Jiří Hořejš; Alois Glanc
O vztahu formy a obsahu v matematice a logice. II

Pokroky matematiky, fyziky a astronomie, Vol. 12 (1967), No. 2, 67--84

Persistent URL: http://dml.cz/dmlcz/137063

POKROKY MATEMATIKY, FYZIKY A ASTRONOMIE
ROČNÍK XII — ČÍSLO 2

O VZTAHU FORMY A OBSAHU V MATEMATICE A LOGICE II

JIŘÍ HOŘEJŠ, ALOIS GLANC, Brno

První část tohoto článku byla otištěna v Pokrocích MFA *10* (1965), č. 6, str. 325.

§ 4

4.1. *Sémantické zadání predikátového počtu*

Predikátem o n proměnných $P(x_1, \ldots, x_n)$ budeme rozumět výraz obsahující tyto proměnné a označující n-člennou relaci nad nějakým oborem $\mathfrak{M}$. Např. predikát $P(x, y)$ může označovat relaci „$x < y$" nad množinou přirozených čísel N či relaci „x je bratr y" nad množinou všech lidí. Výroky budeme považovat za predikáty s nulovým počtem (volných — viz níže) proměnných.

Uvažme nějakou množinu $\mathscr{M}$ predikátů; prvky $\mathscr{M}$ budeme nazývat *atomárními predikáty*. Z nich budeme tvořit další predikáty jednak užitím výrokových spojek (takže např. „jestliže $P(x, y)$, pak $Q(x, y, z)$" — označující např. relaci „jestliže $x = y$, pak $x < y + z$" nad N — je další predikát o třech proměnných), jednak *kvantifikací*. Při kvantifikaci vzniká z predikátu $X(x)$, obsahujícího proměnnou x (a možná další proměnné) predikát „pro každé x je $X(x)$" (tzv. *obecná* kvantifikace) nebo „existuje x tak, že $X(x)$" (tzv. *existenční* kvantifikace). Příklad: „Existuje x tak, že pro každé y je $P(x, y, z)$" je predikát o jediné *volné* proměnné z; proměnná x, resp. y se stala *vázanou* existenčním, resp. obecným kvantifikátorem.

Z predikátů lze získat výroky buď kvantifikací, nebo *substitucí* prvků ze zvoleného oboru $\mathfrak{M}$ za proměnné*) tak, že se zbavíme všech volných proměnných; např. ozna-

*) Připomínáme, že jsme se dohodli nevěnovat zvláštní pozornost rozdílu mezi věcí a jejím názvem. Podobné tolerance (ostatně dobře známé z matematiky) budeme využívat i nadále. Neškodí samozřejmě, když si čtenář uvědomí, že v oblasti sémantiky máme na mysli věci (např. čísla) a ve výrocích o těchto věcech vystupují jejich názvy (symboly je zapisující, např. číslice), zatímco v oblasti syntaxe jsou předmětem vyšetřování symboly, o nichž se vyjadřujeme pomocí metateoretických názvů, za něž často slouží samy symboly uzavřené do uvozovek. Srovnej tvrzení: „*20* je dělitelné *10*" a „„*20*" a „*10*" mají stejné druhé písmeno". Tím, že nedodržujeme explicitně všude přísné rozlišování věcí, názvů věcí, resp. názvů názvů věcí, zjednodušujeme vyjadřování směrem k běžné řeči. Tak doufáme, že nedojde k nedorozumění použitím rčení: „dosazení prvku za proměnnou" místo přesnějšího: „dosazení názvu prvku na místo symbolu proměnné" ap. Také termínu „výrok" si dovolíme užívat ve dvojím smyslu: výrokem budeme rozumět jak výraz typu „$1 < 1 + 3$", tak výraz tvaru „jestliže P, pak Q", v němž P, Q pouze označují některé konkrétní výroky.

čuje-li predikát $Q(x, y, z)$ relaci $x < y + z$ nad N, dostaneme výroky „$1 < 1 + 3$“ (pravdivý výrok), „existuje x tak, že pro každé y je $x < y + 2$“ (pravdivý výrok), „existuje x tak, že pro každé y a pro každé z je $x < y + z$“ (nepravdivý výrok).

Relaci nad $\mathfrak{M}$ označenou nějakým atomárním predikátem o n proměnných lze zadat určením podmnožiny $\mathfrak{N} \subset \mathfrak{M}^n$: z predikátu se stane pravdivý výrok po substituci právě těch n-tic za proměnné predikátu, které leží v $\mathfrak{N}$. Je-li při tom $\mathfrak{N}$ rozhodnutelná (generovatelná), nazývá se tak i příslušná relace. Běžně užívané relace jsou obvykle rozhodnutelné a bývají zadány vztahy z jiných částí matematiky. Příklad: nahoře uvedenou relaci nad N: $x < y + z$ lze zadat množinou $\{(0, 0, 1), (0, 1, 0), (1, 0, 2), (1, 2, 0), \ldots\}$, která je sice nekonečná, ale rozhodnutelná. Nad konečnými obory je každá relace rozhodnutelná, nad nekonečnými existují dokonce negenerovatelné relace.

Predikátový počet dává hlouběji nahlédnout do logické struktury matematických (i jiných) úsudků: pravdivostní hodnota výroku, který vznikne z nějakého atomárního predikátu substitucí, závisí na tom, kterou relaci predikát označuje a na dosazených prvcích: je jejich pravdivostní funkcí. Je-li při tom pro zvolenou množinu $\mathfrak{M}$ struktura nějakého predikátu taková, že ať atomární predikáty označují jakoukoliv relaci (o stejném počtu proměnných) nad $\mathfrak{M}$ (ať např. $P(x, y, z)$ označuje nad N „$x < y + z$“ nebo „$x + y = z$“ nebo „x dělí yz“ nebo ...) a ať jakkoliv dosadíme prvky z $\mathfrak{M}$ za volné proměnné (neboli, což je totéž: při dodatečném přidání zleva obecných kvantifikátorů vážících všechny volné proměnné), je výsledný výrok vždy pravdivý, pak tento predikát X nazveme *tautologií* (*predikátového počtu*) *nad* $\mathfrak{M}$. Je-li nějaký predikát tautologií nad libovolnou neprázdnou množinou, mluvíme prostě o *tautologii*; množinu všech tautologií označíme $\mathscr{T}_p$.

Triviálními příklady tautologií jsou tautologie výrokového počtu. Nad libovolným oborem $\mathfrak{M}$ je tautologií výraz: „jestliže pro každé x je $X(x)$, pak existuje x tak, že $X(x)$“, zatímco obrácená implikace „jestliže existuje x tak, že $X(x)$, pak pro každé x je $X(x)$“ je tautologií jedině nad jednoprvkovými množinami $\mathfrak{M}$. Poslední tvrzení nahlédne čtenář nejsnáze, když si uvědomí, že nad konečnými množinami je možno kvantifikátory nahradit výrokovými spojkami; je-li např. $\mathfrak{M} = \{0, 1, \ldots, m\}$, je predikát „pro každé x je $X(x)$“ totéž co „$X(0) \wedge X(1) \wedge \ldots \wedge X(m)$“, kde $X(i)$ značí výsledek substituce čísla i za proměnnou x. Analogicky lze nahradit existenční kvantifikaci m-násobným užitím spojky „nebo“. Tyto vlastnosti umožňují nahradit libovolný predikát nad konečným oborem $\mathfrak{M}$ jeho výrokovým ekvivalentem (nad $\mathfrak{M}$) a tím mimo jiné např. prověřit, jde-li o tautologii (nad $\mathfrak{M}$) prostředky výrokového počtu (viz **3.1**).

Uvažme např., zda predikát „Existuje-li x tak, že pro každé y je $X(x, y)$, potom pro každé y existuje x tak, že platí rovněž $X(x, y)$“ je tautologií nad $\mathfrak{M} = \{0, 1\}$. Provádějme postupně výše zmíněné nahrazení. Dostaneme: „Existuje-li x tak, že $(X(x, 0) \wedge X(x, 1))$, potom pro každé y $(X(0, y) \vee X(1, y))$“ a dále „$[(X(0, 0) \wedge X(0, 1)) \vee (X(1, 0) \wedge X(1, 1))] \to [(X(0, 0) \vee X(1, 0)) \wedge (X(0, 1) \vee X(1, 1))]$“. Označme ještě výrok $X(0, 0)$ $[X(0, 1), X(1, 0), X(1, 1)]$ písmenem $P[Q, P', Q']$; vidíme, že dostáváme tautologii „$[(P \wedge Q) \vee (P' \wedge Q')] \to [(P \vee P') \wedge (Q \vee Q')]$“.

Jako další příklad můžeme uvážit, zda už zmíněný predikát „Existuje-li x tak, že $X(x)$, potom pro každé x je $X(x)$“ je tautologií jednak nad oborem $\mathfrak{M} = \{0\}$ a jednak zase nad oborem $\mathfrak{M} =$

$= \{0, 1\}$. Pro $\mathfrak{M} = \{0\}$ má příslušný výrokový ekvivalent tvar „$X(0) \to X(0)$“, tj. „$P \to P$“, a patří tedy do $\mathscr{T}_V$ a nad oborem $\mathfrak{M} = \{0, 1\}$ je „$(X(0) \vee X(1)) \to (X(0) \wedge X(1)$“, tj. „$(P \vee Q) \to (P \wedge Q)$“, takže nepatří do $\mathscr{T}_V$.

