$ jest $z + \overline{n} = x$, $z = S(w)$. Podle (6) platí $x = w + \overline{n+1}$, tedy $\overline{n+1} \leq x$.

Tím je věta dokázána; ukážeme ještě další dokazatelnosti v Q.

2.6.3 Věta. Pro libovolné $n, m \in N$ dokazuje Q následující formule:

(1) $\overline{m} + \overline{n} = \overline{m+n},$
(2) $\overline{m} * \overline{n} = \overline{m*n},$
(3) $\overline{m} \neq \overline{n}$ pro $m \neq n,$
(4) $x \leq \overline{n} \equiv .x = \overline{0} \vee x = \overline{1} \vee \ldots \vee x = \overline{n},$
(5) $x \leq \overline{n} \vee \overline{n} \leq x.$

Důkaz. (1) Dokážeme Q$\vdash \overline{m} + \overline{n} = \overline{m+n}$ indukcí dle n. Pro $n = 0$ máme dokázat Q$\vdash \overline{m} + \overline{0} = \overline{m}$, což však plyne z (Q4). Předpokládejme, že už máme důkaz formule (1) a dokazujme v Q: $\overline{m} + \overline{n+1} = \overline{m} + S(\overline{n}) = S(\overline{m} + \overline{n}) = \overline{m+n+1}$. Důkaz tvrzení (2) je podobný.

(3) Nyní ukážeme, že $m \neq n$ implikuje Q$\vdash$ $\overline{m} \neq \overline{m}$. Stačí předpokládat $n < m$. Pro $m = 0$ je podmínka prázdná. Předpokládejme platnost tvrzení pro m a nechť $n < m + 1$. Pak buďto $n = 0$ a (Q1) dává Q$\vdash$ $\overline{n} \neq \overline{m+1}$ nebo $n = n_0 + 1$, máme tedy Q$\vdash$ $\overline{n_0} \neq \overline{m}$ podle indukčního předpokladu; tedy Q$\vdash$ $\overline{n} \neq \overline{m+1}$ podle (Q2).

(4) Sestrojíme požadované důkazy indukcí podle n. Pro $n = 0$ viz předchozí větu část (1). Předpokládejme platnost tvrzení (4) pro n a vyšetřeme $n + 1$. Implikace $\leftarrow$ plyne dle (1); obráceně předpokládejme v Q $x \leq \overline{n+1}$. Je-li $x = \overline{0}$ jsme hotovi; předpokládejme tedy $x \neq \overline{0}$, $x = S(z)$. Dle 2.6.2(5) dostáváme $z \leq \overline{n}$, tedy $z = \overline{0} \vee \ldots \vee z = \overline{n}$, z čehož plyne $x = \overline{1} \vee \ldots \vee x = \overline{n+1}$.

(5) Q$\vdash$ $\overline{0} \leq x$ dle 2.6.2(4). Předpokládejme Q$\vdash$ $\overline{n} \leq x \vee x \leq \overline{n}$ a dokazujme v Q. Jestliže $x \leq \overline{n}$, pak $x \leq \overline{n+1}$ podle (4) a (1); když $\overline{n} \leq x$, pak dle 2.6.2(7) buď $\overline{n} = x$ a tedy $x \leq \overline{n+1}$, nebo $\overline{n+1} \leq x$.

2.6.4 Věta. (Σ_1-úplnost teorie Q.) Budiž $\varphi(x)$ Σ_0-formule s jedinou volnou proměnnou x a nechť $\mathbf{N} \models (\exists x)\varphi(x)$. Pak Q$\vdash$ $(\exists x)\varphi(x)$.

Důkaz. Stačí pro každé $\varphi(x_1, \ldots, x_n) \in \Sigma_0$ ukázat, že $\mathbf{N} \models \varphi(\overline{k_1}, \ldots, \overline{k_n})$ implikuje Q$\vdash$ $\varphi(\overline{k_1}, \ldots, \overline{k_n})$. Ukažme nejprve s užitím 2.6.3(1),(2), že pro každý term $t(x_1, \ldots, x_n)$ a každou n-tici $k_1, \ldots, k_n$ prvků N je

$$Q \vdash t(\overline{k_1}, \ldots, \overline{k_n}) = \overline{Val(t(\overline{k_1}, \ldots, \overline{k_n})}$$

(např. Q$\vdash$ $(\overline{2} * \overline{5}) + \overline{4} = \overline{14}$). Z toho plyne opět dle 2.6.3, že naše tvrzení platí pro φ atomické nebo negované atomické. (Všimněte si, že když $\mathbf{N} \models \neg(\overline{k} \leq \overline{m})$, pak $m < k$ a $Q \vdash \overline{k} \leq \overline{m} \rightarrow (\overline{k} = \overline{0} \vee \ldots \vee \overline{k} = \overline{m})$, tedy Q$\vdash$ $\neg(\overline{k} \leq \overline{m})$.) Indukční krok pro logické spojky je snadný. Předpokládejme tedy ještě, že φ je tvaru $(\exists y \leq x_1)\psi(y, x_1, \ldots, x_n)$ a $\mathbf{N} \models \varphi(\overline{k_1}, \ldots, \overline{k_n})$; tedy pro jisté $k_0 \leq k_1$, $\mathbf{N} \models \psi(\overline{k_0}, \overline{k_1}, \ldots, \overline{k_n})$ a úpodle indukčního předpokladu Q$\vdash$ $\psi(\overline{k_0}, \ldots, \overline{k_n})$. To dává Q$\vdash$ $\varphi(\overline{k_1}, \ldots, \overline{k_n})$. Důkaz pro $\neg\varphi$ tj. pro $(\forall y \leq x)\neg\psi(y, x_1, \ldots, x_n)$ je podobný. (Je však třeba podstatně užít 2.6.3(4).)

