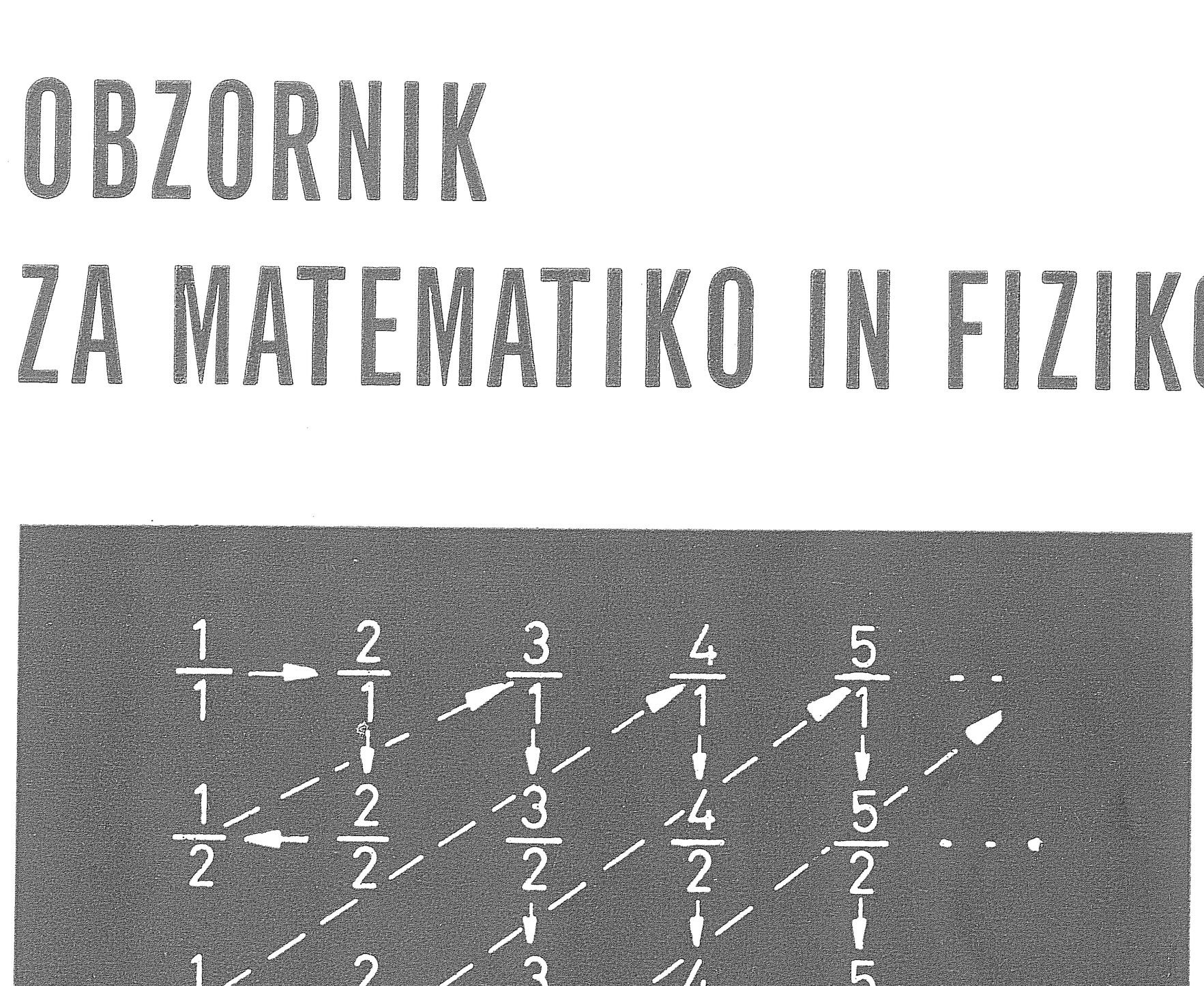
IZDAJA DRUŠTVO MATEMATIKOV, FIZIKOV IN ASTRONOMOV SR SLOVENIJE

OBZORNIK ZA MATEMATIKO IN FIZIKO



1978

letnik 25

LETNIK 25. — ŠTEVILKA 1

OBZORNIK ZA MATEMATIKO IN FIZIKO

LJUBLJANA, JANUAR 1978

Glavni in odgovorni urednik: Janez Strnad.

Uredniški odbor: France Avsec, gimnazija Kranj; Robert Blinc, FNT; Alojz Kodre, FNT; France Kvaternik, tehniška šola za lesarstvo, Ljubljana; Jože Lep, VTŠ, Maribor; Anton Moljk, FNT; Mitja Rosina, FNT; Tomaž Skulj, gimnazija Moste, Ljubljana; Janez Strnad (urednik za fiziko), FNT; Anton Suhadolc (urednik za matematiko), FNT; Ciril Velkovrh (urednik), FNT; Ivan Vidav, FNT; jezikovni pregled Marija Janežič, inštitut za slovenski jezik SAZU. Slike je narisal Miro Lozej.

Naročnina: za posameznike 170.— din (za člane društva je že vračunana članarina), za dijake in študente 80.— din, za ustanove in podjetja 215.— din, za tujino 15 $ = 270.— din, posamezna številka 30.— din, dvojna številka 60.— din.

Dopise pošiljajte in list naročajte na naslov: **Komisija za tisk DMFA SRS,** 61001 Ljubljana, Jadranska c. 19, p. p. 227, tel. št. 265-061/53, žiro račun 50101-678-48363, devizni račun pri Ljubljanski banki 32009-007-900.

Tiska tiskarna Ljudske pravice v Ljubljani, Kopitarjeva ul. 2. Naklada 1500 izvodov.

Izdajo revije sofinancirata Izobraževalna skupnost Slovenije in Raziskovalna skupnost Slovenije.

YU ISSN 0473-7466

VSEBINA

Članki Stran

O teorijah (Vladimir Batagelj) 1
Formalna izgradnja logičnega jezika (Niko Prijatelj) 20
Izrek o dedukciji (Izidor Hafner) 34
Izračunljivost in rešljivost (Tomaž Pisanski) 41
Logika in množice v srednji šoli (Janez Rakovec) 55
Prejeli smo v oceno (France Križanič, Igor Vilfan, Tomaž Pisanski) III

CONTENTS

Articles Page

On theories (Vladimir Batagelj) 1
Formal construction of a logical language (Niko Prijatelj) 20
The deduction theorem (Izidor Hafner) 34
Computability and solvability (Tomaž Pisanski) 41
Logic and set theory in the secondary school (Janez Rakovec) 55
Reviews III

Na ovitku: Enumeracija pozitivnih racionalnih števil, str. 43.

Obzornik mat. fiz. 25 (1978) 1

R- 1771/78.1

Ymv, PG126

O TEORIJAH

VLADIMIR BATAGELJ

AMS Subj. Class. (1970) 02-01, 02 G

Čeprav je matematična logika že razmeroma staro področje, vlada v njej precejšnja terminološka zmeda. Med poskusi postaviti stvari na pravo mesto zasluži posebno pozornost Curryev [4], na katerem temelji tudi ta sestavek. V njem izvemo najprej nekaj o opisnih sredstvih in teorijah, nato pa se seznanimo še z osnovnimi sintaktičnimi in semantičnimi značilnostmi teorij.

ON THEORIES

In the article the basic notions of mathematical logic are introduced.

Opisni jezik, induktivni razredi, konstrukcije

Opisni jezik: Študij matematične teorije je podoben študiju tujega jezika. Tako kot se pri študiju tujega jezika običajno opremo na jezik, ki ga že obvladamo, tako tudi pri študiju teorije potrebujemo jezik, v katerem lahko govorimo o teoriji. Temu jeziku bomo rekli *opisni jezik*. Trditve o teoriji, izražene v opisnem jeziku, sestavljajo *epiteorijo*. Pojma opisnega jezika in epiteorije sta tesno povezana s pojmoma metajezika in metateorije, ki ju srečamo v formalistični metamatematiki. Seveda je mogoče tudi, tako kot pri materinščini, da jezik teorije in opisni jezik sovpadata.

Od opisnega jezika pričakujemo, da je:

— dovolj bogat, da lahko v njem našo teorijo opišemo s poljubno »razumno« stopnjo natančnosti;

— razumljiv za »zainteresirano« skupino ljudi, ki ga uporablja;

— spremenljiv — vanj lahko uvajamo novo simboliko in termine, rabimo stare termine v novem pomenu ali pa jih sploh opustimo...

V tem sestavku bomo za opisni jezik uporabljali slovenščino in jo po potrebi dopolnjevali z imeni za objekte opisa in običajno matematično ter logično simboliko. Za imena objektov bomo uporabljali velike in male latinske črke, številke in druge simbole oziroma njih kombinacije. Če je objekt opisa natančno določen, govorimo o *opisni konstanti*; kadar pa ime označuje poljuben objekt iz dane skupine objektov, govorimo o *opisni spremenljivki*.

Od običajne simbolike bomo uporabljali za okrajšavo pogostejših fraz opisnega jezika naslednje simbole:

$\Rightarrow$	če . . . ., potem	$<$	. . . . je pred . . . .
$\Leftrightarrow$	. . . . natanko takrat, ko	$\vdash$	iz . . . . je izpeljivo . . . .
$\vee$	. . . . ali	$\forall$	za vsak . . . .
$\wedge$	. . . . in	$\exists$	obstaja . . . .
$=$	. . . . je enako	$\neg$	ne . . . .
$\in$	. . . . je element	$\subset$	. . . . je vsebovan v . . . .
$\equiv$	. . . . je (po definiciji) isto kot		

Na tem mestu je treba opozoriti na razliko med pojmoma *simbol* in *znak*. Simboli niso enkratni fizični objekti, temveč tipi objektov. Tako lahko neki simbol srečamo »zapisan«

v več primerkih, ki jih imenujemo inskripcije tega simbola ali znaki. Pri tem zahtevamo, da lahko vsako inskripcijo simbola spoznamo za inskripcijo tega simbola in da jo lahko ločimo od vseh inskripcij drugih simbolov. S tem, ko smo se odločili, da bomo govorili o simbolih in ne o znakih, in tako izbrali enostavnejšo pot, smo naredili tako imenovano *prvo abstrakcijo* ali *abstrakcijo istovetenja*. S tem smo dosegli, da namesto »v zapis besede **matematika** vstopajo trije znaki, podobni (ekvimorfni) znaku **a**«, lahko rečemo »simbol **a** vstopa trikrat v besedo **matematika.**«

Simbole lahko naprej združujemo v *izraze*. Število simbolov v izrazu imenujemo *velikost izraza*. Če pri tem kak simbol vstopa v izraz večkrat, ga tolikokrat tudi štejemo. Ponavadi so izrazi linearna zaporedja simbolov. V teh primerih govorimo namesto o velikosti o *dolžini izraza*. Izraze združujemo naprej v *jezike*. Nabor simbolov, iz katerega so zgrajeni izrazi danega jezika, imenujemo *abeceda* jezika; izrazom pa pogosto pravimo kar *besede*. Z izrazi je povezana *druga abstrakcija*, ki zahteva, da so lahko izrazi poljubno veliki in da imamo na razpolago poljubno število znakov. Ta zahteva in njej podobne zahteve so značilne za vse konstruktivistične pristope k matematiki (obstoj naslednika v formalni aritmetiki, neomejenost traku pri Turingovih strojih, ...). Z njimi uvedemo v naše razpravljanje neskončnost, toda le kot potencialno (kot možnost), ne pa tudi kot aktualno (kot danost), ki je konstruktivna matematika ne priznava. Zato pogosto govorimo kar o *abstrakciji potencialne neskončnosti*.

Ker bi radi govorili o izrazih predvsem kot o objektih, se moramo zateči k rabi imen za izraze. Ena izmed možnosti poimenovanja izrazov je *avtonimna* raba izrazov — izraz sam rabimo tudi za njegovo ime. Ali je to vselej dovoljeno? Poglejmo si naslednji sklep:

Drevo je ozelenelo.
Drevo je beseda iz petih črk.

Obstaja beseda iz petih črk, ki je ozelenela.

Čeprav je sklepanje logično pravilno in so premise smiselne, je zaključek nesmiselen. Zakaj? Očitno smo v prvi premisi govorili o drevesu kot objektu, v drugi pa o drevesu kot imenu. Iz tega pa že vidimo, v katerem grmu tiči zajec. Težave lahko premostimo tako, da izraz, kadar ga rabimo kot njegovo ime, postavimo v enojne narekovaje. Izraz v enojnih narekovajih je nedeljiva celota opisnega jezika. Po tem dogovoru bi drugo premiso zapisali:

‚Drevo‘ je beseda iz petih črk.

Prejšnji sklep sedaj ni več pravilen. Ponavadi je tolikšna natančnost odvečna; način rabe je razviden iz konteksta.

Opisni jezik je okvir, iz katerega ne moremo. Posamezna dejstva o teoriji lahko utemeljimo in razložimo zunaj nje — v opisnem jeziku; opisni jezik pa moramo utemeljevati in razlagati samega v sebi. Zato moramo razpravljanje začeti s skupino pojmov, ki jih privzamemo za znane in se zadovoljimo le z opisom njihovih medsebojnih odnosov in našimi predstavami o njih ter z dogovori o njih rabi.

Konceptualni razredi: V matematiki in sorodnih vedah se nenehno srečujemo z objekti različnih vrst: naravna števila, točke, trikotniki, matrike, grafi, funkcije, programi, formule, množice, vezja, ... Objekti iste vrste sestavljajo razrede objektov, ki jim bomo rekli *konceptualni razredi*.

Konceptualni razredi so običajno podani s končnim spiskom lastnosti, katerim morajo objekti, ki razredu pripadajo, zadoščati. Tako je konceptualni razred praštevil določen z zahtevo

— naravno število $p > 1$ je praštevilo natanko takrat, ko je deljivo samo z 1 in samim seboj

konceptualni razred paralelogramov, pa z zahtevo

— paralelogrami so natanko tisti ravninski četverokotniki, ki imajo po dve in dve stranici vzporedni.

Prvo vprašanje, ki se nam zastavi, ko govorimo o konceptualnih razredih, je vprašanje pripadnosti: ali znamo za dani objekt »v končnem času« ugotoviti, ali pripada danemu konceptualnemu razredu? V splošnem je lahko pripadnost objekta konceptualnemu razredu časovno odvisna, kot je na primer za konceptualni razred telefonskih naročnikov. V matematiki in logiki običajno ni tako — razredi imajo statično naravo.

Za praštevila nam da vedno (vsaj teoretično) odgovor na zastavljeno vprašanje naslednji postopek:

1. $i \leftarrow 2$
2. **dokler** je $(p \bmod i \neq 0) \wedge (i < p)$ **ponavljaj**
21. $i \leftarrow i + 1$
3. **če** je $i = p$ **potem** »p je praštevilo«
drugače »p ni praštevilo«

Zakaj smo v oklepajih zapisali »vsaj teoretično«? Kot vemo, je praštevil neskončno; torej obstaja poljubno veliko praštevilo in če privzamemo, da poteka vsak korak našega postopka končen delček časa, lahko teče postopek sicer vedno končno, a vseeno poljubno dolgo. Torej nam za zadosti velika praštevila ne more v »praktično« sprejemljivem času dati odgovora na zastavljeno vprašanje (najbrž je vprašljiva tudi »praktična« uporabnost takšnih števil). V nadaljnjem se ne bomo ustavljali ob problemu »praktične« izračunljivosti; zadovoljili se bomo s končnostjo (abstrakcija potencialne neskončnosti).

Iz matematike poznamo postopke, ki dajo odgovor še na celo vrsto vprašanj:

— ali ima dani polinom z racionalnimi koeficienti racionalne korene;
— ali je dani sistem linearnih enačb enolično rešljiv;
— ali je dani končni graf povezan (planaren, Eulerjev).
...

Konceptualnim razredom, za katere obstaja postopek, ki da za vsak objekt v končno korakih odgovor na vprašanje pripadnosti, pravimo, da so *odločljivi*. Če pa je odgovor zagotovljen samo, ko dani objekt pripada razredu, drugače pa se lahko postopek nikoli ne ustavi, govorimo o *polodločljivem* ali tudi *pozitivno odločljivem* razredu.

Poleg postopkov, ki dajejo odgovore »da« in »ne« ali pa se nikoli ne ustavijo, obstajajo tudi postopki, ki »sestavijo« ali »izračunajo« posamezni objekt, ki mu pravimo *končni objekt* ali *rezultat*. Taki so na primer postopki za:

— seštevanje (množenje) dveh v desetiškem sistemu končno zapisanih števil;
— določanje največjega skupnega delitelja dveh celih števil (Evklidov algoritem);
— določanje (dolžine) najkrajše poti med dvema krajema;
— načrtovanje krožnice, ki se dotika danih treh krožnic (Apolonijev problem).

Efektivni postopki: V nadaljnjem bomo privzeli, da je vsak postopek podan s končnim naborom pravil (navodil za računanje), ki za vsak *podatek* (*začetni objekt*) iz danega konceptualnega razreda enolično določajo potek »računanja«. Načelno bi lahko računanje prepustili stroju, v katerega bi vgradili ta pravila. Če se za vsak podatek iz danega razreda računanje po končno korakih konča, imenujemo postopek *efektivni postopek* ali *algoritem*. Podatki, za katere se računanje konča, so *dopustni* za dani postopek. Očitno je vprašanje dopustnosti vsaj polodločljivo.

Obstaja več formalizacij (strogih opisov) pojma efektivnega postopka. Med njimi so najbolj znani Turingovi stroji, rekurzivne funkcije in algoritmi Markova. Vsi ti pristopi so, kakor se je izkazalo, med seboj ekvivalentni. Zvezo med njimi in intuitivnim pojmom efektivnega postopka izraža *Churcheva teza*, da se z vsakim izmed njih (zaradi ekvivalentnosti; Church je postavil tezo za rekurzivne funkcije) da opisati poljuben efektivni postopek nad opisu ustreznimi formalnimi objekti. Šele privzem te teze nam omogoči formalno obravnavo problemov odločljivosti in izračunljivosti.

Pojem efektivnega postopka je eden od načinov, kako lahko podajamo konceptualne razrede, ki jih ne moremo podati z naštetjem vseh elementov, ki v razred vstopajo. V razred, določen z danim efektivnim postopkom, spadajo natanko tisti objekti, za katere se postopek konča s pritrdilnim odgovorom (na vprašanje pripadnosti). Pravimo tudi, da smo objekt *razpoznali*. Prevajalniki za programske jezike vsebujejo postopek za razpoznavanje razreda sintaktično (slovnično) pravilnih programov.

Induktivni razredi: Razen z razpoznavanjem lahko konceptualni razred podamo tudi tako, da povemo, kako lahko njegove objekte »sestavimo« iz razreda začetnih objektov. Pravimo tudi, da posamezni objekt *zgeneriramo*. Tako določene konceptualne razrede imenujemo induktivni razredi.

Točneje, *induktivni razred* $\mathscr{I}$ določimo tako, da podamo:

— odločljiv konceptualni razred $\mathscr{B}$ *začetnih objektov*, ki mu pravimo tudi *baza* induktivnega razreda;

— odločljiv konceptualni razred $\mathscr{D}$ *pravil generiranja*. Vsakemu pravilu $\mu \in \mathscr{D}$ pripada naravno število m, ki ga imenujemo stopnja pravila μ. Če uporabimo pravilo μ k zaporedju m objektov razreda $\mathscr{I}$ (argumenti pravila μ), dobimo zopet objekt(e) razreda $\mathscr{I}$. Pri tem zahtevamo, da je vprašanje, ali dobimo dani objekt na ta način iz danih argumentov, odločljivo.

Induktivnemu razredu $\mathscr{I}$ pripadajo natanko tisti objekti, ki jih lahko dobimo iz baze po pravilih generiranja v končno korakih. Pri tem lahko v vmesnih korakih rabimo za argumente samo tiste objekte, ki pripadajo bazi ali pa smo jih že dobili v prejšnjih korakih.

Torej mora induktivni razred $\mathscr{I}$ zadoščati naslednjim zahtevam:

a) vsebuje bazo;
b) je zaprt glede na pravila generiranja;
c) je najmanjši razred, ki zadošča pogojema a in b.

To shemo pogosto srečamo tudi v knjigah pri definicijah konkretnih induktivnih razredov. Pri tem je navajanje zahteve c odvečno, saj je implicitno dana že s tem, ko povemo, da gre za induktivni razred.

V splošnem lahko pri uporabi pravila generiranja nad danimi argumenti dobimo en objekt ali več objektov ali ne dobimo nobenega. Če pa dobimo za vsak nabor argumentov za rezultat največ en objekt, pravimo, da je pravilo *determinirano*. Primer determiniranega pravila je vsota dveh celih števil; primer nedeterminiranega pravila pa je pravilo, ki določi presečišča premice skozi točki T_1 in T_2 in krožnice skozi to točko T_3 s središčem v točki T_4.

Zgled: Kot zanimivost omenimo, da pokažemo nerešljivost treh klasičnih problemov starogrške matematike (podvojitev kocke, trisekcija kota, kvadratura kroga) tako, da pokažemo, da zahtevajo konstrukcijo točke, ki ne spada v induktivni razred $\mathscr{K}$, ki ga določajo dovoljena sredstva (ravnilo brez merila in šestilo):

— točki A in B (ki določata enotno razdaljo) pripadata razredu $\mathscr{K}$;

— točka T pripada razredu $\mathscr{K}$, če jo lahko dobimo kot presečišče: ali dveh različnih premic, ali dveh različnih krožnic ali pa premice in krožnice; pri tem so te premice in krožnice določene s točkami razreda $\mathscr{K}$.

Pri dokazu nerešljivosti problema kvadrature kroga potrebujemo še enega od najpomembnejših matematičnih dosežkov prejšnjega stoletja: število π ni algebrajsko (je transcendentno; Lindemann, 1882).

Konstrukcije in konstrukcijska zaporedja: Oglejmo si malo podrobneje sam postopek generiranja objekta $X \in \mathscr{I}$. Temu postopku bomo rekli *konstrukcija* objekta X. S pojmom konstrukcije je tesno povezan pojem *konstrukcijskega zaporedja* objekta X. To je končno zaporedje objektov razreda $\mathscr{I}$, za katerega velja, da vsak njegov člen ali pripada bazi razreda $\mathscr{I}$ ali pa ga dobimo iz pred njim stoječih členov po nekem pravilu generiranja in je njegov zadnji člen objekt X.

Včasih, iz čisto praktičnih razlogov, delamo z nekoliko razširjeno »bazo«; vanjo vključujemo tudi vse tiste objekte razreda $\mathscr{I}$, za katere že poznamo konstrukcijska zaporedja. S tem dosežemo preglednejši opis; izgubili pa nismo nič, saj če take objekte zamenjamo z njihovimi konstrukcijskimi zaporedji povsod, kjer vstopajo v dano zaporedje, dobimo konstrukcijsko zaporedje danega objekta nad osnovno bazo.

Da pa bi lahko iz danega konstrukcijskega zaporedja prišli nazaj h konstrukciji (jo ponovili ali preverili), moramo vsakemu členu zaporedja dodati informacijo, ki nam pove, iz katerih argumentov (členov zaporedja) in s katerim pravilom generiranja smo dobili dani člen. Tej dodatni informaciji pravimo *analiza* ali *pojasnilo* konstrukcijskega zaporedja.

Poglejmo si še en

Zgled: Razred (enostavnih) aritmetičnih izrazov $\mathscr{E}$ določimo induktivno s pravili:

E1. $a_i, i \in \mathscr{N}$ pripadajo razredu $\mathscr{E}$

Naj izraza E in F pripadata razredu $\mathscr{E}$, potem mu pripadajo tudi izrazi:

E2. (E), E3. $E + F$ in E4. $E \times F$

Napišimo najprej nekaj enostavnih aritmetičnih izrazov:

$$a_{96}, \quad a_0 + a_7 \times a_3, \quad (((a_3)) + (a_{1977} \times a_0 + (a_1)))$$

in nekaj konstrukcijskih zaporedij izraza $a_0 + a_7 \times a_3$:

$$a_7, \quad a_0, \quad a_5, \quad a_0 + a_7, \quad a_3, \quad a_3 + a_5, \quad a_0 + a_7 \times a_3$$
$$a_0, \quad a_3, \quad a_7, \quad a_7 \times a_3, \quad a_0 + a_7 \times a_3$$
$$a_7, \quad a_3, \quad a_7 \times a_3, \quad a_0, \quad a_0 + a_7 \times a_3$$

Dopolnimo zadnje zaporedje še s pojasnilom:

(1)	a_7	E1
(2)	a_3	E1
(3)	$a_7 \times a_3$	E4 (1), (2)
(4)	a_0	E1
(5)	$a_0 + a_7 \times a_3$	E3 (4), (3)

Iz teh primerov vidimo, da nam pojem konstrukcijskega zaporedja pušča še precej svobode. V zaporedju se lahko pojavljajo odvečni členi, pa tudi vrstni red členov se lahko v dovoljenih mejah spreminja. Odvečne člene lahko brez škode izločamo ali dodajamo (razen na konec). Če izločimo iz prvega zaporedja odvečne člene, dobimo novo (okrajšano) konstrukcijsko zaporedje

$$a_7, \quad a_0, \quad a_0 + a_7, \quad a_3, \quad a_0 + a_7 \times a_3$$

Opazimo tudi, da lahko drugo zaporedje s premenami po dveh členov (a_0, a_7) in $(a_0, a_7 \times a_3)$ pretvorimo v tretje (in obratno) pri čemer so tudi vmesna zaporedja konstrukcijska. Takim

zaporedjem pravimo, da so *ekvivalentna*. Ker prvo zaporedje vsebuje neodvečni člen $a_0 + a_7$, drugi dve pa ga ne vsebujeta, jima ne more biti ekvivalentno.

Dvoumnost: Kakšne so posledice obstoja neekvivalentnih konstrukcijskih zaporedij za dani izraz, sprevidimo, če mu pripišemo »pomen«, tako da postavimo $a_0 = 1$, $a_3 = 2$, $a_7 = 3$ in izračunamo objekte, ki jih posamezni členi zaporedja označujejo. Okrajšano prvo zaporedje nam da zaporedje objektov

3, 1, 4, 2, 8

drugo in tretje zaporedje pa dasta

1, 2, 3, 6, 7
3, 2, 6, 1, 7

Vidimo: Neekvivalentna konstrukcijska zaporedja lahko pripišejo danemu izrazu različne objekte (»pomene«). Ekvivalentna zaporedja pa (zaradi možnosti pretvarjanja drugega v drugega) očitno določajo isti objekt, če so le pravila generiranja determinirana. Zato ustreza pojmu konstrukcije pojem ekvivalenčnega razreda konstrukcijskih zaporedij.

Ker ima lahko objekt $X \in \mathscr{I}$ več različnih konstrukcij (več različnih ekvivalenčnih razredov konstrukcijskih zaporedij), ločimo objekte na:

— *monotektonične*; če zanj obstaja natanko ena konstrukcija;
— *politektonične* ali *dvoumne*; če obstaja več konstrukcij.

Ta dva pojma prenesemo tudi na razrede: induktivni razred je dvoumen, če je dvoumen vsaj en objekt, ki mu pripada.

Ponavadi se izkaže, da dvoumnost ni lastnost vseh induktivnih razredov, ki določajo isti konceptualni razred. Problem dvoumnosti je precej dobro obdelan v teoriji programskih jezikov, saj je nedvoumnost ena od bistvenih lastnosti, ki jo mora izpolnjevati vsak program.

Induktivne posplošitve: V zvezi z induktivnimi razredi si oglejmo še pojem *induktivne posplošitve*. Naj bo dan induktivni razred $\mathscr{I}$ z bazo $\mathscr{B}$ in pravili generiranja $\mathscr{D}$. Za to, da pokažemo, da ima vsak objekt $X \in \mathscr{I}$ lastnost P, je dovolj, da pokažemo

IP1. vsak element baze $\mathscr{B}$ ima lastnost P;
IP2. pravila iz $\mathscr{D}$ *ohranjajo* lastnost P — vsak objekt, ki ga dobimo po nekem pravilu iz $\mathscr{D}$ iz objektov razreda $\mathscr{I}$, ki imajo lastnost P, ima tudi sam lastnost P.

O tem se prepričamo takole. Naj bo $X \in \mathscr{I}$, potem obstaja zanj konstrukcija oziroma njej ustrezno konstrukcijsko zaporedje. Če gremo sedaj po zaporedju od člena do člena, vidimo, da imajo po IP1 in IP2 lastnost P vsi členi zaporedja. Torej tudi X. Običajna matematična indukcija je poseben primer induktivne posplošitve za induktivni razred naravnih števil (določen s Peanovimi aksiomi).

Teorije

Osnovni pojmi: V vsakdanji rabi beseda »teorija« označuje nakopičeno znanje o kakem področju človekove dejavnosti, ki je bolj ali manj sistematizirano in logično povezano.

Pri izgradnji *teorije* $\mathscr{T}$ izhajamo iz odločljivega številnega konceptualnega razreda *elementarnih izjav* $\mathscr{E}$ (ki govore o področju, ki ga teorija $\mathscr{T}$ opisuje). V razredu $\mathscr{E}$ določimo (s poskusi ugotovimo, izberemo, definiramo) podrazred $\mathscr{I}$ »resničnih« elementarnih izjav ali *elementarnih izrekov* teorije $\mathscr{T}$. Teorija $\mathscr{T}$ je s tema dvema razredoma natanko določena, kar zapišemo

$$\mathscr{T} = (\mathscr{E}, \mathscr{I})$$

(O elementarnih izjavah in elementarnih izrekih govorimo zato, da bi jih ločili od drugih rab teh dveh pojmov.)

S tako definiranim pojmom teorije zaobsežemo tudi primere, ko gre za nesistematizirano in logično nepovezano (eksperimentalno) znanje o kakem področju — primere, ki predstavljajo začetno stopničko v razvoju večine teorij, ki opisujejo svet okrog nas.

S tem, precej splošnim pojmom teorije lahko opišemo vrsto pojmov, ki so značilni za teorije, in z dodajanjem pogojev pridemo do posameznih tipov teorij:

Teorija $\mathscr{T} = (\mathscr{E}, \mathscr{I})$ je *podteorija* teorije $\mathscr{T}' = (\mathscr{E}', \mathscr{I}')$, kar označimo $\mathscr{T} \subseteq \mathscr{T}'$, če velja $\mathscr{E} \subseteq \mathscr{E}'$ in $\mathscr{I} \subseteq \mathscr{I}'$. Pravimo tudi, da je $\mathscr{T}'$ *razširitev* ali *nadteorija* teorije $\mathscr{T}$. Teorija $\mathscr{T} = (\mathscr{E}, \mathscr{I})$ je *odločljiva*, če je razred elementarnih izrekov $\mathscr{I}$ odločljiv.

Teorije imajo svoje »življenje«, ki ga pogojujejo potrebe, (z)možnosti, prepričanje in okus nosilcev kulture, kateri pripadajo.

Klasičen primer življenja teorije je razvojna pot geometrije. Njeni začetki segajo k starim poljedelskim narodom (Babilonci, Egipčani), ki so za vsakdanje potrebe zbrali kopico geometrijskega znanja. Od njih so ga povzeli in naprej razvijali stari Grki, ki so se zavedeli in začeli proučevati medsebojne odvisnosti med posameznimi trditvami. Ta pojav (sistematizacije in logične izgradnje) je ponavadi tesno povezan z obsežnostjo nakopičenega znanja: po eni strani neurejeno in nepovezano znanje obremenjuje spomin, po drugi strani pa je za ugotovitev medsebojnih zvez potrebna določena količina znanja. Vrh teh prizadevanj so Evklidovi *Elementi* (okrog 300 p. n. š.), v katerih je vsa tedanja geometrija izpeljana iz peščice trditev — aksiomov. Ta pristop sta pred Evklidom utemejila Aristotel (384—321 p. n. š.) in Evdoks (408—355 p. n. š.), prve korake pa je napravil že Tales (624—546 p. n. š.). Grško geometrijo so rešili pred propadom Arabci. Vse do prejšnjega stoletja se v geometriji ni zgodilo skoraj nič bistveno novega, čeprav so se veliko ukvarjali z njo (aksiom o vzporednicah, trije problemi). Omeniti pa je treba le navidez obrobni dogodek — Descartesovo analitično geometrijo (1637), ki daje zvezo med geometrijo in aritmetiko (števili).

V začetku prejšnjega stoletja so Lobačevskij (1829), Bolyai (1833) in Gauss pokazali, zakaj so bila zaman vsa prizadevanja dokazati aksiom o vzporednicah iz ostalih aksiomov. Izkazalo se je, da je od njih neodvisen — obstajajo geometrije, v katerih velja, pa tudi geometrije, v katerih ne velja. To je bila ena prvih »negativnih« rešitev kakega matematičnega problema; sledila pa jih je cela vrsta: nerešljivost treh klasičnih problemov, Gödelov izrek, ...

Geometrija je izgubila svojo »apriornost«. Do tedaj je vladalo prepričanje, da Evklidovi aksiomi izražajo osnovne lastnosti prostora, v katerem živimo, in ga enolično popisujejo. V primerih, ko so objekti znani pred aksiomi in slednji le opisujejo (na ta ali oni način določene) lastnosti objektov, govorimo o *vsebinski* ali *nazorni aksiomatiki*.

Prvo aksiomatizacijo geometrije, ki se ne sprašuje, kaj so pravzaprav objekti, o katerih govore aksiomi, je podal Hilbert leta 1899 v *Grundlagen der Geometrie*. Temu pristopu pravimo *formalna aksiomatika*. V formalnih teorijah je razred objektov implicitno določen z aksiomi in šele zunaj teorije lahko iščemo odgovor na vprašanje, ali sploh obstaja razred objektov, ki zadošča aksiomom. Pri tem nastopi ena od možnosti:

— ne obstaja razred objektov, ki bi zadoščal aksiomom; teorija je *prazna*;

— aksiomi (do izomorfizma) natanko določajo en sam razred objektov; teorija je *kategorična*;

— obstaja več razredov objektov, ki zadoščajo aksiomom; teorija je *večlična*.

Razvoj geometrije je precej vplival tudi na samo učenje o teorijah. V prejšnjem stoletju so se ji pridružili še: prizadevanja za logično utemeljitev analize (realna števila) in za izgradnjo vse matematike na osnovi pojma naravnega števila, proti koncu stoletja pa še teorija množic. Vendar so ta prizadevanja kmalu naletela na hudo prepreko — paradokse. Pri iskanju izhoda iz nastale situacije so se izoblikovale posamezne struje: logicizem, for-

malizem, intuicionizem, konstruktivizem, ..., ki vsaka po svoje odgovarja na vprašanja: Kaj pomeni obstajati? Kaj je neskončnost? Kakšna je povezava med matematiko (logiko) in svetom? Za vse pa je značilno, da si prizadevajo izogniti se paradoksom s strogostjo in natančnostjo.