Posledním příkladem tautologie buď predikát s volnou proměnnou: „$X(x) \to \bigvee x\, X(x)$“.

4.2. *Syntaktická výstavba predikátového počtu*

Definujeme:

Abeceda $\mathbf{S}_P = \mathbf{S}_V \cup \{\wedge, \vee, x, y, z\}$ (nové symboly značí v interpretaci po řadě: pro každé; existuje; proměnné budeme značit $x, y, z, x', y', \ldots$).

Množina formulí $\mathbf{F}_P$: (*i*) do $\mathbf{F}_P$ patří všechny atomární výrazy: $P, Q, R, P', P(x)$, $P(x')$, $P'(xy)$, $P(xx')$, ... (v interpretaci: atomární predikáty o proměnných uvedených — v plném počtu — v závorce), (*ii*) jestliže $X, Y \in \mathbf{F}_P$, pak do $\mathbf{F}_P$ patří též $(X) \wedge (Y), (X) \vee (Y), (X) \to (Y), \sim(X), \bigwedge a(X), \bigvee a(X)$, kde a označuje proměnnou, (*iii*) jiné výrazy než ty, které byly definovány v předchozích bodech, do $\mathbf{F}_P$ nepatří.

Množina $\mathbf{F}_P$ je opět rozhodnutelná; jejím prvkem je např. výraz „$(P''(x'''z'y)) \vee \vee (\bigwedge z'(P(xz')))$“.

Z formálních důvodů zjednodušíme opět způsob zápisu formulí (viz **3.2**); vedle již přijatých konvencí o vypouštění závorek [přičemž budeme předpokládat, že kvantory $\bigwedge, \bigvee$ váží silněji než výrokové spojky, takže např. $\bigwedge x\, P(x) \vee Q(x)$ značí $(\bigwedge x(P(x))) \vee (Q(x))$] se dohodneme m-tici čárek zapisovat číslem m, takže nahoře uvedenou formuli přepíšeme jako $P^2(x^3z^1y) \vee \vee \bigwedge z^1 P(xz^1)$.

Do syntaxe predikátového počtu se přenesou snadno i některé další pojmy známé již ze sémantiky: Jestliže se proměnná a vyskytuje ve formuli Y a formule $\bigwedge a(Y)$, resp. $\bigvee a(Y)$ je částí formule X, pak příslušný výskyt proměnné a v Y nazýváme vázaný v X; není-li daný výskyt proměnné vázaný v X, je v X volný. První (zleva) výskyt proměnné z^1 v nahoře uvedeném příkladě formule je tedy v této formuli volný, druhý vázaný. Dále si čtenář snadno uvědomí, že na půdě syntaxe je možno definovat i pojem výrokového ekvivalentu dané formule nad konečnou množinou $\mathfrak{M}$ (pro zvolenou množinu $\mathfrak{M}$ tak každé formuli z $\mathbf{F}_P$ bude přiřazena některá formule z $\mathbf{F}_V$). V úvahách o vlastnostech našeho formálního systému budeme také často potřebovat označit výsledek současné substitutce proměnných $b_1, \ldots, b_n$ za navzájem různé volné proměnné (po řadě) $a_1, \ldots, a_n$ v nějaké formuli X; pro výslednou formuli užijeme (metateoretického) symbolu

$$\int \begin{matrix} a_1 a_2 \ldots a_n \\ b_1 b_2 \ldots b_n \end{matrix} X .$$

Nestane-li se žádná z proměnných $b_1, \ldots, b_n$ vázanou, píšeme

$$\oint \begin{matrix} a_1 a_2 \ldots a_n \\ b_1 b_2 \ldots b_n \end{matrix} X .$$

Je tedy např.

$$\oint_{yy\ zx}^{xz^2yz} P(xz^2) \vee \sim Q(y) \vee \bigwedge z\, R(z) = P(yy) \vee \sim Q(z) \vee \bigwedge z\, R(z)$$

Množina axiómů $\mathbf{A}_P$: (1) $X \to (Y \to X)$, (2) $(X \to Y) \to ((X \to (Y \to Z)) \to (X \to Z))$, (3) $X \to (Y \to X \wedge Y)$, (4) $X \wedge Y \to X$, (5) $X \wedge Y \to Y$, (6) $X \to X \vee Y$, (7) $Y \to (X \vee Y)$, (8) $(X \to Z) \to ((Y \to X) \to (X \vee Y \to Z))$, (9) $(X \to Y) \to ((X \to \sim Y) \to \sim X)$, (10) $\sim \sim X \to X$, (11) $\bigwedge aX \to \oint_b^a X$, (12) $\oint_b^a X \to \bigvee aX$,

kde $X, Y, Z \in \mathbf{F}_P$.

Množina $\mathbf{A}_P$ je zde nekonečná, ale zřejmě rozhodnutelná, neboť je vyjádřena pomocí konečného počtu tzv. axiómových schémat.

Odvozovací pravidla $\mathbf{O}_P$: 1. pravidlo modus ponens $X, X \to Y \vdash Y$, 2. $Z \to X \vdash Z \to \bigwedge aX$, 3. $X \to Z \vdash \bigvee aX \to Z$, kde Z neobsahuje proměnnou a jako volnou.

Položíme opět $\mathbf{T}_P = \mathbf{O}_P(\mathbf{A}_P)$. Proces odvozování ilustrujeme opět na příkladě; ukážeme, že

„$\bigvee x \bigwedge y\, P(xy) \to \bigwedge y \bigvee x\, P(xy)$“ patří do $\mathbf{T}_P$:
Z_1: $\bigwedge y\, P(xy) \to P(xy)$ axiómové schéma 11
Z_2: $P(xy) \to \bigvee P(xy)$ axiómové schéma 12
Z_3: $(P(xy) \to \bigvee x\, P(xy)) \to (\bigwedge y P(xy) \to (P(xy) \to \bigvee x\, P(xy)))$ axiómové schéma 1
Z_4: $(\bigwedge y\, P(xy) \to (P(xy) \to \bigvee x\, P(xy)))$ aplikací modu ponens na Z_2 a Z_3
Z_5: $(\bigwedge y\, P(xy) \to P(xy)) \to ((\bigwedge y\, P(xy) \to (P(xy) \to \bigvee x\, P(xy)) \to (\bigwedge y\, P(xy) \to \to \bigvee x\, P(xy)))$ axiómové schéma 2
Z_6: $(\bigwedge y\, P(xy) \to (P(xy) \to \bigvee x\, P(xy)) \to (\bigwedge y\, P(xy) \to \bigvee x\, P(xy))$ aplikací modu ponens na Z_1 a Z_5
Z_7: $\bigwedge y\, P(xy) \to \bigvee x\, P(xy)$ aplikací modu ponens na Z_4 a Z_6
Z_8: $\bigwedge y\, P(xy) \to \bigwedge y \bigvee x\, P(xy)$ aplikací odvozovacího pravidla 2 na Z_7
Z_9: $\bigvee x \bigwedge y\, P(xy) \to \bigwedge y \bigvee x\, P(xy)$ aplikací odvozovacího pravidla 3 na Z_8

Sémantickou bezespornost, $\mathbf{T}_P \subset \mathscr{T}_P$, lze ukázat obdobně jako v případě výrokového počtu. Tautologičnost dodatečných axiómů (11), (12) i platnost odvozovacích pravidel 2 a 3 vyplývá přímo z definice tautologie s přihlédnutím ke skutečnosti, že volné proměnné se interpretují, jako kdyby byly vázány obecným kvantifikátorem; všimněme si také, že pravidlo 2 zachycuje následující skutečnost: podaří-li se odvodit vlastnost nějaké proměnné a z předpokladů, neobsahujících tuto proměnnou jako volnou, je možno usoudit, že tuto vlastnost má za daných předpokladů každý prvek uvažovaného oboru; oprávněnost pravidel si čtenář nejlépe uvědomí na příkladě odvození, které je uvedeno nahoře.

Tvrzení, že predikátový počet je *sémanticky úplný*, patří k základním výsledkům

matematické logiky (tzv. Gödelova věta o úplnosti); jeho diskusi odložíme do následujícího odstavce.

Než přistoupíme k důkazu dalších dvou vlastností predikátového počtu, připomeneme, že při zvolené konečné množině $\mathfrak{M}$ lze ke každé formuli z $\mathbf{F}_P$ přiřadit formuli z $\mathbf{F}_V$ jako výrokový ekvivalent (nad $\mathfrak{M}$) dané formule. Nepříliš komplikovanými úvahami se dá zjistit, že při tom každé odvoditelné formuli (tj. formuli z $\mathbf{T}_P$) je takto přiřazena tautologie výrokového počtu (tj. formule z $\mathbf{T}_V$): stačí uvážit, že formule z $\mathbf{A}_P$ mají za své výrokové ekvivalenty tautologie a že se tato vlastnost zachovává aplikací odvozovacích pravidel $\mathbf{O}_P$.