2.6.5 Poznámka. (1) Z předchozí věty plyne okamžitě, že každá teorie obsahující Q je Σ_1-úplná; z první Gödelovy věty, kterou dokážeme v paragrafu 8 však plyne, že žádná "rozumná" teorie obsahující Q není Π_1-úplná.

(2) Máme-li k dispozici axiom indukce, můžeme dokazovat universální tvrzení jedním důkazem; z takového tvrzení plyne okamžitě každý jeho konkrétní případ (instance) vzniklý dosazením libovolného numerálu $\overline{n}$ za univesálně kvantifikovanou proměnnou. O tom bude leccos ve cvičeních; zde aspoň jeden příklad.

2.6.6 Lemma. V PA je dokazatelná formule

$$x + (y + z) = (x + y) + z$$

(asociativita sčítání).

Důkaz. Dokážeme $(x + y) + z = x + (y + z)$ indukcí dle z. Platí ovšem $(x + y) + \overline{0} = x + (y + \overline{0}) = x + y$. Předpokládejme $(x + y) + z = x + (y + z)$ a vyšetřeme $(x+y)+S(z)$. Jest $(x+y)+S(z) = S((x+y)+z) = S(x+(y+z)) =$

$x + S(y+z) = x + (y + (S(z))$. Z toho plyne tvrzení dle axiomu indukce pro formuli $x + (y + z) = (x + y) + z$ jakožto formuli $\varphi(z)$, tj. axiom indukce je

$$[\varphi(\overline{0}) \ \& \ (\forall z)(\varphi(z) \rightarrow \varphi(S(z)))] \rightarrow (\forall z)\varphi(z).$$

2.7 Diagonální lemma

Dokážeme zde slavné diagonální (autoreferenční) lemma, které zhruba říká, že ke každé formuli $\varphi(x)$ jazyka aritmetiky s jednou volnou proměnnou existuje uzavřená formule ψ, která říká "já mám vlastnost φ". Toto lemma hraje podstatnou roli v důkazu Gödelovy věty o neúplnosti a v řadě jejich důkazů v metamatematice aritmetiky. Gödel sám ve své slavné práci z roku 1931 uvedl pouze speciální případ, jeho konstrukce je však obecná. V plné obecnosti se lemma objevilo r.1934 v Carnapově knize Logische Syntax der Sprache.

Připomeňme, že jsme zakódovali syntax aritmetiky v $\mathbf{N}$, t.j. formule, termy atd. jsou pro nás jistá speciální *čísla*. Pro každou formuli φ má tedy smysl mluvit o příslušném numerálu $\overline{\varphi}$; to budeme hojně činit. Nejprve dokážeme jedno technické lemma, které říká, že každá Σ_1 funkce z N do N (parciální) má jistou "velmi dobrou" Σ_1-definici s dodatečnými vlastnostmi.

2.7.1 Lemma. Nechť F je zobrazení, jehož definiční obor i obor hodnot jsou částmi N a nechť F je Σ_1, t.j. graf zobrazení F je Σ_1-relace. Pak existuje Σ_1-formule $\alpha(x, y)$ taková, že pro každé m z definičního oboru funkce F platí

$$Q \vdash \alpha(\overline{m}, y) \equiv y = \overline{F(m)}.$$

Důkaz. (Pokud Vám bude důkaz připadat těžký, odložte jeho čtení až po prostudování důkazu Rosserovy věty v následujícím paragrafu.)

Dle předpokladu existuje Σ_1-formule $(\exists z)\varphi(x, y, z)$ (φ omezená) tak, že pro každé k, m

$$k = F(m), \text{ právě když } \mathbf{N} \models (\exists z)\varphi(\overline{m}, \overline{k}, z).$$

Každé z splňující $\varphi(\overline{m}, \overline{k}, z)$ můžeme nazývat *svědek* toho, že $k = F(m)$. Můžeme předpokládat, že svědek pro $k = F(m)$ je vždy větší než k, přesněji, že $Q \vdash \varphi(x, y, z) \rightarrow z \geq y$ [jinak nahraďte $\varphi(x, y, z)$ formulí $(\exists z_0 \leq z)(\varphi(x, y, z_0) \ \& \ z = z_0 + y)$].

Definujme formuli $\alpha(x, y)$ takto:

$$\alpha(x, y) \equiv (\exists z)[\varphi(x, y, z) \ \& \ (\forall v, w \leq z)(v \neq y \rightarrow \neg\varphi(x, v, w))]$$

(existuje z, které svědčí, že $F(x) = y$ a nic pod z nesvědčí, že $F(x)$ je něco jiného).