Na naslednjih straneh se bomo seznanili z osnovnimi pojmi in spoznanji, ki si jih je nauk o teorijah nabral na prehojeni poti.

Osrednji pojem našega nadaljnjega razmišljanja je pojem

Deduktivne teorije: Teorija $\mathscr{T} = (\mathscr{E}, \mathscr{I})$ je *deduktivna* (ali tudi *efektivno aksiomatizabilna*), če je $\mathscr{I}$ induktivni razred, ki ima za bazo odločljiv razred elementarnih izjav $\mathscr{A}$. Tem izjavam pravimo *aksiomatske izjave* ali kratko kar *aksiomi*. Pravila generiranja razreda $\mathscr{I}$ sestavljajo razred $\mathscr{D}$ *dedukcijskih pravil* ali *pravil izpeljevanja*. Vsako izmed njih da, če ga uporabimo nad ustreznim številom elementarnih izrekov, zopet elementarni izrek. Aksiomi in pravila izpeljevanja določajo skupaj *postulate* teorije $\mathscr{T}$. Konstrukcijskemu zaporedju v deduktivni teoriji pravimo *izpeljava* ali *formalni dokaz*. Termin *dokaz* bomo uporabljali le za sklepanja pri utemeljevanju trditev v opisnem jeziku.

Med deduktivnimi teorijami imajo posebno mesto tako imenovani *sistemi*. To so teorije, za katere določimo razred elementarnih izjav takole: Izhajamo iz konceptualnega razreda *formalnih objektov* in konceptualnega razreda *baznih* ali *osnovnih predikatov*. Vsakemu osnovnemu predikatu je prirejeno naravno število — njegova *stopnja*. Elementarne izjave dobimo tako, da uporabimo bazične predikate nad ustreznimi zaporedji formalnih objektov. Tako $P(a_1, a_2, \ldots, a_n)$ označuje elementarno izjavo, ki jo dobimo, če uporabimo predikat P stopnje n nad zaporedjem $a_1, a_2, \ldots, a_n$, ki ga sestavlja n formalnih objektov.

Primer: Za primer deduktivne teorije si oglejmo teorijo, ki sestavlja jedro večine »klasičnih« teorij — to je *izjavni račun*:

Abecedo izjavnega računa sestavljajo naslednji simboli

$$\neg, \quad \Rightarrow, \quad (, \quad), \quad \mathbf{s}, \quad |$$

Iz njih najprej zgradimo induktivni razred izjavnih spremenljivk, ki je določen s praviloma:

IS1. s je izjavna spremenljivka;

IS2. če je X izjavna spremenljivka, potem je izjavna spremenljivka tudi izraz $X|$.

Očitno so izjavne spremenljivke natanko izrazi oblike

$$\mathbf{s}\underbrace{||||\ldots|}_{i}|$$

za katere vpeljemo okrajšavo s_i. S tem smo dosegli končen zapis pojma spremenljivke, ki ga v opisih izjavnega računa običajno vpeljejo takole: »Naj bo dana števna množica izjavnih spremenljivk $s_0, s_1, s_2, \ldots$«. Razred izjavnih spremenljivk je monotektoničen.

Tudi razred izjav izjavnega računa je induktiven. Določata ga pravili:

IZ1. izjavne spremenljivke so izjave;

IZ2. če sta A in B izjavi, sta izjavi tudi izraza $\neg A$ in $(A \Rightarrow B)$.

Aksiome izjavnega računa določajo tri sheme aksiomov:

IRA1. $(A \Rightarrow (B \Rightarrow A))$

IRA2. $((A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C))$

IRA3. $((\neg B \Rightarrow \neg A) \Rightarrow (A \Rightarrow B))$

pri čemer opisne spremenljivke A, B in C označujejo poljubne izjave.

V izjavnem računu imamo eno samo pravilo izpeljevanja (Modus ponens):

MP. $$\frac{A, \quad (A \Rightarrow B)}{B}$$

Seveda je to samo eden od obstoječih formalnih opisov izjavnega računa.

Pojem deduktivne teorije uporabljamo tudi v računalništvu pri aksiomatizaciji semantike programskih jezikov, na kateri temelji dokazovanje pravilnosti programov [1].

Sheme: V opisu izjavnega računa smo aksiome (in tudi pravila izpeljevanja) podali s tako imenovanimi *shemami aksiomov* (*pravil*). Vsaka shema aksiomov določa cel razred aksiomov. Posamezni primerek aksioma dobimo, če opisne spremenljivke, ki nastopajo v shemi, nadomestimo s konkretnimi izjavami. Tako je na primer

$$((\neg \mathbf{s}\,|\,| \Rightarrow \neg \mathbf{s}\,|) \Rightarrow (\mathbf{s}\,| \Rightarrow \mathbf{s}\,|\,|))$$

aksiom izjavnega računa, ki ga dobimo po shemi IRA3.

Kakor vidimo, imajo opisne spremenljivke pri opisu teorij pomembno vlogo. Pojem spremenljivke pa smo srečali tudi v nekoliko drugačnem pomenu (izjavna spremenljivka v izjavnem računu). Tem spremenljivkam pravimo *formalne spremenljivke*.

Uporabo shem je uvedel leta 1927 von Neumann. Predtem so pri opisu teorije podali le končno število aksiomov; med pravila izpeljevanja pa so vključevali pravilo zamene, ki zagotavlja, da bomo iz vsakega izreka z zameno formalne spremenljivke s poljubno izjavo zopet dobili izrek. Zvezo med temi teorijami in teorijami s shemami aksiomov daje naslednja trditev:

T1. Bodi $\mathscr{T}$ teorija s shemami aksiomov in formalnimi spremenljivkami. Teorija $\mathscr{T}'$ pa naj bo določena takole: aksiome teorije $\mathscr{T}'$ dobimo tako, da različne opisne spremenljivke v shemah teorije $\mathscr{T}$ zamenjamo z različnimi formalnimi spremenljivkami; pravila teorije $\mathscr{T}'$ sestavljajo pravila teorije $\mathscr{T}$, katerim dodamo še pravilo zamene, ki deluje nad formalnimi spremenljivkami; izpolnjen je pogoj invariantnosti — če naredimo zameno v nekem pravilu izpeljevanja, dobimo zopet primerek istega pravila. Potem imata obe teoriji iste elementarne izreke.

Dokaz: Prepričajmo se o tem! Z zameno dobimo v $\mathscr{T}'$ vsak aksiom teorije $\mathscr{T}$. Torej za vsako izpeljavo v teoriji $\mathscr{T}$ obstaja tudi izpeljava v teoriji $\mathscr{T}'$; oziroma $\mathscr{F} \subseteq \mathscr{F}'$. V obratno smer sklepamo takole. Z induktivno posplošitvijo pokažemo najprej, da je pravilo zamene dopustno v $\mathscr{T}$, oziroma da vsaka zamena v izreku teorije $\mathscr{T}$ da zopet izrek teorije $\mathscr{T}$. Res! Trditev za aksiome teorije $\mathscr{T}$ velja, ker da vsaka zamena v aksiomu zopet aksiom; po pogoju invariantnosti pa se po izpeljavi prenaša tudi na izreke. Upoštevajmo še, da je vsak aksiom teorije $\mathscr{T}'$ tudi aksiom teorije $\mathscr{T}$, pa imamo tudi $\mathscr{F}' \subseteq \mathscr{F}$. Trditev je dokazana.

Aksiomatske razširitve: Deduktivno teorijo $\mathscr{T}$ potemtakem določajo: razred elementarnih izjav $\mathscr{E}$, odločljiv razred aksiomov $\mathscr{A}$ in razred (odločljivih) pravil izpeljevanja $\mathscr{D}$. Razred $\mathscr{I}$ izrekov teorije $\mathscr{T}$ določata razreda $\mathscr{A}$ in $\mathscr{D}$, kar bomo zapisali

$$\mathscr{I} = Cn(\mathscr{A}, \mathscr{D})$$

(*Cn* je okrajšava angleške besede *consequence*).

Poglejmo najprej, kaj lahko povemo o razširitvah deduktivnih teorij! Kot vemo, teorijo $\mathscr{T} = (\mathscr{E}, \mathscr{I})$ razširimo, če povečamo razred elementarnih izjav $\mathscr{E}$ ali razred elementarnih izrekov $\mathscr{I}$.

V deduktivnih teorijah, v katerih je tudi razred elementarnih izjav induktiven, lahko slednjega razširimo na več načinov: z uvedbo novih simbolov v abecedo, s povečanjem baze razreda ali z dodajanjem novih pravil generiranja. Če so pri tem aksiomi in pravila izpeljevanja teorije $\mathscr{T}$ podani s shemami, običajno te sheme posplošimo tudi na nove elementarne

izjave. Očitno lahko tedaj razprostremo na nove elementarne izjave tudi vse v teoriji $\mathscr{T}$ izpeljane sheme izrekov in pravil izpeljevanja. Tako na primer dobimo iz vsakega izreka izjavnega računa, če zamenjamo izjavne spremenljivke, ki vanj vstopajo, z dobro oblikovanimi formulami teorije prvega reda, kak izrek te teorije.

Precej zanimivejše razširitve dobimo, če razredu aksiomov $\mathscr{A}$ teorije $\mathscr{T} = (\mathscr{E}, \mathscr{I})$ dodamo kot nove aksiome razred elementarnih izjav $\mathscr{B}$; govorimo o *aksiomatski razširitvi* teorije $\mathscr{T}$. Teorija $\mathscr{T}' = (\mathscr{E}, Cn(\mathscr{A} \cup \mathscr{B}, \mathscr{D}))$, ki jo tako dobimo, je deduktivna, če je razred $\mathscr{B}$ odločljiv in če se odločljivost pravil izpeljevanja pri razširitvi ne poruši.

Deduktivno zaprtje: Pojem aksiomatske razširitve nas navede na misel, da lahko pravzaprav gledamo na $Cn(—, \mathscr{D})$ tudi kot na operacijo (preslikavo), definirano nad vsemi podrazredi razreda $\mathscr{E}$. Ker se pri aksiomatskih razširitvah razred $\mathscr{D}$ ne spreminja, bomo to operacijo krajše označevali kar s Cn.

Operaciji Cn pogosto pravijo tudi *deduktivno zaprtje*, saj ima vse lastnosti, ki jih za zaprtja zahtevamo v matematiki: bodita $\mathscr{A}, \mathscr{B} \subseteq \mathscr{E}$, potem velja (to naj bralec sam preveri):

Cn1. $\mathscr{A} \subseteq Cn(\mathscr{A})$

Cn2. $Cn(Cn(\mathscr{A})) \subseteq Cn(\mathscr{A})$

Cn3. $\mathscr{A} \subseteq \mathscr{B} \Rightarrow Cn(\mathscr{A}) \subseteq Cn(\mathscr{B})$

Poleg tega pa velja še posebna lastnost, ki povzema končnost izpeljav

Cn4. $E \in Cn(\mathscr{A}) \Rightarrow \exists\, \mathscr{B} \subseteq \mathscr{A} : card(\mathscr{B}) < \aleph_0 \wedge E \in Cn(\mathscr{B})$

Navedene štiri lastnosti operacijo Cn za naše namene dovolj natančno opisujejo. Iz njih lahko izpeljemo še vrsto zanimivih lastnosti:

Naj bodo v nadaljnjem $\mathscr{A}, \mathscr{B}, \mathscr{C}, \mathscr{D} \subseteq \mathscr{E}$; potem veljajo naslednje lastnosti

Cn5. $Cn(Cn(\mathscr{A})) = Cn(\mathscr{A})$

Cn6. $\mathscr{A} \subseteq \mathscr{B} \wedge \mathscr{B} \subseteq Cn(\mathscr{C}) \Rightarrow \mathscr{A} \subseteq Cn(\mathscr{C})$

Cn7. $\mathscr{A} \subseteq Cn(\mathscr{B}) \wedge \mathscr{B} \subseteq Cn(\mathscr{C}) \Rightarrow \mathscr{A} \subseteq Cn(\mathscr{C})$

Cn8. $\mathscr{A} \subseteq Cn(\mathscr{B}) \Leftrightarrow Cn(\mathscr{A}) \subseteq Cn(\mathscr{B})$

Cn9. $\mathscr{A} \subseteq Cn(\mathscr{B}) \Rightarrow \mathscr{A} \subseteq Cn(\mathscr{B} \cup \mathscr{C})$

Cn10. $\mathscr{A} \subseteq Cn(\mathscr{C}) \wedge \mathscr{B} \subseteq Cn(\mathscr{C}) \Rightarrow \mathscr{A} \cup \mathscr{B} \subseteq Cn(\mathscr{C})$

Cn11. $Cn(\mathscr{A} \cup \mathscr{B}) = Cn(\mathscr{A} \cup Cn(\mathscr{B})) = Cn(Cn(\mathscr{A}) \cup Cn(\mathscr{B}))$

Cn12. $\mathscr{A} \subseteq Cn(\mathscr{B} \cup \mathscr{C}) \wedge \mathscr{B} \subseteq Cn(\mathscr{D}) \Rightarrow \mathscr{A} \subseteq Cn(\mathscr{C} \cup \mathscr{D})$

Za primer se prepričajmo o veljavnosti lastnosti Cn11.

Ker je relacija $\subseteq$ usklajena (kompatibilna) z operacijo $\cup$, je po Cn 1 $\mathscr{A} \cup \mathscr{B} \subseteq \mathscr{A} \cup Cn(\mathscr{B})$ in $\mathscr{A} \cup Cn(\mathscr{B}) \subseteq Cn(\mathscr{A}) \cup Cn(\mathscr{B})$ in dalje po Cn 3

$$Cn(\mathscr{A} \cup \mathscr{B}) \subseteq Cn(\mathscr{A} \cup Cn(\mathscr{B})) \subseteq Cn(Cn(\mathscr{A}) \cup Cn(\mathscr{B})) \qquad (*)$$

Po isti lastnosti sledi iz $\mathscr{A} \subseteq \mathscr{A} \cup \mathscr{B}$ tudi $Cn(\mathscr{A}) \subseteq Cn(\mathscr{A} \cup \mathscr{B})$. Podobno dobimo še $Cn(\mathscr{B}) \subseteq$ $\subseteq Cn(\mathscr{A} \cup \mathscr{B})$, kar da združeno $Cn(\mathscr{A}) \cup Cn(\mathscr{B}) \subseteq Cn(\mathscr{A} \cup \mathscr{B})$. Upoštevajmo še Cn 3 in Cn 5, pa imamo

$$Cn(Cn(\mathscr{A}) \cup Cn(\mathscr{B})) \subseteq Cn(\mathscr{A} \cup \mathscr{B}) \qquad (**)$$

Združimo (*) in (**) in lastnost Cn 11 je dokazana.

Namesto $E \in Cn(\mathscr{A})$ oziroma $\mathscr{B} \subseteq Cn(\mathscr{A})$ pišejo logiki raje $\mathscr{A} \vdash E$ oziroma $\mathscr{A} \vdash \mathscr{B}$. Prepišimo nekaj lastnosti operacije Cn v to obliko:

Cn1*. $\mathscr{A} \vdash \mathscr{A}$

Cn6*. $\mathscr{A} \subseteq \mathscr{B} \wedge \mathscr{C} \vdash \mathscr{B} \Rightarrow \mathscr{C} \vdash \mathscr{A}$

Cn7*. $\mathscr{C} \vdash \mathscr{B} \wedge \mathscr{B} \vdash \mathscr{A} \Rightarrow \mathscr{C} \vdash \mathscr{A}$

Cn9*. $\mathscr{B} \vdash \mathscr{A} \Rightarrow \mathscr{B} \cup \mathscr{C} \vdash \mathscr{A}$

Cn10*. $\mathscr{C} \vdash \mathscr{A} \wedge \mathscr{C} \vdash \mathscr{B} \Rightarrow \mathscr{C} \vdash \mathscr{A} \cup \mathscr{B}$

Cn12*. $\mathscr{D} \vdash \mathscr{B} \wedge \mathscr{B} \cup \mathscr{C} \vdash \mathscr{A} \Rightarrow \mathscr{D} \cup \mathscr{C} \vdash \mathscr{A}$

Ko je $\mathscr{A}$ razred aksiomov deduktivne teorije $\mathscr{T}$, se namesto $\mathscr{A} \vdash E$ pogosteje uporablja zapis $\vdash_{\tau} E$. V tem smislu trditev $E \in Cn(\mathscr{A} \cup \mathscr{B})$ zapišemo $\mathscr{B} \vdash_{\tau} E$.

Podrobneje se je z operacijo Cn ukvarjal Tarski, ki jo je vzel za osnovo svojega nauka o teorijah. Deduktivno teorijo lahko po Tarskem z operacijo Cn definiramo takole: teorija $\mathscr{T} = (\mathscr{E}, \mathscr{I})$ je deduktivna, če razred elementarnih izrekov $\mathscr{I}$ vsebuje vse svoje posledice, torej če velja

$$\mathscr{I} = Cn(\mathscr{I})$$

Da deduktivne teorije res zadoščajo temu pogoju, je razvidno iz lastnosti Cn5. Vsaka teorija je deduktivna po Tarskem, če vzamemo za Cn kar identiteto.

V tem primeru se postavi vprašanje aksiomatizabilnosti. Kakor bomo videli na naslednjih straneh, obstajajo tudi teorije, ki niso efektivno aksiomatizabilne — ne obstaja odločljiv razred $\mathscr{A}$, tako da velja $\mathscr{I} = Cn(\mathscr{A})$.

Še nekaj o razširitvah: Poleg razredov elementarnih izjav $\mathscr{E}$ in aksiomov $\mathscr{A}$, lahko obogatimo še razred pravil izpeljevanja $\mathscr{D}$. V vseh teh primerih dosežemo želeni učinek $\mathscr{I} \subseteq \mathscr{I}'$. Tega pa lahko dosežemo tudi drugače: z uvedbo novih aksiomov $\mathscr{A}'$ in pravil izpeljevanja $\mathscr{D}'$, ki so deduktivno močnejša:

$$\mathscr{I} = Cn(\mathscr{A}, \mathscr{D}) \subseteq Cn(\mathscr{A}', \mathscr{D}') = \mathscr{I}'$$

Pri tem mora seveda veljati $\mathscr{E} \subseteq \mathscr{E}'$.

V posebnem primeru, ko je $\mathscr{E}' = \mathscr{E}$ in $Cn(\mathscr{A}, \mathscr{D}) = Cn(\mathscr{A}', \mathscr{D}')$, pravimo, da sta teoriji $\mathscr{T}$ in $\mathscr{T}'$ *ekvivalentni*.

Razširitev $\mathscr{T}'$ teorije $\mathscr{T}$ je *konservativna* natanko takrat, ko je

$$Cn(\mathscr{A}, \mathscr{D}) = Cn(\mathscr{A}', \mathscr{D}') \cap \mathscr{E}$$

Če zamenjamo samo razred aksiomov, velja naslednja trditev:

T2. Teorija $\mathscr{T}' = (\mathscr{E}, Cn(\mathscr{A}'))$ je aksiomatska razširitev teorije $\mathscr{T} = (\mathscr{E}, Cn(\mathscr{A}))$ natanko takrat, ko so aksiomi teorije $\mathscr{T}$ izreki teorije $\mathscr{T}'$.

Dokaz: Da so aksiomi teorije $\mathscr{T}$ izreki teorije $\mathscr{T}'$, hitro uvidimo: Ker je $\mathscr{T}'$ razširitev teorije $\mathscr{T}$, je $\mathscr{J} \subseteq \mathscr{J}'$; in ker vsak induktivni razred vsebuje svojo bazo, je $\mathscr{A} \subseteq \mathscr{J}$. Od tu pa po tranzitivnosti relacije $\subseteq$ končno $\mathscr{A} \subseteq \mathscr{J}'$.

V nasprotno smer gre še lažje. Iz besedila trditve izvemo: $\mathscr{A} \subseteq Cn(\mathscr{A}')$. Uporabimo najprej lastnost Cn3 in nato še Cn5, pa smo pri koncu $\mathscr{J} = Cn(\mathscr{A}) \subseteq Cn(Cn(\mathscr{A}')) = Cn(\mathscr{A}') = \mathscr{J}'$

Neprotislovnost, polnost, odločljivost in neodvisnost

Neprotislovnost: Teorije, ki vsebujejo izjavni račun (»običajno« logiko), veljajo za protislovne, če v njih obstaja vsaj ena elementarna izjava E taka, da sta tako E kakor tudi njena negacija $\neg E$ izreka teorije.

Kaj pa lahko naredimo takrat, ko v teoriji ne poznamo negacije? Po analogiji z negacijo lahko rečemo:

Naj bo dana preslikava med elementarnimi izjavami teorije $\mathscr{T}$

$$f: E \mapsto \bar{E}$$

potem je teorija $\mathscr{T} = (\mathscr{E}, \mathscr{I})$ *neprotislovna* (ali *soglasna*) *na preslikavo* f natanko takrat, ko ne obstaja nobena elementarna izjava $E \in \mathscr{E}$, tako da bi bili hkrati E, $\overline{E} \in \mathscr{I}$.

Očitno v na preslikavo f neprotislovni teoriji fiksne točke ($f(E) = E$) preslikave f niso izreki.

Na zastavljeno vprašanje obstaja še en odgovor, ki izhaja iz ugotovitve, da je v protislovni teoriji $\mathscr{T} = (\mathscr{E}, \mathscr{I})$, ki vsebuje izjavni račun, vsaka elementarna izjava izrek.

Razmišljamo takole. Ker je teorija $\mathscr{T}$ protislovna, obstaja elementarna izjava E, tako da sta E, $\neg E \in \mathscr{I}$. Torej

(1) E

(2) $\neg E$

in naprej za katerokoli elementarno izjavo D po izjavnem računu

(3) $(\neg E \Rightarrow (\neg D \Rightarrow \neg E))$	IRA1
(4) $(\neg D \Rightarrow \neg E)$	MP (2), (3)
(5) $((\neg D \Rightarrow \neg E) \Rightarrow (E \Rightarrow D))$	IRA3
(6) $(E \Rightarrow D)$	MP (4), (5)
(7) D	MP (1), (6)

Torej je res $\mathscr{I} = \mathscr{E}$. Iz izpeljave pa lahko povzamemo še, da v izjavnem računu velja pravilo izpeljevanja

$$\frac{E,\ \neg E}{D}$$

Če dokazano trditev posplošimo tudi na teorije, ki ne vsebujejo izjavnega računa, lahko rečemo:

Teorija $\mathscr{T}$ je *absolutno* (ali *po Postu*) *neprotislovna* natanko takrat, ko razreda elementarnih izjav $\mathscr{E}$ in izrekov $\mathscr{I}$ ne sovpadata; oziroma krajše, ko $\mathscr{I} \neq \mathscr{E}$.

Iz pravkar povedanega lahko sklepamo:

T3. Naj v teoriji $\mathscr{T} = (\mathscr{E}, \mathscr{I})$ velja pravilo izpeljevanja

Pf.
$$\frac{E,\ \overline{E}}{D}$$

in naj bo absolutno neprotislovna, potem je neprotislovna tudi na preslikavo $f: E \mapsto \overline{E}$.

Dokaz: Recimo, da to ne bi bilo res. Potem obstaja elementarna izjava E, za katero sta E, $\overline{E} \in \mathscr{J}$. Od tu pa po Pf sledi $\mathscr{J} = \mathscr{E}$, kar je v nasprotju z absolutno neprotislovnostjo teorije $\mathscr{T}$.

V obratno smer velja trditev vedno:

T4. Če je teorija $\mathscr{T} = (\mathscr{E}, \mathscr{I})$ neprotislovna na preslikavo $f: E \mapsto \overline{E}$, je tudi absolutno neprotislovna.

Dokaz: Res. Vzemimo poljubno elementarno izjavo $E \in \mathscr{J}$. Ker je teorija $\mathscr{T}$ neprotislovna na f, elementarna izjava $\overline{E} \notin \mathscr{J}$: torej $\mathscr{E} \neq \mathscr{J}$.

Kako je z razširitvami neprotislovnih teorij? Najbrž trditev:

T5. Konservativna razširitev absolutno neprotislovne teorije je absolutno neprotislovna.

ne potrebuje posebne razlage. Ker lahko s povečanjem razreda elementarnih izjav absolutno protislovno teorijo pretvorimo v absolutno neprotislovno, gornja trditev v obratno smer ne velja. Pač pa velja:

T6. Naj bo $\mathscr{T}' = (\mathscr{E}', \mathscr{I}')$ razširitev teorije $\mathscr{T} = (\mathscr{E}, \mathscr{I})$ in naj bo $\mathscr{T}'$ neprotislovna na $f: E \mapsto \bar{E}$ ter $f(\mathscr{E}) \subset \mathscr{E}$, potem je na f neprotislovna tudi teorija $\mathscr{T}$.

Dokaz: Vzemimo poljubno elementarno izjavo E teorije $\mathscr{T}$. Ker je $\mathscr{T}'$ neprotislovna na f, vsaj ena od izjav E in $\bar{E}$ ni izrek teorije $\mathscr{T}'$ in potemtakem, zaradi $\mathscr{I} \subseteq \mathscr{I}'$, tudi ni izrek teorije $\mathscr{T}$. Teorija $\mathscr{T}$ je neprotislovna na f.

Če v teoriji $\mathscr{T}$ in njeni razširitvi velja pravilo Pf, potem je absolutna neprotislovnost enakovredna z neprotislovnostjo na f in lahko zadnji trditvi združimo v:

T7. Naj v teoriji $\mathscr{T}$ in njeni konservativni razširitvi $\mathscr{T}'$ velja za preslikavo $f: E \mapsto \bar{E}$ pravilo Pf in je $f(\mathscr{E}) \subset \mathscr{E}$, potem je teorija $\mathscr{T}'$ neprotislovna na f natanko takrat, ko je na f neprotislovna teorija $\mathscr{T}$.

Polnost: Naj bo $\mathscr{T}$ neprotislovna teorija, ki vsebuje izjavni račun. Potem je, kakor vemo, za poljubno elementarno izjavo $E \in \mathscr{E}$ kvečjemu ena od izjav E in $\neg E$ izrek teorije $\mathscr{T}$. Zelo lepo bi bilo, če bi ta »kvečjemu« lahko nadomestili z »natanko«. Takim teorijam pravimo, da so polne. Žal je polnost usojena le redkim in precej enostavnim teorijam.

Za nepolnostjo bolehajo vse izrazno kolikor toliko močne teorije, v katerih lahko izrazimo *paradoks lažnivca*. Ta paradoks so poznali v različnih inačicah že v starem veku (Egipčani, Grki). Najbolj znano verzijo (zašla je celo v sveto pismo nove zaveze) pripisujejo Epimenidu (VI. p. n. š.), ki je baje ob neki priliki dejal:

»Vsak Krečan vedno laže.«

Težave so v tem, da je bil Krečan tudi Epimenid sam.

Ta verzija bi bila pravi paradoks le, če bi bil to edini stavek, ki ga je kdaj koli izgovoril kak Krečan. Ta pomanjkljivost je odpravljena v Evbulidovi (IV. p. n. š.) inačici: »Stavek, ki ga pravkar izrekam, je laž.«

Za naše namene bomo paradoks lažnivca nekoliko predelali. Naj izjava I trdi o sebi

Izjava I ni izrek. (1)

(izrek $\equiv$ v teoriji izpeljiva izjava) in privzemimo še

Neresnične izjave niso izreki. (2)

saj pri izgradnji teorij težimo za tem, da bi razred izrekov in razred resničnih izjav sovpadala; vsekakor pa naj bodo izpeljive le resnične izjave. Kaj lahko povemo o izjavi I? Prav gotovo ni neresnična. Recimo, da bi bila. Potem po (1) ne bi ne bila izrek, kar je v nasprotju z (2). Poglejmo si še primer, ko je I resnična. Zaradi (1) ne more biti hkrati tudi izrek. Ostane le še možnost, da je izjava I resnična in ni izrek. Tedaj je njena negacija $\neg I$ neresnična in po (2) tudi ni izrek.

Povzemimo: v teorijah, ki vsebujejo izjavni račun in dopuščajo paradoks lažnivca, obstaja resnična izjava I, tako da pri predpostavki (2) ni nobena od izjav I in $\neg I$ izrek (izpeljiva).

Za samo matematiko je zelo pomemben, sicer pa nič kaj razveseljiv rezultat (Gödel 1931): paradoks lažnivca je izrazljiv v rekurzivni aritmetiki — formalizirani teoriji naravnih števil in funkcij nad njimi. Osnovna ideja Gödelovega dokaza je v prevodu trditev o naravnih številih iz opisnega jezika (na primer z matematičnimi sredstvi pomešane slovenščine) v aritmetiko. S tem je dosegel, da je aritmetika postala sama sebi opisni jezik. Nato je s Cantorjevim diagonalnim sklepom (glej stran 45), ki ga vsak matematik pozna iz dokaza neštevnosti množice realnih števil, prišel do resnične izjave, ki izraža svojo lastno neizpeljivost — paradoks lažnivca. Tako je v teoriji sami dokazal trditev: če je rekurzivna aritmetika neprotislovna teorija, potem ni polna. Še več, izkaže se, da je tudi v teoriji, ki jo

dobimo, če rekurzivno aritmetiko aksiomatsko razširimo z izjavo I, paradoks lažnivca še naprej izrazljiv — rekurzivna aritmetika je bistveno nepolna.

To spoznanje je predvsem hudo prizadelo formalistični program osnovanja matematike, ki ga je začel v začetku tega stoletja Hilbert s somišljeniki. Gödelov izrek je pokazal utopičnost osnovnega cilja formalistov: formalizacije in dokaza neprotislovnosti klasične matematike s »finitnimi« sredstvi. Leta 1936 je Church dokazal na podoben način, da vprašanje, ali je dana izjava izrek rekurzivne aritmetike, ni odločljivo. S tem je pokazal tudi nedosegljivost drugega cilja formalistov: poiskati za področja klasične matematike take efektivne postopke, ki bi dani problem rešili v končnem številu korakov ali pa ugotovili njegovo nerešljivost. Tretji pomemben rezultat, povezan z Gödelovim izrekom, je izrek Tarskega (1931), ki trdi, da v nobeni neprotislovni teoriji, ki vsebuje rekurzivno aritmetiko, ne moremo ustrezno definirati njene lastne semantike (teorije resnice).

Pojem polnosti lahko prenesemo tudi na teorije brez negacije. Podobno kot pri neprotislovnosti, poznamo tudi tu polnost glede na preslikavo f in absolutno polnost.

Teorija $\mathscr{T}$ je *polna na preslikavo* $f: E \mapsto \bar{E}$ natanko takrat, ko je za vsako elementarno izjavo $E \in \mathscr{E}$ natanko ena od izjav E in $\bar{E}$ izrek teorije $\mathscr{T}$.

Če je teorija polna na preslikavo f, očitno ta nima fiksnih točk.

Recimo, da je teorija $\mathscr{T}$ polna na f. Izberimo poljubno elementarno izjavo E, ki ni izrek teorije $\mathscr{T}$. Kaj lahko rečemo o teoriji $\mathscr{T}' = (\mathscr{E}, Cn(\mathscr{I} \cup \{E\}))$? Ker je $\mathscr{T}$ polna in E ni izrek $\mathscr{T}$, je izrek $\bar{E}$. Torej $\bar{E} \in \mathscr{I}$. To pomeni, da sta E in $\bar{E}$ izreka teorije $\mathscr{T}'$, ki je potemtakem protislovna na f. To lastnost izberemo za definicijo absolutne (po Postu) polnosti.

Neprotislovna teorija $\mathscr{T} = (\mathscr{E}, \mathscr{I})$ je *absolutno polna* natanko takrat, ko je za vsako elementarno izjavo $E \in \mathscr{E}$, ki ni elementarni izrek ($E \notin \mathscr{I}$), teorija $(\mathscr{E}, Cn(\mathscr{I} \cup \{E\}))$ protislovna; ali drugače povedano, ko je

$$Cn(\mathscr{I} \cup \{E\}) = \mathscr{E}$$

V nadaljevanju bomo potrebovali še en pojem: Teorija $\mathscr{T} = (\mathscr{E}, \mathscr{I})$ je *neprotislovno razširljiva glede na* f natanko takrat, ko pri aksiomatski razširitvi s poljubno elementarno izjavo E, za katero E in $\bar{E}$ nista izreka, ostane neprotislovna na f. Neprotislovno glede na $\neg$ so razširljive vse teorije, ki vsebujejo izjavni račun in zanje velja izrek o dedukciji (glej str. 34—40).

Kako sta obe polnosti povezani?

T8. Če je glede na f neprotislovno razširljiva teorija $\mathscr{T}$ absolutno polna, potem je polna tudi na preslikavo f.

Dokaz: Predpostavimo nasprotno: teorija ni polna na f. Tedaj obstaja izjava E tako, da $E, \bar{E} \notin \mathscr{I}$. Razširimo $\mathscr{T}$ z E. Tako dobimo zaradi neprotislovne razširljivosti teorije $\mathscr{T}$ glede na f neprotislovno teorijo $\mathscr{T}'$, ki je tudi absolutno neprotislovna; to je v nasprotju s predpostavko o absolutni polnosti teorije $\mathscr{T}$.

V nasprotno smer pa velja:

T9. Če je teorija $\mathscr{T}$ polna na preslikavo f in v njej velja pravilo Pf, potem je tudi absolutno polna.

Dokaz: Poglejmo aksiomatsko razširitev $\mathscr{T}'$ teorije $\mathscr{T}$ s poljubno elementarno izjavo $E \notin \mathscr{I}$. Ker je $\mathscr{T}$ polna glede na f, je $\bar{E} \in \mathscr{I}$ in dalje $E, \bar{E} \in \mathscr{I}'$. Od tu pa po Pf izhaja $\mathscr{I}' = Cn(\mathscr{I} \cup \{E\}) = \mathscr{E}$. Teorija $\mathscr{T}$ je absolutno polna.

Polnost in odločljivost: Polne deduktivne teorije imajo naslednjo pomembno lastnost:

T10. Deduktivna teorija $\mathscr{T}$, ki je polna na f, je tudi odločljiva.

Dokaz: Oštevilčimo na neki način vse elementarne izjave. Iz njih sestavimo razred vseh končnih zaporedij elementarnih izjav. Tudi tega lahko oštevilčimo. Ker sta pojma »biti aksiom« in »sledi po

pravilu izpeljevanja« odločljiva, je tudi pojem »biti izpeljava« odločljiv za vsako končno zaporedje elementarnih izjav. Potemtakem lahko iz razreda vseh končnih zaporedij izberemo razred vseh izpeljav. Vzemimo sedaj poljubno elementarno izjavo $E \in \mathscr{E}$. Ker je $\mathscr{T}$ polna in neprotislovna na f, je natanko ena izmed elementarnih izjav E in $\bar{E}$ izrek (izpeljiva). To pomeni, da obstaja naravno število n, kateremu pripadajoče zaporedje je izpeljava tega izreka. Torej lahko z zaporednim preborom razreda vseh izpeljav za poljubno elementarno izjavo v končnem številu korakov ugotovimo, ali je elementarni izrek ali ni — teorija $\mathscr{T}$ je odločljiva.