Syntaktickou bezespornost, $\mathbf{T}_P \neq \mathbf{F}_P$, lze nyní dokázat velmi jednoduše: stačí uvážit libovolnou formuli z $\mathbf{F}_P$, jejíž výrokový ekvivalent nad nějakou konečnou množinou (např. $\mathfrak{M} = \{0\}$) nepatří do $\mathbf{T}_V$; takovou je však např. zase formule P.

Predikátový počet na rozdíl od výrokového však *není syntakticky úplný*. K důkazu stačí uvést příklad formule, která 1. není odvoditelná (nepatří do $\mathbf{T}_P$), ale 2. jejíž přidání k axiómům nenarušuje syntaktickou bezespornost. Za takovou formuli stačí vzít např. $\bigvee x\, P(x) \to \bigwedge x\, P(x)$. Vlastnost 2. plyne z toho, že výrokový ekvivalent nad $\mathfrak{M} = \{0\}$ této formule patří opět do $\mathbf{T}_V$, vlastnost 1. z toho, že její výrokový ekvivalent (viz výše) nad $\mathfrak{M} = \{0, 1\}$ není již prvkem $\mathbf{T}_V$.

Syntaktická neúplnost není na závadu našemu systému. Spíše naopak: přidáním neodvoditelné formule X (resp. řady takových formulí) k axiómům $\mathbf{A}_P$ získáme v množině $\mathbf{O}_P(\mathbf{A}_P \cup \{X\}) = \mathbf{O}_P(\mathbf{T}_P \cup \{X\})$ množinu formulí ne sice již tautologicky platných, ale všech formulí, které jsou logickými důsledky (tj. které možno aparátem predikátového počtu odvodit z) dodatečného „mimologického" axiómu X, resp. axiomů dalších. Právě tímto způsobem se tvoří formální systémy matematických (příp. i jiných) teorií. Pro námi uvedený příklad dostáváme tak teorii všech jednoprvkových oborů. (Predikátový počet jako základ formalizace teorií poznáme ještě dále; dobrou představu o věci má čtenář možnost získat z článku [H_2]).

Bez důkazu uvedeme ještě jednu důležitou vlastnost predikátového počtu, v níž se podstatně liší od počtu výrokového: je totiž *nerozhodnutelný*, tj. neexistuje algoritmus umožňující o dané (libovolné) formuli X z $\mathbf{F}_P$ rozhodnout, zda $X \in \mathbf{T}_P$ či $X \notin \mathbf{T}_P$, tj. (vzhledem k tomu, že $\mathbf{T}_P = \mathscr{T}_P$) zda X je tautologie.

4.3. *Gödelova věta o úplnosti predikátového počtu*

Aby si čtenář mohl učinit představu o technice práce v oblasti matematické logiky, všimneme si v tomto a následujícím paragrafu poněkud detailněji některých důkazových obratů; i tak bude ovšem třeba odvolat se v podstatě pouze na několik výsledků. Ve zbývající části článku se pak zase omezíme na rámcový způsob výkladu.

K důkazu o sémantické úplnosti by zřejmě stačilo ukázat, že pro libovolnou formuli X z $\mathbf{F}_P$ je buď $X \in \mathbf{T}_P$, nebo $X \notin \mathscr{T}_P$. Naznačíme tento důkaz pouze pro formule

speciálního tvaru (v tzv. *Skolemově formě*), totiž pro formule, které lze zapsat ve tvaru

$$(*) \qquad \bigvee y^1 \bigvee y^2 \ldots \bigvee y^m \bigwedge z^1 \bigwedge z^2 \ldots \bigwedge z^n M\,, \quad m \geqslant 1\,, \quad n \geqslant 0\,,$$

kde M – tzv. *matice* formule – již neobsahuje kvantifikátory a žádné jiné proměnné než $y^1, \ldots, y^m, z^1, \ldots, z^n$. Dá se totiž ukázat, že k libovolné formuli Y lze efektivním způsobem nalézt formuli X v uvedeném tvaru takovou, že $X \in \mathscr{T}_P$ právě když $Y \in \mathscr{T}_P$ (množina všech formulí tvaru (*) tvoří tzv. *třídu redukce*).

Celkem ne zvlášť obtížnými obraty (vytýkáním kvantifikátorů, přeznačením proměnných ap.) lze k dané formuli X, např. $X = \bigvee x\, Q(x) \wedge \bigwedge y\, P(xy)$, sestrojit nejprve formuli Z s ní ekvivalentní (v tom smyslu, že $X \leftrightarrow Z$, tj. $(X \to Z) \wedge (Z \to X)$, je tautologie) takovou, která začíná kvantifikátory (v libovolném pořadí) následovanými maticí bez kvantifikátorů [pro náš jednoduchý příklad dostaneme postupně $\bigvee x \bigwedge y(Q(x) \wedge P(zy))$, a tedy $Z = \bigwedge z \bigvee x \bigwedge y(Q(x) \wedge P(zy))$]. Přechod od takto získané *prenexové formy* ke Skolemově formě (u níž každý existenční kvantifikátor předchází všechny obecné) vyžaduje obecně dalších obratů.

Nechť je tedy dána formule (*) s maticí M, která představuje predikát o uvedených proměnných, $M = M(y^1, \ldots, y^m, z^1, \ldots, z^n)$; tento predikát je sestaven z jistých atomárních predikátů, např. $P(y^1 z)$, $Q(z^3)$, ... Všimněme si nejprve, že kdyby se podařilo odvodit predikát

$$\oint \begin{matrix} y^1 \ldots y^m z^1 & \ldots z^n \\ a_1 \ldots a_m a_{m+1} & \ldots a_{m+n} \end{matrix} M\,,$$

kde posledních n proměnných a_i jsou proměnné navzájem i od předchozích různé (tj. kdybychom po takto provedené substituci dostali výraz z T_V), bylo by možno odvoditi celou formuli X; důkaz je možno realizovat n-násobným užitím pravidla 2, m-násobným užitím axiómu 12 a ovšem pravidla modus ponens (z axiómu 12 plyne např. $\oint \begin{matrix} a_1 \ldots a_k \\ b \ \ldots b \end{matrix} X \to \bigvee a_1 \ldots \bigvee a_k X$).

Provedeme nyní řadu vhodných substitucí proměnných x^i ($x^0 = x, x^1, x^2, \ldots$) v matici M tak, aby na prvých m místech, tj. na místě původních proměnných $y^1, \ldots, y^m$) se vystřídaly jakožto indexy proměnných x^i všechny m-tice přirozených čísel, přičemž vždy na místech zbylých n proměnných budou figurovat proměnné různé od předchozích i navzájem. Dostaneme tak postupně výrazy $B_1, B_2, \ldots$.

Uvedený postup je možno upřesnit např. tím, že uspořádáme všechny m-tice přirozených čísel: $\langle k_1, \ldots, k_m \rangle$ je v tomto uspořádání před $\langle l_1, \ldots, l_m \rangle$, je-li $\max \{k_i\} < \max \{l_i\}$; v případě rovnosti posledních výrazů je uspořádání lexikografické. Označme j-tý člen k-té m-tice $[kj]$. Pak substituce, o které jde, definujeme vztahem:

$$B_K = \int \begin{matrix} y^1 & \ldots y^m & z^1 & \ldots z^n \\ x^{[K1]} & \ldots x^{[Km]} & x^{K(n-1)+1} & \ldots x^{Kn} \end{matrix} M\,.$$

Položme nyní $C_k = B_1 \vee B_2 \vee \ldots \vee B_k$. Rozlišme dva případy:

1. Pro jisté k je $C_k \in \mathbf{T}_P$. V tomto případě lze odvodit i celou formuli $X : X \in \mathbf{T}_P$; důkaz indukcí podle k využívá obratů, které jsme nahoře naznačili (v podstatě pro případ $B_k \in \mathbf{T}_P$); detaily ponecháváme čtenáři.