Nechť $k = F(m)$. Pak zřejmě $\mathbf{N} \models \alpha(\overline{m}, \overline{k})$, t.j. existuje svědek $q \in N$ takový, že $N \models \varphi(\overline{m}, \overline{k}, \overline{q})$. Dále $\mathbf{N} \models (\forall v, w \leq \overline{q})(v \neq \overline{k} \rightarrow \neg\varphi(\overline{m}, v, w))$; kdyby tomu tak nebylo, mělo by F pro argument m dva různé obrazy. Díky Σ_1-úplnosti (viz 2.6.4) dostáváme

$Q \vdash \varphi(\overline{m}, \overline{k}, \overline{q})$ & $(\forall v, n \leq \overline{q})(v \neq \overline{k} \rightarrow \neg\varphi(\overline{m}, v, w))$, (*)
tedy
$Q \vdash y = \overline{F(m)} \rightarrow \alpha(\overline{m}, y)$.
Obráceně, nechť m, k, q jsou jako výše a v Q předpokládejme
$y \neq \overline{F(m)}$ & $\alpha(\overline{m}, y)$; *chceme* odvodit spor. Dokazujeme v Q. $\alpha(\overline{m}, y)$ znamená
$(\exists z \geq y)(\varphi(\overline{m}, y, z)$ & $(\forall r, w \leq z)(r \neq y \rightarrow \neg\varphi(\overline{m}, v, w))$. (**)
Zvolme takové z a rozlišme dva případy:
Případ 1. $z \leq \overline{q}$ - pak $\varphi(\overline{m}, y, z)$ je ve sporu s (*);
Případ 2. $\overline{q} \leq z$ - pak $\varphi(\overline{m}, \overline{k}, \overline{q})$ je ve sporu s (**).
Tím je lemma dokázáno.

2.7.2 Diagonální lemma. (1) *Neparametrická verse.* Nechť $\varphi(x)$ je formule aritmetiky s jednou volnou proměnnou x. Pak existuje uzavřená formule ψ taková, že

$$Q \vdash \psi \equiv \varphi(\overline{\psi}).$$

(2) *Parametrická verse.* Nechť $\varphi(x, z)$ je formule aritmetiky se dvěma volnými proměnnými x, z. Pak existuje formule $\psi(z)$ taková, že pro každé $k \in N$

$$Q \vdash \psi(\overline{k}) \equiv \varphi(\overline{(\psi(\overline{k})}, \overline{k}).$$

Důkaz. Dokážeme jen (1). Nechť $\varphi(x)$ je dáno. Vyšetřujeme funkci F přiřazující každé formuli $\delta(x)$ s jednou volnou proměnnou uzavřenou formuli $\delta(\overline{\delta})$ (t.j. $Subst(\delta, x, \overline{\delta})$). Tato funkce je zřejmě Σ_1 definovatelná v $\mathbf{N}$ ($\delta(x)$ i $\delta(\overline{\delta})$ jsou čísla!), tedy dle předchozího lemmatu existuje formule $\alpha(x, y)$ taková, že

$$Q \vdash \alpha(\overline{\delta}, y) \equiv y = \overline{F(\delta)}$$

pro každé δ (formuli s jednoiu volnou proměnnou). Položme

$$\chi(x) \equiv (\exists v)(\alpha(x, v) \ \& \ \varphi(v))$$

a $\psi \equiv F(\chi)$ (t.j. ψ je $Subst(\chi, x, \overline{\chi})$). Pak Q dokazuje následující ekvivalence: $\psi \equiv \chi(\overline{\chi}) \equiv (\exists v)(\alpha(\overline{\chi}, v)$ & $\varphi(v)) \equiv (\exists v)(v = \overline{F(\chi)}$ & $\varphi(v)) \equiv \varphi(\overline{F(\chi)}) \equiv \varphi(\overline{\chi(\overline{\chi})}) \equiv \varphi(\overline{\psi})$.

Tím je lemma dokázáno. (Důkaz části (2) lze nalézt v citované monografii Hájka a Pudláka.)

2.8 Gödelovy věty o neúplnosti, Rosserova věta

Toto je centrální paragraf; zde dokážeme věty, které v třicátých letech tohoto století radikálně změnily představy o tom, co je matematická logika a ukázaly mimo jiné, že pravdu o přirozených číslech nelze úplně postihnout žádnou teorií, která má rekursivní axiomatiku (formulujeme to přesněji a obecněji).

2.8.1 Definice. (1) teorie T je *axiomatizovaná*, je-li její množina axiomů Δ_1 množina (t.j. rekursivní). (2) Teorie T v jazyce aritmetiky je Σ_1-*korektní*, je-li každá uzavřená Σ_1 formule dokazatelná v T pravdivá v $\mathbf{N}$.

2.8.2 Poznámka. Je-li T axiomatizovaná, pak množina všech důkazů v teorii T je Δ_1 množina; množina všech formulí dokazatelných v T je zřejmě Σ_1 množina.

2.8.3 Definice. Nechť T je axomatizovaná a nechť $\pi(x)$ je nějaká Σ_1 definice množiny všech formulí dokazatelných v T. Formule ν splňující $Q \vdash \nu \equiv \neg\pi(\overline{\nu})$ (existující dle diagonálního lemmatu) se nazývá *Gödelova formule* pro T. (ν říká "já jsem nedokazatelná".)

2.8.4 Věta. (první Gödelova věta o neúplnosti).

Nechť T je axiomatizovaná teorie v jazyce aritmetiky obsahující Q a Σ_1-korektní. Pak T je neúplná; Gödelova formule není ani dokazatelná ani vyvratitelná.

Důkaz. Nechť $T \vdash \nu$, pak $N \models \pi(\overline{\nu})$ (neboť π definuje dokazatelné formule), tedy $T \vdash \pi(\overline{\nu})$ díky Σ_1-úplnosti, tedy $T \vdash \neg\overline{\nu}$ a T je sporná. Tedy T nedokazuje ν.

Nechť $T \vdash \neg\nu$, tedy $T \vdash \pi(\overline{\nu})$ (dle definice Gödelovy formule), tedy $\mathbf{N} \models \pi(\overline{\nu})$ díky Σ_1-korektnosti, tedy $T \vdash \nu$ a T je sporné. Tedy T nedokazuje $\neg\nu$.