Polnost nam zagotavlja končnost opisanega postopka prebora. V nepolni teoriji se namreč lahko zgodi, da za neko elementarno izjavo E niti E niti $\bar{E}$ ni izrek teorije. V tem primeru bi opisani postopek prebora tekel v neskončnost.

Poglejmo si še en pomemben rezultat v zvezi s polnostjo teorij — izrek Lindenbauma:

T11. Naj bo v neprotislovni na f teoriji $\mathscr{T} = (\mathscr{E}, \mathscr{I})$ vsaka njena nepolna razširitev neprotislovno aksiomatsko razširljiva; potem obstaja polna teorija $\mathscr{T}^* = (\mathscr{E}, \mathscr{I}^*)$, ki je aksiomatska razširitev teorije $\mathscr{T}$.

Dokaz: Označimo z $\mathscr{N}$ razred vseh podrazredov razreda elementarnih izjav $\mathscr{E}$, katerih deduktivno zaprtje (glede na $\mathscr{T}$) je neprotislovno

$$\mathscr{N} = \{\mathscr{A} \mid \mathscr{A} \subset \mathscr{E} \wedge \neg \exists E \in \mathscr{E} : E,\ \bar{E} \in Cn(\mathscr{I} \cup \mathscr{A})\}$$

Pokažimo najprej, da ima razred $\mathscr{N}$ *končen značaj*: to pomeni, da razred $\mathscr{A} \subset \mathscr{E}$ pripada razredu $\mathscr{N}$ natanko takrat, ko pripada razredu $\mathscr{N}$ vsak njegov končni podrazred $\mathscr{A}' \subset \mathscr{A}$. Če je $\mathscr{A} \in \mathscr{N}$, vidimo iz lastnosti Cn3, da velja

$$\mathscr{A}' \subseteq \mathscr{A} \wedge \mathscr{A} \in \mathscr{N} \Rightarrow \mathscr{A}' \in \mathscr{N}$$

No, če $\mathscr{A} \notin \mathscr{N}$, pa lahko vedno dobimo končen podrazred $\mathscr{A}' \subseteq \mathscr{A}$, tako da tudi $\mathscr{A}' \notin \mathscr{N}$. Ker $\mathscr{A} \notin \mathscr{N}$,

$$\exists E \in \mathscr{E} : E,\ \bar{E} \in Cn(\mathscr{I} \cup \mathscr{A})$$

Po Cn4 obstajata končna razreda $\mathscr{B}, \mathscr{C} \subset \mathscr{A}$, tako da je $\mathscr{B} \vdash_\tau E$ in $\mathscr{C} \vdash_\tau \bar{E}$. Postavimo $\mathscr{A}' = \mathscr{B} \cup \mathscr{C}$, pa vidimo: $\mathscr{A}'$ je končen in $\mathscr{A}' \vdash_\tau E, \bar{E}$ oziroma $\mathscr{A}' \notin \mathscr{N}$. S tem je končni značaj razreda $\mathscr{N}$ dokazan.

Za razrede s končnim značajem velja (iz teorije množic sposojena) lema Teichmüller-Tukeya, ki je enakovredna aksiomu izbire in zagotavlja:

Vsak neprazen razred končnega značaja $\mathscr{K}$ podrazredov razreda $\mathscr{E}$ ima *maksimalni element* — razred, ki ni podrazred nobenega drugega razreda iz $\mathscr{K}$.

Po tej lemi obstaja v $\mathscr{N}$ razred $\mathscr{A}^*$, ki je maksimalni element razreda $\mathscr{N}$. Ker je $\mathscr{A}^* \in \mathscr{N}$, je teorija $\mathscr{T}^* = (\mathscr{E}, \mathscr{I}^*)$, pri čemer je $\mathscr{I}^* = Cn(\mathscr{I} \cup \mathscr{A}^*)$, neprotislovna na f razširitev teorije $\mathscr{T}$. Pokažimo še, da je $\mathscr{T}^*$ tudi polna na f.

Dokazujemo s protislovjem. Recimo, da $\mathscr{T}^*$ ni polna. Potem obstaja $E \in \mathscr{E}$, tako da $E, \bar{E} \notin \mathscr{I}^*$ in je zaradi neprotislovne razširljivosti tudi teorija $\mathscr{T}' = (\mathscr{E}, Cn(\mathscr{I}^* \cup \{E\}))$ neprotislovna razširitev teorije $\mathscr{T}$ ter zato $\mathscr{A}^* \cup \{E\} \in \mathscr{N}$; to pa je v nasprotju z maksimalnostjo razreda $\mathscr{A}^*$.

Na videz je Lindenbaumov izrek v nasprotju z ugotovitvama, da so vse kolikor toliko bogate (deduktivne) teorije neodločljive (Gödel, Church) in da so polne deduktivne teorije odločljive. Edini možni odgovor, če verjamemo izrekom, je, da polne razširitve teorij, ki zadoščajo Gödelovemu izreku in njegovim inačicam, niso deduktivne — efektivno aksiomatizabilne: torej so zaman vsi upi, da bo kdajkoli mogoče formalno opisati vso matematiko.

Neodvisnost: Naj bo znan razred elementarnih izjav $\mathscr{E}$ in razred pravil izpeljevanja $\mathscr{D}$. Potem pravimo, da je razred $\mathscr{K} \subset \mathscr{E}$ *neodvisen* od razreda $\mathscr{L} \subset \mathscr{E}$ natanko takrat, ko velja

$$\mathscr{K} \cap Cn(\mathscr{L}, \mathscr{D}) = \emptyset$$

Posebno je zanimivo vprašanje (medsebojne) neodvisnosti aksiomov dane teorije $\mathscr{T}$.

Aksiomi teorije $\mathscr{T}$ so *neodvisni* natanko takrat, ko je vsak zase neodvisen od drugih, oziroma ko noben pravi podrazred aksiomov teorije $\mathscr{T}$ ne poraja več ekvivalentne teorije.

Čeprav je neodvisnost aksiomov navidez le lepotna odlika aksiomatizacije dane teorije $\mathscr{T}$, to popolnoma ne drži. Spomnimo se samo posledic, ki jih je imelo spoznanje, da je aksiom o vzporednicah neodvisen od ostalih aksiomov geometrije.

Enega izmed načinov, kako pokazati neodvisnost aksiomov, nam daje naslednja trditev:

T12. Bodi teorija $\mathscr{T} = (\mathscr{E}, Cn(\mathscr{K} \cup \{\overline{E}\}))$ neprotislovna na f, potem je izjava E neodvisna od $\mathscr{K}$.

Dokaz: Dokazujemo s protislovjem. Recimo, da je E odvisna od $\mathscr{K}$. Potem je $E \in Cn(\mathscr{K}) \subseteq$ $\subseteq Cn(\mathscr{K} \cup \{\overline{E}\})$, kar pomeni, da sta $E, \overline{E} \in Cn(\mathscr{K} \cup \{\overline{E}\})$. To pa je v nasprotju s predpostavko o neprotislovnosti teorije $\mathscr{T}$.

Interpretacije teorij

Osnovni pojmi: Teorija kot razred elementarnih izrekov je za nas v glavnem zanimiva le, če obstaja neka zveza med njo in vsebinskim področjem, ki ga poznamo neodvisno od nje. Ta zveza je podana z relacijo med elementarnimi izjavami teorije in določenimi vsebinskimi izjavami, ki se nanašajo na dano področje. Pravimo, da je s to relacijo podana *interpretacija* naše teorije v tem področju.

Interpretacija je *polna*, če vsaki elementarni izjavi ustreza neka vsebinska izjava — njen *interpretant*; drugače je *delna*. Ko je interpretant vsakega elementarnega izreka »resničen«, pravimo, da je interpretacija *pravilna*, teorija pa *osnovana* ali *utemeljena*. Kadar pa je vsaka elementarna izjava, katere interpretant je resničen, elementarni izrek v naši teoriji, je interpretacija *adekvatna* ali *ustrezna*, teorija pa *popolna*. Ti pojmi so analogni neprotislovnosti in polnosti teorij in imajo isto naravo kot vsebinsko področje; če je to empirično, so tudi sami empirični.

Navadno zgradimo in proučujemo teorijo z nekim namenom. Kadar teorija temu namenu ustreza, pravimo, da je *sprejemljiva*. Sprejemljivost teorije predpostavlja njeno pravilnost. No, izmed dveh pravilnih teorij je lahko ena primernejša od druge — odvisno od naših namenov in drugih zahtev (enostavnost, nazornost, elegantnost ...).

Vsi opisani pojmi so relativni. Odvisni so od našega znanja v danem času, od naših zahtev in namenov. Vrsto lepih primerov, ki potrjujejo to spoznanje, nam daje zgodovina razvoja fizikalnih teorij (optika, modeli atoma ...).

Pri opisu pojma interpretacija sistema ima glavno besedo pojem *ocene*. To je relacija med razredom formalnih objektov in nekim razredom konkretnih objektov; pri tem je lahko različnim formalnim objektom pripisan isti konkretni objekt — njihova *vrednost*. Kadar je razred formalnih objektov induktiven, ponavadi pripišemo vrednosti samo elementom baze. Vrednosti drugih formalnih objektov pa določimo s konkretnimi operacijami, ki ustrezajo pravilom generiranja.

Ko poznamo oceno, določimo interpretacijo tako, da vsakemu baznemu predikatu pripišemo njegov interpretant — predikat, definiran nad vrednostmi. Taki interpretaciji bomo rekli *prema*.

Drugo vrsto interpretacije dobimo tako, da definiramo interpretante nad nekim razredom ocen. Tej interpretaciji je blizu pojem *modela*, ki je definiran za teorije prvega reda (glej str. 27—30). Tudi tu imamo opravka z razredom ocen. Vsaki elementarni izjavi priredimo neko funkcijo, definirano nad tem razredom. Interpretant take izjave pa je izjava o tem, da je ta funkcija »resnična« za vse ocene. S tem smo dobili *polmodel*, ki je model, če je pravilen.

Zgled: Kako je z interpretacijami izjavnega računa? Oglejmo si dve interpretaciji v množici $\mathscr{B} = \{0, 1\}$.

Najprej prema interpretacija: Vrednosti pripišemo le razredu izjavnih spremenljivk. S tem v bistvu podamo preslikavo.

$$v : s_i \mapsto \mathscr{B}$$

ki jo lahko z operacijama

	N
0	1
1	0

*	0	1
0	1	1
1	0	1

s predpisoma

$$v(\neg A) = \mathrm{N}v(A) \qquad \text{in} \qquad v(A \Rightarrow B) = v(A) * v(B)$$

(po konstrukciji) razširimo tudi na izjave. Premo interpretacijo dobimo, če vzamemo za interpretant predikata $\vdash$, ki ga vključimo med simbole izjavnega računa, predikat »biti enak 1«. Izkaže se, da je, če vzamemo, da predikat »biti enak 1« določa pojem resničnosti, vsaka taka interpretacija pravilna.

Bralec se lahko sam prepriča, da imata operaciji N in * naslednje lastnosti: $a * 1 = 1$, $1 * a = a$, $a * a = 1$, $a * (b * c) = (a * b) * (a * c)$ in $a * b = Nb * Na$. Te uporabimo pri dokazu trditve, da imajo vsi aksiomi vrednost 1. Pri tem označimo $v(A) \equiv a$, ...

$$v(A \Rightarrow (B \Rightarrow A)) = a * (b * a) = (a * b) * (a * a) = (a * b) * 1 = 1$$

$$v((A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C))) = (a * (b * c)) * ((a * b) * (a * c)) =$$
$$= (a * (b * c)) * (a * (b * c)) = 1$$

$$v((\neg B \Rightarrow \neg A) \Rightarrow (A \Rightarrow B)) = (Nb * Na) * (a * b) = (a * b) * (a * b) = 1$$

Pokažimo še, da pravilo MP ohranja vrednost 1

$$v(A) = 1 \wedge v(A \Rightarrow B) = 1 \Rightarrow v(B) = 1$$

Dokaz je kratek

$$1 = v(A \Rightarrow B) = v(A) * v(B) = 1 * v(B) = v(B)$$

Iz obojega pa po induktivni posplošitvi sledi, da imajo vsi izreki vrednost 1 — interpretacija je pravilna.

Vendar ta interpretacija ni ustrezna, saj ima izjava $(\mathrm{s} \Rightarrow \mathrm{s}\,|\,)$ za $v(\mathrm{s}) = v(\mathrm{s}\,|\,) = 1$ vrednost 1, za $v(\mathrm{s}) = 1$ in $v(\mathrm{s}\,|\,) = 0$ pa vrednost 0. Torej imajo lahko vrednost 1 tudi izjave, ki niso izreki.

To pomanjkljivost odpravimo z drugo interpretacijo. Pri tej vzamemo za razred ocen vse možne preslikave izjavnih spremenljivk v množico $\mathscr{B} = \{0, 1\}$. Operaciji N in * ostaneta isti. Izjavi A, ki ima za vsako oceno vrednost 1, recimo *tavtologija*; če ima za vsako oceno vrednost 0, pa *protislovje*. Tavtologije in protislovja sestavljajo razred *splošno veljavnih izjav*. Da je izjava A tavtologija, zapišemo tudi $\models A$. Predikat $\vdash$ tokrat interpretirajmo s predikatom »biti tavtologija«.

Kakor vemo iz prve interpretacije, je tudi ta interpretacija pravilna, saj velja

$$\vdash A \Rightarrow \models A$$

Pokazati pa je mogoče tudi, da je ustrezna

$$\models A \Rightarrow \vdash A$$

Interpretacije in neprotislovnost: Uporaba interpretacije ima pomembno vlogo pri dokazovanju neprotislovnosti teorij. Če je interpretacija teorije $\mathscr{T}$ v teoriji $\mathscr{T}'$ polna in pravilna, obstaja za vsak objekt ali pojem teorije $\mathscr{T}$ prirejeni objekt ali pojem v teoriji $\mathscr{T}'$; aksiomom teorije $\mathscr{T}$ pa so prirejeni izreki v teoriji $\mathscr{T}'$. Naj bo interpretacija tudi ustrezna in naj teoriji $\mathscr{T}$ in $\mathscr{T}'$ vsebujeta izjavni račun, potem je teorija $\mathscr{T}$ neprotislovna, če je le neprotislovna teorija $\mathscr{T}'$. Seveda je na ta način dokazana le *relativna* (*pogojna*) *neprotislovnost*.

S to metodo je Beltrami (1868) pokazal, da je geometrija Lobačevskega neprotislovna, če je le neprotislovna klasična Evklidova geometrija. Za to (in za druge) pa lahko z Descartesovo analitično geometrijo pokažemo, da je (so) neprotislovna(e), če je neprotislovna

teorija realnih števil. Šele leta 1906 je Veblenu in Busseyu uspelo pokazati nepogojno neprotislovnost nekaterih enostavnih projektivnih geometrij s postavitvijo končnih (po številu interpretantov) interpretacij.

Pogosto pri dokazu neprotislovnosti uporabljamo naslednji prijem.

T13. Recimo, da za elementarne izjave teorije $\mathscr{T}$ poznamo neko lastnost P, tako da:

— aksiomi imajo lastnost P;

— pravila izpeljevanja lastnost P ohranjajo;

— za nobeno elementarno izjavo E izjavi E in $\overline{E}$ nimata hkrati lastnosti P;

potem je teorija $\mathscr{T}$ neprotislovna glede na f.

Dokaz: Po induktivni posplošitvi imajo vsi izreki lastnost P; po zadnji zahtevi pa izjavi E in $\overline{E}$ ne moreta biti hkrati izreka, kar zagotavlja neprotislovnost teorije $\mathscr{T}$.

Interpretacija in izjavni račun: Ker predikata »biti enak 1« in »biti tavtologija« zadoščata pogojem, ki smo jih naložili na lastnost P, je izjavni račun neprotisloven.

Zaradi ustreznosti in pravilnosti druge interpretacije izjavnega računa je izjava A izrek natanko takrat, ko je tavtologija (izreki so potemtakem ravno vse vedno za vsako oceno »resnične« izjave). Ker je negacija tavtologije protislovje (in obratno), je izjavni račun, če vzamemo za elementarne izjave splošno veljavne izjave, polna na $\neg$, in po T9 tudi absolutno polna, teorija. Dalje, ker je izjavni račun deduktivna teorija, je v tem primeru tudi odločljiva teorija. Odločitveni postopek je naslednji: Ker je vsaka izjava A izjavnega računa končen niz znakov, vanjo vstopa končno, recimo n, izjavnih spremenljivk. Izračunajmo za vsako od 2^n možnih ocen vrednost izjave A. Če so vse vrednosti enake, je A splošno veljavna oziroma elementarna izjava, in je izrek natanko takrat, ko je tavtologija (vse vrednosti so enake 1).

Za izjavni račun je neprotislovnost in polnost prvi dokazal Post (1921).

Kaj pa, če vzamemo za elementarne izjave vse izjave izjavnega računa in ne samo splošno veljavne? Tedaj izjavni račun ni poln na $\neg$, saj za poljubno izjavo A, ki ni splošno veljavna, nobena od izjav A in $\neg A$ ni izrek (za vsako namreč obstaja ocena, za katero ima vrednost 0). Pač pa je v tem primeru v nekem smislu absolutno polna: Vzemimo poljubno izjavo A, ki ni izrek, in nadomestimo v njej izjavne spremenljivke z opisnimi. Tako dobimo neko izjavno shemo. Če izjavni račun s to shemo aksiomatsko razširimo, je dobljena razširitev protislovna.

Z interpretacijo ponavadi dokazujemo tudi neodvisnost (shem) aksiomov. Metoda je podobna tisti, ki jo uporabljamo pri dokazovanju neprotislovnosti:

T14. Recimo, da za elementarne izjave teorije $\mathscr{T}$ poznamo neko lastnost P, tako da:

— vsi aksiomi, razen tistih, ki pripadajo razredu $\mathscr{K}$, imajo lastnost P;

— pravila izpeljevanja lastnost P ohranjajo;

potem je razred $\mathscr{K}$ neodvisen od ostalih aksiomov teorije $\mathscr{T}$.

Sheme aksiomov izjavnega računa so neodvisne.

To pokažemo tako, da vzamemo za razred ocen vse preslikave izjavnih spremenljivk v množico $\mathscr{M} = \{0, 1, 2\}$, vrednost nato posplošimo na izjave, tako kot smo to že prej storili. Za lastnost P pa si izberemo predikat »$v(A) = 0$ za vse ocene«. Izjavam, ki imajo lastnost P, bomo rekli, da so izbrane. Operaciji N in * določimo za vsak primer posebej:

Pri dokazu neodvisnosti aksioma IRA1 določimo operaciji N in * takole

	N
0	1
1	1
2	0

*	0	1	2
0	0	2	2
1	2	2	0
2	0	0	0

IRA1 ne določa izbranih izjav, ker je $1 * (2 * 1) \neq 0$.

Za dokaz neodvisnosti IRA2 postavimo

	N
0	1
1	1
2	1

*	0	1	2
0	0	2	1
1	0	2	0
2	0	0	0

IRA2 ne določa izbranih izjav, ker je $(0 * (2 * 2)) * ((0 * 2) * (0 * 2)) \neq 0$

Za IRA3 pa vzamemo

	N
0	1
1	1
2	1

*	0	1	2
0	0	1	2
1	0	0	2
2	0	1	0

IRA3 ne določa izbranih izjav, ker je $(N1 * N2) * (2 * 1) \neq 0$.

Dokaz izbranosti drugih aksiomov in da MP ohranja izbranost, je za vse tri primere prepuščen bralcu.

Na tem mestu se zaradi prostorske stiske naše skupno srečanje s teorijami konča.

LITERATURA

[1] S. Alagić, *Principi programiranja*. Sarajevo, Svjetlost 1976.

[2] V. Batagelj, *Rekurzivna aritmetika*, diplomsko delo. Ljubljana 1973.

[3] N. Bourbaki, *Théorie des ensembles*. Paris, Hermann 1960 (ruski prevod: Moskva, Mir 1965; vsebuje tudi prevod: *Éléments d'histoire des mathématiques*).

[4] H.B. Curry, *Foundations of Mathematical Logic*. New York, Mc-Graw-Hill 1963 (ruski prevod: Moskva, Mir 1969).

[5] S.C. Kleene, *Introduction to Metamathematics*. New York, Van Nostrand 1952 (ruski prevod: Moskva, IL 1957).

[6] S.C. Kleene, *Mathematical Logic*. New York, John Wiley 1967 (ruski prevod: Moskva, Mir 1973).

[7] R.C. Lyndon, *Notes on Logic*. Princeton, Van Nostrand 1966 (ruski prevod: Moskva, Mir 1968).

[8] A.A. Markov, *O logike konstruktivnoj matematiki*. Vestnik Moskovskoga universiteta (matematika, mehanika) **2** (1970) 7—29.

[9] E. Mendelson, *Introduction to Mathematical Logic*. Princeton, Van Nostrand 1963 (ruski prevod: Moskva, Nauka 1971).

[10] J.A. Petrov, *Logičeskie problemy abstrakcij beskonečnosti i osuščestvimosti*. Moskva, Nauka 1967.

[11] S.B. Prešić, *Elementi matematičke logike*. Beograd, 1968 (Matematička biblioteka).

[12] N. Prijatelj, *Uvod v matematično logiko*. Ljubljana, MK 1960 (Knjižnica Sigma; 3b).

[13] H. Rasiowa, R. Sikorski, *The Mathematics of Metamathematics*. Warszawa, Panstwowe Wydawnictwo Naukowe 1963 (ruski prevod: Moskva, Nauka 1972).

[14] J.R. Shoenfield, *Mathematical Logic*. Reading, Mass., Addison-Wesley 1967 (ruski prevod: Moskva, Nauka 1975).

[15] A. Tarski, *Uvod u matematičku logiku i metodologiju matematike*. Beograd, Rad 1973.

[16] A. Tarski, *Logic, Semantics, and Metamathematics*. Oxford, 1956.

[17] I. Vidav, *Števila in matematične teorije*. Ljubljana, MK, 1965 (Knjižnica Sigma; 11a).

Obzornik mat. fiz. **25** (1978) 1

FORMALNA IZGRADNJA LOGIČNEGA JEZIKA

NIKO PRIJATELJ

AMS Subj. Class. (1970) 02—01

V članku sta na kratko predstavljeni sintaksa in semantika predikatnega jezika prvega reda in opisani so nekateri temeljni odnosi med njima.

FORMAL CONSTRUCTION OF A LOGICAL LANGUAGE

In the article a short exposition of syntax and semantics of the first-order predicate language is given and some of the fundamental relations between them are outlined.

Naša naloga je, da dopolnimo splošna razmišljanja, podana v prejšnjem prispevku, z dejansko izgradnjo določenega tipa logičnega jezika. Za ta namen smo izbrali tako imenovani *jezik prvega reda*, ki je sorazmerno preprost in hkrati izrazno dovolj bogat, da je v njem mogoče zapisati temeljne matematične teorije. Nasploh imenujemo tiste teorije, ki so izrazljive v logičnem jeziku prvega reda, *teorije prvega reda*.

Pri naslednjem opisu bomo strogo razlikovali med *sintakso* in *semantiko* jezika, se pravi med njegovo *slovnico* in *pomenoslovjem*. Zato se bomo v 1. razdelku ubadali izključno s sintaktičnimi, v 2. razdelku pa s semantičnimi pojmi, ki zadevajo naš logični jezik. Šele v 3. razdelku bomo govorili o vzajemnem odnosu med sintakso in semantiko in bomo v tej zvezi navedli nekatere temeljne probleme pa tudi rešitve, ki sodijo v domeno klasične matematične logike. Glede na prostor, ki nam je na razpolago, se moramo pri tem seveda omejiti le na kratka sporočila in pojasnila izidov, brez ustreznih dolgih in večinoma tudi zapletenih dokazov. Te lahko najde bravec, ki bi se utegnil globlje zanimati za opisane probleme, v katerikoli izmed knjig, navedenih v bibliografiji.

1.

Če naj izgradimo *jezik*, moramo kajpak najprej našteti *znake*, iz katerih je sestavljen. Te znake imenujemo *primitivne simbole* jezika in so v našem primeru naslednji:

(1) številno neskončna množica znakov

$x_1, x_2, \ldots x_n, \ldots$

ki jih imenujemo *individualne spremenljivke*; pri tem je x_n n-ta individualna spremenljivka;

(2) končna ali številno neskončna množica znakov

$a_1, a_2, \ldots a_n, \ldots$

ki jih imenujemo *individualne konstante*; pri tem je a_n n-ta individualna konstanta;

(3) končna ali številno neskončna množica znakov

$$\begin{array}{l} f^1_1, f^1_2, \ldots f^1_n, \ldots \\ f^2_1, f^2_2, \ldots f^2_n, \ldots \\ \quad\vdots \\ f^k_1, f^k_2, \ldots f^k_n, \ldots \\ \quad\vdots \end{array}$$

ki jih imenujemo *funkcijski* znaki; pri tem je f^k_n n-ti funkcijski znak za k-mestno funkcijo;

(4) neprazna končna ali števno neskončna množica znakov

$$P^1_1, P^1_2, \ldots P^1_n, \ldots$$
$$P^2_1, P^2_2, \ldots P^2_n, \ldots$$
$$\vdots$$
$$P^k_1, P^k_2, \ldots P^k_n, \ldots$$
$$\vdots$$

ki jih imenujemo *predikatni* znaki; pri tem je P^k_n n-ti predikatni znak za k-mestni predikat;

(5) znaka *povezave*

$\neg$ in $\Rightarrow$

$\neg$ imenujemo znak *negacije*, $\Rightarrow$ pa znak *implikacije*;

(6) znak $\forall$, ki ga imenujemo *univerzalnostni kvantifikator*;

(7) znaki *ločil* (in) in ,, ki jih imenujemo *levi* in *desni oklepaj*, in *vejica*.

Iz te liste je razvidno, da je naš jezik sicer strogo določen glede *sorte* znakov, ki ga sestavljajo, nikakor pa ne glede *števila* znakov. Ker je seveda prazna množica tudi končna, je po (2) in (3) mogoče, da je jezik celo brez individualnih konstant ali brez funkcijskih znakov. Vsekakor pa mora vsebovati števno neskončno mnogo individualnih spremenljivk, vsaj en predikatni znak in pa znake (5) in (6). Znaki ločil (7) sicer niso neogibno potrebni, vendar so koristni, ker napravimo z njimi zapise v jeziku bolj pregledne. *Koliko* znakov posamezne sorte v danem konkretnem primeru dejansko uporabimo, je pač odvisno od teorije, ki jo želimo zapisati v tem jeziku. To bomo še kasneje razložili na dveh primerih. Pri splošnih razmišljanjih o jeziku prvega reda pa se glede števila posameznih sort znakov kajpada ne bomo omejevali bolj, kot smo to že storili v predstavljeni listi.

V nadaljnjem bomo jezik prvega reda, ki je *predmet* našega pogovora, na kratko označevali s simbolom *JPR*. Opozarjamo bravca, da ta simbol *ne spada* v *JPR*, marveč je del jezika, *v katerem govorimo* o *JPR*. Ta jezik, imenovali ga bomo, za razloček od *JPR*, *meta jezik*, je pač v našem primeru bolj ali manj dobra slovenščina, dopolnjena z nekaterimi znanimi matematičnimi izrazi in pa ad hoc konstruiranimi simboli, kot na primer *JPR*, ki jim bomo rekli *meta simboli*. Seveda predpostavljamo, da vsi prizadeti meta jezik dobro *obvladamo* in *razumemo*, se pravi, da poznamo njegovo slovnico in pomenoslovje.

Vsak končen nabor primitivnih simbolov *JPR*, ki so nanizani brez presledka drug za drugim, imenujemo *izraz* v *JPR*. Tako je na primer tale nabor

$$,) f^3_2 (\neg \Rightarrow P^1_4, x_2 a_3, \forall \neg x_2 ( )$$

že izraz v *JPR*. Za vsak simbol, ki je v takem izrazu, pravimo, da *nastopa* v izrazu. Razume se, da lahko isti simbol tudi večkrat nastopi v danem izrazu. Ker je število simbolov v vsakem izrazu končno, moremo govoriti o prvem, drugem, ... zadnjem nastopu določenega simbola v danem izrazu.

Naprej nas bodo zanimali le taki izrazi v *JPR*, ki bodo konstruirani na čisto določen način in jih bomo imeli za edine sintaktično pravilne izraze. Ti sintaktično pravilni izrazi se dele na *terme* in *dobro oblikovane formule*. Preden jih opredelimo, vpeljimo še, zaradi udobnejšega izražanja, dve sorti meta simbolov in eno okrajšavo.

Terme nasploh bomo označevali z malimi pisanimi črkami a, b, ... t itd., ki jim bomo po potrebi obesili še indekse, torej tudi t_2, t_1, ... t_5 itd.

Dobro oblikovane formule nasploh bomo označevali z velikimi pisanimi črkami $\mathscr{A}$, $\mathscr{B}$, ... $\mathscr{F}$ itd., ki jim bomo po potrebi dodali še indekse, torej tudi $\mathscr{F}_3$, $\mathscr{F}_2$, ... $\mathscr{F}_7$ itd.

Dobro oblikovane formule bomo imenovali s kratico *dof*.

Zdaj pa definirajmo najprej terme z naslednjo induktivno definicijo:

(1) vsaka individualna spremenljivka je term;

(2) vsaka individualna konstanta je term;

(3) če je f_n^k n-ti funkcijski znak za k-mestno funkcijo in so $t_1, t_2, \ldots t_k$ termi, potem je $f_n^k(t_1, t_2, \ldots t_k)$ term;

(4) dani izraz je term natanko tedaj, če ga lahko konstruiramo na osnovi (1), (2) in (3).

Tudi dobro oblikovane formule so opredeljene z induktivno definicijo:

(1′) če je P_n^k n-ti predikatni znak za k-mestni predikat in so $t_1, t_2, \ldots t_k$ termi, potem je $P_n^k(t_1, t_2, \ldots t_k)$ *dof*, ki jo imenujemo tudi *atomska formula*;

(2′) če je $\mathscr{A}$ *dof*, je tudi $(\neg \mathscr{A})$ *dof*;

(3′) če sta $\mathscr{A}$ in $\mathscr{B}$ *dof*, je tudi $(\mathscr{A} \Rightarrow \mathscr{B})$ *dof*;

(4′) če je $\mathscr{A}$ *dof* in je x_n individualna spremenljivka, je tudi $(\forall x_n)\,\mathscr{A}$ *dof*;

(5′) dani izraz je *dof* natanko tedaj, če ga lahko konstruiramo na osnovi (1′), (2′), (3′) in (4′).

Ker se nekatere konstrukcije *dof* pogosto ponavljajo, je ugodno, če vpeljemo še nove znake povezav; uporabljamo pa jih *le kot okrajšave* za ustrezne *dof* v *JPR*. Tako bomo, ako sta $\mathscr{A}$ in $\mathscr{B}$ *dof*, pisali:

(D) $\mathscr{A} \vee \mathscr{B}$ kot okrajšavo za *dof* $(\neg \mathscr{A}) \Rightarrow \mathscr{B}$. Znak $\vee$ imenujemo znak *disjunkcije*.

(K) $\mathscr{A} \wedge \mathscr{B}$ kot okrajšavo za *dof* $\neg(\mathscr{A} \Rightarrow (\neg \mathscr{B}))$. Znak $\wedge$ imenujemo znak *konjunkcije*.

(E) $\mathscr{A} \Leftrightarrow \mathscr{B}$ kot okrajšavo za *dof* $\neg((\mathscr{A} \Rightarrow \mathscr{B}) \Rightarrow (\neg(\mathscr{B} \Rightarrow \mathscr{A})))$. Znak $\Leftrightarrow$ imenujemo znak *ekvivalence*.

(EK) $(\exists x_n)\,\mathscr{A}$ kot okrajšavo za *dof* $\neg((\forall x_n)(\neg \mathscr{A}))$. Znak $\exists$ imenujemo *eksistencialnostni kvantifikator*.

Naj bo $\mathscr{A}$ *dof*. Potem imenujemo vsak izraz $\mathscr{B}$, ki je *del dof* $\mathscr{A}$ in je tudi sam *dof*, *dobro oblikovani del dof* $\mathscr{A}$.

Če je $(\forall x_n)\,\mathscr{B}$ dobro oblikovani del dane *dof* $\mathscr{A}$, potem je *dof* $\mathscr{B}$ *domena učinka*, ki pripada temu nastopu univerzalnostnega kvantifikatorja $(\forall x_n)$ v *dof* $\mathscr{A}$. Vsak nastop spremenljivke x_n v *dof* $(\forall x_n)\,\mathscr{B}$ je *vezan nastop* x_n *v dof* $\mathscr{A}$. Za vsak nastop spremenljivke x_n v $\mathscr{A}$, ki *ni* vezan, pravimo, da je *prost v* $\mathscr{A}$.

Iz povedanega je očitno, da ima lahko ista spremenljivka x_n v dani *dof* $\mathscr{A}$ hkrati vezane in proste nastope. Tako sta na primer v *dof*

$$(\forall x_1) P_1^1(x_1) \Rightarrow P_1^2(x_1, x_3)$$

prva dva nastopa spremenljivke x_1 vezana, tretji nastop te spremenljivke pa je prost. Nasprotno pa so v *dof*

$$(\forall x_1)\,(P_1^1(x_1) \Rightarrow P_1^2(x_1, x_3))$$

vsi nastopi spremenljivke x_1 vezani. Očitno je v obeh *dof* nastop spremenljivke x_3 prost.

Pravimo, da je spremenljivka x_n *vezana* (*prosta*) v dani *dof* $\mathscr{A}$, brž ko je vsaj en nastop spremenljivke x_n v *dof* $\mathscr{A}$ vezan (prost). Potemtakem more biti spremenljivka x_n v dani *dof* $\mathscr{A}$ *hkrati* vezana in prosta.

Vsako *dof*, ki je brez *prostih* spremenljivk, imenujemo *stavek*. Poseben primerek stavka je taka *dof*, v kateri sploh ni spremenljivk. Za tako *dof* rečemo, da je *prosta* spremenljivk.