2. Pro každé k je $C_k \notin \mathbf{T}_P$. Ukážeme, že v tomto případě není X tautologií nad N, a tedy ani — tím spíš — tautologií, tj. není $X \in \mathscr{T}_P$. Substituujme za proměnné $x^0, x^1, x^2, \ldots$ figurující ve formuli B_k ($k = 1, 2, \ldots$) po řadě čísla $0, 1, 2, \ldots$. Poněvadž žádné jiné proměnné v B_k nejsou, lze výsledek této substituce — označme ho $\tilde{B}_k$ — považovat za výraz výrokového počtu: $\tilde{B}_k$ sestává z výrazů jako $P(0, 3)$, $P(2, 5)$, $Q(7)$ ap., které mohou hrát role atomárních výroků (jde o jistou formu výrokového ekvivalentu nad množinou $\mathfrak{M} = \{0, 1, \ldots, t\}$, kde ovšem t roste s rostoucím k). Ve formulích $\tilde{B}_1, \tilde{B}_2, \ldots$ figuruje postupně celá řada takových atomárních výroků: uspořádejme je vhodně (nejlépe tak, jak vystupují zleva doprava v $B_1, B_2, \ldots$) a označme je $A_1, A_2, A_3, \ldots$. Každému atomárnímu výroku A_i lze přisoudit pravdivostní hodnotu $h_i = p$ nebo $= n$. Každým takovým ohodnocením definujeme částečně původní atomární predikáty (tj. určujeme relace nad N, které budou těmito predikáty označovány), z nichž se skládá matice M a současně je jím jednoznačně definována pravdivostní hodnota všech $\tilde{B}_k$. Položme nyní ještě $\tilde{C}_k = \tilde{B}_1 \vee \ldots \vee \tilde{B}_k$; poněvadž $C_k \notin \mathbf{T}_P$, platí samozřejmě $\tilde{C}_k \notin \mathbf{T}_V$. Představme si, že pro všechny možnosti volby hodnot $h_1, h_2, \ldots$ je hodnota některého $\tilde{C}_k$ rovna p; v tomto případě je ovšem $\tilde{C}_k$ tautologií výrokového počtu. Spor s $\tilde{C}_k \notin \mathbf{T}_V$ ukazuje, že existuje taková volba hodnot $h_1, h_2, \ldots$, že pro všechna k je hodnota $\tilde{C}_k$ rovna n; říkejme této volbě *vyvracející ohodnocení* formule X a definujme atomární predikáty z C_k v souhlase s vyvracejícím ohodnocením. Připomeňme nyní, že ať zvolíme jakkoliv m-tici čísel $i_1, \ldots, i_m$, bude tato m-tice dosazena za prvých m proměnných v M ve vhodné formuli B_k; kdyby existovala čísla $i_1, \ldots, i_m$ tak, že pro libovolná čísla $j_1, \ldots, j_n$ je $M(i_1, \ldots, i_m, j_1, \ldots, j_n)$ pravdivý výrok, měl by být pravdivý výrok B_k, který vznikne uvažovanou substitucí $i_1, \ldots, i_m$ za prvých m-proměnných a nějakou substitucí $j_1, \ldots, j_n$ za zbývající proměnné. Není tedy pravda, že formule $X = \bigvee y^1 \ldots \bigvee y^m \bigwedge z^1 \ldots \bigwedge z^n M$ je tautologií nad oborem přirozených čísel N.

4.4. *Procedura Friedmanové*

Jak bylo naznačeno již v odst. **4.2**, predikátový počet je už velmi mocný prostředek k tomu, aby v něm bylo možno formalizovat dostatečně zajímavé matematické teorie (v § 5 ukážeme příklad takové formalizace). Jsou-li $X_1, X_2, \ldots, X_m$ mimologické axiómy takového matematického formalizovaného systému, pak otázka, zda Y plyne z axiómů $X_1, \ldots, X_m$ je ekvivalentní otázce, zda $X_1 \wedge \ldots \wedge X_m \to Y \in \mathbf{T}_P$. V důsledku nerozhodnutelnosti množiny $\mathbf{T}_P$ je vhodné zaměřit se na hledání algoritmů, jež rozhodují nějaké (syntakticky zadané) podmnožiny množiny $\mathbf{F}_P$. Úvahy předchozího odstavce nám dávají možnost získat dostatečně obecný nástroj pro tyto účely. Z nich totiž plyne, že pro libovolnou formuli X ve Skolemově formě platí „$X \in \mathbf{T}_P$ právě když neexistuje vyvracející ohodnocení formule X“. J. Fried-

manová ([F]) sestrojila proceduru analyzující možnosti sestrojení vyvracejícího ohodnocení. Podala řadu pravidel, která z apriori možných ohodnocení vylučují ta, jež se nemohou stát vyvracejícím. Nezbude-li po aplikaci těchto pravidel žádný „kandidát", je předložená formule tautologií.

Pro konkrétnější představu naznačíme funkci jednoho z takových pravidel. Před jeho formulací především poznamenejme, že za pravdivostní hodnoty $h_1, \ldots, h_k$ (takové k-tici budeme říkat systém) atomárních výroků $A_{i1}, \ldots, A_{ik}$ figurujících ve výroku $\tilde{B}_i$ (v označení předchozího odstavce) má smysl — aby výsledná pravdivostní hodnota B_i byla n (jak chceme) — brát jen takové, které dosazeny po řadě za atomární predikáty $X_1, \ldots, X_k$, z nichž je tvořena matice M, dávají pravdivostní hodnotu n. Množinu všech takových systémů označíme S. Již toto omezení na množinu S může značně zmenšit počet vyšetřovaných systémů (v níže uvedeném příkladě sestává S pouze ze dvou systémů místo 2^6 apriori možných). Vlastní pravidlo — jehož oprávněnost má svůj původ ve skutečnosti, že uvažované systémy nemohou být pro jednotlivé B_i vybírány zcela nahodile (přiřadíme-li např. atomárnímu výroku $P(03)$, který figuruje např. v B_5, hodnotu n, nemůžeme atomárnímu výroku $P(03)$, který figuruje např. v B_{12}, přiřadit hodnotu p) — má následující tvar:

Pravidlo. Nechť $X_1, \ldots, X_N$ je soupis libovolných atomárních výrazů z M, jež obsahují pouze proměnné $y^1, \ldots, y^m$ a nechť $a_1, \ldots, a_m$ je nějaká m-tice vybraná z proměnných $y^1, \ldots, y^m, z^1, \ldots, z^n$. Nechť $h_1, \ldots, h_N$ je nějaká N-tice pravdivostních hodnot. Předpokládejme, že v S není systém, v němž $X_1 = h_1, \ldots, X_N = h_N$, a v němž libovolným dvěma atomárním výrazům Y_1, Y_2, pro něž

$$\int \begin{matrix} y^1 \ldots y^m z^1 \ldots z^n \\ a_1 \ldots a_m x^1 \ldots x^n \end{matrix} Y_1 = \int \begin{matrix} y^1 \ldots y^m z^1 \ldots z^n \\ a_1 \ldots a_m x^1 \ldots x^n \end{matrix} Y_2 ,$$

jsou přiřazeny tytéž hodnoty. Pak je možno vyloučit ze S všechny systémy, v nichž

$$\int \begin{matrix} y^1 \ldots y^m \\ a_1 \ldots a_m \end{matrix} X_1 = h_1, \ldots, \int \begin{matrix} y^1 \ldots y^m \\ a_1 \ldots a_m \end{matrix} X_N = h_n .$$

[Abychom mohli tohoto pravidla vůbec užít, je třeba, aby matice M obsahovala všechny tzv. „přípustné" atomární predikáty, tj. obsahuje-li X $(a_1, \ldots, a_k)$, pak musí také obsahovat X $(b_1, \ldots, b_k)$, kde $b_1, \ldots, b_k$ je libovolná k-tice vybraná z proměnných $y^1, \ldots, y^m, z^1, \ldots, z^m$. Matici M lze vždy doplnit tak, aby obsahovala všechny přípustné atomární predikáty. V našem případě stačí brát místo M matici $M \wedge (X(b_1, \ldots, b_k) \vee \sim X(b_1, \ldots, b_k))$.]

Příklad. Nechť je dána formule

$$\bigvee y^1 \bigvee y^2 \bigwedge z((P^1(y^1) \vee P^2(y^1) \vee \sim P^1(y^2) \vee \sim P^2(y^2) \vee \sim P^1(z) \vee P^2(z)) \wedge$$
$$\wedge (P^1(y^1) \vee \sim P^2(y^1) \vee P^1(y^2) \vee \sim P^2(y^2) \vee \sim P^1(z) \vee P^2(z)) ,$$

jejíž matici odpovídá množina S vyvracejících systémů: $S = \{s_1, s_2\}$

$$\begin{array}{cccccccc} & P^1(y^1) & P^2(y_1) & P^1(y^2) & P^2(y^2) & P^1(z) & P^2(z)\,, \\ s_1 & n & n & p & p & p & n\,, \\ s_2 & n & p & n & p & p & n\,. \end{array}$$

V S není systém, v němž $P^1(y^1) = p$, $P^2(y^2) = n$. Aplikujíce *Pravidlo* vyloučíme tedy ze S ty systémy, pro něž

$$\int \begin{matrix} y^1 y^2 \\ z\ y^2 \end{matrix} P^1(y^1) = P^1(z) = p \quad \text{a} \quad \int \begin{matrix} y^1 y^2 \\ z\ y^2 \end{matrix} P^2(y^1) = P^2(z) = n\,.$$

Zbude tedy prázdná množina vyvracejících systémů, což znamená, že naše formule náleží do $\mathbf{T}_P$.

Existuje celá řada speciálních podtříd formulí predikátového počtu, které mají důležitou vlastnost: jsou rozhodnutelné. Mezi takové třídy patří např. třída všech formulí, v jejichž prenexové formě vystupují nejprve kvantifikátory obecné a pak teprve všechny existenční. Že nejde o zvlášť úzkou speciální třídu formulí, ukazuje fakt, že všechny formule predikátového počtu uvedené ve slavném Russelově-Whiteheadově díle Principia mathematica se dají převést na tento tvar. Formule této třídy se dají rozhodnout různými algoritmy; jeden z nejefektivnějších — a nejvhodnějších k zpracování na počítači — poskytuje opět procedura Friedmanové. Ukazuje se, že pro formule této třídy ukáží pravidla procedury, že žádné vyvracející ohodnocení neexistuje, právě když předložená formule je tautologií. Procedura je pro tento případ tedy procedurou rozhodující.