Poznámka. Všimněte si, že předpoklad Σ_1-korektnosti není potřeba k důkazu nedokazatelnosti formule ν.

2.8.5 Definice. Buď $T \supseteq Q$ axiomatizovaná teorie, buď $(\exists u)\beta(x,u)$ Σ_1-definice množiny všech formulí dokazatelných v T a $(\exists u)\gamma(x,u)$ Σ_1-definice množiny všech formulí vyvratitelných v T (t.j. všech φ takových, že $T \vdash \neg\varphi$; zřejmě tato množina je Σ_1). Formule β, γ jsou omezené. *Rosserova formule* ρ je formule splňující

$$Q \vdash \rho \equiv (\exists u)(\gamma(\overline{\rho}, u) \ \& \ (\forall v \leq u)\neg\beta(\overline{\rho}, v))$$

(říká: "existuje mé vyvrácení, pod nímž není žádné mé ověření"). Zřejmě ρ existuje podle diagonálního lemmatu.

2.8.6 Věta (Rosserova). Je-li T bezesporná axiomatizovaná teorie obsahující Q, pak formule ρ není ani dokazatelná ani vyvratitelná v T.

Důkaz. Nechť $T \vdash \rho$; tedy existuje d takové, že $N \models \beta(\overline{\rho}, \overline{d})$. Tedy $\alpha \vdash \beta(\overline{\rho}, \overline{d})$ z Σ_1-úplnosti. Dokazujeme v T:

Mějme u zaručené formulí ρ, t.j. takové, že

$$\gamma(\overline{\rho}, u) \ \& \ (\forall v \leq u)\neg\beta(\overline{\rho}, v).$$

Je tedy $u \leq \overline{d}$, tedy $(\exists u \leq \overline{d})\gamma(\overline{\rho}, u)$, tedy $\gamma(\overline{\rho}, \overline{0}) \vee \ldots \vee \gamma(\overline{\rho}, \overline{d})$. Zjistili jsme $T \vdash \bigwedge_{e \leq d} \gamma(\overline{\rho}, \overline{e})$; ale z bezespornosti teorie T plyne, že T nedokazuje $\neg\rho$, t.j. $N \models \neg\gamma(\overline{\rho}, \overline{e})$ pro libovolné e, tedy $T \vdash \neg\gamma(\overline{\rho}, \overline{e})$ z Σ_1-úplnosti, tedy $T \vdash \bigwedge_{e \leq d} \neg\gamma(\overline{\rho}, \overline{e})$, tedy T je sporná, což je spor. Tedy T nedokazuje ρ.

Za druhé nechť $T \vdash \neg\rho$, tedy $T \vdash (\forall u)(\gamma(\overline{\rho}, u) \rightarrow (\exists v \leq u)\beta(\overline{\rho}, v))$. Přitom $N \models \gamma(\overline{\rho}, \overline{d})$ pro nějaké d (neboť ρ je vyvratitelné), tedy $T \vdash \gamma(\overline{\rho}, \overline{d})$ z Σ_1-korektnosti, tedy $T \vdash (\exists v \leq \overline{d})\beta(\overline{\rho}, v)$, tedy $T \vdash \bigwedge_{e \leq d} \beta(\overline{\rho}, \overline{e})$; ale T nedokazuje ρ, tedy $\mathbf{N} \models \neg\beta(\overline{\rho}, \overline{e})$ pro $e \leq d$, tedy $T \vdash \bigwedge_{e \leq d} \neg\beta(\overline{\rho}, \overline{e})$, což je spor v T; tedy T nedokazuje $\neg\rho$.

Tím jsme ukončili důkaz Rosserovy věty. Gödelova první věta o neúplnosti má pozoruhodný důsledek (kterého si byl vědom už Gödel, říká se mu druhá Gödelova věta o neúplnosti), který v podstatě říká, že žádná "rozumná" aritmetika nemůže dokázat svou vlastní bezespornost. To je pozoruhodný výsledek; pokud se dohodneme, že *finitní prostředky* jsou formalizovatelné v PA, pak tvrzení, že PA nedokazuje svou bezespornost, znamená, že bezespornost aritmetiky nelze dokázat finitními prostředky. Do filosofických diskusí se nebudeme pouštět; definujeme nejprve, jak se bezespornost nějaké teorie *vyjádří* v ní samé.

2.8.7 Definice. Buď T-axiomatizovaná teorie v jazyce aritmetiky obsahující Q, nechť $\pi(x)$ je Σ_1 formule definující v $\mathbf{N}$ množinu všech formulí dokazatelných v T. Pak Con_π značí formuli $\neg\pi(\overline{\overline{0} = \overline{1}})$.

Formule Con_π říká, že formule $\overline{0} = \overline{1}$ (vyvratitelná v T) není dokazatelná v T, přesněji: $N \models Con_\pi$, právě když formule $\overline{0} = \overline{1}$ není dokazatená v T. Jde o to, zda T může dokázat Con_π. K důkazu, že nemůže, potřebujeme další předpoklady o formuli π.

2.8.8 Definice. Buď T, π jako výše. *Hilbert-Bernaysovy podmínky dokazatelnosti* jsou následující podmínky (1)-(3) (pro každé φ, ψ)

(1) Když $T \vdash \varphi$, pak $T \vdash \pi(\overline{\varphi})$,

(2) $T \vdash \pi(\overline{\varphi}) \rightarrow \pi(\overline{\pi(\overline{\varphi})})$,

(3) $T \vdash \pi(\overline{\varphi \rightarrow \psi}) \rightarrow (\pi(\overline{\varphi}) \rightarrow \pi(\overline{\psi}))$.