Bodi $\mathscr{A}$ *dof*, v kateri so $x_1, x_2, \ldots x_n$ natanko vse proste spremenljivke. Potem imenujemo *dof*

$$(\forall x_1)\,(\forall x_2) \ldots (\forall x_n)\,\mathscr{A}$$

univerzalno zaprtje dof $\mathscr{A}$. Ker univerzalno zaprtje dane *dof* $\mathscr{A}$ potemtakem nima več nobene proste spremenljivke, je stavek.

V zvezi z *dof* vpeljimo še postopek, ki ga imenujemo *substitucija*. Ako je $\mathscr{A}$ *dof*, potem označimo z

$$S_{t_k}^{x_n} \mathscr{A} \mid$$

dof, ki jo dobimo iz $\mathscr{A}$ tako, da v $\mathscr{A}$ zamenjamo *vsak prost nastop* spremenljivke x_n s termom t_k.

V dani *dof* $\mathscr{A}$ pravimo nadalje, da je term t_k *prost* spremenljivke x_n natanko tedaj, če *noben* prost nastop spremenljivke x_n v $\mathscr{A}$ *ni* v kakšnem dobro oblikovanem delu *dof* $\mathscr{A}$, ki ima obliko $(\forall x_i)\mathscr{B}$ in je x_i individualna spremenljivka, ki nastopa v termu t_k. Na primer v *dof*

$$(\forall x_2) P_1^2(x_1, x_2) \Rightarrow P_1^3(x_1, x_2, x_3)$$

je spremenljivka x_2, prosta spremenljivke x_3, ni pa prosta spremenljivke x_1.

Že v uvodu smo povedali, da uporabljamo *JPR* za opis in študij tako imenovanih *teorij prvega reda*. Vsaka taka teorija izhaja iz *aksiomov*, ki niso nič drugega kot določene *dof* v *JPR*, in obstoji v tem, da izvaja iz njih na podlagi eksplicitno formuliranih *pravil sklepanja* nove *dof* v *JPR*, ki jih imenujemo *izreke* ustrezne teorije. To naj še dopolnimo z naslednjima pojasniloma:

a) Nasploh imajo teorije prvega reda *neskončno mnogo* aksiomov. Da bi lahko vse zajeli, si pomagamo s tako imenovanimi *aksiomskimi shemami*. Te sheme so zapisane z meta simboli in vsaka posamezna *dof* iz *JPR*, ki jo dobimo, če v taki shemi nadomestimo meta simbole z ustreznimi simboli *JPR*, je aksiom ustrezne teorije. Razume se, da iz takih aksiomskih shem s pravili sklepanja ne bomo dobili že posamičnih izrekov teorije, marveč spet z meta simboli izražene sheme, ki zajemajo vse izreke določenega tipa, in jih zato tudi imenujemo *sheme izrekov*.

b) Omenjena pravila sklepanja so mišljena strogo sintaktično in nimajo, vsaj v tem razdelku, nikakršne vsebinske komponente. Gre torej za popolnoma *formalen*, toda v vsakem konkretnem primeru *preverljiv* opis pogojev, ki omogočajo *prehod* iz danih *dof* na nove *dof*.

Iz povedanega je torej razvidno, da je vsaka teorija popolnoma opredeljena, brž ko poznamo njene aksiome oziroma aksiomske sheme in pravila sklepanja. Vse teorije prvega reda pa imajo za skupno osnovo tako imenovane *logične* aksiomske sheme in vse uporabljajo le *dvoje* pravil sklepanja. Razloček med posameznimi teorijami prvega reda izhaja potemtakem šele iz aksiomov oziroma aksiomskih shem, ki jih *dodamo* tej skupni osnovi in jih zato imenujemo *lastne* aksiome ustrezne teorije. Teorija, ki je *brez* dodatnih lastnih aksiomov, je torej *čista logična* teorija, ki jo imenujemo *predikatni račun prvega reda*.

Aksiomske sheme predikatnega računa lahko do neke mere variiramo. Tukaj smo izbrali naslednje:

Ako so $\mathscr{A}, \mathscr{B}, \mathscr{C}$ *dof* v *JPR*, potem so aksiomske sheme predikatnega računa prvega reda:

(PR_1) $\mathscr{A} \Rightarrow (\mathscr{B} \Rightarrow \mathscr{A})$;

(PR_2) $(\mathscr{A} \Rightarrow (\mathscr{B} \Rightarrow \mathscr{C})) \Rightarrow ((\mathscr{A} \Rightarrow \mathscr{B}) \Rightarrow (\mathscr{A} \Rightarrow \mathscr{C}))$;

(PR_3) $(\neg \mathscr{B} \Rightarrow \neg \mathscr{A}) \Rightarrow ((\neg \mathscr{B} \Rightarrow \mathscr{A}) \Rightarrow \mathscr{B})$;

(PR_4) $(\forall x_n)\mathscr{A} \Rightarrow S_{t_k}^{x_n} \mathscr{A} \mid$, če je term t_k *prost* spremenljivke x_n v $\mathscr{A}$;

(PR_5) $(\forall x_n)(\mathscr{A} \Rightarrow \mathscr{B}) \Rightarrow (\mathscr{A} \Rightarrow (\forall x_n)\mathscr{B})$, če v *dof* $\mathscr{A}$ spremenljivka x_n *ne* nastopa prosto;

V (PR_3) smo »tiho« upoštevali »dogovor«, da veže znak $\neg$ ože kot znak $\Rightarrow$. Ta dogovor naj velja tudi za naprej.

Navedimo zdaj še obe pravili sklepanja:

(MP) *Modus ponens*: ako sta $\mathscr{A}$, $\mathscr{B}$ *dof* v *JPR*, potem iz $\mathscr{A}$ in $\mathscr{A} \Rightarrow \mathscr{B}$ sklepamo na $\mathscr{B}$.

(G) *Generalizacija*: ako je $\mathscr{A}$ *dof* v *JPR*, potem iz $\mathscr{A}$ sklepamo na $(\forall x_n)\mathscr{A}$.

Preden nadaljujemo splošna izvajanja, opišimo tri posebne teorije, od katerih je ena *vsebovana* v predikatnem računu prvega reda, drugi dve pa ga *vsebujeta*, se pravi, da imata poleg logičnih aksiomov še lastne.

(A) Stavčni račun

Če se omejimo le na take *dof* v *JPR*, ki so *proste* spremenljivk, torej na posebne primerke *stavkov*, potem je na dlani, da sta zanje aksiomski shemi (PR_4) in (PR_5) *odveč* in prav tako tudi pravilo sklepanja (G). Po drugi plati pa je tudi res, da brž ko sta $\mathscr{A}$ in $\mathscr{B}$ *dof brez* spremenljivk, sta taki tudi *dof* $\neg\mathscr{A}$ in $\mathscr{A} \Rightarrow \mathscr{B}$ in zato seveda tudi *dof*, ki se izražajo okrajšano z $\mathscr{A} \vee \mathscr{B}$, $\mathscr{A} \wedge \mathscr{B}$ in $\mathscr{A} \Leftrightarrow \mathscr{B}$. Če se torej gibljemo le v okviru *dof brez* spremenljivk, s tem da jih med seboj povezujemo z vpeljanimi znaki povezav ter postavimo zanje aksiomske sheme (PR_1), (PR_2) in (PR_3), za pravilo sklepanja pa (MP), potem dobimo tako *logično* teorijo, ki je zajeta v predikatnem računu prvega reda in jo imenujemo *stavčni račun*.

(B) Elementarna teorija naravnih števil

Kakor smo že povedali, moramo pri vsaki teoriji prvega reda najprej natanko našteti individualne konstante ter funkcijske in predikatne znake, ki v njej nastopajo, in seveda navesti lastne aksiome ustrezne teorije. V elementarni teoriji naravnih števil je stvar takale:

Teorija ima eno samo individualno konstanto a_1, ki jo bomo v nadaljnjem pisali »po domače« 0 in jo imenovali *številka nič*.

V teoriji so trije funkcijski znaki, in sicer f_1^1, f_1^2 in f_2^2. Znak f_1^1 imenujemo znak *neposrednega naslednika*, znak f_1^2 je znak *vsote*, znak f_2^2 pa znak *produkta*. Ako sta t_1 in t_2 terma, potem bomo

term $f_1^1(t_1)$ pisali raje t_1'

term $f_1^2(t_1, t_2)$ pisali bolj »po domače« $t_1 + t_2$

term $f_2^2(t_1, t_2)$ pisali spet bolj »po domače« $t_1 \cdot t_2$

Teorija premore en sam predikatni znak P_1^2, ki ga imenujemo znak *enakosti*. Ako sta t_1 in t_2 terma, potem bomo $P_1^2(t_1, t_2)$ pisali seveda v skladu z navado $t_1 = t_2$.

Poleg logičnih aksiomskih shem predikatnega računa prvega reda ima elementarna teorija naravnih števil še tele lastne aksiome:

($ETNŠ_1$) $x_1 = x_2 \Rightarrow (x_1 = x_3 \Rightarrow x_2 = x_3)$

($ETNŠ_2$) $x_1 = x_2 \Rightarrow x_1' = x_2'$

($ETNŠ_3$) $\neg(0 = x_1')$

($ETNŠ_4$) $x_1' = x_2' \Rightarrow x_1 = x_2$

($ETNŠ_5$) $x_1 + 0 = x_1$

($ETNŠ_6$) $x_1 + x_2' = (x_1 + x_2)'$

($ETNŠ_7$) $x_1 \cdot 0 = 0$

($ETNŠ_8$) $x_1 \cdot x_2' = (x_1 \cdot x_2) + x_1$

($ETNŠ_9$) Za vsako *dof* $\mathscr{A}$ elementarne teorije naravnih števil je

$$S_0^{x_n}\mathscr{A} \mid \Rightarrow ((\forall x_n)(\mathscr{A} \Rightarrow S_{x_n}^{x_n}, \mathscr{A} \mid) \Rightarrow (\forall x_n)\mathscr{A})$$

Naj opozorimo bravca na zanimivost, da so vsi lastni aksiomi elementarne teorije naravnih števil »pravi« aksiomi, le zadnji, ($ETNŠ_9$), tako imenovani »aksiom o indukciji«, je aksiomska shema.

(C) Elementarna teorija množic

Teorija ima eno samo individualno konstanto a_1, ki jo bomo v nadaljnjem pisali $\emptyset$ in jo imenovali *znak za prazno množico*.

Teorija je brez funkcijskih znakov. Potemtakem so edini termi teorije individualne spremenljivke in individualna konstanta $\emptyset$. Zato bomo za individualne spremenljivke nasploh uporabljali kot meta simbole črke x, y, z, u, v, t.

Teorija ima en sam predikatni znak P_1^2, ki ga bomo pisali $\in$ in imenovali *znak pripadnosti*. Ako sta t_1 in t_2 terma, potem pišemo namesto $\in (t_1, t_2)$ raje $t_1 \in t_2$.

Znak enakosti $=$ uporabljamo v teoriji le kot *okrajšavo*. Ako sta namreč t_1 in t_2 terma, pišemo

$$t_1 = t_2 \text{ kot okrajšavo za } dof\,(\forall x)\,(x \in t_1 \Leftrightarrow x \in t_2)$$

Za lastne aksiome elementarne teorije množic, *brez* aksioma izbire, lahko vzamemo na primer tele *dof*:

(ETM_1) $t_1 = t_2 \Rightarrow (\forall x)\,(t_1 \in x \Leftrightarrow t_2 \in x)$

To je tako imenovani *aksiom ekstenzionalnosti*.

(ETM_2) $(\forall x)\,(\exists y)\,(\forall z)\,(z \in y \Leftrightarrow (\exists u)\,(u \in x \wedge z \in u))$

To je *aksiom o uniji*.

Ako sta t_1, t_2 terma, pišimo $t_1 \subseteq t_2$ kot okrajšavo za $dof\,(\forall x)\,(x \in t_1 \Rightarrow x \in t_2)$. Zdaj lahko udobno formuliramo tudi tako imenovani *aksiom o potenčni množici*, ki se glasi

(ETM_3) $(\forall x)\,(\exists y)\,(\forall z)\,(z \in y \Leftrightarrow z \subseteq x)$

Naslednji aksiom je *aksiom regularnosti*, ki pravi

(ETM_4) $(\forall x)\,(\neg\,(x = \emptyset) \Rightarrow (\exists y)\,(y \in x \wedge (\forall z)\,(z \in y \Rightarrow \neg\,(z \in x))$

Neskončnost si priborimo z *aksiomom o neskončnosti*, ki je zajet v tejle *dof*

(ETM_5) $(\exists x)\,(\emptyset \in x \wedge (\forall y)\,(y \in x \Rightarrow (\exists z)\,(z \in x \wedge (\forall u)\,(u \in z \Leftrightarrow (u \in y \vee u = y)))))$

Zapišimo naposled še tako imenovano *aksiomsko shemo substitucije*. Če je $\mathscr{A}$ *dof* elementarne teorije množic, potem je

$$(ETM_6)\ (\forall x)\,(\forall y)\,(\forall z)\,(\forall u)\,((y \in x \wedge S_y^{x_1} S_z^{x_2} \mathscr{A} \wedge S_y^{x_1} S_u^{x_2} \mathscr{A}) \Rightarrow z = u) \Rightarrow$$
$$\Rightarrow (\exists v)\,(\forall z)\,(z \in v \Leftrightarrow (\exists y)\,(y \in x \wedge S_y^{x_1} S_z^{x_2} \mathscr{A}))$$

Po teh ilustracijah se vrnimo spet k splošnim razmišljanjem.

Bodi torej T poljubna teorija prvega reda in H dana množica *dof* te teorije. Potem imenujemo *vsako končno zaporedje dof*

$$\mathscr{A}_1, \mathscr{A}_2, \ldots \mathscr{A}_n \tag{8}$$

dedukcijo dof $\mathscr{A}_n$ *iz množice hipotez* H natanko tedaj, kadar velja za vsak $k = 1, 2, \ldots n$ ena od naslednjih možnosti:

(DH_1) $\mathscr{A}_k$ je iz H, torej ena izmed hipotez;

(DH_2) $\mathscr{A}_k$ je eden izmed aksiomov teorije T;

(DH$_3$) $\mathscr{A}_k$ je rezultat uporabe pravila sklepanja (MP) na *dof*, ki sta v dedukciji (8) *pred* $dof\,\mathscr{A}_k$. Se pravi, da obstajata indeksa i, j, *manjša* od k, in je $\mathscr{A}_j$ okrajšava za $dof\,\mathscr{A}_i \Rightarrow \mathscr{A}_k$.

(DH$_4$) $\mathscr{A}_k$ je rezultat uporabe pravila sklepanja (G) na *dof*, ki stoji v dedukciji (8) *pred* $dof\,\mathscr{A}_k$. Se pravi, da obstaja indeks i, *manjši* od k, in je $\mathscr{A}_k$ okrajšava za $dof\,(\forall x_n)\,\mathscr{A}_i$. Pri tem pa individualna spremenljivka x_n *ne sme biti prosta v nobeni dof, ki so* v H.

Za vsako $dof\,\mathscr{A}$, za katero obstaja kakšna dedukcija iz dane množice hipotez H, rečemo, da je *posledica hipotez* H v teoriji T in to simbolično označimo s

$$H \vdash_T \mathscr{A}$$

Kadar je popolnoma nedvoumno, znotraj katere teorije T poteka dedukcija, pišemo tudi enostavneje

$$H \vdash \mathscr{A}$$

Posebno pomemben pa je primer, kadar je množica hipotez H *prazna*. Takrat imenujemo dedukcijo (8) *dokaz* $dof\,\mathscr{A}_n$ v teoriji T, $dof\,\mathscr{A}_n$, ki je zadnji člen dokaza, pa *izrek teorije* T.

Izrek teorije T je potemtakem vsaka *dof* te teorije, za katero obstaja dokaz. Iz povedanega je razvidno, da je po tej sintaktični opredelitvi tudi vsak aksiom teorije hkrati izrek teorije.

Da je dana $dof\,\mathscr{A}$ izrek teorije T, bomo nakazali simbolično z

$$\vdash_T \mathscr{A}$$

oziroma tudi kar z

$$\vdash \mathscr{A}$$

kadar je docela jasno, v kateri teoriji T se gibljemo.

Če se pri dokazu glede aksiomov omejimo le na logične aksiomske sheme (PR$_1$), (PR$_2$), (PR$_3$), (PR$_4$), (PR$_5$), potem je kajpak naša teorija T logična teorija predikatnega računa prvega reda in ustrezni izreki, ali točneje sheme izrekov, ki so izidi teh dokazov, so seveda čisti *logični* izreki.

Pokažimo na primer, da je za poljubno $dof\,\mathscr{A}\ dof\,\mathscr{A} \Rightarrow \mathscr{A}$ izrek predikatnega računa prvega reda, se pravi, da je

(0) $\vdash \mathscr{A} \Rightarrow \mathscr{A}$

Dokaz je v tem primeru tole končno zaporedje *dof*:

(1) $(\mathscr{A} \Rightarrow ((\mathscr{A} \Rightarrow \mathscr{A}) \Rightarrow \mathscr{A})) \Rightarrow ((\mathscr{A} \Rightarrow (\mathscr{A} \Rightarrow \mathscr{A})) \Rightarrow (\mathscr{A} \Rightarrow \mathscr{A}))$

To je primerek aksiomske sheme (PR$_2$), če vzamemo za $dof\,\mathscr{B}\ dof\,\mathscr{A} \Rightarrow \mathscr{A}$ in za $dof\,\mathscr{C}\ dof\,\mathscr{A}$

(2) $\mathscr{A} \Rightarrow ((\mathscr{A} \Rightarrow \mathscr{A}) \Rightarrow \mathscr{A})$

To je primerek aksiomske sheme (PR$_1$), če vzamemo za $dof\,\mathscr{B}\ dof\,\mathscr{A} \Rightarrow \mathscr{A}$

(3) $(\mathscr{A} \Rightarrow (\mathscr{A} \Rightarrow \mathscr{A})) \Rightarrow (\mathscr{A} \Rightarrow \mathscr{A})$

To je rezultat uporabe pravila sklepanja (MP) na (1) in (2)

(4) $\mathscr{A} \Rightarrow (\mathscr{A} \Rightarrow \mathscr{A})$

To je aksiomska shema (PR$_1$), če vzamemo za $dof\,\mathscr{B}\ dof\,\mathscr{A}$

(5) $\mathscr{A} \Rightarrow \mathscr{A}$

To je rezultat uporabe pravila sklepanja (MP) na (3) in (4). Ker je zadnji člen (5) tega dokaza prav *dof* (0), je torej *dof* (0) res izrek predikatnega računa prvega reda.

Pri tem dokazu smo uporabljali le aksiomski shemi (PR$_1$) in (PR$_2$) ter pravilo sklepanja (MP). Zato je *dof* (0), če se seveda omejimo le na *dof*, ki so proste spremenljivk, tudi izrek v logični teoriji *stavčnega računa*.

Kakor smo že omenili, je bistvo vsake teorije v tem, da iz danih aksiomov ali aksiomskih shem izvaja izreke, se pravi, nabira tiste *dof* teorije, za katere obstajajo dokazi. V tej zvezi je popolnoma naravno, da vprašujemo naslednje:

Če je T dana teorija, ali obstaja kakšen *splošen* in *efektiven* postopek, torej kak *algoritem*, s katerim bi mogli za *vsako dof* teorije *odločiti*, ali *je* izrek ali *ni*?

To je tako imenovani *problem odločljivosti*. Teorije, za katere tak algoritem obstaja, imenujemo *odločljive*.

Ta problem je za teorije, ki smo jih tukaj navedli, razrešen takole:

Logična teorija stavčnega računa je odločljiva. *Nobena* teorija prvega reda, ki obsega predikatni račun prvega reda in vsebuje *vse* predikatne znake P_n^k, *ni* odločljiva. Elementarna teorija naravnih števil *ni* odločljiva. Elementarna teorija množic *ni* odločljiva.

Na kratko bi lahko rekli: razen stavčnega računa nobena logična ali matematična teorija, ki je dovolj »bogata«, da je »zanimiva«, ni odločljiva.

Kaj nam ta negativni rezultat pravzaprav pove? Nič drugega kot tole:

Nobenega razloga ni za up ali strah, da bi kdajkoli lahko človeško ustvarjalnost v logiki in matematiki popolnoma nadomestili s še tako popolnim mehanizmom. Izrekov dane teorije torej nasploh ni mogoče odkriti z mehanično uporabo kakšnega algoritma, marveč le s konstrukcijo ustreznega dokaza. Ta pa se, vsaj v načelu, upira vsakemu algoritmu, zelo pa je odvisna od iznajdljivosti in intuicije iskalca. Pri tem *iskanju* dokazov nam je v krepko oporo tako imenovani *izrek o dedukciji*, o katerem je govor v posebnem prispevku.

2.

Če smo se v 1. razdelku hote izmikali vsaki razlagi *pomena* znakov, termov in formul *JPR* in smo vztrajno opisovali le sintaktična pravila jezika, je zdaj čas, da sklenemo že to »prazno« igro s »čistimi« simboli in jo *osmislimo*. To se pravi, da sintaksi jezika pridružimo še njegovo semantiko. Simboli jezika pa zadobijo *pomen* samo z *interpretacijo*. Taka interpretacija obstoji v naslednjem:

Dani sta *neprazna* množica D, ki jo imenujemo *domena* interpretacije, in preslikava F, tako imenovana *interpretacijska funkcija*, ki priredi:

(a) individualni konstanti a_n element $F(a_n)$ domene D;

(b) n-temu funkcijskemu znaku za k-mestno funkcijo f_n^k k-mestno funkcijo $F(f_n^k) : D^k \to D$;

(c) n-temu predikatnemu znaku za k-mestni predikat P_n^k k-mestno relacijo $F(P_n^k)$ v domeni D, za katero vemo iz teorije množic, da je neka podmnožica kartezičnega produkta D^k.

V nasprotju s tem pa lahko pri dani interpretaciji vsaka individualna spremenljivka x_n oziroma vsaka prosta individualna spremenljivka v poljubni *dof* pomeni *vsak* element domene D. Zato tudi pravimo, da ima vsaka individualna spremenljivka domeno interpretacije D za *zalogo vrednosti*, ki jih lahko zavzame, ali tudi, da vsaka individualna spremenljivka *preteče* domeno D. Iz tega je očitno, da moreta zavzeti dve *različni* individualni spremenljivki tudi *isto* vrednost. Seveda pa se prav tako razume, da obdrži v dani miselni zvezi vsaka individualna spremenljivka *isti* pomen.

Brž ko je dana neka interpretacija, označimo jo v nadaljnjem z I, lahko vsakemu *stavku*, se pravi vsaki *dof* v *JPR*, ki je *brez* prostih spremenljivk, priredimo neko *izjavo*, ki se nanaša na elemente interpretacijske domene D in ki je bodisi *pravilna* ali pa *nepravilna* pri tej interpretaciji. Če je izjava, ki pripada stavku $\mathscr{A}$, pri interpretaciji I pravilna, potem bomo to dejstvo simbolično zapisali z

$$I \models \mathscr{A}$$

in bomo rekli kratko kar, da je stavek $\mathscr{A}$ pravilen pri interpretaciji I. Ko pa je izjava nepravilna, bomo pisali

$$I \not\models \mathscr{A}$$

in bomo spet rekli poenostavljeno, da je pri interpretaciji I stavek $\mathscr{A}$ nepravilen.

Glede na induktivno definicijo *dof*, ki smo jo podali v 1. razdelku, je tudi pravilnost oziroma nepravilnost stavkov pri interpretaciji I popolnoma določena z naslednjo induktivno definicijo:

(1″) Če je P_n^k n-ti predikatni znak za k-mestni predikat in so $a_1, a_2, \ldots a_k$ individualne konstante, potem je $I \models P_n^k(a_1, a_2, \ldots a_n)$, če je $(F(a_1), F(a_2), \ldots F(a_n)) \in F(P_n^k)$ in $I \not\models P_n^k(a_1, a_2, \ldots a_n)$ v vsakem drugem primeru.

(2″) Če je $\mathscr{A}$ stavek, potem je $I \models \neg\mathscr{A}$, če je $I \not\models \mathscr{A}$ in $I \not\models \neg\mathscr{A}$ v vsakem drugem primeru.

(3″) Če sta $\mathscr{A}$ in $\mathscr{B}$ stavka, potem je $I \not\models \mathscr{A} \Rightarrow \mathscr{B}$, če je $I \models \mathscr{A}$ in $I \not\models \mathscr{B}$ in $I \models \mathscr{A} \Rightarrow \mathscr{B}$ v vsakem drugem primeru.

(4″) Če je $\mathscr{A}$ *dof*, ki ima x_n za edino prosto spremenljivko, potem je seveda *dof* $(\forall x_n)\mathscr{A}$ stavek. V tem primeru je $I \models (\forall x_n)\mathscr{A}$, če je pravilna *vsaka* izjava, ki je prirejena *dof* $\mathscr{A}$, brž ko zavzame prosta individualna spremenljivka x_n *katerikoli* element interpretacijske domene D in $I \not\models (\forall x_n)\mathscr{A}$ v vsakem drugem primeru.

Zdaj lahko razširimo definicijo pravilnosti oziroma nepravilnosti tudi na poljubne *dof*. Najprej na podlagi (4″) rečemo:

(5″) Ako je $\mathscr{A}$ *dof*, ki ima x_n za edino prosto spremenljivko, potem je $I \models \mathscr{A}$, če je $I \models (\forall x_n)\mathscr{A}$ in $I \not\models \mathscr{A}$ v vsakem drugem primeru.

(6″) In če je $\mathscr{A}$ *dof*, v kateri so $x_1, x_2, \ldots x_n$ natanko vse proste spremenljivke, potem je kajpak prirejeno univerzalno zaprtje $(\forall x_1)(\forall x_2)\ldots(\forall x_n)\mathscr{A}$ stavek, za katerega je $I \models \models (\forall x_1)(\forall x_2)\ldots(\forall x_n)\mathscr{A}$, če je pravilna *vsaka* izjava, ki je prirejena *dof* $\mathscr{A}$, brž ko zavzamejo proste individualne spremenljivke $x_1, x_2, \ldots x_n$, *neodvisno* druga od druge, *katerekoli* elemente interpretacijske domene D in $I \not\models (\forall x_1)(\forall x_2)\ldots(\forall x_n)\mathscr{A}$ v vsakem drugem primeru.

Potemtakem bomo tudi sklenili:

(7″) Ako je $\mathscr{A}$ *dof*, v kateri so $x_1, x_2, \ldots x_n$ natanko vse proste spremenljivke, potem je $I \models \mathscr{A}$, če je $I \models (\forall x_1)(\forall x_2)\ldots(\forall x_n)\mathscr{A}$ in $I \not\models \mathscr{A}$ v vsakem drugem primeru.

Razume se, da so s temi opredelitvami pravilnosti oziroma nepravilnosti *dof* pri dani interpretaciji I določene že tudi ustrezne opredelitve vseh okrajšanih zapisov *dof* (D), (K), (E) in (EK).

Pa naj bosta $\mathscr{A}$ in $\mathscr{B}$ poljubni *dof*.

Iz (D), (3″) in (2″) dobimo takoj

(8″) $I \not\models \mathscr{A} \vee \mathscr{B}$, če je $I \not\models \mathscr{A}$ in $I \not\models \mathscr{B}$ in $I \models \mathscr{A} \vee \mathscr{B}$ v vsakem drugem primeru.

Iz (K), (2″) in (3″) pa sledi tudi brž

(9″) $I \models \mathscr{A} \wedge \mathscr{B}$, če je $I \models \mathscr{A}$ in $I \models \mathscr{B}$ in $I \not\models \mathscr{A} \wedge \mathscr{B}$ v vsakem drugem primeru.

Iz (E) pride po (2″) najprej $I \models \mathscr{A} \Leftrightarrow \mathscr{B}$ le, če je $I \not\models (\mathscr{A} \Rightarrow \mathscr{B}) \Rightarrow (\neg(\mathscr{B} \Rightarrow \mathscr{A}))$. Zato je po (3″) in (2″) naprej $I \models \mathscr{A} \Leftrightarrow \mathscr{B}$ le, če je $I \models \mathscr{A} \Rightarrow \mathscr{B}$ in $I \models \mathscr{B} \Rightarrow \mathscr{A}$ se pravi le, če *ni* $I \models \mathscr{A}$ in $I \not\models \mathscr{B}$ pa tudi *ne* $I \models \mathscr{B}$ in $I \not\models \mathscr{A}$. Odtod vidimo, da je torej

(10″) $I \models \mathscr{A} \Leftrightarrow \mathscr{B}$, če je $I \models \mathscr{A}$ in $I \models \mathscr{B}$ ali pa $I \not\models \mathscr{A}$ in $I \not\models \mathscr{B}$ in $I \not\models \mathscr{A} \Leftrightarrow \mathscr{B}$ v vsakem drugem primeru.

Bodi naposled $\mathscr{A}$ *dof*, ki ima x_n za edino prosto spremenljivko. Potem je po (EK) *dof* $(\exists x_n)\mathscr{A}$ stavek, za katerega je po (2″) $I \models (\exists x_n)\mathscr{A}$ le, če je $I \not\models (\forall x_n)(\neg \mathscr{A})$. Po (4″) to spet pomeni $I \models (\exists x_n)\mathscr{A}$ le, če *ni* pravilna vsaj ena izjava, ki je prirejena *dof* $\neg \mathscr{A}$, ko preteče prosta spremenljivka x_n domeno D. Zaradi (2″) lahko torej tudi rečemo

(11″) Če je $\mathscr{A}$ *dof*, ki ima x_n za edino prosto spremenljivko, potem je $I \models (\exists x_n)\mathscr{A}$, če je pravilna izjava, ki je prirejena *dof* $\mathscr{A}$, za *vsaj en* element interpretacijske domene D, ki ga zavzame prosta individualna spremenljivka x_n in $I \not\models (\exists x_n)\mathscr{A}$ v vsakem drugem primeru.

Na podlagi določil od (1″) do (11″) lahko torej pri dani interpretaciji I vsaki *dof* pa tudi vsakemu okrajšanemu zapisu *dof* enolično priredimo natanko eno izmed vrednosti: pravilno oziroma nepravilno. Iz teh določil pa tudi brž razvidimo, da se *pomeni* obeh znakov povezav $\neg$ in $\Rightarrow$, univerzalnostnega kvantifikatorja $\forall$ in tudi znakov $\vee$, $\wedge$, $\Leftrightarrow$, $\exists$, ki smo jih uporabili pri okrajšavah *dof*, vsaj do neke mere *pokrivajo* s pomeni določenih besed naravnega jezika. Vsaj do neke mere rečemo zato, ker imamo po eni strani opraviti z znaki, katerih pomen je z navedenimi določili nedvoumno opredeljen, po drugi strani pa z besedami živega jezika, ki se načelno izmikajo takim togim opredelitvam in katerih pomen zaznavamo le iz njihove običajne rabe v vsakdanji jezikovni praksi. Vendar pa:

Iz (2″) je lahko ugotoviti, da se pomen znaka $\neg$ zadovoljivo ujema s pomenom slovenske besedice *ne*;

iz (3″) vidimo, da se pomen znaka $\Rightarrow$ še kar zadovoljivo ujema s pomenom, se pravi z običajno rabo para slovenskih besedic *če* ... *potem* ...;

iz (4″) razberemo, da lahko znak $\forall$ zadovoljivo slovenimo z besedicama *za vsak* ...;

iz (8″) je očitno, da se pomen znaka $\vee$ še kar dobro ujema s pomenom slovenske besedice *ali*;

iz (9″) odkrijemo, da se pomen znaka $\wedge$ zadovoljivo ujema s pomenom slovenskega veznika *in*;

iz (10″) sledi, da se pomen znaka $\Leftrightarrow$ zadovoljivo pokriva s pomenom, se pravi z običajno rabo slovenskih besed ... *natanko tedaj kot* ...;

iz (11″) pa lahko sklenemo, da moremo znak $\exists$ zadovoljivo sloveniti z besedami *za vsaj en* ...

Seveda pa se razume tole: kadarkoli uporabljamo navedene slovenske besede v okviru logike, tedaj imamo vedno njihov pomen za *istoveten* s pomenom znakov, ki jih te besede zastopajo, ne oziraje se na to, ali je to v skladu z običajno jezikovno prakso ali ne.

Glede na očitno resnico, da imamo na voljo *različne mogoče* interpretacije, je kajpak lahko dana *dof* $\mathscr{A}$ pravilna pri eni in nepravilna pri drugi interpretaciji. Če pa je $\mathscr{A}$ taka *dof*, ki je pravilna pri *vsaki* interpretaciji I, potem rečemo, da je *dof* $\mathscr{A}$ *logično pravilna*. In če je *dof* $\mathscr{A}$ nepravilna pri *vsaki* interpretaciji I, pravimo, da je *logično nepravilna*.

Dejstvo, da je *dof* $\mathscr{A}$ logično pravilna, bomo simbolično zapisali z

$$\models \mathscr{A}$$

Če pa je *dof* $\mathscr{A}$ logično nepravilna, bomo to označili z

$$\not\models \mathscr{A}$$

Povejmo takoj zdaj, da so vse *dof*, ki so zajete v aksiomskih shemah predikatnega računa prvega reda, logično pravilne. Prepričajmo se o tem le za sheme (PR_1), (PR_2) in (PR_3).

Aksiomska shema (PR_1) bi bila nepravilna le pri taki interpretaciji I, pri kateri bi bilo na podlagi (3″):

$$I \models \mathscr{A} \quad \text{in} \quad I \not\models \mathscr{B} \Rightarrow \mathscr{A}$$

in zato spet po (3″)

$$I \models \mathscr{A} \quad \text{in} \quad I \models \mathscr{B} \quad \text{in} \quad I \not\models \mathscr{A}$$

To pa seveda pri nobeni interpretaciji I ni mogoče.

Aksiomska shema (PR_2) bi bila nepravilna le pri taki interpretaciji I, pri kateri bi bilo na podlagi (3″)

(a) $$I \models \mathscr{A} \Rightarrow (\mathscr{B} \Rightarrow \mathscr{C}) \quad \text{in} \quad I \not\models (\mathscr{A} \Rightarrow \mathscr{B}) \Rightarrow (\mathscr{A} \Rightarrow \mathscr{C})$$

se pravi

$$I \models \mathscr{A} \Rightarrow (\mathscr{B} \Rightarrow \mathscr{C}) \quad \text{in} \quad I \models \mathscr{A} \Rightarrow \mathscr{B} \quad \text{in} \quad I \not\models \mathscr{A} \Rightarrow \mathscr{C}$$

Odtod pa spet sledi na podlagi (3″), da bi moralo biti: $I \models \mathscr{A}$ in $I \not\models \mathscr{C}$, torej $I \models \mathscr{B}$. Toda potem bi bilo $I \not\models \mathscr{B} \Rightarrow \mathscr{C}$ in ker je $I \models \mathscr{A}$, bi dobili $I \not\models \mathscr{A} \Rightarrow (\mathscr{B} \Rightarrow \mathscr{C})$ in to je očitno spet nezdružljivo z (a).