Stejnou vlastnost mají i další třídy, např. ty, jejichž formule v prenexové formě mají posloupnosti kvantifikátorů tvaru

$$\wedge \ldots \wedge \vee \wedge \ldots \wedge \quad \text{nebo} \quad \wedge \ldots \wedge \vee \vee \wedge \ldots \wedge\,.$$

4.5. Gentzenův systém predikátového počtu

I pro predikátový počt platí to, co bylo řečeno pro výrokový počet v odstavci **3.2**: je možná celá řada více či méně podobných formálních systémů, které ho popisují stejně dokonale. Rozšíříme-li např. množinu $\mathbf{S}_P$ o prvky „;“ a „$\supset$“ a definujeme-li množinu $\mathbf{F}_{GP}$ jako množinu sestávající z výrazů typu $\alpha \supset \beta$, kde písmeny řecké abecedy budeme značit posloupnosti prvků z $\mathbf{F}_P$ oddělených středníkem, pak při vhodném doplnění množiny $\mathbf{O}_V$ odvozovacích pravidel (o pravidle týkající se kvantifikátorů a mající podobný tvar jako pravidla z $\mathbf{O}_P$) je možno z axiómů spadajících pod schéma $\alpha; X; \beta \supset \gamma; X; \delta$ (rozdíl proti $\mathbf{A}_G$ záleží v tom, že všechny uvažované formule patří nyní do širší třídy $\mathbf{F}_{GP}$) odvodit výrazy, jejichž množina — při interpretaci analogické té, kterou jsme poznali v **3.3**, odpovídá množině všech tautologií predikátového počtu.

Jak víme, odvozovací pravidla systému z **3.3** se dala obrátit, takže systém byl vhodný pro rozhodování formulí výrokového počtu strojem; k dané formuli, která byla odvoditelná, dokonce nebylo těžké najít její odvození. Něco podobného nemůžeme ovšem očekávat od jakéhokoliv systému popisujícího predikátový počet: vylučuje to jeho nerozhodnutelnost. Je však možné, že přesto úloha hledat důkazy odvoditelných formulí může být v jednom systému vzhledem k mohutnosti a jisté „přirozenosti" jeho odvozovacího aparátu pohodlnější než v druhém — a ukazuje se, že tuto vlastnost výhodné *heuristiky* zachovává Gentzenův systém (jehož popis jsme právě stručně naznačili) i pro predikátový počet. Navíc platí, že pro vhodné podtřídy formulí jsou naznačená odvozovací pravidla obratitelná a tvoří pak rozhodující proceduru jako v případě počtu výrokového. Zájemce o detailnější diskusi odkazujeme zase na práci Hao Wanga [W]; při jejím studiu využije některé z myšlenek uvedených v předchozích odstavcích.

§ 5.

Čtenář má jistě dobrou představu o intuitivní aritmetice, zná, umí dokázat a užívá řadu jejích tvrzení. Nebudeme se proto nijak vzlášť zabývat množinami $\mathscr{F}_A$ a $\mathscr{T}_A$; připomeneme jen, že do aritmetiky zařadíme ty výroky o přirozených číslech, které je možno utvořit pomocí specificky aritmetických predikátů $x = y + z$, $x = y\,z$ výrazovými prostředky predikátového počtu. Čtenář si snadno všimne, že vhodnými definicemi je možno takto do aritmetiky započítat běžné výroky o dělitelnosti, rozkladech v prvočísla atd. Hlavní úkol bude nyní záležet v tom, nalézt vhodný formální ekvivalent této teorie, to jest formální systém — *formální aritmetiku* — který by dobře vystihoval sémanticky chápanou aritmetiku. Není těžké navrhnout systém, který z historického hlediska snadno obstojí: již z počátku tohoto století je známa Peanova axiomatika aritmetiky; přidáme-li k vhodně formalizovaným Peanovým axiómům aparát predikátového počtu, měla by vzniknout hledaná teorie. Ukazuje se však, že takto stvořená teorie není sémanticky úplná a že dokonce žádný formální systém není s to v tomto smyslu dokonale zachytit aritmetiku (a ani žádnou jinou teorii, která je dostatečně „bohatá"). Toto fundamentální tvrzení matematické logiky s dalekosáhlými filosofickými aspekty dokázal roku 1931 opět Gödel ([G]), jeden z nejvýznamnějších matematiků zabývajících se logikou (pro českého čtenáře by nemusela být nezajímavá poznámka, že Kurt Gödel — žijící v USA — je brněnský rodák). V následujících odstavcích popíšeme strukturu formalizace peanovské aritmetiky; mimo jiné i proto, aby si čtenář mohl udělat představu o tom, jak lze formalizovat konkrétní teorii, v níž se zájem soustřeďuje ne na obecné vlastnosti blíže neurčených predikátů, ale v níž vystupují knnkrétní, specifické *základní predikáty* a také *základní konstanty* a *základní funkce* (viz [H_2]). Všimneme si jak metamatematických tvrzení (zejména o neúplnosti a nerozhodnutelnosti), tak i současných pokusů o strojové dokazování v oblasti aritmetiky.

5.1. *Syntaktická výstavba formální aritmetiky*

Abeceda $\mathbf{S}_A = \{\vee, \wedge, \rightarrow, \sim, \bigvee, \bigwedge, =, +, ., 0, x, y, z, \mathsf{I}, ', (,)\}$ (základní predikát $=$, základní funkce $+, .$, funkce následníka I základní konstanta 0 budou mít v interpretaci význam běžný z aritmetiky; $(0)\mathsf{I}$ bude značit 1, $((0)\mathsf{I})\mathsf{I}$ číslo 2, ...; smysl ostatních symbolů je týž jako v dříve uvedených příkladech).

Množina termů $\mathbf{R}$: (*i*) $0 \in \mathbf{R}$, (*ii*) každá individuová proměnná $x, y, z, x', y', z', x'', \ldots$ je term, (*iii*) jsou-li $s, t \in \mathbf{R}$, pak $(s)\mathsf{I}$, $(s) + (t)$, $(s) . (t) \in \mathbf{R}$, (*iV*) jiné výrazy než ty, které byly definovány v předchozích bodech, nepatří do $\mathbf{R}$ (termům odpovídají v interpretaci aritmetické výrazy označující pomocí proměnných a konstant přirozená čísla).

Množina formulí $\mathbf{F}_A$: (*i*) je-li $s, t \in \mathbf{R}$, pak $s = t \in \mathbf{F}_A$, (*ii*) je-li $X, Y \in \mathbf{F}_A$, pak do $\mathbf{F}_A$ patří též $(X) \vee (Y)$, $(X) \wedge (Y)$, $(X) \rightarrow (Y)$, $\sim(X)$, $\bigwedge$ a (X), $\bigvee$ a (X), kde a označuje proměnnou, (*iii*) jiné výrazy než ty, které byly definovány v předchozích bodech, do $\mathbf{F}_A$ nepatří

Příklady termů: $(x'')\mathsf{I}$, $(x)\mathsf{I} + (((0)\mathsf{I})\mathsf{I})\mathsf{I}$. Zkráceně je budeme zapisovat $x^2\mathsf{I}$, $x\mathsf{I} + 0\mathsf{III}$. Místo $0\mathsf{I}\ldots\mathsf{I}$ (k čárek) budeme psát k jako metamatematické označení pro tento symbol, který interpretujeme jako přirozené číslo k. Příklady formulí: $\bigvee z(x = z\mathsf{I} + 0\mathsf{I})$ [v interpretaci: x je větší než 1], $\bigvee z(x . z\mathsf{I} = y)$ [v interpretaci: x dělí y].

Množina axiómů $\mathbf{A}_A$ sestává jednak z axiómů (1) – (12) predikátového počtu, kde nyní ovšem $X, Y, Z \in \mathbf{F}_A$ a v $\oint_b^a$ značí b libovolný term, přičemž platí, že žádná z proměnných vyskytujících se v tomto termu se nestane po substituci vázanou. Dále přistupují specifické

axiómy aritmetiky: (13) $X(0) \wedge \bigwedge a(X(a) \rightarrow X(a\mathsf{I})) \rightarrow X(a)$ (14) $x\mathsf{I} = y\mathsf{I} \rightarrow x = y$ (15) $\sim(x\mathsf{I} = 0)$ (16) $x = y \rightarrow (x = z \rightarrow y = z)$ (17) $x = y \rightarrow x\mathsf{I} = y\mathsf{I}$ (18) $x + 0 = x$ (19) $x + y\mathsf{I} = (x + y)\mathsf{I}$ (20) $x . 0 = 0$ (21) $x . y\mathsf{I} = x . y + x$.