Poznámka. Podmínka (1) je za našich předpokladů splněna, je-li T Σ_1-korektní. Je-li $T \vdash \varphi$, pak $\mathbf{N} \models \pi(\overline{\varphi})$ (neboť π definuje v $\mathbf{N}$ množinu čísel formulí dokazatelných v T) a π je Σ_1-formule, tudíž dostáváme $T \vdash \pi(\overline{\varphi})$. Podmínky (2) a (3) jsou jemné podmínky na zvolenou definici π: (2) vyjadřuje formalizovanou Σ_1-korektnost, (3) vyjadřuje uzavřenost množiny dokazatelných formulí na modus ponens. (Pozor: formule z (2),(3) jsou pravdivé v $\mathbf{N}$; podmínky však vyžadují, že jsou tyto formule dokazatelné v T. (Lze sestrojit protipříklady.)

2.8.9 Lemma. Nechť T, π jsou jako v 2.8.7 a nechť T, π splňují podmínky dokazatelnosti. Pak pro každou uzavřenou formuli φ platí

$$T \vdash Con_\pi \equiv (\neg\pi(\overline{\varphi}) \vee \neg\pi(\overline{\neg\varphi})).$$

(Čteme: teorie definovaná formulí π je bezesporná, právě když buď φ nebo $\neg\varphi$ je nedokazatelná.)

Důkaz. Platí $T \vdash \varphi \rightarrow (\neg\varphi \rightarrow \overline{0} = \overline{1})$, tedy $T \vdash \pi(\overline{\varphi \rightarrow (\neg\varphi \rightarrow \overline{0} = \overline{1}})$, tedy $T \vdash \pi(\overline{\varphi}) \rightarrow (\pi(\overline{\neg\varphi}) \rightarrow \pi(\overline{\overline{0} = \overline{1}})$ (dle podmínky (3)), tedy $T \vdash \pi(\overline{\varphi}\ \&\ \pi(\overline{\neg\varphi}) \rightarrow \neg Con_\pi$.

Obráceně platí $T \vdash \neg(\overline{0} = \overline{1})$, t.j. $T \vdash \pi(\overline{\neg(\overline{0} = \overline{1})})$, a též $T \vdash \pi(\overline{\neg\overline{0} = \overline{1}}) \rightarrow (\pi(\overline{\overline{0} = \overline{1}}) \rightarrow \pi(\overline{\varphi})\ \&\ \pi(\overline{\neg\varphi}))$ (neboť $T \vdash \pi(\overline{\neg(\overline{0} = \overline{1}) \rightarrow (\overline{0} = \overline{1} \rightarrow \varphi})$) a podobně s $(\neg\varphi)$ místo φ). Tedy $T \vdash \neg Con_\pi \rightarrow \pi(\overline{\varphi})\ \&\ \pi(\overline{\neg\varphi})$. Tím je důkaz proveden.

2.8.10 Věta. Je-li T axiomatizovaná teorie v jazyce aritmetiky obsahující Q a je-li π Σ_1-formule definující v **N** množinu všech *formulí dokazatelných* v T, a platí-li podmínky dokazatelnosti pro T, φ, pak

$$T \vdash Con_\pi \equiv \nu,$$

kde ν je Gödelova formule (viz výše). Je-li tedy T bezesporná, pak formule Con_π je nedokazatelná v T. (To je *druhá Gödelova věta o neúplnosti.*)

Důkaz. Jest $T \vdash \nu \rightarrow \neg\pi(\overline{\nu})$ (z definice ν), tedy dle předchozího lemmatu $T \vdash \nu \rightarrow Con_\pi$. Obráceně jest $T \vdash \neg\nu \rightarrow \pi(\overline{\nu})$, dále $T \vdash \pi(\overline{\nu}) \rightarrow \pi(\overline{\pi(\overline{\nu})})$ (podmínka (2)); také $T \vdash \pi(\overline{\nu}) \rightarrow \neg\nu$, tedy $T \vdash \pi(\overline{\pi(\overline{\nu})}) \rightarrow \pi(\neg\overline{\nu})$, tedy máme

$$T \vdash \neg\nu \rightarrow \pi(\overline{\nu}),\ T \vdash \neg\nu \rightarrow \pi(\overline{\neg\nu}),$$

$$T \vdash \neg\nu \rightarrow \pi(\overline{\nu})\ \&\ \pi(\overline{\neg\nu}),$$

$$T \vdash \neg\nu \rightarrow \neg Con_\pi.$$

Celkem $T \vdash \nu \equiv Con_\pi$.

Je-li T bezesporná, pak T nedokazuje ν (v důkazu 1. Gödelovy věty jsme upozornili, že pro nedokazatelnost formule ν stačí bezespornost, není třeba Σ_1-korektnost); tedy T nedokazuje Con_π.

2.9 Nerozhodnutelnost aritmetiky

Víme, že je-li teorie T v jazyce aritmetiky (množina axiomů) Σ_1 (zejména je-li Δ_1 nebo Δ_0), pak množina všech formulí dokazatelných v T je Σ_1, jinými slovy: je-li T rekursivně axiomatizovaná teorie, je množina Pr_T formulí dokazatelných v T rekursivně spočetná. Ukážeme, že je-li T bezesporná, pak množina Pr_T není rekursivní (není Δ_1). tedy neexistuje algoritmus, který pro každou formuli φ rozhodne, zda φ je či není dokazatelná.