Aksiomska shema (PR_3) bi bila nepravilna na osnovi (3″) le, če bi bilo

$$I \models \neg \mathscr{B} \Rightarrow \neg \mathscr{A} \quad \text{in} \quad I \not\models (\neg \mathscr{B} \Rightarrow \mathscr{A}) \Rightarrow \mathscr{B}$$

torej

$$I \models \neg \mathscr{B} \Rightarrow \neg \mathscr{A} \quad \text{in} \quad I \models \neg \mathscr{B} \Rightarrow \mathscr{A} \quad \text{in} \quad I \not\models \mathscr{B}$$

Odtod razberemo, če upoštevamo še (2″), da bi moralo biti: $I \models \neg \mathscr{B}$ in zato $I \models \mathscr{A}$ pa tudi $I \models \neg \mathscr{A}$. To pa kajpak ni mogoče pri nobeni interpretaciji I.

Prav tako, le z malce več truda in besed, bi ugotovili, da sta logično pravilni tudi shemi (PR_4) in (PR_5).

Predikatni račun prvega reda, ki smo ga označili za čisto logično teorijo, je potemtakem taka teorija prvega reda, ki ima za svoje aksiomske sheme logično pravilne *dof*, se pravi take *dof*, ki so pravilne pri *vsaki* interpretaciji. Brž pa ko ima kakšna teorija prvega reda T za lastne aksiome še take *dof*, ki *niso* logično pravilne, je seveda temeljnega pomena vprašanje, ali *sploh obstaja* kakšna interpretacija I, pri kateri so tudi *vsi* lastni aksiomi te teorije pravilni. Vsako tako interpretacijo, če seveda obstaja, imenujemo *model* ustrezne teorije T.

3.

Brž ko smo tako opisu sintakse *JPR* v 1. razdelku pridružili v 2. razdelku še osnove njegove splošne semantike, se nam v tej zvezi odpirajo nekateri problemi, ki utegnejo biti, če že ne rešljivi, pa vsaj zanimivi.

Naj bo T dana teorija prvega reda in I poljuben njen model. Prvo vprašanje, ki se nam ob tem zastavlja, je naslednje:

Ali so, poleg logičnih aksiomskih shem in lastnih aksiomov teorije T, v modelu I pravilni tudi *vsi izreki* teorije T? Ali lahko torej pri *vsakem* modelu I teorije T, za vsako *dof* $\mathscr{A}$

(Z) iz $\vdash_T \mathscr{A}$ sklepamo na $I \models \mathscr{A}$.

Če je T kar predikatni račun prvega reda, nam pra-vilnost tega sklepa očitno zagotavlja, da je tudi vsak izrek predikatnega računa logično pravilen.

Teorije, za katere ta sklep velja, imenujemo, iz popolnoma razumljivih razlogov, *zdrave*. Na dlani je namreč, da teorija, ki bi imela model, v katerem bi bili nekateri izreki pravilni, drugi pa nepravilni, vsaj v spoznavnem smislu, ne more biti kaj prida. In naj se še tako sprenevedamo, češ da gre pri sintaksi le za popolnoma svojevoljno čisto igro s simboli, je vendarle res, da je to zelo premetena igra, ki je bila zamišljena samo zato, da bi z njo dosegli popolnoma določen spoznavni cilj.

Iz 1. razdelka vemo, da je izrek dane teorije T vsaka taka *dof* $\mathscr{A}$, za katero obstaja dokaz. Dokaz *dof* $\mathscr{A}$ pa je končno zaporedje *dof*, katerega členi so bodisi aksiomi teorije T ali pa

dof, ki so rezultat uporabe pravil sklepanja (MP) oziroma (G) na členih zaporedja, ki so *pred* ustreznimi *dof*, in je *dof* $\mathscr{A}$ zadnji člen tega zaporedja. Glede na to, da so vsi aksiomi teorije T po definiciji modela pravilni v vsakem modelu teorije T, se bo izkazala tudi pravilnost vsakega člena v dokazu *dof* $\mathscr{A}$, torej tudi pravilnost *dof* $\mathscr{A}$, brž ko ugotovimo tole: rezultati uporabe pravil sklepanja (MP) oziroma (G) na *pravilnih dof* so *pravilne dof*. To pa je res.

Po (MP) sklepamo namreč iz *dof* $\mathscr{A}$ in $\mathscr{A} \Rightarrow \mathscr{B}$ na *dof* $\mathscr{B}$. Toda po (3″) velja: ako sta $\mathscr{A}$ in $\mathscr{A} \Rightarrow \mathscr{B}$ pravilni, mora biti pravilna tudi *dof* $\mathscr{B}$.

Po (G) sklepamo iz *dof* $\mathscr{A}$ na *dof* $(\forall x_n)\,\mathscr{A}$. Pa recimo, da je *dof* $\mathscr{A}$ pravilna in ločimo dve možnosti:

Spremenljivka x_n *ne* nastopa prosto v *dof* $\mathscr{A}$. V tem primeru je kajpada učinek kvantifikatorja $(\forall x_n)$ na *dof* $\mathscr{A}$ ničen in zato je seveda *dof* $(\forall x_n)\,\mathscr{A}$ pravilna natanko tedaj, ko je pravilna *dof* $\mathscr{A}$.

V *dof* $\mathscr{A}$ so $x_1, x_2, \ldots x_n$ natanko vse proste spremenljivke. Se pravi, da so v *dof* $(\forall x_n)\,\mathscr{A}$ le še $x_1, x_2, \ldots x_{n-1}$ natanko vse proste spremenljivke. Po (7″) pa je *dof* $\mathscr{A}$ pravilna le, če je pravilen stavek $(\forall x_1)\,(\forall x_2)\ldots(\forall x_{n-1})\,(\forall x_n)\,\mathscr{A}$ in je *dof* $(\forall x_n)\,\mathscr{A}$ pravilna le, če je pravilen stavek $((\forall x_1)\,(\forall x_2)\ldots(\forall x_{n-1}))\,(\forall x_n)\,\mathscr{A}$. Po (6″) pa gre v obeh primerih očitno za isti stavek.

Potemtakem smo dobili naslednji izid:

Vse teorije, ki imajo modele in uporabljajo le pravili sklepanja (MP) in (G), so zdrave.

Na pravkar razrešeno prvo vprašanje se čisto naravno navezuje naslednje:

Če je spet I poljuben model dane teorije T, ali je tudi obratno, vsaka pravilna *dof* tudi *izrek* teorije T? Ali torej lahko za vsako *dof* $\mathscr{A}$

(P) iz $I \models \mathscr{A}$ za vsak model I teorije T sklepamo na $\vdash_T \mathscr{A}$.

Zdravo teorijo, pri kateri ta sklep velja, imenujemo *popolno*. Tako označbo tudi zasluži, saj se pri njej sintaktični pojem *izreka* natanko pokriva s semantičnim pojmom *pravilnosti*, se pravi, da so pri taki teoriji pravilne natanko tiste trditve, ki so tudi dokazljive.

V tej zvezi omenimo le dva klasična rezultata, od katerih je eden pozitiven, drugi pa negativen:

Leta 1930 je *Gödel* dokazal, da je predikatni račun prvega reda popoln. Izreki predikatnega računa so potemtakem natanko vse logično pravilne *dof*.

Drugi, negativni rezultat pa se nanaša na elementarno teorijo naravnih števil, torej na ETNŠ. *Če privzamemo*, da so naravna števila $N = \{0, 1, \ldots n, \ldots\}$, kakor jih sicer poznamo iz matematike, model teorije prvega reda ETNŠ, potem ta teorija *ni* popolna. To pomeni, da obstaja taka *dof* teorije, ki je pravilna, pa ni izrek, se pravi, ni dokazljiva. Tudi do tega spoznanja se je prvi dokopal *Gödel* leta 1931.

Seveda bi si utegnili ta negativni rezultat razlagati tako, da je pač sistem aksiomov ETNŠ preozek, da bi lahko iz njega dokazali vse pravilne *dof* elementarne aritmetike in da bi popolnost lahko dosegli, če bi sistem dopolnili še s kakšnim aksiomom, na primer kar s tisto *dof*, ki je pravilna, pa ni izrek. Vendar bi bila taka razlaga le slepilo, ki bi samo dokazovalo, da nismo popolnoma dojeli bistva Gödelovega rezultata. Ta je namreč v tem, da *nobena* formalna teorija, ki ima množico naravnih števil N za model, *ni* popolna. Ako bi torej sistem aksiomov ETNŠ dopolnili še z *dof*, ki je sicer pravilna, pa na podlagi tega sistema ni dokazljiva, potem bi spet obstajala neka *druga dof*, ki bi bila pravilna, pa tudi v tako razširjenem sistemu aksiomov ne dokazljiva. Gödelov izid odkriva potemtakem *načelno* nemoč formalizacije elementarne aritmetike nasploh.

Nadaljnji problem, fundamentalnega pomena za vsako formalno teorijo, je tako imenovani problem *neprotislovnosti*. Za dano teorijo T pravimo, da je neprotislovna, če *ne*

obstaja taka *dof* $\mathscr{A}$ teorije, da bi bila *hkrati* $\mathscr{A}$ in $\neg\mathscr{A}$ izreka teorije, se pravi, da bi veljalo hkrati $\vdash_T \mathscr{A}$ in $\vdash_T \neg\mathscr{A}$. Z uporabo pravila sklepanja (MP) se da brž pokazati, da je teorija T neprotislovna natanko tedaj, kadar *niso vse dof* teorije tudi izreki teorije. Ker bi bila teorija, v kateri bi bile *vse dof* tudi izreki, že v čisto sintaktičnem pogledu popolnoma nezanimiva, semantično pa očitno brez vsake spoznavne vrednosti, je na dlani, da se je smiselno ukvarjati *le* z neprotislovnimi teorijami. Potemtakem je zelo razumljiva želja, da bi, preden se sploh zares lotimo študija kakšne teorije, nedvoumno preskusili njeno neprotislovnost. Kako je torej z uresničitvijo te upravičene želje?

Najprej navedimo tale vzpodbudni rezultat:

(M) Dana teorija T je neprotislovna tedaj in le tedaj, kadar ima model.

Da je vsaka teorija, ki ima model, neprotislovna, po vsem, kar smo že povedali o interpretacijah in modelih, bržčas ni potrebno še kako posebej utemeljevati. Da pa ima vsaka neprotislovna teorija model, je vsekakor manj razvidna trditev, ki bi jo bilo treba natanko preskusiti. Povejmo le, da je bilo to storjeno z vso potrebno strogostjo in na več načinov.

Šibka stran izida (M), kar zadeva njegovo uporabo, je v *metodah* in *sredstvih*, s katerimi ugotavljamo, da je določena interpretacija I res model dane teorije T. Če so namreč te metode in ta sredstva logično manj zanesljiva kot pa tista, ki jih nudi sama teorija, katere neprotislovnost želimo dokazati, potem je kajpak tak dokaz neprotislovnosti, če že ne vprašljiv, pa vsaj ne povsem zadovoljiv. Glede tega povejmo naslednje, danes že klasične rezultate:

Neprotislovnost predikatnega računa prvega reda je dokončno izpričana.

Neprotislovnost ETNŠ je nepričakovano trd oreh. *Vsi* doslej znani dokazi o neprotislovnosti elementarne teorije naravnih števil, prva dva je konstruiral *Gentzen* v letih 1936 in 1938, kasneje pa so sledili še dokazi *Ackermanna* (1940), *Lorenzena* (1951), *Schütteja* (1951 in 1960) in *Hlodovskega* (1959), naj so še tako domiselni in vredni občudovanja, zblede ob dejstvu, da uporabljajo metode in sredstva, ki so logično krhkejša od tistih, katere hočejo utemeljiti. Zaupanje v morebitno odkritje novih, prepričljivejših dokazov pa je žal krepko ohromljeno zaradi naslednjega spoznanja, ki je tudi sad *Gödelovih* raziskav:

(N) V ETNŠ lahko konstruiramo *dof* $\mathscr{A}$, katere *pomen* je: »ETNŠ je neprotislovna teorija.« Vendar pa velja:

Če je ETNŠ neprotislovna teorija, potem *dof* $\mathscr{A}$ *ni* izrek v ETNŠ.

Drugače povedano:

Če je ETNŠ neprotislovna teorija, potem te neprotislovnosti *ni mogoče dokazati* le na osnovi aksiomov ETNŠ, se pravi *znotraj* ETNŠ. *Vsak* dokaz neprotislovnosti ETNŠ *mora* potemtakem uporabljati tudi metode in sredstva, ki *niso* zajeta v ETNŠ.

Ta Gödelov izsledek pa velja tudi za vsako teorijo prvega (in ne samo prvega) reda, ki je dovolj bogata, da je v njej zajeta tudi elementarna aritmetika. Potemtakem je z njim zadeta tudi elementarna teorija množic ETM in kajpak vsaka matematična teorija, ki je zgrajena na teoriji množic. Za vse te teorije torej velja: če so neprotislovne, njihove neprotislovnosti ne moremo dokazati le s sredstvi in metodami, ki izhajajo iz aksiomov teh teorij. Nobena teh teorij, če je neprotislovna, ne more potemtakem izpričati svoje lastne neprotislovnosti.

Za sklep omenimo še en problem, ki zadeva formalne teorije in ki je, če že ne tako dramatičen kot problem neprotislovnosti, pa vendarle vir presenetljivih miselnih razpletov. To je tako imenovani *problem neodvisnosti* aksiomov.

Bodi S sistem aksiomov dane neprotislovne teorije T. Potem rečemo, da je aksiom $\mathscr{A} \in S$ neodvisen od drugih aksiomov sistema S, če $\mathscr{A}$ *ni* izrek v teoriji T', ki ima za sistem aksiomov S' vse aksiome sistema S *razen* aksioma $\mathscr{A}$, sicer pa ista pravila sklepanja kot teorija T. Ako je *vsak* aksiom sistema S neodvisen od drugih aksiomov tega sistema, potem pravimo, da je neodvisen sistem aksiomov S.

Neodvisnost aksioma $\mathscr{A} \in S$ od drugih aksiomov sistema S pokažemo lahko običajno tako, da poskušamo konstruirati kako interpretacijo I, pri kateri je aksiom $\mathscr{A}$ nepravilen, *vsi* drugi aksiomi sistema S pa so pravilni. Če namreč taka interpretacija obstaja, potem brž lahko sklenemo, da aksioma $\mathscr{A}$ res ni mogoče dokazati iz preostalih aksiomov sistema S, ki ga imamo seveda za zdravega.

V zgodovini matematike imamo dva znamenita primera neodvisnosti aksiomov. Prvi je neodvisnost aksioma o vzporednicah od drugih aksiomov elementarne geometrije. Posledica te neodvisnosti je bilo rojstvo neevklidskih geometrij. Drugi primer pa je novejšega datuma (1963) in zadeva neodvisnost aksioma izbire od drugih aksiomov elementarne teorije množic. Posledice tega spoznanja pa do danes še niso popolnoma odkrite.

LITERATURA

[1] E. Mendelson, *Introduction to Mathematical Logic*, D. Van Nostrand Company, Inc., New Jersey, Princeton 1966.

[2] J.W. Robbin, *Mathematical Logic*, A first Course, New York, W.A. Benjamin 1969.

[3] J.R. Shoenfield, *Mathematical Logic*, Reading, Massachusetts, Addison-Wesley Publishing Company 1967.

Obzornik mat. fiz. **25** (1978) 1

IZREK O DEDUKCIJI

IZIDOR HAFNER

AMS Subj. Class. (1970) 02 B 10

V tem članku je dokazan izrek o dedukciji.

THE DEDUCTION THEOREM

In this article the deduction theorem is proved.

V tem članku bomo privzeli terminologijo iz razprave [1], zaradi lažjega razumevanja pa bomo ponovili nekaj definicij.

Formalni dokazi popolnoma elementarnih izrekov so ponavadi zelo dolgi. S formalizacijo teorije dobimo eksplicitno definicijo tega, kar je dokaz v tej teoriji. Ko smo to dosegli, ni vedno nujno sklicevati se direktno na to definicijo. Formalno dokazljivost neke formule (okrajšava za dobro oblikovano formulo) dosti laže dosežemo z uporabo metamatematičnih izrekov, ki govorijo o eksistenci formalnih dokazov. Dokazi teh metaizrekov pa morajo vsaj implicitno vsebovati metodo, kako pridemo do formalnih dokazov.

Najbolj enostavne take izreke bomo imenovali **izpeljana pravila,** ker izražajo principe, za katere lahko rečemo, da so izpeljani iz postuliranih pravil; dokazano je, da ne povečamo množice dokazljivih formul, če te principe uporabimo kot dodatne metode izpeljevanja.

V formalnih sistemih ima dokaz najbolj enostavno možno strukturo, sestoji namreč iz enega samega končnega zaporedja formul. V matematiki pa imajo dokazi večkrat bolj komplicirano strukturo; pogosto na primer dokazujemo tako, da naredimo kakšno predpostavko.

Definirajmo zdaj pojem formalne izpeljivosti iz hipotez v dani formalni teoriji.

Naj bo dana prazna ali končna množica formul $\{\mathscr{A}_1, \ldots, \mathscr{A}_n\}$. Vsako končno zaporedje formul imenujemo **dedukcija** ali **izpeljava** iz hipotez $\mathscr{A}_1, \ldots, \mathscr{A}_n$, če za vsako formulo v tem zaporedju velja ena izmed naslednjih možnosti:

— da je ena izmed formul $\mathscr{A}_1, \ldots, \mathscr{A}_n$;
— da je aksiom;
— da je dobljena iz formul, ki stojijo v zaporedju pred njo, po nekem pravilu sklepanja.

Rekli bomo, da je to zaporedje **dedukcija** njegove zadnje formule iz hipotez $\mathscr{A}_1, \ldots, \mathscr{A}_n$. Simbolični izraz

$$\mathscr{A}_1, \ldots, \mathscr{A}_n \vdash \mathscr{E}$$

bo izražal trditev, da je formula $\mathscr{E}$ izpeljiva iz hipotez $\mathscr{A}_1, \ldots, \mathscr{A}_n$, to je, da obstaja dedukcija formule $\mathscr{E}$ iz hipotez $\mathscr{A}_1, \ldots, \mathscr{A}_n$.

V posebnem primeru, ko je množica hipotez prazna, pravimo, da je formula $\mathscr{E}$ **dokazljiva.**

Naš glavni rezultat, izrek o dedukciji, bomo dokazali za teorije, ki imajo poleg drugih tudi naslednje aksiome (bolj natančno — aksiomske sheme):

(A1) $\mathscr{A} \Rightarrow (\mathscr{B} \Rightarrow \mathscr{A})$;

(A2) $(\mathscr{A} \Rightarrow (\mathscr{B} \Rightarrow \mathscr{C})) \Rightarrow ((\mathscr{A} \Rightarrow \mathscr{B}) \Rightarrow (\mathscr{A} \Rightarrow \mathscr{C}))$;

(A3) $(\forall x)(\mathscr{A} \Rightarrow \mathscr{B}) \Rightarrow (\mathscr{A} \Rightarrow (\forall x)\mathscr{B})$, kjer spremenljivka x ne nastopa prosto v v formuli $\mathscr{A}$; edini pravili sklepanja pa sta:

(MP) modus ponens ali pravilo odcepitve: iz $\mathscr{A}$ in $\mathscr{A} \Rightarrow \mathscr{B}$ sklepamo na $\mathscr{B}$;

(G) generalizacija: iz $\mathscr{A}$ sklepamo na $(\forall x)\mathscr{A}$.

Vidimo torej, da nismo izčrpali celotnega spiska aksiomov predikatnega računa (aksiomi PR1—PR5 v [1]). Preostali dve aksiomski shemi sta:

(A4) $(\neg \mathscr{B} \Rightarrow \neg \mathscr{A}) \Rightarrow ((\neg \mathscr{B} \Rightarrow \mathscr{A}) \Rightarrow \mathscr{B})$

(A5) $(\forall x)\mathscr{A} \Rightarrow S_t^x \mathscr{A} \mid$, kjer je term t prost za spremenljivko x v formuli $\mathscr{A}$.

To sta shemi PR3 in PR4 iz [1].

Za take formalne teorije je definicija dedukcije naslednja:

Končno zaporedje formul $\mathscr{B}_1, \ldots, \mathscr{B}_m$ je dedukcija (formule $\mathscr{B}_m$) iz hipotez $\mathscr{A}_1, \ldots, \mathscr{A}_n$ natanko tedaj, kadar za vsak $k = 1, 2, \ldots, m$ velja natanko ena izmed točk

(DH1) $\mathscr{B}_k$ je ena izmed formul $\mathscr{A}_1, \ldots, \mathscr{A}_n$;

(DH2) $\mathscr{B}_k$ je aksiom;

(DH3) obstajata taki naravni števili $i, j < k$, da je formula $\mathscr{B}_k$ dobljena iz formul $\mathscr{B}_i$ in $\mathscr{B}_j$ po pravilu (MP) (tedaj je $\mathscr{B}_j$ kar $\mathscr{B}_i \Rightarrow \mathscr{B}_k$);

(DH4) obstaja tako naravno število $i < k$, da je $\mathscr{B}_k$ dobljena iz formule $\mathscr{B}_i$ z generalizacijo ($\mathscr{B}_k$ je torej $(\forall x)\mathscr{B}_i$).

Pri omenjenih predpostavkah glede formalne teorije velja naslednji **izrek o dedukciji:**

Če obstaja dedukcija formule $\mathscr{B}$ iz hipotez $\mathscr{A}_1, \ldots, \mathscr{A}_n$, v kateri ni uporabljeno pravilo generalizacije na nobeno izmed spremenljivk, ki nastopajo prosto v formuli $\mathscr{A}_n$, potem obstaja dedukcija formule $\mathscr{A}_n \Rightarrow \mathscr{B}$ iz hipotez $\mathscr{A}_1, \ldots, \mathscr{A}_{n-1}$.

Iz dokaza tega izreka bo razvidno, kako dedukcijo formule $\mathscr{A}_n \Rightarrow \mathscr{B}$ iz hipotez $\mathscr{A}_1, \ldots, \mathscr{A}_{n-1}$ tudi dobimo, če poznamo dedukcijo formule $\mathscr{B}$ iz hipotez $\mathscr{A}_1, \ldots, \mathscr{A}_n$. Ta izrek bomo torej lahko uporabljali kot izvedeno pravilo: če hočemo dokazati $\vdash \mathscr{A} \Rightarrow \mathscr{B}$, to dokažemo s trditvijo $\mathscr{A} \vdash \mathscr{B}$, to je, da privzamemo $\mathscr{A}$ kot hipotezo.

Preden se lotimo dokaza izreka o dedukciji, moramo dokazati dva pomožna izreka.

Lema 1. Velja $\vdash \mathscr{A} \Rightarrow \mathscr{A}$ (formula $\mathscr{A} \Rightarrow \mathscr{A}$ je dokazljiva).

Dokaz. Naslednje zaporedje formul je dokaz formule $\mathscr{A} \Rightarrow \mathscr{A}$.

(1) $(\mathscr{A} \Rightarrow ((\mathscr{A} \Rightarrow \mathscr{A}) \Rightarrow \mathscr{A})) \Rightarrow ((\mathscr{A} \Rightarrow (\mathscr{A} \Rightarrow \mathscr{A})) \Rightarrow (\mathscr{A} \Rightarrow \mathscr{A}))$

To je aksiom po shemi (A2), če vstavimo namesto $\mathscr{A}$, $\mathscr{B}$ in $\mathscr{C}$ formule $\mathscr{A}$, $\mathscr{A} \Rightarrow \mathscr{A}$, $\mathscr{A}$.

(2) $\mathscr{A} \Rightarrow ((\mathscr{A} \Rightarrow \mathscr{A}) \Rightarrow \mathscr{A})$

To je aksiom po shemi (A1), če vstavimo za $\mathscr{A}$ in $\mathscr{B}$ formuli $\mathscr{A}$ in $\mathscr{A} \Rightarrow \mathscr{A}$.

(3) $(\mathscr{A} \Rightarrow (\mathscr{A} \Rightarrow \mathscr{A})) \Rightarrow (\mathscr{A} \Rightarrow \mathscr{A})$

Ta točka je posledica točk (1) in (2) po pravilu (MP).

(4) $\mathscr{A} \Rightarrow (\mathscr{A} \Rightarrow \mathscr{A})$

Točka (4) je aksiom po shemi (A1).

(5) $\mathscr{A} \Rightarrow \mathscr{A}$

To dobimo iz točk (3) in (4) po pravilu (MP).

Lema 2. Če velja $\mathscr{A}_1, \mathscr{A}_2, \ldots, \mathscr{A}_n \vdash \mathscr{B}$ in $\mathscr{A}_1, \mathscr{A}_2, \ldots, \mathscr{A}_n \vdash \mathscr{B} \Rightarrow \mathscr{C}$, potem velja $\mathscr{A}_1, \mathscr{A}_2, \ldots, \mathscr{A}_n \vdash \mathscr{C}$.

Dokaz. Predpostavimo $\mathscr{A}_1, \ldots, \mathscr{A}_n \vdash \mathscr{B}$ in $\mathscr{A}_1, \ldots, \mathscr{A}_n \vdash \mathscr{B} \Rightarrow \mathscr{C}$. Tedaj obstaja dedukcija $\mathscr{B}_1, \ldots, \mathscr{B}_m$ formule $\mathscr{B}$ iz $\mathscr{A}_1, \ldots, \mathscr{A}_n$ ($\mathscr{B}_m$ je $\mathscr{B}$) in dedukcija $\mathscr{C}_1, \mathscr{C}_2, \ldots, \mathscr{C}_k$ formule $\mathscr{B} \Rightarrow \mathscr{C}$ iz $\mathscr{A}_1, \mathscr{A}_2, \ldots, \mathscr{A}_n$ ($\mathscr{C}_k$ je torej $\mathscr{B} \Rightarrow \mathscr{C}$). Potem je zaporedje $\mathscr{B}_1, \mathscr{B}_2, \ldots, \mathscr{B}_m$, $\mathscr{C}_1, \ldots, \mathscr{C}_k, \mathscr{C}$ dedukcija formule $\mathscr{C}$ iz $\mathscr{A}_1, \ldots, \mathscr{A}_n$, saj je formula $\mathscr{C}$ dobljena iz $\mathscr{B}_m$ in $\mathscr{C}_k$ po pravilu (MP).

Lema 2 se često uporablja v dokazovanju, včasih je navedena kot uporaba pravila (MP).

Dokaz izreka o dedukciji. Predpostavimo, da velja $\mathscr{A}_1, \mathscr{A}_2, \ldots, \mathscr{A}_n \vdash \mathscr{B}$. Potem obstaja dedukcija $\mathscr{B}_1, \mathscr{B}_2, \ldots, \mathscr{B}_m$ formule $\mathscr{B}$ iz hipotez $\mathscr{A}_1, \mathscr{A}_2, \ldots, \mathscr{A}_n$ ($\mathscr{B}$ je $\mathscr{B}_m$).

Dokazali bomo

(1) $\mathscr{A}_1, \mathscr{A}_2, \ldots, \mathscr{A}_{n-1} \vdash \mathscr{A}_n \Rightarrow \mathscr{B}_k$ za $k = 1, 2, \ldots, m$. Če postavimo $k = m$ v (1), dobimo trditev izreka o dedukciji.

Trditev (1) bomo dokazali z indukcijo. Po pravilu matematične indukcije moramo dokazati, da velja formula za število 1 in če velja za število k, da velja tudi za $k + 1$. Tokrat pa bo sklepanje malo drugačno.

Veljavnost kake trditve za vsa naravna števila pokažemo tako, da iz predpostavke, da ta trditev velja za vsa naravna števila, ki so manjša od števila k, sklepamo o pravilnosti trditve za število k. Stavek, da velja trditev za vsa naravna števila, ki so manjša od 1, je vedno izpolnjen, saj ni nobenega števila, manjšega od 1.

Primer 1. Predpostavimo, da $\mathscr{B}_k$ izpolnjuje točko (DH1) definicije dedukcije iz hipotez. Potem je formula $\mathscr{B}_k$ ena izmed hipotez, na primer $\mathscr{A}_j$, $j \in \{1, 2, \ldots, n\}$.

Primer 1 a. $j \in \{1, 2, \ldots, n - 1\}$. Iz točke (DH1) sledi

$$\mathscr{A}_1, \mathscr{A}_2, \ldots, \mathscr{A}_{n-1} \vdash \mathscr{A}_j \ (\equiv \mathscr{B}_k)$$

Po točki (DH2) in (A1) velja

$$\mathscr{A}_1, \mathscr{A}_2, \ldots, \mathscr{A}_{n-1} \vdash \mathscr{B}_k \Rightarrow (\mathscr{A}_n \Rightarrow \mathscr{B}_k)$$

Iz leme 2 sledi

$$\mathscr{A}_1, \mathscr{A}_2, \ldots, \mathscr{A}_{n-1} \vdash \mathscr{A}_n \Rightarrow \mathscr{B}_k$$

Primer 1 b. Naj bo j = n. Potem je $\mathscr{A}_n \Rightarrow \mathscr{B}_k$ kar $\mathscr{A}_n \Rightarrow \mathscr{A}_n$ in zato $\mathscr{A}_1, \mathscr{A}_2, \ldots, \mathscr{A}_{n-1} \vdash$ $\vdash \mathscr{A}_n \Rightarrow \mathscr{B}_\kappa$ po lemi 1 (Lema 1 trdi $\vdash \mathscr{A}_n \Rightarrow \mathscr{A}_n$, to pa implicira $\mathscr{A}_1, \mathscr{A}_2, \ldots, \mathscr{A}_{n-1} \vdash \mathscr{A}_n \Rightarrow$ $\Rightarrow \mathscr{A}_n$, saj je vsaka dokazljiva formula tudi izpeljiva iz kakršnekoli množice hipotez).

Primer 2. Vzemimo, da $\mathscr{B}_k$ izpolnjuje točko (DH2). Potem je $\mathscr{B}_k$ aksiom dane teorije in seveda velja

$$\mathscr{A}_1, \mathscr{A}_2, \ldots, \mathscr{A}_{n-1} \vdash \mathscr{B}_k$$

Iz enakega razloga velja tudi

$$\mathscr{A}_1, \mathscr{A}_2, \ldots, \mathscr{A}_{n-1} \vdash \mathscr{B}_k \Rightarrow (\mathscr{A}_n \Rightarrow \mathscr{B}_k)$$

saj je desna stran glede na $\vdash$ aksiom po (A1).

Po lemi 2 dobimo

$$\mathscr{A}_1, \mathscr{A}_2, \ldots, \mathscr{A}_{n-1} \vdash \mathscr{A}_n \Rightarrow \mathscr{B}_k$$

Primer 3. Vzemimo, da formula $\mathscr{B}_k$ izpolnjuje točko (DH3) definicije. Potem obstajata naravni števili $i, j < k$, da je $\mathscr{B}_j$ kar $\mathscr{B}_i \Rightarrow \mathscr{B}_k$. Zaradi indukcijske hipoteze imamo

(2) $\mathscr{A}_1, \mathscr{A}_2, \ldots, \mathscr{A}_{n-1} \vdash \mathscr{A}_n \Rightarrow \mathscr{B}_i$ in
(3) $\mathscr{A}_1, \mathscr{A}_2, \ldots, \mathscr{A}_{n-1} \vdash \mathscr{A}_n \Rightarrow \mathscr{B}_j \ (\equiv \mathscr{A}_n \Rightarrow (\mathscr{B}_i \Rightarrow \mathscr{B}_k))$

Po shemi (A2) dobimo

(4) $\mathscr{A}_1, \mathscr{A}_2, \ldots, \mathscr{A}_{n-1} \vdash (\mathscr{A}_n \Rightarrow (\mathscr{B}_i \Rightarrow \mathscr{B}_k)) \Rightarrow ((\mathscr{A}_n \Rightarrow \mathscr{B}_i) \Rightarrow (\mathscr{A}_n \Rightarrow \mathscr{B}_k))$

Iz točk (3) in (4) z uporabo leme 2 dobimo

(5) $\mathscr{A}_1, \mathscr{A}_2, \ldots, \mathscr{A}_{n-1} \vdash (\mathscr{A}_n \Rightarrow \mathscr{B}_i) \Rightarrow (\mathscr{A}_n \Rightarrow \mathscr{B}_k)$

Še enkrat uporabimo lemo 2 na točki (2) in (5) pa sledi

$$\mathscr{A}_1, \mathscr{A}_2, \ldots, \mathscr{A}_{n-1} \vdash \mathscr{A}_n \Rightarrow \mathscr{B}_k$$

Primer 4. Vzemimo, da formula $\mathscr{B}_k$ izpolnjuje točko (DH4) definicije. Potem $\mathscr{B}_k$ dobimo iz neke formule $\mathscr{B}_i$ $(i < k)$ z generalizacijo. $\mathscr{B}_k$ je torej $(\forall x)\, \mathscr{B}_i$ in x ne nastopa prosto v $\mathscr{A}_n$. Po indukcijski hipotezi imamo

$$\mathscr{A}_1, \mathscr{A}_2, \ldots, \mathscr{A}_{n-1} \vdash \mathscr{A}_n \Rightarrow \mathscr{B}_i$$

Z generalizacijo od tod dobimo

$$\mathscr{A}_1, \mathscr{A}_2, \ldots, \mathscr{A}_{n-1} \vdash (\forall x)\, (\mathscr{A}_n \Rightarrow \mathscr{B}_i)$$

Po točki (DH2) in ker je (A3) aksiomska shema, imamo

$$\mathscr{A}_1, \mathscr{A}_2, \ldots, \mathscr{A}_{n-1} \vdash (\forall x)\,(\mathscr{A}_n \Rightarrow \mathscr{B}_i) \Rightarrow (\mathscr{A}_n \Rightarrow (\forall x)\,\mathscr{B}_i)$$

Po lemi 2 velja $$\mathscr{A}_1, \mathscr{A}_2, \ldots, \mathscr{A}_{n-1} \vdash \mathscr{A}_n \Rightarrow (\forall x)\,\mathscr{B}_i$$

oziroma $$\mathscr{A}_1, \mathscr{A}_2, \ldots, \mathscr{A}_{n-1} \vdash \mathscr{A}_n \Rightarrow \mathscr{B}_\kappa$$

Predpostavko, da x ne nastopa prosto v $\mathscr{A}_n$, smo potrebovali zaradi uporabe aksioma (A3).

Tako smo izrek o dedukciji dokazali.