Axiómové schéma (13) vyjadřuje známý princip matematické indukce.
Axiómy (14) – (21) mají jasný význam.
Odvozovací pravidla $\mathbf{O}_A$: jsou definována stejně jako odvozovací pravidla $\mathbf{O}_P$, kde nyní $X, Y, Z \in \mathbf{F}_A$ a $b \in \mathbf{R}$.
Nakonec položíme zase $\mathbf{T}_A = \mathbf{O}_A(\mathbf{A}_A)$.
Čtenář se může pokusit o odvození řady formulí z $\mathbf{T}_A$; např. formule $x = x$, formule $x = y \rightarrow x + z = y + z$ atd. Mechanismus odvozování zde nepřináší žádné nové momenty (i když o jeho pracnosti nemůže být pochyb).

5.2. *Gödelovy „pesimistické" věty*

V tomto odstavci nastíníme nejprve klasickou verzi zmíněného výsledku o neúplnosti formální aritmetiky. Základní myšlenka důkazu je prostá: Ve formální aritmetice (tj. v $\mathbf{F}_A$) se sestrojí formule Q, která v řeči interpretace říká „já jsem nedokazatelná" (srovnej se známým paradoxem Kréťana, který říká „teď lžu" – lže nebo mluví pravdu?); tato formule nemůže být podle toho, co říká (za předpokladu syn-

taktické bezespornosti, který nyní přijmeme) dokazatelná, tj. $Q \notin \mathbf{T}_A$. Na druhé straně musí být intuitivně pravdivá, tj. $Q \in \mathscr{T}_A$, neboť jinak by bylo pravdivé opačné tvrzení a formule Q by byla dokazatelná. To by bylo opět ve sporu s tím, co říká. Vidíme tedy, že jsme nalezli formuli, náležející do $\mathscr{T}_A$, ale nikoliv do $\mathbf{T}_A$; z toho můžeme usoudit, že formální aritmetika není sémanticky úplná.

Předložená myšlenka je jednoduchá, přesto však jistě vzbudila ve čtenáři nedůvěru; jeho hlavní námitka asi zní: jak je možno v řeči formální aritmetiky vybudované za účelem postihnutí vlastností přirozených čísel a jednoduchých operací nad nimi sestavit formuli, která znamená "já jsem nedokazatelná"? Skutečně — ukázat, že je to možné, je hlavním úkolem v důkazu. Naznačíme řešení tohoto úkolu. Především přizpůsobíme formální aritmetiku tak, aby jednotlivé objekty její metateorie (pojem formule, důkazu apod.) bylo možno popisovat opět v rámci aritmetiky; toho dosáhneme vhodným kódováním, tzv. *aritmetizací* použitého formálního aparátu. V rámci této aritmetizace přiřadíme nejprve jistá přirozená čísla symbolům abecedy $\mathbf{S}_A$, další čísla posloupnostem těchto symbolů (speciálně: formulím) a další čísla posloupnostem těchto posloupností (speciálně: důkazům). Toto přiřazení objektů a jejich *Gödelových čísel* je možno provést vzájemně jednoznačně a efektivně.

Nejběžnější aritmetizace přiřazuje Gödelova čísla objektům formální aritmetiky takto: nejprve přiřadí čísla *1* až *17* symbolům abecedy $\mathbf{S}_A$ (např. po řadě tak, jak byly vyjmenovány v předchozím odstavci, takže symbolu 0 je přiřazeno Gödelovo číslo *10* atd.); posloupnosti n symbolů, resp. n posloupností, které mají po řadě čísla $g_1, \ldots, g_n$ přiřadí číslo $2^{g_1} \ldots p_n^{g_n}$, kde p_n označuje n-té prvočíslo. Má tedy term (0) | za své Gödelovo číslo $2^{16} \cdot 3^{10} \cdot 5^{17} \cdot 7^{12}$; čtenář si může určit Gödelovo číslo některého axiómu či dokonce důkazu, který si sám sestavil. Pozná, že čísla, která takto vznikají, se dají jednoznačně „dekódovat" — a tuto skutečnost snadno pochopí, i když praktické zacházení s nimi ho asi odradí od detailní relizace našich rad.

Po provedení aritmetizace jsme v pozici, kdy můžeme prakticky o všech důležitých věcech aritmetizovaného formálního systému (jímž je v našem případě formální aritmetika) mluvit v řeči teorie čísel: výroky a predikáty týkající se formulí a formálních důkazů se stanou výroky či predikáty, které se týkají jistých přirozených čísel. Řada takových metateoretických tvrzení má svůj formální ekvivalent v jisté formuli z $\mathbf{F}_A$. Tuto úvahu je možno precizovat: predikát $P(x_1, \ldots x_n)$ intuitivní aritmetiky považujeme za *reprezentovatelný* ve formální aritmetice, resp. v nějaké množině $\mathbf{M}$ jejích formulí ($\mathbf{M} \subset \mathbf{F}_A$), lze-li najít takovou formuli X z $\mathbf{F}_A$ (resp. z $\mathbf{M}$) o volných proměnných $a_1, \ldots, a_n$ tak, že pro libovolná přirozená $k_1, \ldots, k_n$ platí: $P(k_1, \ldots, k_n)$ je pravdivý výrok právě když

$$\int \begin{matrix} a_1 \ldots a_n \\ k_1 \ldots k_n \end{matrix} X \in \mathbf{T}_A \quad (\text{resp.} \in \mathbf{M}),$$

a $P(k_1, \ldots, k_n)$ je nepravdivý výrok právě když

$$\int \begin{matrix} a_1 \ldots a_n \\ k_1 \ldots k_n \end{matrix} \sim X \in \mathbf{T}_A \quad (\text{resp.} \in \mathbf{M}).$$

Uvažme nyní metateoretický predikát $P(u, v)$ = „u je Gödelovým číslem nějaké formule o jedné volné proměnné z F_A (tuto formuli označme $X_u(x)$) a v je Gödelovým číslem formálního důkazu formule $X_u(u)$".

Dále sestrojme formuli (o jediné volné proměnné x): $\sim\bigvee y Y(x, y)$, kde $Y(x, y)$ označuje formuli reprezentující ve formální aritmetice metateoretický predikát $P(u, v)$. Nově sestrojená formule má samozřejmě nějaké Gödelovo číslo, řekněme w. Jaký smysl v interpretaci lze nyní přisoudit výroku formulí bez volných proměnných $\sim\bigvee y Y(w, y)$? Tvrdí, že neexistuje číslo y (tedy neexistuje důkaz) formule o G. čísle w; avšak w je G. číslem právě uvažované formule. Tím jsme získali hledanou formuli Q.

V kostře důkazu, který jsme provedli, bylo mnoho mezer; nejvážnější – a v podstatě jediná, které se nemůžeme zbavit tím, že ji přenecháme k doplnění čtenáři, který nás sledoval až sem – záleží v předpokladu, že predikát $P(u, v)$ můžeme skutečně ve formální aritmetice reprezentovat vhodnou formulí $Y(x, y)$. I když se domníváme, že námitky proti tomuto tvrzení nejsou nyní již tak silné jako na počátku tohoto odstavce (kdy nebylo vůbec jasné, jak je možno do formální aritmetiky „vtělit" nějaké podobné „nearitmetické" obraty), je třeba uznat, že po technické stránce je tato část důkazu daleko nejkomplikovanější. Obvykle se důkaz opírá o dvě skutečnosti: 1. Predikát $P(u, v)$ je rozhodnutelný.

(Jak jsme se zmínili v **2.1**, dá se tento pojem precizovat v rámci aritmetiky — např. v teorii rekurzívních funkcí: ukáže se, že funkce rozhodující predikát P se může získat z jednoduchých funkcí operacemi substituce a rekurze. Při zvolené aritmetizaci jde o práci mravenčí, ale v podstatě nijak složitou.)

2. Všechny rozhodnutelné predikáty jsou reprezentovatelné ve formální aritmetice (tuto část důkazu přenechal čtenáři i Gödel ve své slavné práci [G]; při této příležitosti poznamenejme pro zajímavost, že právě v této práci se poprvé objevuje pojem rekurzívní funkce, a to pro účely, o kterých je zde řeč; obecnější souvislosti tohoto pojmu s teorií formálních systémů a teorií algoritmů vyvstaly teprve později). Citované skutečnosti umožňují nejen zpřesnit výše prováděné úvahy, ale umožňují podívat se z „modernějšího" a obecnějšího hlediska i na celý problém rozhodnutelnosti a úplnosti:

Platí důležité tvrzení: je-li každý rozhodnutelný predikát reprezentovatelný v nějaké množině $\mathbf{M}(\mathbf{M} \subset \mathbf{F}_A)$, pak množina $\mathbf{M}$ je nerozhodnutelná. K důkazu uspořádejme všechny formule o jedné volné proměnné nějakým efektivním způsobem v posloupnost: $X_0(x), X_1(x), X_2(x), \ldots$. Utvořme nyní množinu K těch čísel k, pro něž formule $X_k(\mathrm{k})$ patří do $\mathbf{M}$. Je-li rozhodnutelná $\mathbf{M}$, je zjevně rozhodnutelná i K; podle předpokladů reprezentovatelnosti je tedy pro jistou formuli X_p: $n \in \mathrm{K}$ právě když $X_p(\mathrm{n}) \in \mathbf{M}$ a $n \notin \mathrm{K}$ právě když $\sim X_p(\mathrm{n}) \in \mathbf{M}$. Dosadíme-li do těchto vztahů p za n, dostáváme spor (opětné použití obratu, který se traduje v literatuře o teorii množin pod názvem Cantorovy diagonální metody).