2.9.1 Věta. Nechť T je bezesporná axiomatizovaná teorie v jazyce aritmetiky obsahující Q, nechť $\pi(x)$ je Σ_1 formule definující v $\mathbf{N}$ množinu všech formulí dokazatelných v T. Pak $\pi(x)$ *není* Δ_1 formule v $\mathbf{N}$.

Důkaz se opírá o následující lemma.

2.9.2 Lemma. Je-li T bezesporná teorie v jazyce aritmetiky a množina Pr_T všech formulí dokazatelných v T je Δ_1 v $\mathbf{N}$, pak existuje úplná bezesporná teorie $\hat{T}$ taková, že množina $\hat{T}$ je Δ_1 v $\mathbf{N}$.

Důkaz spočívá v ověření, že klasická konstrukce bezesporného úplného rozšíření bezesporné teorie (který je mj. součástí důkazu Gödelovy věty o úplnosti) dává k Δ_1 teorii Δ_1 rozšíření. Vskutku nechť F je Δ_1 funkce, $F : N \to N$, taková, že jejím oborem hodnot jsou všechny uzavřené formule. (Existence plyne z toho, že množina všech uzavřených formulí je nekonečná Δ_1 část množiny N.) Definujme $G(0) = F(0)$, pokud $T \vdash F(0)$, jinak $G(0) = \neg F(0)$; máme-li $G(0), \ldots, G(k)$, definujme $G(k+1) = F(k+1)$, pokud $(T, G(0), \ldots, G(k)) \vdash F(k+1)$, jinak $G(k+1) = \neg(F(k+1))$. Podle předpokladu, že Pr_T je Δ_1 v $\mathbf{N}$, je relace $T, G(0), \ldots, G(k) \vdash F(k+1)$ také Δ_1 v $\mathbf{N}$ (věta o dedukci). Funkce G vzniká z F primitivní rekursí (přesněji, jistou *variantou* primitivní rekurse) a je tedy Δ_1 podle věty 2.3.8; teorie $\hat{T} = \{G(k) \mid k \in N\}$ je bezesporné úplné rozšíření teorie T (neboť pro každé k je teorie $(T, G(0), \ldots, G(k))$ bezesporná dle konstrukce). Teorie $\hat{T}$ je Σ_1 v $\mathbf{N}$.

Nechť $\alpha(x,y)$ je Δ_1 v $\mathbf{N}$ a definuje relaci "$\varphi = F(k)$", nechť $\beta(x,y)$ je Δ_1 v $\mathbf{N}$ a definuje relaci "$\varphi = G(k)$". Pak pro každou uzavřenou formuli φ platí: $\varphi \in \hat{T}$, právě když $\mathbf{N} \models (\exists x)(\alpha(\overline{\varphi}, x)\ \&\ \beta(\overline{\varphi}, x))$ (t.j. v kroku k takovém, že $\varphi = F(k)$, je $\varphi = G(k)$), t.j. $\hat{T}$ je Σ_1 v $\mathbf{N}$;

$$\varphi \notin \hat{T} \text{ právě když } \mathbf{N} \models (\exists x)(\alpha(\overline{\varphi}, x)\ \&\ \beta(\overline{\varphi}, x))$$

(t.j. v kroku k, pro nějž $\varphi = F(k)$, je $G(k) = (\neg\varphi)$).

Tím je lemma dokázáno.

2.9.3 Důkaz věty 2.9.2: Kdyby Pr_T bylo Δ_1 v $\mathbf{N}$, pak by T mělo úplné bezesporné rozšíření $\hat{T}$, které by bylo Δ_1 v $\mathbf{N}$. Takové rozšíření je však neúplné dle 1.Gödelovy věty o neúplnosti.

2.10 Epilog

Pokud jste, vážená čtenářko a vážený čtenáři dočetl(a) tento text až sem a máte za sebou seriosní pokus o podrobné prostudování předloženého materiálu, ptáte se patrně: na co to bylo? Co jsem se naučil(a)? V tomto závěrečném odstavci shrneme některé základní aspekty, které se Vám měly ozřejmit.

(1) Pravdivost a dokazatelnost Definovali jsme dokazatelnost ve výrokovém počtu, v predikátovém počtu, v axiomatických teoriích. Definovali jsme *dvojí* pojem pravdivosti: *tautologičnost* (pravdivost při všech evaluacích resp. ve všech modelech) a na druhé straně pravdivost v jednom konkrétním modelu. Pro aritmetiky (teorie v jazyce aritmetiky) nás velice zajímala pravdivost ve *standardním modelu* **N**. Je pravdivost ekvivalentní dokazatelnosti? Na to jsou dvě odpovědi: pokud pravdivost znamená tautologičnost (pravdivost ve všech modelech), pak odpověď je ANO: to je věta o úplnosti, analogicky i silná věta o úplnosti (pro teorii a všechny její modely). Pokud však pracujeme s libovolnou axiomatizovanou teorií T v jazyce aritmetiky, jejímž jedním modelem je **N** (t.j. každá formule dokazatelná v T je pravdivá v **N**) a "pravdivost" znamená "pravdivost v **N**", pak odpověď je NE: T není úplná (dle 1. Gödelovy věty o neúplnosti), existuje formule ν pravdivá v **N** a nedokazatelná v T. Přidáte-li ν k T, dostanete jinou teorii T' a jinou ν' pravdivou v **N** a nedokazatelnou v T'. To lze iterovat, dokonce transfinitně (to však už je delikátní věc). Hlavní je toto: pravda v **N** není ekvivalentní dokazatelnosti v žádné axiomatizované teorii T.