Aksiomsko shemo (A3) smo uporabili le v primeru 4. To pa pomeni, da v teorijah, v katerih je pravilo (MP) edino pravilo sklepanja, lahko dokažemo izrek o dedukciji že z aksiomskima shemama (A1) in (A2).

Taka teorija je na primer stavčni račun iz [1]. Tako smo dokazali:

Posledica 1. Če je $\mathscr{A}_1, \mathscr{A}_2, \ldots, \mathscr{A}_n \vdash \mathscr{B}$, potem je $\mathscr{A}_1, \mathscr{A}_2, \ldots, \mathscr{A}_{n-1} \vdash \mathscr{A}_n \Rightarrow \mathscr{B}$, kjer je $\vdash$ znak za relacijo izpeljivosti v stavčnem računu.

Posledica 2. Če velja $\mathscr{A}_1, \mathscr{A}_2, \ldots, \mathscr{A}_n \vdash \mathscr{B}$ in obstaja taka dedukcija, da v njej nismo uporabili pravila generalizacije na nobeno izmed spremenljivk, ki nastopajo prosto v katerikoli izmed hipotez, potem velja $\vdash \mathscr{A}_1 \Rightarrow (\mathscr{A}_2 \Rightarrow \ldots (\mathscr{A}_n \Rightarrow \mathscr{B}) \ldots)$. To posledico pokažemo tako, da n-krat uporabimo izrek o dedukciji. S tem izrekom pa smo pojem izpeljivosti iz hipotez prevedli na pojem dokazljivosti.

Opomba. Kako iz dane dedukcije $\mathscr{B}_1, \mathscr{B}_2, \ldots, \mathscr{B}_m$ dobimo dedukcijo formule $\mathscr{A}_n \Rightarrow \mathscr{B}$ iz hipotez $\mathscr{A}_1, \ldots, \mathscr{A}_{n-1}$? To naredimo tako, da drugo za drugo tvorimo dedukcije formul $\mathscr{A}_n \Rightarrow \mathscr{B}_k$ $(k = 1, 2, \ldots, m)$ iz hipotez $\mathscr{A}_1, \ldots, \mathscr{A}_{n-1}$ in sicer tako, kot nam pove dokaz izreka o dedukciji. Če smo na primer $\mathscr{B}_k$ dobili po točki (DH4) in je $\mathscr{B}_1', \ldots, \mathscr{B}_l', \mathscr{A}_n \Rightarrow \mathscr{B}_i$ dedukcija formule $\mathscr{A}_n \Rightarrow \mathscr{B}_i$, potem je

$$\mathscr{B}_1', \mathscr{B}_2', \ldots, \mathscr{B}_l', \mathscr{A}_n \Rightarrow \mathscr{B}_i, (\forall x)\,(\mathscr{A}_n \Rightarrow \mathscr{B}_i), (\forall x)\,(\mathscr{A}_n \Rightarrow \mathscr{B}_i) \Rightarrow (\mathscr{A}_n \Rightarrow (\forall x)\,\mathscr{B}_i),$$
$$\mathscr{A}_n \Rightarrow (\forall x)\,\mathscr{B}_i$$

dedukcija formule $\mathscr{A}_n \Rightarrow (\forall x)\,\mathscr{B}_i$ $(\equiv \mathscr{A}_n \Rightarrow \mathscr{B}_\kappa)$ iz hipotez $\mathscr{A}_1, \ldots, \mathscr{A}_{n-1}$.

V nadaljevanju bomo dokazali nekaj izrekov z uporabo izreka o dedukciji. Primeri 1 do 4 veljajo za stavčni račun in seveda za vse teorije, ki stavčni račun vsebujejo.

Primer 1. Dokažimo trditev

$$\vdash (\mathscr{A} \Rightarrow \mathscr{B}) \Rightarrow ((\mathscr{B} \Rightarrow \mathscr{C}) \Rightarrow (\mathscr{A} \Rightarrow \mathscr{C}))$$

Dokaz poteka takole:

(1) $\mathscr{A} \Rightarrow \mathscr{B}, \mathscr{B} \Rightarrow \mathscr{C}, \mathscr{A} \vdash \mathscr{A} \Rightarrow \mathscr{B}$
(2) $\mathscr{A} \Rightarrow \mathscr{B}, \mathscr{B} \Rightarrow \mathscr{C}, \mathscr{A} \vdash \mathscr{A}$
(3) $\mathscr{A} \Rightarrow \mathscr{B}, \mathscr{B} \Rightarrow \mathscr{C}, \mathscr{A} \vdash \mathscr{B}$
(4) $\mathscr{A} \Rightarrow \mathscr{B}, \mathscr{B} \Rightarrow \mathscr{C}, \mathscr{A} \vdash \mathscr{B} \Rightarrow \mathscr{C}$
(5) $\mathscr{A} \Rightarrow \mathscr{B}, \mathscr{B} \Rightarrow \mathscr{C}, \mathscr{A} \vdash \mathscr{C}$
(6) $\mathscr{A} \Rightarrow \mathscr{B}, \mathscr{B} \Rightarrow \mathscr{C} \vdash \mathscr{A} \Rightarrow \mathscr{C}$

Vrstice (1), (2) in (4) so veljavne, saj so na desni strani hipoteze. Vrstici (3) in (5) sta dobljeni iz prejšnjih vrtic po pravilu (MP). Vrstica (6) pa je dobljena z uporabo izreka o dedukciji iz (5). Če uporabimo izrek o dedukciji še dvakrat, dobimo našo trditev. Izpeljano pravilo, ki ga določa vrstica (6), bomo kasneje večkrat uporabili.

Primer 2. Zaporedje formul $\mathscr{A}, \mathscr{A} \Rightarrow \mathscr{B}, \mathscr{B}$ je dedukcija formule $\mathscr{B}$ iz formul $\mathscr{A}, \mathscr{A} \Rightarrow \mathscr{B}$. To bomo predstavili v stolpcu

(1) $\mathscr{A}, \mathscr{A} \Rightarrow \mathscr{B} \vdash \mathscr{A}$
(2) $\mathscr{A}, \mathscr{A} \Rightarrow \mathscr{B} \vdash \mathscr{A} \Rightarrow \mathscr{B}$
(3) $\mathscr{A}, \mathscr{A} \Rightarrow \mathscr{B} \vdash \mathscr{B}$

Dokaz izreka o dedukciji nam omogoča, da to dedukcijo spremenimo v dedukcijo formule $(\mathscr{A} \Rightarrow \mathscr{B}) \Rightarrow \mathscr{B}$ iz hipoteze $\mathscr{A}$. Glede na dokaz izreka o dedukciji moramo konstruirati dedukcijo $\mathscr{A} \vdash (\mathscr{A} \Rightarrow \mathscr{B}) \Rightarrow \mathscr{A}$. To je primer 1a dokaza izreka o dedukciji:

$\mathscr{A} \vdash \mathscr{A}$
$\mathscr{A} \vdash \mathscr{A} \Rightarrow ((\mathscr{A} \Rightarrow \mathscr{B}) \Rightarrow \mathscr{A})$
$\mathscr{A} \vdash (\mathscr{A} \Rightarrow \mathscr{B}) \Rightarrow \mathscr{A}$

Imamo namreč $n = 2$; formule $\mathscr{A}_1, \mathscr{A}_2, \mathscr{B}_x$ so zaporedoma $\mathscr{A}, \mathscr{A} \Rightarrow \mathscr{B}, \mathscr{A}$.

Nato moramo dokazati

$$\mathscr{A} \vdash (\mathscr{A} \Rightarrow \mathscr{B}) \Rightarrow (\mathscr{A} \Rightarrow \mathscr{B})$$

To je primer 1b dokaza izreka o dedukciji. Uporabiti moramo dokaz leme 1.

Ostane še primer

$$\mathscr{A} \vdash (\mathscr{A} \Rightarrow \mathscr{B}) \Rightarrow \mathscr{B}$$

To je primer 3 dokaza izreka o dedukciji, kjer so formule $\mathscr{B}_i$, $\mathscr{B}_j$, in $\mathscr{B}_k$ kar zaporedoma $\mathscr{A}$, $\mathscr{A} \Rightarrow \mathscr{B}$, $\mathscr{B}$.

Če zdaj vse skupaj strnemo v zaporedje formul, dobimo dedukcijo formule $(\mathscr{A} \Rightarrow \mathscr{B}) \Rightarrow \mathscr{B}$ iz hipoteze $\mathscr{A}$:

$\mathscr{A}$, $\mathscr{A} \Rightarrow ((\mathscr{A} \Rightarrow \mathscr{B}) \Rightarrow \mathscr{A})$, $(\mathscr{A} \Rightarrow \mathscr{B}) \Rightarrow \mathscr{A}$, $((\mathscr{A} \Rightarrow \mathscr{B}) \Rightarrow (((\mathscr{A} \Rightarrow \mathscr{B}) \Rightarrow (\mathscr{A} \Rightarrow \mathscr{B})) \Rightarrow (\mathscr{A} \Rightarrow \mathscr{B})))$ $\Rightarrow (((\mathscr{A} \Rightarrow \mathscr{B}) \Rightarrow ((\mathscr{A} \Rightarrow \mathscr{B}) \Rightarrow (\mathscr{A} \Rightarrow \mathscr{B}))) \Rightarrow ((\mathscr{A} \Rightarrow \mathscr{B}) \Rightarrow (\mathscr{A} \Rightarrow \mathscr{B})))$,
$(\mathscr{A} \Rightarrow \mathscr{B}) \Rightarrow (((\mathscr{A} \Rightarrow \mathscr{B}) \Rightarrow (\mathscr{A} \Rightarrow \mathscr{B})) \Rightarrow (\mathscr{A} \Rightarrow \mathscr{B}))$,
$((\mathscr{A} \Rightarrow \mathscr{B}) \Rightarrow ((\mathscr{A} \Rightarrow \mathscr{B}) \Rightarrow (\mathscr{A} \Rightarrow \mathscr{B}))) \Rightarrow ((\mathscr{A} \Rightarrow \mathscr{B}) \Rightarrow (\mathscr{A} \Rightarrow \mathscr{B}))$,
$(\mathscr{A} \Rightarrow \mathscr{B}) \Rightarrow ((\mathscr{A} \Rightarrow \mathscr{B}) \Rightarrow (\mathscr{A} \Rightarrow \mathscr{B}))$,
$(\mathscr{A} \Rightarrow \mathscr{B}) \Rightarrow (\mathscr{A} \Rightarrow \mathscr{B})$,
$((\mathscr{A} \Rightarrow \mathscr{B}) \Rightarrow (\mathscr{A} \Rightarrow \mathscr{B})) \Rightarrow (((\mathscr{A} \Rightarrow \mathscr{B}) \Rightarrow \mathscr{A}) \Rightarrow ((\mathscr{A} \Rightarrow \mathscr{B}) \Rightarrow \mathscr{B}))$,
$((\mathscr{A} \Rightarrow \mathscr{B}) \Rightarrow \mathscr{A}) \Rightarrow ((\mathscr{A} \Rightarrow \mathscr{B}) \Rightarrow \mathscr{B})$,
$(\mathscr{A} \Rightarrow \mathscr{B}) \Rightarrow \mathscr{B}$

Da je to res iskana dedukcija, se lahko prepričamo neposredno iz definicije dedukcije. Ta zgled nam je tudi pokazal, koliko se skrajša sklepanje z uporabo izvedenih pravil.

Primer 3. Velja $\mathscr{A} \Rightarrow (\mathscr{B} \Rightarrow \mathscr{C})$, $\mathscr{B} \vdash \mathscr{A} \Rightarrow \mathscr{C}$.

Dokaz. (1) $(\mathscr{A} \Rightarrow (\mathscr{B} \Rightarrow \mathscr{C})) \Rightarrow ((\mathscr{A} \Rightarrow \mathscr{B}) \Rightarrow (\mathscr{A} \Rightarrow \mathscr{C}))$
(2) $\mathscr{A} \Rightarrow (\mathscr{B} \Rightarrow \mathscr{C})$
(3) $(\mathscr{A} \Rightarrow \mathscr{B}) \Rightarrow (\mathscr{A} \Rightarrow \mathscr{C})$
(4) $\mathscr{B}$
(5) $\mathscr{B} \Rightarrow (\mathscr{A} \Rightarrow \mathscr{B})$
(6) $\mathscr{A} \Rightarrow \mathscr{B}$
(7) $\mathscr{A} \Rightarrow \mathscr{C}$

Točka (1) je aksiom (A2), v točkah (2) in (4) nastopata hipotezi, točka (5) je aksiom (A1), (6) dobimo z uporabo (MP) v (4) in (5) in točko (7) z uporabo (MP) v (3) in (6).

Primer 4. (a) $\vdash \neg\neg\mathscr{B} \Rightarrow \mathscr{B}$
(b) $\vdash \mathscr{B} \Rightarrow \neg\neg\mathscr{B}$
(c) $\vdash (\neg\mathscr{B} \Rightarrow \neg\mathscr{A}) \Rightarrow (\mathscr{A} \Rightarrow \mathscr{B})$
(d) $\vdash (\mathscr{A} \Rightarrow \mathscr{B}) \Rightarrow (\neg\mathscr{B} \Rightarrow \neg\mathscr{A})$

Dokaz.

(a) (1) $(\neg\mathscr{B} \Rightarrow \neg\neg\mathscr{B}) \Rightarrow ((\neg\mathscr{B} \Rightarrow \neg\mathscr{B}) \Rightarrow \mathscr{B})$
(aksiom po (A4))

(2) $\neg \mathscr{B} \Rightarrow \neg \mathscr{B}$ (lema 1)
(3) $(\neg \mathscr{B} \Rightarrow \neg \neg \mathscr{B}) \Rightarrow \mathscr{B}$ (iz (1) in (2) po primeru 3)
(4) $\neg \neg \mathscr{B} \Rightarrow (\neg \mathscr{B} \Rightarrow \neg \neg \mathscr{B})$ (aksiom (A1))
(5) $\neg \neg \mathscr{B} \Rightarrow \mathscr{B}$ (primer 1 iz (3) in (4))

(b) (1) $(\neg \neg \neg \mathscr{B} \Rightarrow \neg \mathscr{B}) \Rightarrow ((\neg \neg \neg \mathscr{B} \Rightarrow \mathscr{B}) \Rightarrow \neg \neg \mathscr{B})$
(aksiom (A4))
(2) $\neg \neg \neg \mathscr{B} \Rightarrow \neg \mathscr{B}$ (točka (a) tega primera)
(3) $((\neg \neg \neg \mathscr{B} \Rightarrow \mathscr{B}) \Rightarrow \neg \neg \mathscr{B})$ (iz (1) in (2) po (MP))
(4) $\mathscr{B} \Rightarrow (\neg \neg \neg \mathscr{B} \Rightarrow \mathscr{B})$ (aksiom (A1))
(5) $\mathscr{B} \Rightarrow \neg \neg \mathscr{B}$ (iz (3) in (4) po primeru 1)

(c) (1) $\neg \mathscr{B} \Rightarrow \neg \mathscr{A}$ (hipoteza)
(2) $\mathscr{A}$ (hipoteza)
(3) $(\neg \mathscr{B} \Rightarrow \neg \mathscr{A}) \Rightarrow ((\neg \mathscr{B} \Rightarrow \mathscr{A}) \Rightarrow \mathscr{B})$ (aksiom po (A4))
(4) $\mathscr{A} \Rightarrow (\neg \mathscr{B} \Rightarrow \mathscr{A})$ (aksiom po (A1))
(5) $(\neg \mathscr{B} \Rightarrow \mathscr{A}) \Rightarrow \mathscr{B}$ (iz (1) in (3) po (MP))
(6) $\mathscr{A} \Rightarrow \mathscr{B}$ (iz (4) in (5) po primeru 1)
(7) $\mathscr{B}$ (iz (2) in (6) po (MP))

Iskani rezultat dobimo z dvakratno uporabo izreka o dedukciji.

(d) (1) $\mathscr{A} \Rightarrow \mathscr{B}$ (hipoteza)
(2) $\neg \neg \mathscr{A} \Rightarrow \mathscr{A}$ (točka (a) primera 4)
(3) $\neg \neg \mathscr{A} \Rightarrow \mathscr{B}$ (primer 1)
(4) $\mathscr{B} \Rightarrow \neg \neg \mathscr{B}$ (točka (b))
(5) $\neg \neg \mathscr{A} \Rightarrow \neg \neg \mathscr{B}$ (iz (3) in (4) po primeru 1)
(6) $(\neg \neg \mathscr{A} \Rightarrow \neg \neg \mathscr{B}) \Rightarrow (\neg \mathscr{B} \Rightarrow \neg \mathscr{A})$ (točka (c))
(7) $\neg \mathscr{B} \Rightarrow \neg \mathscr{A}$ (iz (5) in (6) po (MP))

Nato uporabimo izrek o dedukciji.

Primer 5. Razpravljanje bomo končali z dokazom trditve

$$\vdash (\exists y)(\forall x)\mathscr{A} \Rightarrow (\forall x)(\exists y)\mathscr{A}$$

v predikatnem računu. Spomnimo se, da smo eksistenčni kvantifikator uvedli v [1] z definicijo

$$(\exists x)\mathscr{A} \text{ je okrajšava za } \neg (\forall x) \neg \mathscr{A}$$

Obrat zgornje formule, namreč formula

$$(\forall x)(\exists y)\mathscr{A} \Rightarrow (\exists y)(\forall x)\mathscr{A}$$

ni logično veljavna. Vzemimo interpretacijo, katere domena je množica naravnih števil, formula $\mathscr{A}$ pa naj pomeni, da je število y večje od števila x. Potem je leva stran implikacije pravilna:

k vsakemu naravnemu številu obstaja večje število; desna stran pa je nepravilna: obstaja naravno število, ki je večje od vseh.

Svojo trditev bomo izpeljali iz naslednjih trditev:

(1) $\vdash \mathscr{A} \Rightarrow (\exists y)\mathscr{A}$
(2) $\vdash (\forall x)(\mathscr{A} \Rightarrow \mathscr{B}) \Rightarrow ((\forall x)\mathscr{A} \Rightarrow (\forall x)\mathscr{B})$
(3) $\vdash (\forall x)(\mathscr{A} \Rightarrow \mathscr{B}) \Rightarrow ((\exists x)\mathscr{A} \Rightarrow \mathscr{B})$

pri čemer v (3) x ne nastopa prosto v $\mathscr{B}$.

Predpostavimo, da smo trditve (1), (2) in (3) že dokazali. Potem z generalizacijo iz (1) dobimo

(4) $(\forall x)\,(\mathscr{A} \Rightarrow (\exists y)\,\mathscr{A})$

Če zdaj v (2) pišemo $(\exists y)\,\mathscr{A}$ namesto $\mathscr{B}$, potem s pravilom (MP) iz (2) in (4) dobimo

(5) $(\forall x)\,\mathscr{A} \Rightarrow (\forall x)\,(\exists y)\,\mathscr{A}$

iz tega pa z generalizacijo

(6) $(\forall y)\,((\forall x)\,\mathscr{A} \Rightarrow (\forall x)\,(\exists y)\,\mathscr{A})$

Če v (3) pišemo y, $(\forall x)\,\mathscr{A}$, $(\forall x)\,(\exists y)\,\mathscr{A}$ namesto x, $\mathscr{A}$, $\mathscr{B}$ in uporabimo pravilo (MP) na (3) in (6), dobimo

$$(\exists y)\,(\forall x)\,\mathscr{A} \Rightarrow (\forall x)\,(\exists y)\,\mathscr{A}$$

Preostane nam torej samo še, da dokažemo točke (1), (2) in (3). Preden se lotimo dokaza, moramo izpeljati še pravilo *reductio ad absurdum*:

iz $\Gamma, \neg\mathscr{B} \vdash \neg\mathscr{A}$ in $\Gamma, \neg\mathscr{B} \vdash \mathscr{A}$ sledi $\Gamma \vdash \mathscr{B}$, kjer je Γ neka končna množica formul in v teh izpeljavah ne uporabljamo generalizacije na spremenljivke, ki so proste v $\mathscr{B}$.

Če uporabimo izrek o dedukciji na hipotezi, dobimo $\Gamma \vdash \neg\mathscr{B} \Rightarrow \neg\mathscr{A}$ in $\Gamma \vdash \neg\mathscr{B} \Rightarrow \mathscr{A}$. Od tod z dvakratno uporabo pravila (MP) in aksioma (A4)

$$(\neg\mathscr{B} \Rightarrow \neg\mathscr{A}) \Rightarrow ((\neg\mathscr{B} \Rightarrow \mathscr{A}) \Rightarrow \mathscr{B})$$

dobimo $\Gamma \vdash \mathscr{B}$.

Dokaz točke (1):

(i) $(\forall y)\,\neg\mathscr{A} \Rightarrow \neg\mathscr{A}$	(aksiom (A5), vzamemo $S_y^y\,\neg\mathscr{A}\,\vert$, ki je $\neg\mathscr{A}$)
(ii) $\neg\neg\mathscr{A} \Rightarrow \neg\,(\forall y)\,\neg\mathscr{A}$	(iz (i) po točki (d) primera 4)
(iii) $\mathscr{A} \Rightarrow \neg\neg\mathscr{A}$	(točka (b) primera 4)
(iv) $\mathscr{A} \Rightarrow (\exists y)\,\mathscr{A}$	(dobimo iz (ii) in (iii) po primeru 1 in uporabimo definicijo za $\exists$).

Dokaz točke (2) sledi iz pravilnosti naslednjih vrstic:

$(\forall x)\,(\mathscr{A} \Rightarrow \mathscr{B}),\ (\forall x)\,\mathscr{A} \vdash \mathscr{A} \Rightarrow \mathscr{B}$	(uporabimo aksiom (A5) in (MP), $S_x^x(\mathscr{A} \Rightarrow \mathscr{B})\,\vert$ je kar $\mathscr{A} \Rightarrow \mathscr{B}$)
$(\forall x)\,(\mathscr{A} \Rightarrow \mathscr{B}),\ (\forall x)\,\mathscr{A} \vdash \mathscr{A}$	(uporabimo (A5) in (MP), $S_x^x\mathscr{A}\,\vert$ je $\mathscr{A}$)
$(\forall x)\,(\mathscr{A} \Rightarrow \mathscr{B}),\ (\forall x)\,\mathscr{A} \vdash \mathscr{B}$	(iz prejšnjih vrstic po (MP))
$(\forall x)\,(\mathscr{A} \Rightarrow \mathscr{B}),\ (\forall x)\,\mathscr{A} \vdash (\forall x)\,\mathscr{B}$	(z generalizacijo iz prejšnje vrstice).

Trditev (2) dobimo nato z dvakratno uporabo izreka o dedukciji.

Dokaz točke (3):

$(\forall x)\,(\mathscr{A} \Rightarrow \mathscr{B}),\ (\exists x)\,\mathscr{A},\ \neg\mathscr{B} \vdash \mathscr{A} \Rightarrow \mathscr{B}$	(tako kot v prvi vrstici dokaza točke (2))
$(\forall x)\,(\mathscr{A} \Rightarrow \mathscr{B}),\ (\exists x)\,\mathscr{A},\ \neg\mathscr{B} \vdash \neg\mathscr{B}$	(definicija dedukcije: (DH1))
$(\forall x)\,(\mathscr{A} \Rightarrow \mathscr{B}),\ (\exists x)\,\mathscr{A},\ \neg\mathscr{B} \vdash \neg\mathscr{A}$	(posledica točke (d) primera 4)
$(\forall x)\,(\mathscr{A} \Rightarrow \mathscr{B}),\ (\exists x)\,\mathscr{A},\ \neg\mathscr{B} \vdash (\forall x)\,\neg\mathscr{A}$	(z generalizacijo iz prejšnje vrstice)
$(\forall x)\,(\mathscr{A} \Rightarrow \mathscr{B}),\ (\exists x)\,\mathscr{A},\ \neg\mathscr{B} \vdash \neg\,(\forall x)\,\neg\mathscr{A}$	(definicija dedukcije (DH1) in definicija za $\exists$)
$(\forall x)\,(\mathscr{A} \Rightarrow \mathscr{B}),\ (\exists x)\,\mathscr{A} \vdash \mathscr{B}$	(reductio ad absurdum).

Izid dobimo, ko uporabimo izrek o dedukciji.

LITERATURA

[1] Niko Prijatelj, *Formalna izgradnja logičnega jezika*, Obzornik mat. fiz., **25** (1978) 20—33.

Obzornik mat. fiz. 25 (1978) 1

IZRAČUNLJIVOST IN REŠLJIVOST

TOMAŽ PISANSKI

AMS Subj. Class. (1970) 02—01, 02F15

V članku vpeljemo pojem izračunljivosti s Turingovimi stroji. Omenjen je tudi problem ustavitve.

COMPUTABILITY AND SOLVABILITY

In this paper the notion of the computability is introduced via Turing machines. The halting problem is mentioned.

Uvod

Matematiki rešujejo probleme. Za mnoge probleme so našli obrazce ali pa točno določene postopke, algoritme, v katere je potrebno vstaviti le ustrezne podatke, potem pa reševanje lahko poteka popolnoma avtomatizirano. Reševanje problema po točno določenih navodilih je seveda za matematika nezanimivo, je pa kot nalašč za računalnike. Za matematika je problem rešen, ko pozna obrazec ali postopek za reševanje. Bolj ko je obrazec splošen, več problemov lahko z njim rešimo. Ko so števila pisali še z rimskimi številkami, je množenje malo večjih števil zahtevalo dosti spretnosti in iznajdljivosti, danes pa je to popolnoma rutinska operacija. Skoraj vsakdo zna zmnožiti večmestni števili, pa čeprav ju vidi prvič v življenju. To pomeni, da pozna *postopek,* ki mu omogoča, da načelno lahko zmnoži poljubni števili. Ko spoznamo obrazec za reševanje kvadratne enačbe, lahko tako reševanje prevedemo na osnovne računske operacije. Tudi to postane rutina. Bolj ko se je večalo matematično znanje, več problemov se je prevedlo na rutinske operacije. Cela področja matematike je uspelo prevesti na druga. Tako je na primer Descartes reduciral geometrijo na algebro. Zato sta se pojavili dve vprašanji:

Ali obstaja splošni algoritem, ki bi mu kot podatek zastavili poljuben matematični problem, za rezultat pa bi dobili rešitev problema. Seveda bi naj bil ta »univerzalni algoritem« tak, da bi ga v načelu lahko realizirali z mehansko napravo.

Ali se da vsak matematični problem rešiti algoritmično? Negativni odgovor na drugo vprašanje pomeni hkrati tudi negativnega za prvo vprašanje. Ta prispevek želi prikazati nekaj argumentov, zaradi katerih danes matematiki mislijo, da je odgovor na drugo vprašanje: **ne.**

Števnost

Najprej bomo razširili pojem funkcije. Običajno definiramo funkcijo f, $f: A \to B$ kot predpis, ki *vsakemu* elementu x množice A priredi točno določen element $y = f(x)$ množice B. Element y je *slika originala* x. Množica $\mathscr{D}f = A$ je *domena* ali *definicijsko območje* funkcije f, $\mathscr{R}f = \{y \in B \mid \exists x \in A, y = f(x)\}$ pa je *zaloga vrednosti* funkcije f. V splošnem je $\mathscr{R}f \subseteq B$. Če je $\mathscr{R}f = B$, je funkcija *surjektivna*. Funkcija, ki različnim originalom priredi različni sliki, je *injektivna*. Če je f hkrati surjektivna in injektivna, je *bijektivna*. Množici, med katerima obstaja bijektivna preslikava, sta *enako močni* (imata enako »število« elementov).

Posplošitev funkcije, ki jo predlagamo, je preprosta. Dovolili bomo, da f priredi le *nekaterim* elementom množice A vrednosti iz B, pri drugih elementih pa je lahko *nedefinirana*. Z drugimi besedami: množica originalov $\mathscr{D}f$ je lahko podmnožica množice A. Funkcije v

običajnem smislu preimenujemo v *totalne* funkcije. Če je $\mathscr{D}f$ prava podmnožica množice A, je *f parcialna* funkcija. Odslej bo za nas beseda funkcija pomenila totalno in parcialno funkcijo.

Velik del našega razmišljanja se bo sukal okoli množice *naravnih števil* $\mathscr{N} = \{1, 2, 3, 4, \ldots\}$ Z njo definiramo pojem števne množice. Lahko bi rekli: Množica S je *števna*, če je enako močna kot kakšna podmnožica množice naravnih števil $\mathscr{N}$. Kako torej po tej definiciji ugotovimo, da je S števna? Izberemo podmnožico M množice naravnih števil. Izberemo bijektivno (totalno) funkcijo g, $g: M \to S$. Z drugimi besedami: množica S je števna, če obstaja bijekcija $g: M \to S$ in je $M \subseteq \mathscr{N}$. Seveda lahko g gledamo kot parcialno surjektivno funkcijo $g': \mathscr{N} \to S$, ki je na svojem definicijskem območju $\mathscr{D}g' = M$ injektivna in je povsod, kjer je definirana, enaka g.

Poskusimo z drugo definicijo števnosti, ki eksplicitno omenja funkcijo, ki števnost zagotavlja:

Množica S je *števna*, če obstaja surjektivna (totalna ali parcialna) funkcija f, $f: \mathscr{N} \to S$. f imenujemo v tem primeru *enumeracija* množice S.

g' je enumeracija množice S. Zato je vsaka množica, števna po prvi definiciji, števna tudi po drugi. Pokazati moramo, da druga definicija ne daje nobenih »novih« števnih množic. Za vsako enumeracijo f, $f: \mathscr{N} \to S$ lahko definiramo funkcijo f' takole:

$$f'(n) = \begin{cases} f(n) \text{ — če je za vsa naravna števila } m,\ m < n \Rightarrow f(m) \neq f(n) \\ \text{nedefinirana — v vseh drugih primerih} \end{cases}$$

f' je enumeracija množice S, ki je na $\mathscr{D}f'$ injektivna. Zato je f', če jo gledamo kot funkcijo $f': \mathscr{D}f' \to S$, bijektivna in je S enako močna kot $\mathscr{D}f' \subseteq \mathscr{N}$. S je števna tudi po prvi definiciji.

Naštejmo nekaj lastnosti števnih množic, ki jih lahko bralec sam preveri:

1. Vsaka podmnožica števne množice je števna.

2. Vsaka števna množica je bodisi končna bodisi po moči enaka množici naravnih števil.

3. Za vsako števno množico obstaja enumeracija $e: \mathscr{N} \to S$ z lastnostjo: če $e(n)$ ni definirana za neko naravno število n, potem $e(m)$ ni definirana za nobeno naravno število m, večje od n. Z drugimi besedami: Če je S neskončna, potem je e (totalna) bijekcija, če pa je S končna množica z n elementi, je e definirana za vsa naravna števila, manjša od $n + 1$, in je nedefinirana za $n + 1$, $n + 2$, $n + 3$, ...

4. Vsaka končna množica je števna.

Enumerirati množico v bistvu pomeni razvrstiti vse njene elemente v zaporedje. Če v tem zaporedju v korakih pregledujemo člene od prvega naprej, naletimo na poljuben element množice po končno mnogo korakih.

Zgled 1: Enumeracija množice naravnih števil. Identiteta, definirana za vsako naravno število n: $i(n) = n$, je običajna enumeracija naravnih števil.

Definirajmo funkcijo f takole:

$$f(n) = \begin{cases} n - 1 \text{ — če je } n \text{ sodo število} \\ n + 1 \text{ — če je } n \text{ liho število} \end{cases}$$

Za lažjo predstavo si oglejmo razpredelnico:

n	1	2	3	4	5	6	...
$f(n)$	2	1	4	3	6	5	...

Tudi f je enumeracija množice naravnih števil.

Pokazali bomo še eno enumeracijo naravnih števil. Začnimo s popolnimi kvadrati: 1, 4, 9, 16, 25, 36, 49, 64, 81, ... Vsako naravno število je bodisi popoln kvadrat ali pa leži med dvema popolnima kvadratoma. Funkcijo s definiramo takole: $s(n) = m$, če je $(m-1)^2 < n \leq m^2$. S tem je m pri vsakem n enolično določen. Ker je $s(n^2) = n$, je $\mathscr{R}s = \mathscr{N}$. Tudi s je enumeracija naravnih števil.

n	1	2	3	4	5	6	...
$s(n)$	1	2	2	2	3	3	...

Naslednja funkcija p je za razliko od enumeracij i, f in s parcialna.

$$p(n) = \begin{cases} n/2 & \text{— če je } n \text{ sodo število} \\ \text{nedefiniran} & \text{— v vseh drugih primerih} \end{cases}$$

n	1	2	3	4	5	6	7	...
$p(n)$	-	1	-	2	-	3	-	...

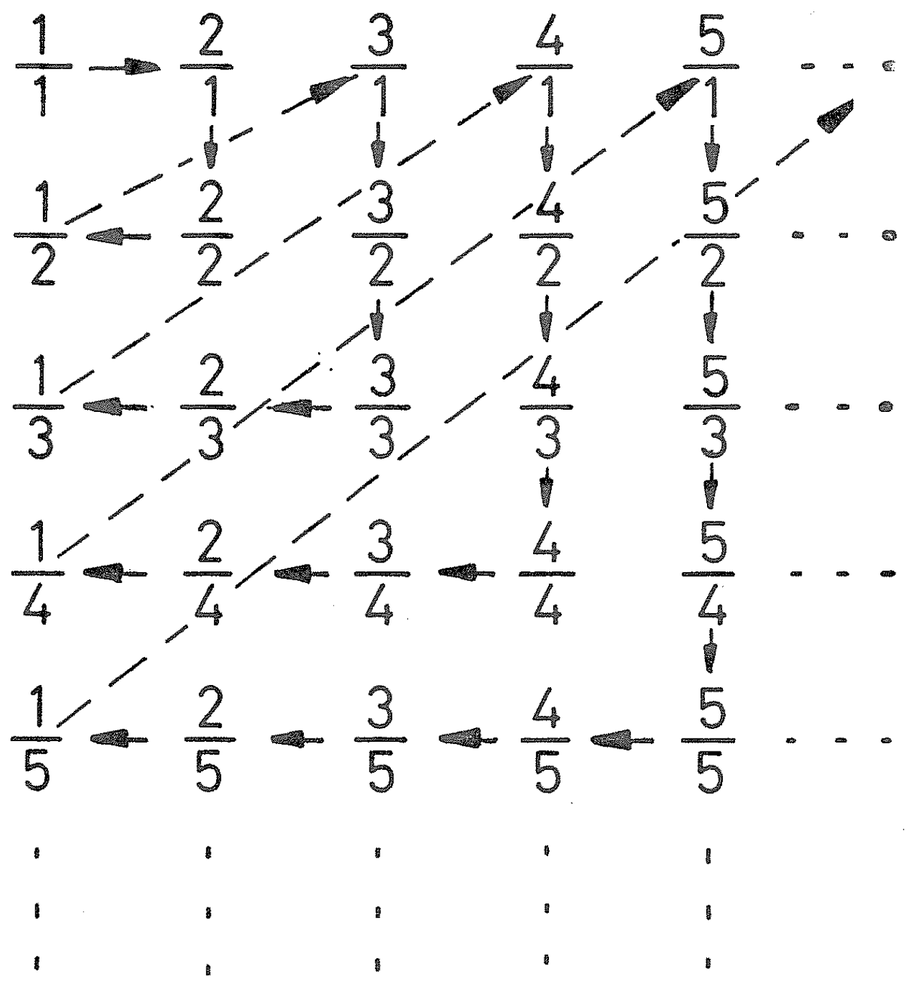
Spet je $\mathscr{R}p = \mathscr{N}$ in je p enumeracija množice $\mathscr{N}$.