Z odvozené věty vyplývá podle bodu 2. nahoře *nerozhodnutelnost formální aritmetiky*. Dá se ukázat, že potřebnou vlastnost reprezentovatelnosti mají i některé

systémy „slabší" (u nichž $\mathbf{T} \subset \mathbf{T}_A$) a samozřejmě i systémy silnější ($\mathbf{T} \supset \mathbf{T}_A$): jakékoliv obohacení předloženého systému formální aritmetiky o dodatečné axiómy nenapraví — pokud zachováváme syntaktickou bezespornost — její nerozhodnutelnost: je *podstatně nerozhodnutelná.*

Od nerozhodnutelnosti se dostaneme snadno k syntaktické neúplnosti. Uvažme nejprve, že musí existovat taková formule $X \in \mathbf{F}_A$, že ani X ani $\sim X$ nepatří do $\mathbf{T}_A$ (říkáme, že formální aritmetika je *klasicky neúplná*): jinak bychom dovedli o libovolné předložené formuli X rozhodnout, zda patří nebo nepatří do $\mathbf{T}_A$ jednoduše tak, že bychom postupně generovali všechny prvky $\mathbf{T}_A$ (víme, že jde o množinu generovatelnou!) a narazili tak dříve nebo později na X nebo na $\sim X$. Přidáme-li tedy jednu z těchto formulí k axiómům, nemůžeme dostat systém (klasicky, a tedy ani syntakticky) sporný (pořád za předpokládané syntaktické bezespornosti původního systému), což dosvědčuje, že formální aritmetika *není syntakticky úplná.* (Toto tvrzení bylo možno získat i bezprostřednějšími metodami užitými na začátku tohoto odstavce.) Právě získaný výsledek lze opět přenést i na systémy silnější: formální aritmetika je *podstatně neúplná.*

Během úvah tohoto odstavce jsme několikrát zdůraznili předpoklad syntaktické bezespornosti (*sémantickou bezespornost* nahlédneme snadno jako v případech teorií předchozích dvou paragrafů). Čtenář proto možná očekává, že se pokusíme uvést důkaz této vlastnosti — v každém případě rozhodující a podstatné. To však neuděláme, a to nejen z důvodu pohodlnosti a z potřeby dát čtenáři oddechnout. Známé důkazy skutečnosti, že formální aritmetika je syntakticky bezesporná, vyžadují totiž použití nefinitních prostředků (Gentzenův důkaz používal např. transfinitní indukce): metodologická cena takových důkazů je ovšem sporná; vyrážejí klín klínem. Aby dokázaly bezespornost jedné teorie (formalizované), předpokládají bezespornost druhé (intuitivní) teorie, která je dokonce podezřelejší než původní (co se týká užitých prostředků). „Korektními" finitními prostředky se podařilo dokázat syntaktickou bezespornost jen částí aritmetiky (u nichž byla omezena funkce axiómů indukce apod.); naopak pro celou formální aritmetiku se podařilo — opět Gödelovi — dokázat, že takový důkaz nebude příliš jednoduchý: není možno ho vyjádřit známými prostředky z formální aritmetiky.

Poslední tvrzení nevybočuje příliš z úvah počátku tohoto odstavce. Podobně jako výroky o neúplnosti lze i výroky o bezespornosti reprezentovat v samotné formální aritmetice. Gödel ukázal, že reprezentuje-li formule X tvrzení „formální aritmetika je bezesporná", je $X \to Q \in \mathbf{T}_A$ (Q s významem nahoře uvedeným; připomeňme, že tam byl výrok „Q není formálně dokazatelné" dokázán z předpokladu syntaktické bezespornosti), odkud snadno plyne $X \notin \mathbf{T}_A$.

V tomto odstavci byly citovány některé výsledky, které jsou závažné nejen z hlediska teoretické práce v logice a matematice, ale mají i další významy. Doufáme, že čtenář již dříve získal dojem, že práce v daném formálním systému může někdy být — lépe či hůře podle jeho vhodnosti k řešení předloženého úkolu — realizována na číslicovém počítači vhodných parametrů. Tak lze např. na počítači rozhodovat o pravdivosti tautologií výrokového počtu a části tautologií predikátového počtu

a odvoditelných formulí formální aritmetiky; množinu všech tautologií predikátového počtu a všech odvoditelných formulí formální aritmetiky lze aspoň generovat. Poznáme v dalším odstavci, že i pro nerozhodnutelné formální systémy lze často sestavovat vhodné algoritmy pro zpracování zadané problematiky strojem. Formální aritmetika není na tom tedy nejhůř přes svou nerozhodnutelnost; avšak intuitivní aritmetika jako celek nemůže být plně modelována na žádném počítači, neboť neexistuje úplněji vystihující formální systém. „Pesimistické" Gödelovy věty (o podstatné neúplnosti a nerozhodnutelnosti formální aritmetiky) jsou tedy pesimistické v tom smyslu, že ukazují hranice možností mechanického a formálního zpracování matematických disciplín; na druhé straně jsou optimistické v dnešní době tím, že nechávají otevřené cesty pro lidskou invenci — nemožnost formálního důkazu nikterak neznamená nemožnost řešení a nemožnost přesvědčivého důkazu vůbec.

5.3. *Strojové dokazování v aritmetice*

Zatímco pro výrokový počet existují velmi účinné systémy pro rozhodování, resp. generování odvoditelných formulí (jeden z nich jsme poznali v odst. **3.3**), pro predikátový počet dává prakticky realizovatelnou semirozhodovací (příp. pro speciální případy: rozhodovací) proceduru Friedmanové systém či modifikace Gentzenova (**4.4**, **4.5**). Naproti tomu formální systém, který jsme uvedli k popisu aritmetiky, měl (podobně jako systém z **3.2** a přímá aplikace systému z **4.2**) cenu pouze pro metateoretická vyšetřování: přímá odvození složitějších formulí z axiómů jsou v něm prakticky neuskutečnitelná.

Je jasné, že pro vlastní práci v teorii se obecně lépe hodí systémy s poměrně velkým počtem axiómů a pružnými odvozovacími pravidly a příp. i s rozšířeným počtem základních predikátů, funkcí a konstant. Obohatíme-li vhodně v tomto směru formální systém aritmetiky, zvětšíme pravděpodobnost, že použitím vhodné strategie se podaří najít důkaz dané odvoditelné formule. Jindy je naopak možno dokázat o dané formuli $\sim X$, že v dané formální aritmetice není odvoditelná. Podaří-li se nám totiž např. za předpokladu odvoditelnosti formule $\sim X$ bez volných proměnných odvodit spor (tj. např. formule Y a $\sim Y$), je odvoditelná formule X a její důkaz lze efektivně sestrojit na základě předpokládaného odvození sporu. (Obrat se opírá o výrokovou tautologii $(X \to (Y \wedge \sim Y)) \to \sim X$.) Podobné platí i pro formule s volnými proměnnými, kde ovšem při negování musíme uvážit platnost vztahu $\sim \bigwedge x X(x) \leftrightarrow$ $\leftrightarrow \bigvee x \sim X(x)$. Přesvědčíme-li se takto o odvoditelnosti (a tím i intuitivní pravdivosti) formule X, řekneme, že ji demonstrujeme.

Také pro odvozování sporů v rámci formálního systému je možno užít různě účinných strategií. Jednu z takových strategií — představuje jistou semirozhodující proceduru pro aritmetiku — navrhl Hao Wang [W_1]; popíšeme stručně její funkci.

Předpokládejme, že naším úkolem bude demonstrovat nějaké formule odpovídající (v interpretaci; té se budeme teď z metodických důvodů častěji odvolávat, i když platí zase: v případě potřeby vystačíme s pouhou syntaxí, srozumitelnou i tak nená-

paditému zařízení, jako je počítač) tvrzením, která se týkají dělitelnosti přirozených čísel. Obohatíme proto náš systém formální aritmetiky o základní predikáty Py (y je prvočíslo), x/y (x dělí y), $x > y$ (x je větší než y); není těžké zapsat tyto predikáty pomocí původních základních – částečně jsme to dokonce udělali ve formě příkladů v **5.2**. Naším úkolem teď však není redukce, nýbrž naopak rozšíření výrazových prostředků. K množině axiómů přidáme řadu formulí, jejichž dokazatelnost je patrná (byla prověřena dříve); tuto množinu, je možno během odvozování rozšiřovat; je vhodné nazvat ji např. *soupisem znalostí*. Soupis znalostí tak odpovídá (neustále rostoucí) zásobě znalostí matematika postaveného před úkol dokazovat matematická tvrzení ze zvoleného oboru; všimněme si, že na každé etapě matematikovy práce je tato zásoba rovněž konečná a zpravidla nijak zvlášť obsáhlá ve srovnání s paměťovými možnostmi současných počítačů.