(2) Logika a informatika Jaké jsou vztahy logiky k informatice? Četné. Hned výrokový počet a jím dané booleovské funkce (zobrazení z $\{0,1\}^n$ do $\{0,1\}$) mají uplatnění na hardwarové úrovni počítačů. Logika je podstatná v logickém programování (jazyk PROLOG). Teorie výpočetní složitosti (PNP problém a podobné) má velmi úzký vztah ke slabým aritmetikám, např. k teorii, která vznikne z PA tím, že přijmeme jen axiomy indukce odpovídající *omezeným* formulím (omezená aritmetika). V umělé inteligenci jsou velmi užitečné neklasické logiky, které se liší od výrokového (predikátového) počtu tím, že mají více pravdivostních hodnot než dvě (fuzzy logiky) nebo tím, že užívají různé modality ($\Box\varphi$ znamená "nutně φ" a pod.), t.j. různé *modální logiky*, zejména v souvislosti s usuzováním za nejistoty (logiky domnění). Je řada dalších souvislostí, třeba logiky programů a jiné. Logické systémy, které jsme vyložili, jsou základem všech těchto logik.

(3) Logika jako metamatematika Matematická logika je matematická disciplina studující formalizované matematické teorie (např. PA). Studuje např. *modely* dané teorie a může dát důkazy bezespornosti nějaké teorie tím, že sestrojí její model (za nějakých předpokladů, třeba předpokladu, že jiná teorie má model). I zde má Gödel světoznámý výsledek (z r.1939): Ukázal, že z libovolného modelu teorie množin lze sestrojit jiný model teorie množin (podmodel prvního), v němž platí axiom výběru; ukázal tak, že je-li teorie množin bezesporná, zůstane bezesporná i po přidání axiomu výběru (a též po přidání hypotézy kontinua, i ta platí v jeho modelu). V r.1963 sestrojil P.J.Cohen jiný model, který ukázal, že na druhé straně lze k teorii množin přidat bezesporně negaci axiomu výběru, t.j. že axiom výběru je nedokazatelný v teorii množin (pokud ta je bezesporná). Teorie modelů teorie množin je nesmírně bohatá disciplina.

(4) Poslání matematického logika je dvojí: jednak ukazovat, kam až lze jít metodami a prostředky formální logiky, tyto prostředky zbohacovat, studovat a aplikovat, jednak ovšem ukazovat, kam už jít nelze, které cíle jsou nereálné a neuskutečnitelné (např. důkaz bezespornosti teorie množin vedený v ní samé nebo algoritmus rozhodující o každé formuli, zda je či není dokazatelná v aritmetice).

Pokud soudíte, že to je úkol počestný, krásný a dobrodružný, uvažte, zda se nechcete matematickou logikou zabývat hlouběji.

Cvičení

1. (a) Dokažte, že relace dělitelnosti, relace nesoudělnosti, množina všech druhých mocnin přirozených čísel a množina všech prvočísel jsou v $\mathbf{N}$ Δ_0-definovatelné.
   (b) Dokažte, že množina všech mocnin dvojky je v $\mathbf{N}$ Δ_0-definovatelná.
   Návod k (b). Obejděte se bez faktu, že funkce $x \mapsto 2^x$ je Δ_0-definovatelná. Je to pravda, ale důkaz je obtížný.

2. (a) Dokažte, že každá jednoprvková množina je definovatelná ve struktuře $\langle N, < \rangle$. Nechť dále R je relace
   $$\{ [x,y] \; ; \; |x-y| = 1 \}$$
   Dokažte, že i ve struktuře $\langle N, R \rangle$ je každá jednoprvková množina definovatelná.

3. Dokažte, že množina všech sudých čísel není definovatelná ve struktuře $\langle N, 0, .+1 \rangle$.
   Návod. Využijte cvičení 16 v par. 1.4.

4. Je-li relace $R \subseteq N^k$ definovatelná ve struktuře $\langle N, 0, .+1 \rangle$, pak existuje číslo m takové, že pro každé i a každou volbu čísel $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_k$ množina
   $$\{ x \; ; \; [a_1, \ldots, a_{i-1}, x, a_{i+1}, \ldots, a_k] \in R \}$$
   nebo její komplement má nejvýše m prvků. Dokažte. Platí analogická věta i pro strukturu $\langle N, 0, .+1, < \rangle$? Rozhodněte, zda relace $<$ je ve struktuře $\langle N, 0, .+1 \rangle$ definovatelná.

5. Dokažte, že funkce $x \mapsto x+1$ je definovatelná ve struktuře $\langle N, < \rangle$.

6. Dokažte, že ve struktuře $\langle N, 0, .+1, \cdot \rangle$ je definovatelné sčítání přirozených čísel.
   Návod. Ověřte a využijte implikaci
   $$a + b = c \Rightarrow (1+ac)(1+bc) = 1 + c^2(1+ab)$$

7. Nechť $\mathbf{M}$ je libovolný nestandardní model Peanovy aritmetiky. Dokažte, že standardní část modelu $\mathbf{M}$ (t.j. množina hodnot všech numerálů) není v $\mathbf{M}$ definovatelná.