Zgled 2: Čeprav najbrž vsi vemo, da je množica celih števil $\mathscr{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$ števna, si oglejmo njeno enumeracijo:

$$f(n) = \begin{cases} -(n-1)/2 & \text{— če je } n \text{ liho število} \\ n/2 & \text{— če je } n \text{ sodo število} \end{cases}$$

n	1	2	3	4	5	6	7	8	...
$f(n)$	0	1	-1	2	-2	3	-3	4	...

Zgled 3: Množica pozitivnih racionalnih števil je števna. Pozitivna racionalna števila so ravno tista realna števila, ki se dajo zapisati kot ulomek dveh naravnih števil. V naslednji razpredelnici so razvrščeni vsi ulomki:



Vzemimo poljubno racionalno pozitivno število. Po definiciji ga lahko zapišemo v obliki $r = m/n$, kjer sta m in n naravni števili. r gotovo nastopa v razpredelnici. Najdemo ga na presečišču m-tega stolpca z n-to vrstico. Pojavlja pa se celo na neskončno mnogo mestih razpredelnice, saj je $m/n = (2m)/(2n) = (3m)/(3n) = \ldots = r$. Zato bomo z enumeracijo elementov razpredelnice enumerirali tudi vsa pozitivna racionalna števila. Če začnemo

z ulomkom 1/1 in sledimo puščicam v tabeli, dobimo enumeracijo f: $f(1) = 1/1$, $f(2) = 2/1$, $f(3) = 2/2$, $f(4) = 1/2$, $f(5) = 3/1$, ... Vsakdo se lahko prepriča, da imamo v mislih ravno funkcijo:

$$f(n) = \begin{cases} s(n)/(n - (s(n) - 1)^2) & \text{— če je } s(n) \geq n - (s(n) - 1)^2 \\ ((s(n))^2 + 1 - n)/s(n) & \text{— v vseh drugih primerih} \end{cases}$$

Pri tem smo uporabili funkcijo s iz zgleda 1.

Zgled 4: Množica besed nad števno neskončno abecedo je števna. Naj bo A množica števno neskončno mnogo *simbolov*:

$$A = \{a_1, a_2, a_3, \ldots\}$$

Pravimo, da je A *abeceda*. Končna zaporedja simbolov so *besede*. Sestavimo množico A^* vseh besed nad abecedo A (vseh končnih nizov simbolov iz A). Trdimo, da je A^* števna množica.

Besede iz A^* bomo razvrstili v zaporedje. Najprej množico A^* razbijemo v razrede $A_1, A_2, \ldots, A_k, \ldots$ tako, da so v razredu A_k ravno vse besede oblike $a_{k_1}, a_{k_2}, \ldots a_{k_p}$, za katere velja: $k_1 + k_2 + \ldots + k_p = k$. V A_k sodijo tiste besede, katerih vsota indeksov simbolov je k. Tako je na primer:

$$A_3 = \{a_1a_1a_1, a_1a_2, a_2a_1, a_3\}$$

Vsak razred (množica) A_k je končen. Vse besede v A_κ so namreč dolge največ k simbolov. Nobena beseda iz A_k pa ne vsebuje simbola a_n, ki bi imel indeks n večji od k. Ker je množica vseh besed z največ k simboli, izbranimi iz množice $\{a_1, a_2, \ldots, a_k\}$, končna, je tudi množica A_k končna.

Izbrati moramo še vrstni red besed znotraj razreda A_k. Takole primerjamo besedi z isto vsoto indeksov simbolov: Pregledujemo simbol za simbolom od leve proti desni hkrati v obeh besedah. Ko prvič naletimo na različna simbola, izberemo tisto besedo, pri kateri ima simbol *manjši* indeks. V zaporedju jo postavimo *pred* drugo besedo. To nam zdaj omogoča primerjati poljubni besedi iz A^*. Beseda $a_{k_1}a_{k_2} \ldots a_{k_p}$ stoji v zaporedju, ki ga gradimo *pred* besedo $a_{j_1}a_{j_2} \ldots a_{j_q}$, če je vsota $k_1 + k_2 + \ldots + k_p$ manjša od vsote $j_1 + j_2 + \ldots + j_q$ (besedi sta v različnih razredih), če pa sta vsoti enaki, pa tedaj, ko obstaja tak i, da je:

$$a_{k_1} = a_{j_1}, \quad a_{k_2} = a_{j_2}, \ldots, a_{ki-1} = a_{ji-1} \quad \text{in} \quad a_{ki} < a_{ji}$$

V množico A^* smo vpeljali *leksikografski red*, ki določa tole enumeracijo:

1	2	3	4	5	6	7	8	9	...
a_1	a_1a_1	a_2	$a_1a_1a_1$	a_1a_2	a_2a_1	a_3	$a_1a_1a_1a_1$	$a_1a_1a_2$	...
A_1	A_2		A_3				A_4		

Oglejmo si še eno enumeracijo, ki je dosti bolj »potratna«, je pa mogoče lažje razumljiva. Najprej vsakemu simbolu iz A priredimo enolično naravno število:

a_1	a_2	a_3	a_4	a_5	...
12	122	1222	12222	122222	...

Simbolu a_n torej pripada naravno število x_n, ki se v desetiškem zapisu zapiše z enico, ki ji sledi n dvojk.

Enumeracijo $f: \mathcal{N} \to A^*$ definiramo takole:

$$f(n) = \begin{cases} a_{k_1}a_{k_2} \ldots a_{k_p} & \text{— če je } n \text{ v desetiškem sistemu oblike } x_{k_1}x_{k_2} \ldots x_{k_p} \\ \text{nedefiniran} & \text{— v vseh drugih primerih} \end{cases}$$

Funkcija f je definirana le za tista naravna števila, ki se v desetiškem zapisu zapišejo s samimi enicami in dvojkami, se začenjajo z enico in za vsako enico stoji vsaj ena dvojka. Pri takih n je razcep na x—e enoličen. f je parcialna funkcija in velja $\mathscr{R}f = A^*$, torej je res enumeracija.

n	1	2	...	11	12	13	...	122	...	1212	...
$f(n)$	—	—	...	—	a_1	—	...	a_2	...	a_1a_1	...

Diagonalizacija

Zgled 3 bi lahko uporabili za vzorec dokaza tegale dejstva: Števna unija števnih množic je števna množica.

Nepoučeni bi najbrž verjel, da so kar vse množice števne. Vendar ni tako. O tem se je prvi prepričal že Georg Cantor, oče teorije množic in kardinalne aritmetike. Pri dokazu, da množica realnih števil *ni* števna, je uporabil izredno duhovito in, kot se je pozneje izkazalo, plodno metodo. Imenovali jo bomo *diagonalizacija*.

Začnemo z značilno shemo (končno ali neskončno) oblike:

$$\begin{array}{|c|cccc} \hline a_{11} & a_{12} & a_{13} & \dots & a_{1n} & \dots \\ \hline a_{21} & \multicolumn{1}{|c|}{a_{22}} & a_{23} & \dots & a_{2n} & \dots \\ \cline{2-2} a_{31} & a_{32} & \multicolumn{1}{|c|}{a_{33}} & \dots & a_{3n} & \dots \\ \cline{3-3} \vdots & \vdots & \vdots & & \vdots & \\ & & & & \multicolumn{1}{|c|}{a_{nn}} & \\ a_{n1} & a_{n2} & a_{n3} & \dots & \cline{5-5} \dots & \dots \\ \vdots & \vdots & \vdots & & \vdots & \end{array}$$

Kaj so elementi sheme, niti ni važno. Če je shema končna, naj bo kvadratna. Zanimajo nas vrstice. Shemo lahko tolmačimo kot zaporedje vrstic. Iz diagonalnih elementov sheme, torej iz elementov oblike a_{nn}, lahko sestavimo *diagonalno vrstico*:

$$a_{11} \quad a_{22} \quad a_{33} \quad \dots \quad a_{nn} \quad \dots$$

Če primerjamo diagonalno vrstico z vrsticami sheme, se lahko zgodi, da je diagonalna vrstica različna od vseh vrstic sheme, lahko pa je tudi enaka kakšni vrstici sheme. Pri tem sta dve vrstici enaki, če je prvi element prve enak prvemu elementu druge, drugi element prve enak drugemu elementu druge, ... n-ti element prve enak n-temu elementu druge, ...

Zdaj pa bomo sestavili vrstico, ki je *čisto zagotovo ni* med vrsticami sheme. Vrstica:

$$b_1 \quad b_2 \quad b_3 \quad \dots \quad b_n \quad \dots$$

naj ima tole lastnost: $b_1 \neq a_{11}$, $b_2 \neq a_{22}$, ..., $b_n \neq a_{nn}$, ... Drugače povedano, vrstica naj se na nobenem mestu ne ujema z diagonalno vrstico. Taki vrstici rečemo *antidiagonalna vrstica*.

Trdimo, da antidiagonalna vrstica ni enaka *nobeni* vrstici sheme. No, pa denimo, da bi bilo narobe res. Denimo, da je antidiagonalna vrstica enaka neki, recimo m-ti vrstici sheme. Torej je: $b_1 = a_{m1}$, $b_2 = a_{m2}$, ..., $b_m = a_{mm}$, ... Protislovje je tu! Po definiciji je $b_n \neq a_{nn}$ za vsak n. Zato je tudi $b_m \neq a_{mm}$. Po drugi strani pa bi moralo veljati $b_m = a_{mm}$. Pokazali smo, da antidiagonalne vrstice ni med vrsticami sheme. Uporabo metode bomo prikazali na zgledih.

Zgled 5: Množica $\mathscr{P}(\mathscr{N})$ vseh podmnožic množice naravnih števil $\mathscr{N}$ ni števna.

Denimo, da je $\mathscr{P}(\mathscr{N})$ števna. Potem bi obstajala surjekcija $f: \mathscr{N} \to \mathscr{P}(\mathscr{N})$. Naj bo $f(n) = S_n \in \mathscr{P}(\mathscr{N})$. Ker je $S_n \subseteq \mathscr{N}$, lahko definiramo funkcijo:

$s_n : \mathcal{N} \to \{0, 1\}$ takole:

$$s_n(m) = \begin{cases} 1 & \text{— če je } m \in S_n \\ 0 & \text{— v vseh drugih primerih} \end{cases}$$

Mimogrede, s_n je *karakteristična* funkcija množice S_n. Vsaka totalna funkcija iz $\mathcal{N}$ v $\{0, 1\}$ je karakteristična funkcija neke podmnožice naravnih števil. Podmnožica sama pa je s karakteristično funkcijo enolično določena. Je namreč sestavljena iz vseh tistih naravnih števil, pri katerih je vrednost karakteristične funkcije enaka 1.

Sestavimo shemo:

$$\begin{array}{cccccc} s_1(1) & s_1(2) & \dots & s_1(n) & \dots \\ s_2(1) & s_2(2) & \dots & s_2(n) & \dots \\ \vdots & \vdots & & \vdots & \\ s_n(1) & s_n(2) & \dots & s_n(n) & \dots \\ \vdots & \vdots & & \vdots & \end{array}$$

n-ta vrstica določa ravno $f(n)$. Postavimo $a(n) = 1 - s_n(n)$. Tako smo definirali antidiagonalno funkcijo $a : \mathcal{N} \to \{0, 1\}$, za katero vemo, da ni enaka nobeni funkciji s_n. Zato je tudi množica A, ki jo določa, različna od vseh S_n. A torej ni slika nobenega naravnega števila glede na f, kar je v protislovju z domnevo na začetku. Bralec lahko za vajo poskusi trditev dokazati neposredno, brez karakterističnih funkcij.

Zgled 6: Množica funkcij oblike $f : \mathcal{N} \to \mathcal{N}$ ni števna. Denimo, da bi nam uspelo vse take funkcije razvrstiti v zaporedje $f_1, f_2, \dots, f_n, \dots$ Definirajmo totalno funkcijo $a : \mathcal{N} \to \mathcal{N}$ takole:

$$a(n) = \begin{cases} f_n(n) + 1 & \text{— če je } f_n(n) \text{ definiran} \\ 1 & \text{— v vseh drugih primerih} \end{cases}$$

a je antidiagonalna funkcija, saj ne more biti $a(m) = f_m(m)$ za noben m. Trditev je dokazana.

Do tega sklepa bi lahko prišli že z ugotovitvijo zgleda 5. Funkciji z različnima domenama sta gotovo različni. Ker je vsaka podmnožica množice naravnih števil domena kakšne funkcije, je funkcij vsaj toliko, kot je elementov v $\mathcal{P}(\mathcal{N})$, torej neštevno. Pa tudi če se omejimo na totalne funkcije oblike $f : \mathcal{N} \to \mathcal{N}$, lahko pokažemo, da sestavljajo neštevno množico. Kot argument za to trditev lahko spet uporabimo funkcijo a. Lahko pa sklepamo tako kot prej, le da namesto domen funkcij opazujemo njihove zaloge vrednosti.

Zgled 7: Množica realnih števil na intervalu [0, 1) ni števna. Približno takole je dokazoval Cantor:

Vsako realno število med 0 in 1 lahko enolično zapišemo v obliki neskončnega decimalnega ulomka:

$$\begin{array}{ll} & 0, x_1 x_2 x_3 \dots \quad x_n \quad \dots \\ \text{Na primer:} & 0, 33333 \dots 3333 \dots \\ & 0, 50000 \dots 0000 \dots \end{array}$$

Prepovemo le uporabo zaporedja samih devetk, saj je npr.

$$0{,}9245999999 \dots 9999 \dots = 0{,}92460 \dots 0000 \dots$$

Torej: vsako zaporedje cifer 0, 1, 2, ..., 9, ki se ne končuje s samimi devetkami, enolično določa realno število na intervalu [0, 1). Zaporedje $s_1\, s_2\, s_3 \dots$ določa število $0, s_1 s_2 s_3 \dots$ Če je množica takih zaporedij števna, lahko poiščemo enumeracijo, ki dajo shemo:

$$\begin{array}{l} s_{11}\ s_{12} \dots \\ s_{21}\ s_{22} \dots \\ \dots\dots\dots \end{array}$$

Število s_{ij} torej pomeni številko, ki se pri i-tem realnem številu zaporedja pojavi na j-tem mestu za decimalno vejico.

Antidiagonalno zaporedje $a_1\, a_2\, a_3 \ldots$, določeno z

$$a_n = \begin{cases} 1 \text{ — če je } s_{nn} \neq 1 \\ 0 \text{ — če je } s_{nn} = 1 \end{cases}$$

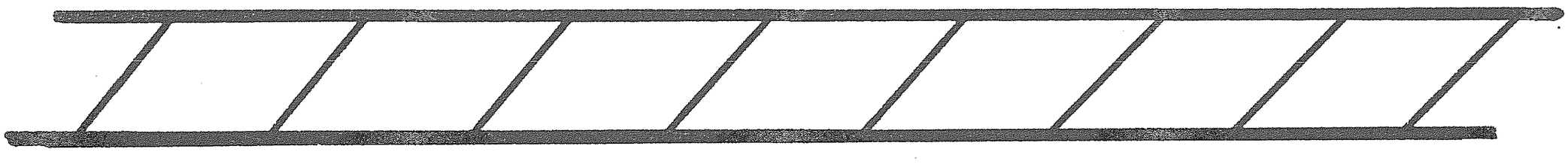
je spet istega tipa (ne vsebuje neskončnega zaporedja devetk) in prišli smo do protislovja.

Turingov stroj

Načrtali bomo napravo, nekakšen abstrakten stroj, ki je zmožen *računati* po vnaprej dogovorjenih točno določenih pravilih brez zunanjih vplivov, torej tudi brez človekove volje. Turingov stroj, tako se namreč imenuje naprava, nas od daleč spominja na računalnik. In res, Turingov stroj zmore računati vse, kar zmorejo najbolj izpopolnjeni in največji računalniki. Toda o tem več kasneje!

Turingov stroj bomo najprej intuitivno opisali, nato pa tudi »strogo« definirali. S strogostjo pa ne nameravamo oteževati intuitivne predstave, saj lahko kritični bralec zve v knjigah, npr. v [1], [2], kako je treba premostiti vrzeli, posledice naše ohlapnosti.

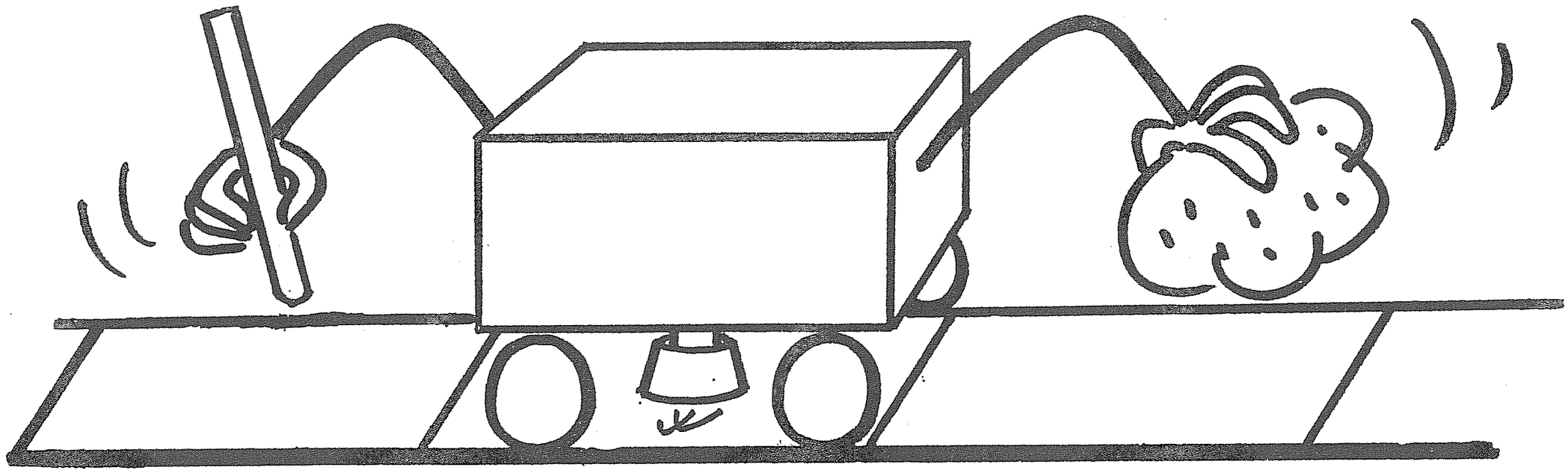
Zamislimo si voziček, ki se prevaža po traku, razdeljenem na kvadratke. *Trak* naj bo v obe smeri neomejen.



Če koga moti dejanska (aktualna) neskončnost traku, si lahko predstavlja, da je trak sicer končen, vendar stoji na vsaki strani traku robot; brž ko ta opazi, da bi voziček lahko naletel na konec traku, trak podaljša, tako da prilepi *prazen* kvadratek.

Vsak kvadrat je bodisi *prazen* bodisi je na njem zapisan eden od končno mnogo simbolov: $s_1, s_2, \ldots, s_i$. Lahko si mislimo, da je prazen kvadratek v resnici zapolnjen s posebnim, *praznim simbolom* s_0. Prazni simbol poznamo v vsakdanjem življenju kot »presledek«. Na pisalnem stroju je presledek predstavljen s posebno, podolgovato tipko. Na traku je v vsakem trenutku le končno mnogo kvadratkov popisanih. Seveda je lahko tudi ves trak prazen.

V vozičku je vgrajena posebna naprava, splet mehanizmov, ki opravlja različne funkcije. Voziček se lahko *premika* po traku. Naprava deluje v *taktih*, v diskretnih *trenutkih*. V vsakem trenutku stoji voziček nad nekim kvadratom na traku. Na spodnji strani vozička je senzor (oko, televizijska kamera, radar ali kaj podobnega), ki *pregleduje* simbol pod njim



Tako si lahko zamišljamo Turingov stroj. Stoji nad nekim kvadratom. Simbol x, ki je na njem napisan, opazuje s televizijsko kamero. Z gobo lahko x zbriše, s kredo pa namesto njega nariše nov simbol (ilustr. Borut Pečar)

in ga tudi *razpozna*. Naprava je opremljena z mehanizmom, ki lahko simbol pod vozičkom zbriše (radirka, goba) in na isto mesto napiše novega (svinčnik, kreda). Voziček se lahko v enem taktu, torej med dvema trenutkoma, premakne za en kvadratek v levo ali desno.

Stroj ima tudi *končen spomin*. Na razpolago ima končno mnogo *stanj* $q_1, q_2, \ldots, q_m$. V vsakem trenutku ve, v katerem od m stanj se nahaja. Lahko si predstavljamo, da ima stanja realizirana kot ploščico z m vdolbinami. V eni od vdolbin, recimo v i-ti, leži kroglica. To pomeni, da je stroj v tem trenutku v stanju q_i. Ob vsaki vdolbini je pripravljen paket $n + 1$ kuvert. V vsaki kuverti je listek, popisan na obeh straneh. Na listku je napisan *ukaz*.

Na prvi strani listka je napisana ena od naslednjih zahtev:

1. Ustavi se! Delo je končano.
2. Premakni se za kvadratek v levo!
3. Premakni se za kvadratek v desno!
4. Zbriši simbol pod seboj in na njegovo mesto napiši s_1!
5. Zbriši simbol pod seboj in na njegovo mesto napiši s_2!

. . .

$n + 3$. Zbriši simbol pod seboj in na njegovo mesto napiši s_n!

$n + 4$. Zbriši simbol pod seboj (in na njegovo mesto napiši s_0)!

Na hrbtni strani pa je zapisan eden od tehle stavkov:

1. Kroglico postavi v vdolbino q_1.
2. Kroglico postavi v vdolbino q_2.

. . .

m. Kroglico postavi v vdolbino q_m.

Ker je na eni strani $n + 4$ mogočih zahtev, na drugi strani listka pa m zahtev, obstaja vsega skupaj $m(n + 4)$ različnih ukazov. Seveda so lahko vsebine različnih listkov enake!

Zdaj pa že lahko razložimo delovanje stroja. V stroju je robot, ki izvaja vse naloge. Ko stroj poženemo, začne robot ponavljati naslednja enolična dejanja:

Pogleda simbol s, ki ga senzor razpoznava. Pogleda stanje q, v katerem se trenutno nahaja, torej poišče vdolbino s kroglico. Iz kupa kuvert ob vdolbini q izbere tisto, na kateri je zapisan simbol s. Ovojnico odpre, izvleče listek, ga prebere, položi nazaj v ovojnico in ovojnico vrne na njeno mesto. Potem izvede ukaz, ki ga je na listku prebral. Izvede seveda oba dela ukaza: premakne kroglico in bodisi napiše nov simbol bodisi premakne voziček za eno mesto ali pa se ustavi.

To ponavlja dokler ne naleti na ukaz: ustavi se! Potem obmiruje. Seveda se lahko zgodi, da se stroj *nikoli* ne ustavi, da robot *nikoli* ne izvleče odrešilnega listka: ustavi se. V takem primeru dela kot Sizif v neskončnost.

Preden stroj poženemo, postavimo kroglico v vdolbino q_1. Stroj je v *začetnem stanju*. Na trak napišemo končno mnogo simbolov. Stroj postavimo nad neki kvadratek na traku in ga poženemo. To je *Turingov stroj*.

Zgled 8: Turingov stroj, ki na prazen trak napiše $s_1s_1s_1$ in se ustavi.

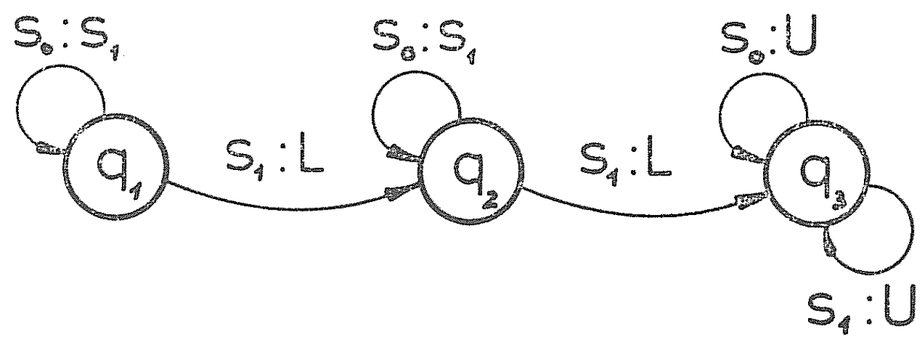
Poleg praznega simbola s_0 potrebujemo le simbol s_1. Torej, $n = 1$. Stroj bomo realizirali s tremi stanji, q_1, q_2, q_3; $m = 3$. Stroj najlažje opišemo kar z razpredelnico, v kateri so zapisane vsebine listkov.

stanje	simbol na kuverti: s_0, prvi del: napiši:	s_0, drugi del: kroglico v:	s_1, prvi del: premik v L(evo)	s_1, drugi del: kroglico v:	
q_1	s_1	q_1		q_2	
q_2	s_1	q_2		q_3	
q_3	s_1	q_3	U(stavi se)	q_3	

Če se dogovorimo, da L pomeni premik v levo, D premik v desno in U ustavi se, lahko stroj ravno tako dobro opišemo z dosti manj pisanja:

	s_0	s_1
q_1	s_1q_1	Lq_2
q_2	s_1q_2	Lq_3
q_3	s_1q_3	Uq_3

Za opazovanje delovanja Turingovega stroja je morda najprimernejši zapis v obliki grafa. Stanja predočimo kot točke grafa (krožci na sliki). Prehode iz enega stanja v drugega pa prikažemo s povezavami (puščicami). Oznaka $s : x$ ob puščici pomeni, da pride do tega prehoda, če je stroj v stanju, od koder puščica izvira, pregleduje pa simbol s. x pomeni akcijo, ki jo stroj pri prehodu izvede (zapiše simbol ali pa se premakne v levo ali desno, oziroma se ustavi).



Poleg tabelaričnega zapisa in zapisa v obliki grafa si bomo ogledali še *linearni* zapis Turingovega stroja. Če s pomeni trenutni simbol, ki ga stroj pregleduje v stanju q, x akcijo, ki jo mora pri prehodu izvesti, q' pa novo stanje, v katerem se znajde po prehodu, lahko vse skupaj zapišemo preprosto takole: $sqxq'$. Če vse mogoče prehode zapišemo v enem samem nizu, dobimo linearni zapis stroja. V našem primeru dobimo:

$$s_0q_1s_1q_1s_1q_1Lq_2s_0q_2s_1q_2s_1q_2Lq_3s_0q_3s_1q_3s_1q_3Uq_3$$

Seveda vrstni red četverk znakov (prehodov) ni pomemben. Tako bi lahko v linearnem zapisu napisali zaporedje $s_0q_1s_1q_1$ namesto na začetku tudi kje v sredini ali na koncu. Obstaja več linearnih zapisov istega Turingovega stroja.

Zdaj ko smo se dogovorili, kako bomo opisovali Turingove stroje, si poglejmo, kako naš stroj deluje. Če za stroj v nekem trenutku vemo, v katerem stanju se nahaja, kaj je v tem trenutku na traku in kje na traku je, je njegovo nadaljnje delovanje popolnoma določeno. Vsebino traku bomo zapisali kot besedo nad abecedo $s_0, s_1, \ldots, s_n$. Besedi lahko dodamo ali odvzamemo na začetku ali na koncu poljubno mnogo simbolov s_0. Beseda opisuje vsebino traku na nekem končnem odseku. Pri tem se razume, da je trak zunaj tega odseka prazen. Pod simbolom, ki ga stroj v danem trenutku pregleduje, bomo napisali stanje, v katerem se

nahaja. Če nas stanje ne zanima, bomo pod simbolom narisali puščico. Temu opisu rečemo *konfiguracija*.

Zapis:

$$s_0 s_0 s_0 s_0 s_0 s_0 s_0$$
$$q_1$$

predstavlja začetno konfiguracijo našega stroja. Trak je prazen, stroj v stanju q_1 pregleduje simbol s_0. Pa še tole: zaradi lažjega pisanja bomo povsod tam, kjer ne bo možnosti za dvoumnost, namesto simbolov s_i pisali kar indeks i in namesto q_j ravno tako. Začetna konfiguracija je torej:

0000000
1

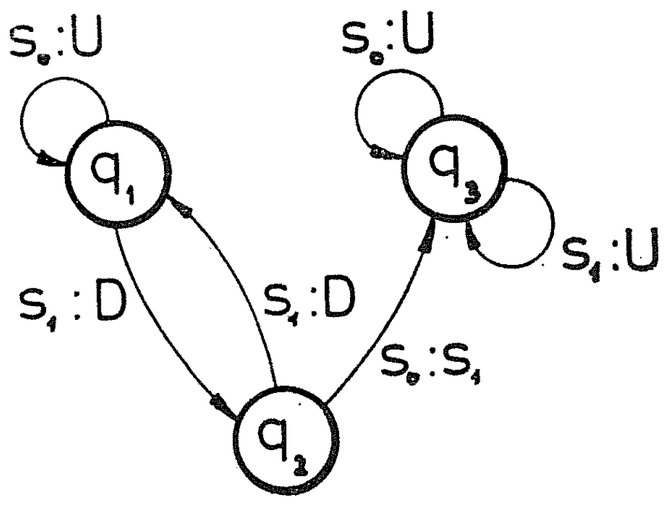
Naslednja razpredelnica kaže, kako deluje naš stroj, če začne na praznem traku:

trenutek	konfiguracija	novo stanje	zapisan simbol	premik
1.	**0000000** **1**	1	1	—
2.	**0000100** **1**	2	—	*L*
3.	**0000100** **2**	2	1	—
4.	**0001100** **2**	3	—	*L*
5.	**0001100** **3**	3	1	—
6.	**0011100** **3**	3	USTAVI SE!	
7.	**0011100** **3**	(stroj stoji)		

Zgled 9: Turingov stroj, ki ugotovi, ali je število enic v strnjenem zaporedju enic na sicer praznem traku sodo ali liho. Takole se domenimo! Na začetku naj stroj stoji nad najbolj levo enico v nizu enic. Začetna konfiguracija stroja je:

111 . . . 1
1

Na koncu pa naj stoji nad enico, če je število enic na začetku liho, sicer naj se ustavi nad praznim kvadratkom (nad ničlo!). Stroj se bo premikal na desno preko enic, pri tem bo skakal iz enega stanja (liho) v drugo (sodo) in narobe. Ko bo naletel na prazno mesto, se bo glede na stanje bodisi ustavil bodisi napisal enico in se ustavil takoj za tem. Stroj konstruiramo tako, da narišemo graf. Iz grafa sestavimo razpredelnico:



	s_0	s_1
q_1	Uq_1	Dq_2
q_2	s_1q_3	Dq_1
q_3	Uq_3	Uq_3

Iz razpredelnice ni težko določiti linearni zapis:

$$s_0q_1Uq_1s_1q_1Dq_2s_0q_2s_1q_3s_1q_2Dq_1s_1q_3Uq_3s_0q_3Uq_3$$

Zakaj smo sploh vpeljali linearni zapis Turingovega stroja, ko pa je vse prej kot pregleden? Odgovor: zato, da bomo dokazali, da je množica vseh Turingovih strojev števna.

Vzemimo abecedo $A = \{U, D, L, s_0, q_1, s_1, q_2, s_2, \ldots\}$. A je števno neskončna abeceda. Zato je števna tudi množica A^* vseh besed nad A. O tem nas je prepričal zgled 4. Ker lahko poljuben Turingov stroj zapišemo v linearni obliki, ta pa ni nič drugega kot beseda iz A^*, je tudi množica vseh Turingovih strojev števna.