Pro naše účely zahrneme do uvažované množiny např.:

$$Z_1\colon\ \sim(x < x),\quad Z_2\colon\ (x < y \wedge y < z) \to x < z\,,$$
$$Z_3\colon\ x/x,\quad Z_4\colon\ (x/y) \wedge (y/z) \to (x/z)\,,$$
$$Z_5\colon\ \sim Py \leftrightarrow \bigvee x(1 < x \wedge x < y \wedge x/y)\,.$$

Je také vhodné uzpůsobit odvozovací pravidla. Uvidíme, že je možno omezit se na odvozovací pravidla výrokového počtu, jejich pružné využití umožní dosáhnout cíle v rámci níže citované strategie. Nedělalo by zvláštních potíží uvést explicitně řadu vhodných odvozovacích pravidel. Spokojíme se však s tím, že jich budeme užívat, aniž bychom je vypisovali. Situace ve výrokovém počtu je tak jednoduchá, že nám to snadno umožní – ostatně má čtenář dobrý vzor: odvozovací pravidla systému z **3.3**.

Mějme nyní za úkol demonstrovat nějakou formuli obsahující volné proměnné $x, y, \ldots$, tj. odpovídající nějakému tvrzení, které platí pro libovolnou volbu čísel $x, y, \ldots$. Naše strategie spočívá v předpokladu, že tvrzení je nepravdivé a že je tedy možné nalézt vhodný protipříklad. Přesněji řečeno: budeme předpokládat, že existují nějaká (zatím blíže neurčená) čísla, *neurčené konstanty*, které dosazeny za volné proměnné do negace dokazovaného tvrzení dávají odvoditelnou formuli. Ze sporu, který dostaneme, usoudíme na odvoditelnost formule. Přitom v zápisech vypouštíme obecné kvantifikátory ve shodě s interpretací volných proměnných z **4.1**, zatímco proměnné vázané existenčními kvantifikátory nahrazujeme neurčenými konstantami, o nichž předpokládáme, že mají vlastnosti požadované dokazovaným tvrzením. (Aby čtenář pochopil snadněji tento obrat, nechť si všimne, že např. formuli $\bigwedge x \bigvee y X(x, y)$ je možno se zachováním sémantického významu přepsat do tvaru $X(x, y(x))$, kde $y(x)$ označuje prvek, jehož existenci první formule tvrdí; tento prvek ovšem obecně závisí na x).

Příklad. Uvažme formuli $x > 1 \to \bigvee y(Py \wedge (y/x))$.
Pro číslo m, které by tvořilo hledaný protipříklad, by tedy platilo $m > 1 \wedge (Py \to \sim(y/m))$.

Chceme-li co nejdřív dospět k (předpokládanému) sporu, využijeme všech vlast-

ností čísel tvořících protipříklad. Kromě toho, že mají všechny vlastnosti čísel a všechny vlastnosti dané formulemi, do kterých byly dosazeny, můžeme využít i nějaké jejich speciální volby: budeme předpokládat, že jsou to nejmenší čísla tvořící protipříklad.

Pro náš příklad tak dostáváme další formuli:
$1 < x \wedge x < m \to Py(x) \wedge (y(x)/x)$ (m je nejmenší číslo nedělitelné žádným prvočíslem; ke každému číslu x menšímu než m již existuje „neurčená konstanta" $y(x)$, která je prvočíslem a dělí x).

Vlastní práce záleží v realizaci více či méně jednoduchého algoritmu strategie. Tak je možno např. sestavit algoritmus na základě pravidel: I. sepiš jednotlivé podmínky pro nejmenší číslo tvořící protipříklad, II. zaveď potřebné neurčené konstanty a dosaď je do předchozích formulí důkazu, III. aplikuj všechna odvozovací pravidla ke všem dosud získaným výrokům (formulím bez volných proměnných); neurčené konstanty přitom nepokládáme za volné proměnné, IV. zařaď do důkazu vhodné formule ze soupisu znalostí (vhodné jsou ty, které mají tvar $X \to Y$, kde X je výrok obsažený mezi již získanými formulemi a v Y nejsou žádné funkce a predikáty, které se dosud nevyskytly v důkazu), V. hledej spor v dosud odvozených formulích. Je naděje, že postupným opakováním pravidel hledaný spor skutečně objevíme.

Ilustrujme postup práce algoritmu na našem příkladě.
V posloupnosti formulí dostáváme postupně:

(1) $m > 1$,
(2) $Py \to \sim (y/m)$,
(3) $1 < x \wedge x < m \to Py(x) \wedge (y(x)/x)$.

Neurčenou konstantu m dosadíme do předchozích formulí za x a y:

(4) $Pm \to \sim (m/m)$,
(5) $1 < m \wedge m < m \to Py(m) \wedge (y(m)/m)$.

Aplikací odvozovacích pravidel se přesvědčíme o zbytečnosti formule (5) pro další postup ($m < m$ je nepravdivé; viz Z_1) a z formule (4) dostaneme (viz Z_3):

(6) $\sim Pm$.

Opětným užitím odvozovacích pravidel vyškrtneme (4) (srv. (4) a (6)); z Z_5 dále obdržíme:

(7) $\sim Pm \to \bigvee x(1 < x \wedge x < m \wedge (x/m))$.

Z (6) a (7) dostaneme po známé již náhradě proměnné vázané existenčním kvantifikátorem neurčenou konstantou:

(8) $1 < x(m) \wedge x(m) < m$,
(9) $x(m)/m$.

Poněvadž $x(m)$ je nová neurčená konstanta, dosadíme ji do předchozích formulí (2), (3) na místo volné proměnné:

(10) $Px(m) \to \sim (x(m)/m)$,
(11) $1 < x(m) \wedge x(m) < m \to Py(x(m)) \wedge (y(x(m))/x(m))$.

Podobně jako prve dostáváme z (9) a (10):

(12) $\sim Px(m)$.

Z (8) a (11) odvodíme:

(13) $Py(x(m))$,
(14) $y(x(m))/x(m)$.

Podle (9), (14) a Z_4 můžeme psát:

(15) $y(x(m))/m$.

Konečně dosazením neurčené konstanty $y(x(m))$ do (2) a (3):

(16) $P(y(x(m))) \to \sim (y(x(m))/m)$,

(17) $(1 < y(x(m)) \wedge (y(x(m)) < m) \to Py(y(x(m)))/y(x(m))$.

Podle (15) a (16) tedy:

(18) $\sim Py(x(m))$.

Na této etapě se uplatní poslední pravidlo algoritmu: formule (18) a (13) ukazují, že existence protipříkladu je nemožná; původní formule je tedy demonstrována.

Náš popis práce s formálním systémem, podaný v tomto odstavci, má samozřejmě daleko do formy bezprostředně použitelné k naprogramování. Že se zde však tato možnost ukazuje, je snad patrné. Budoucnost ukáže, do jaké míry se podobné obraty ukáží účinné. A to jak pro aritmetiku (v [W_1] se ukazuje, jak je možno uvedenou metodou dokázat i již poměrně zajímavá tvrzení; např. o tom, že rovnice $x^2 - 2 = 0$ nemá řešení v oboru racionálních čísel), tak pro jiné formální systémy.

Přehled, který jsme se snažili podat v tomto článku, by nebyl úplný, kdybychom se aspoň stručně nezmínili o dalších možnostech, které se ukázaly být schůdné při aplikacích formálních systémů pro práci v matematických teoriích. Byly vypracovány různé metody, které umožnily prakticky efektivní hledání důkazů vět elementární geometrie (Gelertner), symbolické (ne numerické) integrování (Slagle), řešení šachových úloh aj. [že jde v podstatě o práce ve „formálních systémech", je nasnadě (viz [C])]. Tyto metody spadají do širokého proudu heuristiky a koncepce *umělé inteligence* (artificial intelligence) srov. sborník [C]) a záleží v nahrazování beznadějného probírání všech možností (tzv. „*British museum method*") obraty, které připomínají lidskou invenci a zručnost. Budou se zřejmě ve stále větší míře uplatňovat v různých složkách výzkumu. Formální systémy, zavedené a vyšetřované ještě před druhou světovou válkou v matematické logice pro značně abstraktní účely metateoretického výzkumu, mohou v nedaleké budoucnosti prokázat cennou službu všestrannému rozvoji vědění.

Literatura

K literatuře citované v I. části článku přistupuje:

[F] FRIEDMAN J.: A Semidecision Procedure for the Functional Calculus. Journal of the Association for Computing Machinery *10* (1963), 1—24.

[G] GÖDEL K.: Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I. Monatshefte für Mathematik und Physik *38* (1931), 173—198.

[H_2] HÁJEK P.: Syntaktické metody matematické logiky. Pokroky MFA *11* (1966), 1.

[C] *Computers and Thought*; eds E. A. Feigenbaum, J. Feldman. McGraw-Hill 1963, 535.

[W_1] WANG H.: Formalization and automatic theorem-proving. Proceedings of IFIP CONGRESS 65, *1*, 1965. (edit. W. Kalenich).

Poznámka. Prosíme čtenáře, aby si opravil nepříjemnou tiskovou chybu v I. části článku, str. 336, 3. ř. zdola: $Z_1 : Q \supset P; Q; R$; na str. 331, 12. ř. zdola má dále být 2^3 místo 23 a na str. 331, 9. ř. zdola má být „„jestliže Q, pak R" pravdivý," místo „„jestliže Q, pak R" nepravdivý,".