8. Dokažte, že následující formule jsou dokazatelné v PA
   $$\begin{array}{ll} \overline{0} + x = x & S(y) + x = S(y+x) \\ (z+y)+x = z+(y+x) & y+x = x+y \\ \overline{0} \cdot x = \overline{0} & S(y) \cdot x = y \cdot x + x \end{array}$$

$$
\begin{array}{ll}
y \cdot x = x \cdot y & z \cdot (y + x) = z \cdot y + z \cdot x \\
(z \cdot y) \cdot x = z \cdot (y \cdot x) & \forall x \exists y (x = y + y \vee x = y + y + \overline{1}) \\
y + x = x \rightarrow y = \overline{0} & \forall x \forall y \exists u (u + x = y \vee u + y = x) \\
x \leq y \mathbin{\&} y \leq z \rightarrow x \leq z & x \leq x \\
x \leq y \mathbin{\&} y \leq x \rightarrow x = y & x \leq y \vee y \leq x \\
x \leq S(y) \equiv (x = S(y) \vee x \leq y) &
\end{array}
$$

9. Dokažte, že je-li φ libovolná aritmetická formule, pak každá z následujících formulí je dokazatelná v PA

$$\forall u \leq x \exists v \varphi(u,v) \rightarrow \exists y \forall u \leq x \exists v \leq y \varphi(u,v)$$

$$\begin{aligned}\forall x \forall y (\varphi(x,y) \mathbin{\&} x \neq \overline{0} \rightarrow \exists u \exists v (\varphi(u,v) \mathbin{\&} v < y)) \\ \rightarrow (\exists x \exists y \varphi(x,y) \rightarrow \exists y \varphi(\overline{0}, y))\end{aligned}$$

$$\begin{aligned}\varphi(\overline{0},\overline{0}) \mathbin{\&} \forall x \forall y (\varphi(x,y) \rightarrow \varphi(x, S(y))) \mathbin{\&} \forall x (\forall y \varphi(x,y) \rightarrow \varphi(S(x), \overline{0})) \\ \rightarrow \forall x \forall y \varphi(x,y)\end{aligned}$$

10. Rozhodněte, zda platí: je-li x substituovatelná za v ve formuli φ, pak každá formule tvaru

$$\varphi_v(\overline{0}) \mathbin{\&} \forall x (\varphi_v(x) \rightarrow \varphi_v(S(x))) \rightarrow \forall x \varphi_v(x)$$

je dokazatelná v PA.
Návod. Celá formule může mít volné výskyty proměnné x.

11. Rozhodněte, zda platí
(a) Je-li $\exists x \varphi(x)$ aritmetická sentence taková, že PA $\vdash \exists x \varphi(x)$, pak existuje číslo n takové, že PA $\vdash \varphi(\overline{n})$.
(b) Je-li $\exists x \varphi(x)$ aritmetická sentence taková, že φ je omezená a PA $\vdash \exists x \varphi(x)$, pak existuje číslo n takové, že PA $\vdash \varphi(\overline{n})$.
Návod. V (a) vezměte omezenou formuli $\psi(y)$, pro kterou platí $\mathbf{N} \models \forall y \psi(y)$, ale PA $\nvdash \forall y \psi(y)$. Existenci takové sentence zaručuje první Gödelova věta. Dále uvažujte sentenci $\exists x \forall y (\psi(y) \vee \neg \psi(x))$.

12. Rozhodněte, zda platí
(a) Jsou-li φ, ψ aritmetické sentence takové, že PA $\vdash \varphi \vee \psi$, pak platí PA $\vdash \varphi$ nebo PA $\vdash \psi$.
(b) Jsou-li φ, ψ aritmetické Σ_1-sentence takové, že PA $\vdash \varphi \vee \psi$, pak platí PA $\vdash \varphi$ nebo PA $\vdash \psi$.
Návod k (b). Použijte Σ_1-korektnost na disjunkci $\varphi \vee \psi$ a Σ-úplnost zvlášť na φ a na ψ.

13. Tvrzení, že každé sudé číslo větší než 3 je součtem dvou prvočísel, se nazývá Goldbachova domněnka a není o něm známo, zda je pravdivé. Dokažte, že je-li toto tvrzení nezávislé na PA, pak platí v **N**.
Návod. Určete pozici daného tvrzení v aritmetické klasifikaci formulí a použijte Σ-úplnost.

14. Dokažte, že model $\mathbf{N}^- + \mathbf{Z}^-$ se nedá rozšířit (ani funkcí, která není definovatelná) na model teorie $Th(\langle N, +, 0, .+1\rangle)$.
Návod. Vezměte nestandardní prvek a a uvažujte, zda $a + a$ může být v konečné vzdálenosti od a nebo od 0. Jedno z toho by nastat muselo.

15. Nechť **M** je spočetný nestandardní model teorie PA. Uvažujte relaci $\sim$ jako v příkladu 6 paragrafu 1.4: $a \sim b$ právě když vzdálenost a a b je konečná. Dokažte, že když $a_1 \sim a_2$ a $b_1 \sim b_2$, pak $a_1 + b_1 \sim a_2 + b_2$. Tedy $\sim$ je kongruence vůči sčítání. Je $\sim$ kongruentní i vůči násobení? Uvažujte dále jen uspořádání. Dokažte, že $\langle M - \{x\,; x \sim 0\}, <\rangle / \sim$, t.j. struktura vzniklá z $\langle M, <\rangle$ odstraněním standardní části a faktorizací podle ekvivalence $\sim$, je izomorfní s uspořádáním racionálních čísel $\langle Q, <\rangle$.
Návod. Uvažujte o dvojnásobcích, polovinách a aritmetických průměrech nestandardních resp. dvojic nestandardních prvků podobně jako v cvičení 14.