Izračunljivost

Turingove stroje lahko uporabimo za računanje funkcij. Argument x nekako zapišemo na trak. Stroj poženemo in počakamo, da se ustavi (če se sploh ustavi!). Pogledamo na trak in odčitamo funkcijsko vrednost y. Turingov stroj lahko pojmujemo kot predpis, ki začetni konfiguraciji priredi končno konfiguracijo (če se ustavi po končnem številu korakov). Ker nas zanimajo funkcije oblike: $f: \mathcal{N} \to \mathcal{N}$, $f: \mathcal{N} \times \mathcal{N} \to \mathcal{N}$, ..., torej funkcije, ki naravnim številom prirejajo naravna števila, imajo pa lahko enega ali več argumentov, se moramo predvsem domeniti, kako bomo *zapisovali* argumente na trak in kako bomo brali oziroma *interpretirali* rezultate. Števila bi namreč lahko pisali v različnih številskih sistemih. Zato ni vseeno, ali rezultat 121 odčitamo kot število v desetiškem ali trojiškem sistemu! Odločiti se moramo sami in se seveda dogovora ves čas držati. Takole bomo napravili: Naravno število n predstavimo s strnjenim zaporedjem enic (simbolov s_1). Število enic v nizu naj bo točno n. Če ima funkcija več argumentov, jih na začetku zapišemo, tako kot smo se domenili, drugega za drugim na trak, ločene s po enim praznim znakom. Začetna konfiguracija naj bo taka, da stroj stoji nad najbolj levo enico prvega argumenta. Razen tega pa naj na traku ne bo napisano nič drugega. Rezultat, če seveda obstaja, naj bo zapisan v isti obliki, torej kot strnjeno zaporedje enic na sicer praznem traku. Stroj naj stoji nad najbolj levo enico v nizu. Denimo, da želimo sestaviti Turingov stroj za računanje funkcije $f(x, y, z) = x + y + z$. Če naj stroj izračuna $f(5, 2, 3)$, bomo pripravili tole začetno konfiguracijo:

111110110111
1

Ko se stroj ustavi, pa bomo konfiguracijo:

1111111111
1

odčitali kot »deset«. Takim konfiguracijam bomo rekli *standardna* konfiguracija. Če se stroj ne ustavi ali pa se ustavi v konfiguraciji, ki ni standardna, bomo menili, da je funkcijska vrednost pač *nedefinirana*. Oglejmo si štiri primere nestandardnih konfiguracij:

11111
1

11101
1

011111
1

000000
1

Iz tega, kar smo doslej povedali, izhaja, da vsak Turingov stroj, ki razpoznava poleg praznega simbola s_0 vsaj en neprazni simbol s_1, računa natančno eno funkcijo oblike $f: \mathcal{N} \to \mathcal{N}$. Argument podamo s standardno konfiguracijo in, če se stroj ustavi v standardni konfiguraciji, na koncu računanja odčitamo funkcijsko vrednost. Seveda je v splošnem funkcija $f_T: \mathcal{N} \to \mathcal{N}$, ki pripada Turingovemu stroju T, lahko parcialna (če se stroj T pri začetni standardni konfiguraciji sploh ne ustavi ali pa se ustavi v nestandardni konfiguraciji). Za funkcije f_T pravimo, da so *izračunljive*, natančneje: *izračunljive s Turingovimi stroji.* Če so totalne, so *totalno izračunljive*, sicer pa so *parcialno izračunljive*. Ker je Turingovih strojev le številno mnogo, je tudi izračunljivih funkcij le številno mnogo. Ker pa je vseh funkcij oblike $f: \mathcal{N} \to \mathcal{N}$ neštevno mnogo, spoznamo, da *obstajajo neizračunljive funkcije*. Še več! Z diagonalizacijo lahko celo s prstom pokažemo na neizračunljivo funkcijo. Kot vemo, lahko Turingove stroje enumeriramo, torej zapišemo v vrsti: $T_1, T_2, \ldots$ S tem tudi enumeriramo vse izračunljive funkcije $f_{T_1}, f_{T_2}, \ldots$ Funkcijo $a: \mathcal{N} \to \mathcal{N}$, definiramo takole:

$$a(n) = \begin{cases} f_{Tn}(n) + 1 & \text{— če je } f_{Tn} \text{ definirana pri } n \\ 1 & \text{— v vseh drugih primerih} \end{cases}$$

Seveda je a spet antidiagonalna funkcija in je, čeprav totalna, neizračunljiva. Denimo, da izvedemo enumeracijo množice vseh besed nad številno neskončno abecedo tako, kot smo napravili na koncu zgleda 4, da med besedami izberemo le linearne zapise Turingovih strojev; potem lahko poiščemo nekaj prvih funkcij f_{Tn}:

n	n'	beseda	T_n	f_{Tn}
1	1	U	$s_0q_1Uq_1s_1q_1Uq_1$	identiteta
…	…	D	…	…
	12	UU		
	…	…		
	122	$s_0q_1Uq_1s_1q_1Uq_1$		
	…	…		
	1212			
	…			
	122221 … 122222			
	…			

Ker je f_{T_1} identiteta, je po definiciji $a(1) = f_{T_1}(1) + 1 = 2$. Kaj zdaj to pomeni? Pravimo, da a ni izračunljiva, pa vendar smo določili $a(1)$! Z malo več napora bi lahko izračunali a še pri nekaterih drugih vrednostih. Pomislimo, kako bi določili $a(n)$ v splošnem. Najprej bi morali poiskati T_n. To ja načelno mogoče, vendar zelo zamudno. Potem bi simulirali T_n pri argumentu n in počakali, da se ustavi. Prištejemo rezultatu enico in imamo vrednost $a(n)$. Kaj pa, če se T_n ne ustavi? Kako naj vemo, ali se bo stroj sploh kdaj ustavil ali ne? Za nekatere Turingove stroje zlahka ugotovimo, ali se bodo ustavili ali ne. Vprašanje pa je, ali znamo v končno mnogo korakih ugotoviti, ali se *poljuben* Turingov stroj ustavi ali ne. O tem bomo spregovorili v naslednjem razdelku. Zdaj pa raje pokramljajmo malo o izračunljivosti. S Turingovimi stroji smo *točno* in nedvoumno opredelili množico izračunljivih funkcij. Seveda pa je ta množica vezana na Turingove stroje. Kaj pa če bi namesto Turingovih strojev vpeljali drugačen mehanizem za izračunavanje? Denimo, da bi idealizirali računalnik! Idealizirani računalnik bi imel številno neskončen spomin in v vsaki celici bi lahko hranil poljubno naravno število. S takim računalnikom bi lahko definirali drugače izračunljive funkcije. Ali je tako definirana množica izračunljivih funkcij bogatejša ali revnejša od one, ki je definirana s Turingovimi stroji? Približno hkrati s Turingovimi stroji so se pojavile

tudi druge formalizacije mehanizmov za računanje (normalni algoritmi Markova, rekurzivne funkcije, semi-thuevski sistemi, Postovi sistemi, ...). Za vsakega od njih pa se je izkazalo, da je *ekvivalenten* konceptu Turingovih strojev!! Z vsakim od teh sistemov lahko definiramo razred izračunljivih funkcij. In pomislite, vsi ti razredi med seboj sovpadajo! Kaže, *da so funkcije, izračunljive s Turingovimi stroji ravno funkcije, ki so izračunljive v intuitivnem smislu.* To domnevo je prvi postavil *Alonzo Church* in se po njem imenuje *Churcheva teza*. Churcheva teza je seveda *nedokazljiva*, saj pojem »izračunljivost v intuitivnem smislu« ni matematičen pojem. Tezo pa bi lahko *ovrgli*, če bi nam uspelo sestaviti formalen aparat za računanje, ki bi ne bil ekvivalenten Turingovim strojem. Tega pa doslej še nikomur ni uspelo napraviti. Zato je danes večina matematikov in logikov mnenja, da Churcheva teza velja. Omogoča nam formalno lotevanje problemov izračunljivosti. Če tezo privzamemo, se pomen Turingovih strojev bistveno poveča! Problem, ki ga ne reši *noben* Turingov stroj, je *nerešljiv*.

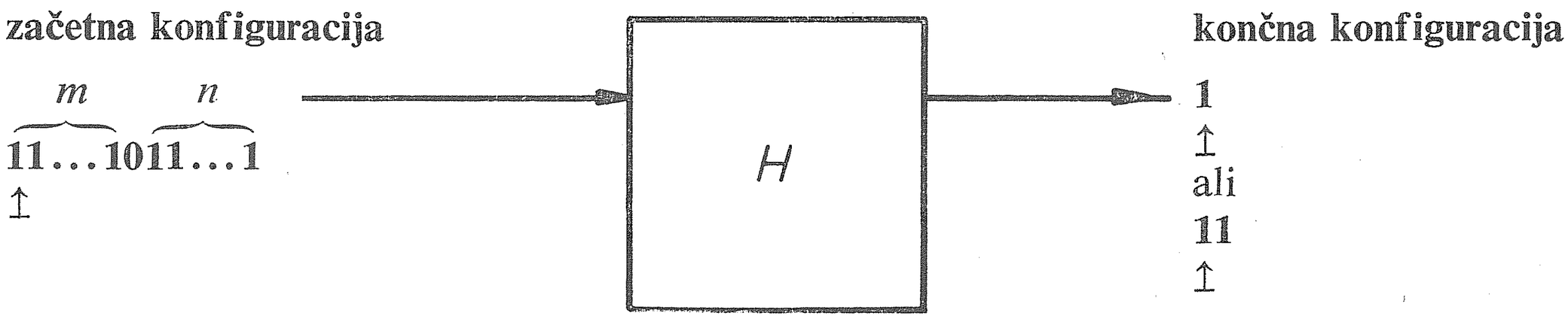
Nerešljivost

Povrnimo se k problemu, ki smo ga načeli že v prejšnjem razdelku: Kako ugotoviti, ali se bo Turingov stroj, ki začne delovati v standardni konfiguraciji, ustavil? Takole bomo preformulirali problem:

Vsak Turingov stroj T lahko zapišemo v linearni obliki, torej kot besedo nad znano abecedo. Vsako besedo lahko *kodiramo* z nekim naravnim številom tako, da lahko iz števila brez težav rekonstruiramo besedo. V mislih imamo kodiranje s številom, ki se v desetiškem sistemu izraža izključno z enicami in dvojkami in smo ga spoznali v zgledu 4! Torej lahko tudi stroj T kodiramo z naravnim številom $\alpha(T)$, tako da znamo T rekonstruirati, če poznamo $\alpha(T)$. Še več, pri tem kodiranju znamo za vsako naravno število m ugotoviti, ali ustreza kakšnemu stroju T ali ne. Stroj T pa, kot vemo, realizira funkcijo $f_T: \mathcal{N} \to \mathcal{N}$, ki je v splošnem lahko parcialna. Definiramo funkcijo $h: \mathcal{N} \times \mathcal{N} \to \mathcal{N}$ takole:

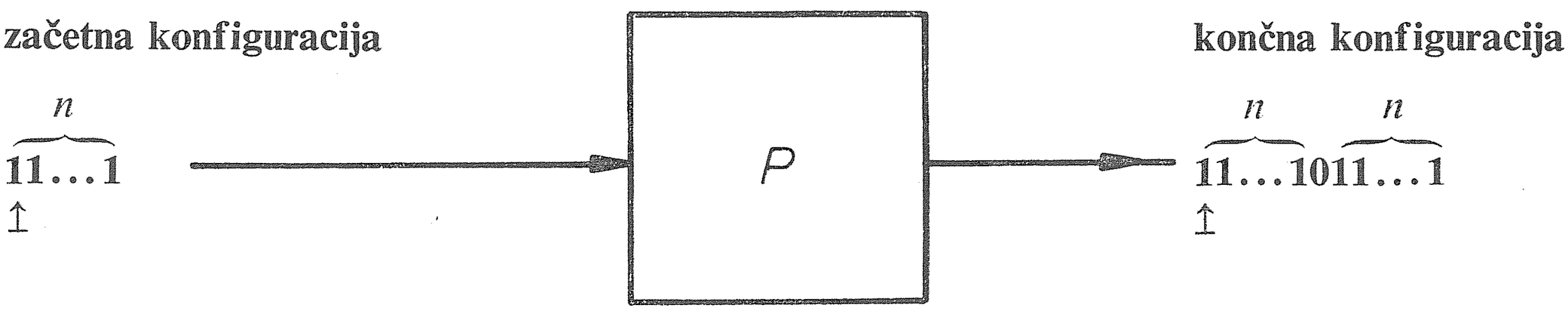
$$h(m, n) = \begin{cases} 1 \text{ — če obstaja tak } T, \text{ tako da je } m = \alpha(T) \text{ in se } T \text{ ustavi pri računanju z argumentom } n \\ 2 \text{ — v vseh drugih primerih} \end{cases}$$

Problem ustavitve Turingovega stroja se zdaj glasi: Poišči tak Turingov stroj, H ki realizira funkcijo h! Denimo, da smo H sestavili. Deluje takole:

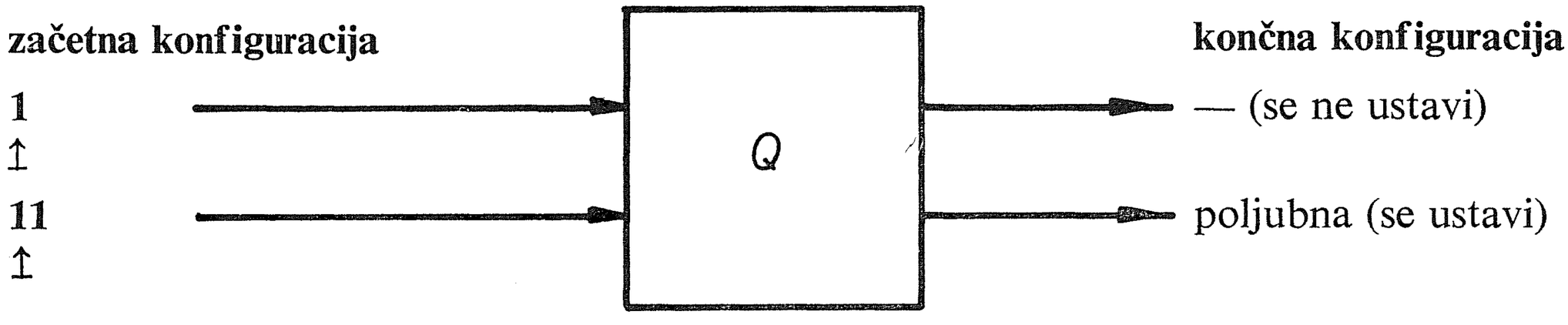


Bralec lahko za vajo določi Turingova stroja P in Q, ki delujeta takole:

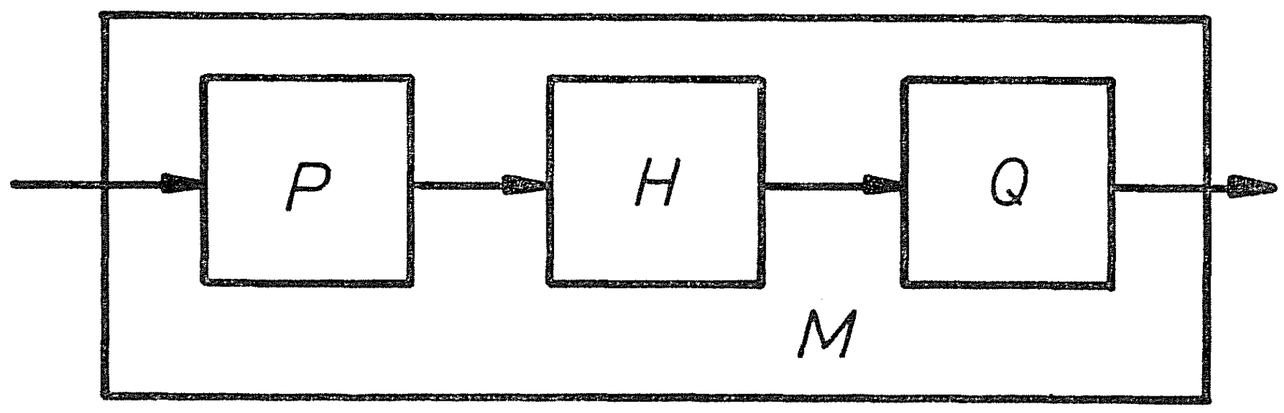
P naj argument n v standardni konfiguraciji podvoji takole:



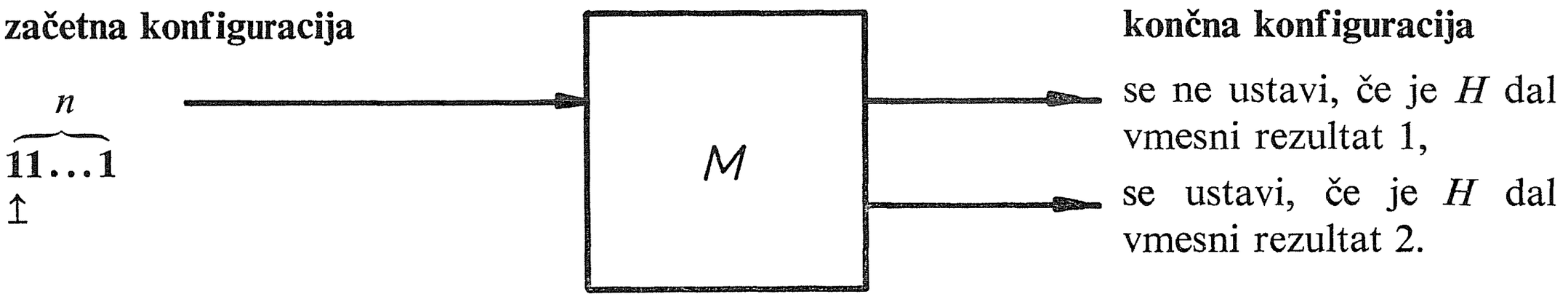
Q pa naj se pri argumentu 1 v standardni konfiguraciji sploh ne ustavi, pri argumentu 2 pa naj se ustavi (v poljubni konfiguraciji):



Iz vseh treh strojev P, H in Q sestavimo Turingov stroj M



ki deluje takole:



M namreč pri argumentu n deluje najprej kot P, torej pripravi (n, n), argumenta za H. H izračuna $h(n, n)$, ki je bodisi 1 bodisi 2. Potem prevzame delo Q, ki se ustavi ali ne.

Zdaj pa povejmo, čemu vse to! Ker je M Turingov stroj, mu kot vsakemu Turingovemu stroju pripada število $m = \alpha(M)$. Če M poženemo pri argumentu m, deluje takole: med računanjem določi $h(m, m)$, ki je lahko 1 ali 2. Če je $h(m, m) = 1$, bi se moral po definiciji funkcije h stroj M (pri argumentu m) ustaviti. To pa ni res, saj je zadnji del stroja M, ki smo ga imenovali Q, sestavljen tako, da se pri $h(m, m) = 1$ *ne* ustavi. Torej $h(m, m)$ ne more biti 1, zato je kvečjemu 2. Ker je m koda stroja M, pomeni $h(m, m) = 2$, da se M pri argumentu m ne sme ustaviti. Žal pa je M sestavljen tako, da se pri vmesnem rezultatu $h(m, m) = 2$ zagotovo ustavi! Torej M sploh ne obstaja! Ker pa P in Q obstajata, bi M obstajal, če bi obstajal H. Torej tudi H ne obstaja: ne obstaja tak Turingov stroj, ki bi povedal, ali se poljuben Turingov stroj pri računanju s poljubnim argumentom ustavi ali ne! Če privzamemo Churchevo tezo, lahko rečemo: *Problem ustavitve Turingovega stroja je nerešljiv.*

LITERATURA

[1] Martin Davis, Computability and Unsolvability, New York, Toronto, London, McGraw-Hill 1958.

[2] Hans Hermes, Enumerability, Decidability, Computability, Berlin, Heidelberg, New York, Springer-Verlag 1965.

[3] George S. Boolos, Richard C. Jeffrey, Computability and Logic, London, New York, Cambridge University Press 1974.

Obzornik mat. fiz. 25 (1978) 1

LOGIKA IN MNOŽICE V SREDNJI ŠOLI

JANEZ RAKOVEC

AMS Subj. Class. (1970) 02—01, 04—01, 97 A 99

Nekaj misli k izboljšanju pouka matematične logike in teorije množic v srednji šoli.

LOGIC AND SET THEORY IN THE SECONDARY SCHOOL

Some ideas to improve teaching of mathematical logic and set theory in the secondary school.

1. Uvod

Matematično logiko in teorijo množic štejemo med novejša področja matematike. Upoštevati pa je treba, da so osnovni pojmi o logiki in o množicah navzoči v matematiki že od nekdaj, čeprav ne vselej eksplicitno. Znani francoski matematik René Thom celo pravi: »Vsakdo uporablja teorijo množic od trenutka, ko začne živeti, ravno tako kot M. Jourdain v Molièrovem Le Bourgeois Gentilhomme uporablja prozo, ne da bi se tega zavedal.« V tem stavku gre seveda za osnovno, nazorno teorijo množic. Veliki Georg Cantor pa je zelo razširil dotedanja obzorja s svojo sistematično teorijo množic, ki je postala temelj sodobne, formalizirane matematike; še posebej gre Cantorju zasluga za raziskovanje neskončnih množic. Za tradicionalno logično izkustvo pa pomeni velik napredek sodobna matematična logika, ki je doslej rešila ali vsaj razjasnila številne težke logične probleme v osnovah matematike. — Poudarimo še, da sta matematična logika in teorija množic tesno povezani, s čimer je tudi opravičen njun skupni nastop v tem članku.

Kakor je na primer za tehnika, ki uporablja fizikalne zakone, zaželjeno tudi teoretično poznavanje fizike, tako je za srednješolca koristno poglobljeno srečanje z logiko in množicami: pomagalo mu bo k jasnemu razumevanju matematičnih načel, ki bi jih sicer dojemal le podzavestno in razdrobljeno.

Ker sta logika in teorija množic navzoči povsod v matematiki, je prav, da vpeljemo njune osnovne pojme že takoj v začetku srednje šole. Pridobljeno znanje nato postopno širimo, oziraje se na njegovo uporabo v drugih poglavjih matematike. Skrbimo tudi za smiselno povezavo obravnav logike in teorije množic. Končno naj dijaki dobijo vpogled v matematično logiko in teorijo množic kot celoti in tako čimbolje razumejo osnove matematike.

V učnih knjigah [1] do [6] pogosto srečujemo logiko in množice. V naslednjem želim pokazati, kako bi ta srečanja kar najbolj izrabili in tu in tam še kaj dodali. Če je kak del predlagane snovi preobširen za že tako omejeni čas pouka, bi bil morda primeren za matematični krožek.

2. Izjavni račun

Izjave in povezave izjav so predmet izjavnega računa; izjave pojmujemo tu kot enote in se ne ukvarjamo z njihovo notranjo zgradbo (glej II. poglavje v [10]). Osnovne pojme izjavnega računa vpeljemo v začetku srednješolskega pouka matematike (glej *Uvod* k I. poglavju v [1]). Pri tem najprej poudarimo, da v logiki izraz »izjava« pomeni pripovedno izjavo (stavek); zanjo je značilno prav to, da je bodisi pravilna (resnična) bodisi nepravilna

(neresnična). Vsebina izjav je lahko kakršnakoli; to omogoča najširšo uporabo matematične logike.

Po tem razmisleku takoj preidemo na *povezave* izjav — negacijo, konjunkcijo, disjunkcijo, implikacijo in ekvivalenco — ter vpeljemo ustrezne znake. Ti znaki so sicer prevodi besed: ne, in, ali, ..., vendar pa je pomen omenjenih povezav najbolj natančno določen s tem, kdaj so tako sestavljene izjave pravilne in kdaj ne (glej [10], str. 26—31 in [1], str. 10, 11). Posebno skrbno je treba obdelati, kdaj je pravilna implikacija in kdaj ekvivalenca dveh izjav (in ob tem uvesti pojma zadostnega in potrebnega pogoja). Iz pravilnostne definicije za implikacijo takoj sledi znano pravilo sklepanja *modus ponens*: če sta pravilni implikacija $\alpha \Rightarrow \beta$ in sama izjava α, je pravilna tudi izjava β. Če pa je pravilna ekvivalenca $\alpha \Leftrightarrow \beta$, sklepamo iz pravilnosti α na pravilnost β in obratno.

Obravnavano snov lepo ponazorimo s stavki iz vsakdanjega življenja ali matematike, ki jih med seboj povezujemo; te povezave prevajamo v jezik izjavnega računa in preverjamo njihovo pravilnost oziroma nepravilnost. Ne ustrašimo se tudi takšnih sestavljenih izjav, v katerih nastopa več povezav. — Če utegnemo, spremljamo celotno izvajanje s *pravilnostnimi tabelami* (matrikami); glej [10], str. 33 in [4], str. 30, 31. S tabelami potem ugotavljamo, kdaj so kakšne zapletene sestavljene izjave pravilne in kdaj ne.

Z izjavnim računom povežemo tudi osnovne pojme o množicah — več o tem v 5. razdelku.

Logično pravilne izjave. V začetku prvega razreda je zelo koristno navesti še nekaj preprostih logično pravilnih izjav, npr.: $\alpha \vee \neg \alpha$, $\alpha \wedge \beta \Rightarrow \alpha$, $\alpha \Rightarrow \alpha \vee \beta$, $\alpha \wedge \beta \Leftrightarrow \beta \wedge \alpha$, $\alpha \vee \beta \Leftrightarrow \beta \vee \alpha$.* Dijaki naj s premislekom ugotovijo, da so takšne izjave vedno pravilne, neglede na pravilnost ali nepravilnost osnovnih izjav. Primer: če je izjava α pravilna, je — po svoji definiciji — pravilna tudi disjunkcija $\alpha \vee \beta$ (neglede na to, kakšen je β) in je torej implikacija $\alpha \Rightarrow \alpha \vee \beta$ pravilna; pri nepravilnem α pa je implikacija že tako pravilna. — Kot nasprotje k logično pravilnim izjavam pa si je treba ogledati še kakšno logično nepravilno izjavo, npr.: $\alpha \wedge \neg \alpha$.

Pozneje je primerno še večkrat omeniti to ali ono logično pravilno izjavo, najbolje tedaj, ko jo pri matematiki rabimo. Precej uporabna je npr. logična implikacija $(\alpha \vee \beta) \wedge \wedge \neg \alpha \Rightarrow \beta$, prav tako tudi logične ekvivalence $\alpha \Rightarrow \beta \Leftrightarrow \neg \beta \Rightarrow \neg \alpha$, $\alpha \wedge (\beta \vee \gamma) \Leftrightarrow \Leftrightarrow (\alpha \wedge \beta) \vee (\alpha \wedge \gamma)$, $\neg (\alpha \vee \beta) \Leftrightarrow \neg \alpha \wedge \neg \beta$ itd. O logični pravilnosti teh izjav se prepričamo čim nazorneje, na primer: naj velja $\alpha \Rightarrow \beta$; če tedaj ne velja β, tudi α ne velja, saj bi iz pravilnosti α sledila pravilnost β — torej iz $\alpha \Rightarrow \beta$ logično sledi $\neg \beta \Rightarrow \neg \alpha$. — Zaokroženo zbirko *logičnih ekvivalenc in implikacij* najdemo v [10], str. 39—41, 69—71; precejšen del teh formul rabimo pri obdelavi razdelka *Algebra množic* v [3].

Logične ekvivalence in implikacije so osnovno orodje logičnega sklepanja: pri dani logični implikaciji sklepamo iz pravilnosti izjave na levi strani na pravilnost izjave na desni strani; logična ekvivalenca pa nam ponuja takšna sklepa v obeh smereh. Iz že znanih pravilnih trditev dobivamo tako »nove« trditve. Le-te so sicer logično odvisne od prejšnjih trditev in so torej v njih vsebovane; vendar so »nove« v tem pomenu, da prej nismo vedeli za njihovo pravilnost in smo do nje prišli šele z logičnim sklepanjem.

Če spremljamo izjavni račun s pravilnostnimi tabelami, si z njimi zelo poenostavimo utemeljevanje posameznih logičnih ekvivalenc in implikacij. Pri tem pa seveda ne pojmujemo pravilnostnih tabel kot nekakšen mehanizem, ki naj bi nadomestil človekovo mišljenje. Uporabljamo jih predvsem za preverjanje svojega razmišljanja oziroma sklepanja.

Uporaba izjavnega računa. Poznavanje logičnega jezika pripomore k čim natančnejši formulaciji raznih matematičnih trditev. V posebno pomoč pa so nam seveda logične

---

* Pri tem sta α in β poljubni, lahko tudi sestavljeni izjavi.

implikacije in ekvivalence. Med slednjimi pride pogosto v poštev tale: $\alpha \Rightarrow \beta \Leftrightarrow \neg \beta \Rightarrow \neg \alpha$; njeno uporabo navadno imenujemo *metoda posrednega* (*indirektnega*) *dokaza*. Z njo npr. ugotovimo, da v poljubnem kolobarju velja: $a \neq b \Rightarrow a + c \neq b + c$ — potem ko že vemo, da iz $a + c = b + c$ sledi $a = b$.

Iz $a \neq b$ sledi v urejenem kolobarju $a < b$ ali $a > b$; do tega pridemo z upoštevanjem trihotomije in logične implikacije $(\alpha \vee \beta) \wedge \neg \alpha \Rightarrow \beta$ (pri čemer za α vstavimo $a = b$, za β pa $(a < b) \vee (a > b)$). Distributivnost disjunkcije glede na konjunkcijo pa nam omogoči tale sklep: $(a \leqq b) \wedge (a \geqq b) \Leftrightarrow ((a = b) \vee (a < b)) \wedge ((a = b) \vee (a > b)) \Leftrightarrow$ $\Leftrightarrow (a = b) \vee ((a < b) \wedge (a > b)) \Leftrightarrow a = b$ (upoštevali smo, da je izjava $(a < b) \wedge (a > b)$ nepravilna). Če je v urejenem kolobarju $a \neq 0$ in $b \neq 0$, je $a > 0$ ali $a < 0$ in hkrati $b > 0$ ali $b < 0$, torej $ab > 0$ ali $ab < 0$ in s tem $ab \neq 0$. Od tod dobimo z metodo posrednega dokaza, da iz $ab = 0$ sledi $a = 0$ ali $b = 0$ (upoštevati je treba še *De Morganov zakon*: $\neg ((a = 0) \vee (b = 0)) \Leftrightarrow (a \neq 0) \wedge (b \neq 0)$).

Navedli smo nekaj značilnih primerov iz algebre; logično sklepanje nam tu pomaga do pripravnih ugotovitev, ki jih pozneje velikokrat rabimo. — O vlogi izjavnega računa pri algebri množic bo tekla beseda v 5. razdelku, zdaj pa omenimo še nekaj primerov za metodo posrednega dokaza v geometriji (primerjaj tudi [5], str. 69).

Če imata neki premici dve skupni točki, sta — po aksiomu I/1 — identični; torej imata različni premici kvečjemu eno skupno točko. Če premica leži v ravnini danega trikotnika, ne gre skozi nobeno njegovo oglišče in ne seka dveh njegovih stranic, tudi ne seka tretje stranice — saj bi sicer po Paschevem aksiomu sekala eno od prvih dveh stranic. V poljubnem trikotniku velja: $AC < BC \Rightarrow \sphericalangle B < \sphericalangle A$, $AC \equiv BC \Rightarrow \sphericalangle B \equiv \sphericalangle A$, $AC > BC \Rightarrow$ $\Rightarrow \sphericalangle B > \sphericalangle A$; od tod logično sledi npr.: $\sphericalangle B < \sphericalangle A \Rightarrow AC < BC$ (sicer bi bilo $AC \equiv BC$ ali $AC > BC$ in s tem $\sphericalangle B \equiv \sphericalangle A$ ali $\sphericalangle B > \sphericalangle A$). Če za točke A, B, M v ravnini Π velja: $AM \equiv BM$, leži M na simetrali daljice AB (sicer bi bilo namreč $AM < BM$ ali $AM > BM$). Iz aksioma o vzporednicah sledi, da oklepa prečnica z vzporednicama paroma skladne protikote (sicer bi namreč k neki premici obstajali dve vzporednici skozi isto točko).

Izjavni račun kot model Boolove algebre je posebno lepo opisan v [4], str. 30—32. Če prevedemo aksiome Boolove algebre v jezik izjavnega računa, dobimo ravno logične ekvivalence, katerih veljavnost preverimo s tabelami pravilnosti. Z uporabo logičnih ekvivalenc lahko sestavljene izjave poenostavljamo ali pa izrazimo pri njih vse povezave le s *Shefferjevo operacijo*: $\neg \alpha \vee \neg \beta$. Včasih štejemo vse izjave, ki so med seboj logično ekvivalentne, za eno samo izjavo; po tem dogovoru so izjave v bijektivni zvezi z *Boolovimi funkcijami* ([4], str. 32—35). V bistvu isti model Boolove algebre kakor izjavni račun je še teorija *preklopnih vezij*; glej [10], str. 49—58 in [4], str. 35—39.

3. Predikatni račun

Notranja zgradba izjav je predmet predikatnega računa (glej III. poglavje v [10]). Osnovne pojme o notranji zgradbi je koristno vpeljati že v začetku 1. razreda, takoj za vpeljavo izjav in njihovih povezav. Ob zgledih ugotovimo, da vsaka izjava govori o eni ali o več rečeh (elementih) nekega področja (univerzuma). V prvem primeru pravimo, da izjava nekemu elementu pripisuje neko *lastnost*, v drugem primeru pa gre za neki *odnos* (relacijo), ki naj velja med dvema elementoma oziroma več elementi. Tako npr. izjava »a je naravno število« govori o neki lastnosti elementa a, izjava »$a \neq b$« pa govori o nekem odnosu med a in b.

Spremenljivke in izjavne formule. Ob vpeljavi spremenljivk v [1], str. 76, je primerno dijakom osvetliti vlogo konstant in spremenljivk v logiki (in s tem v matematiki). Konstanta je znak za neki določen element danega univerzuma. Spremenljivko pa navadno

pojmujemo kot znak za katerikoli element univerzuma. Vendar ni umestno označevati različne elemente z istim znakom (dvoumje!); zato rajši recimo: spremenljivka je čist znak, ki nič ne označuje, zamenjamo pa jo lahko s katerokoli konstanto (ki označuje kak element danega univerzuma).

Izjava »$a > 0$« (kjer konstanta a označuje neko določeno število) je pravilna le, če je a res pozitiven. Pri izrazu »$x > 0$« pa ne moremo govoriti o pravilnosti ali nepravilnosti, saj spremenljivka x ne označuje ničesar; zato »$x > 0$« še ni izjava. Šele ko zamenjamo x v tem izrazu s kakšno konstanto (vrednostjo spremenljivke x), dobimo izjavo.

Ob teh opažanjih je dobro vpeljati izraz »izjavna formula«: med izjavne formule štejemo vse izjave in vse tiste izraze, ki so po obliki enaki izjavam, le da v njih nastopajo spremenljivke namesto (ali poleg) konstant. Izjavna formula, ki vsebuje kakšno prosto** spremenljivko, ne more biti pravilna ali nepravilna v pravem pomenu besede; lahko pa vendarle rečemo, da je formula pravilna, oziroma nepravilna, pri tistih zamenjavah (vrednostih) spremenljivk(e), pri katerih dobimo iz formule pravilno, oziroma nepravilno, izjavo. Tako je npr. formula »$x > 0$« pravilna natanko pri vseh pozitivnih vrednostih spremenljivke x. Lahko tudi rečemo: množica vseh tistih vrednosti za x, ki ustrezajo pogoju »$x > 0$«, vsebuje ravno tiste vrednosti, pri katerih je formula »$x > 0$« pravilna. — Še opozorilo: beseda »formula« v tradicionalnem pomenu označuje le takšno izjavno formulo, ki je pravilna za vse vrednosti spremenljivk(e).

Vzemimo poljubno funkcijo $y = f(x)$. Predpis f priredi dani vrednosti za x takšno vrednost za y, da je formula $y = f(x)$ pri teh dveh vrednostih pravilna. Graf funkcije $f(x)$ je množica tistih točk — vrednosti za »tekočo točko« $T(x, y)$, pri katerih je formula $y = f(x)$ pravilna. — Formula oblike $f(x) = 0$ se imenuje enačba in je seveda smiselna pri vsaki vrednosti spremenljivke (neznanke) x iz definicijskega območja funkcije $f(x)$. Vse tiste vrednosti za x, pri katerih je formula $f(x) = 0$ pravilna, pa imenujemo rešitve te enačbe. Dve enačbi $f(x) = 0$ in $g(x) = 0$ imenujemo ekvivalentni, kadar imata isto množico rešitev — to je, kadar sta formuli $f(x) = 0$ in $g(x) = 0$ pravilni pri natanko istih vrednostih za x. To pa pomeni: enačbi $f(x) = 0$ in $g(x) = 0$ sta ekvivalentni, kadar je ekvivalenca $f(x) = 0 \Leftrightarrow g(x) = 0$ pravilna pri vsaki vrednosti za x.

Podobno kakor izjave lahko tudi poljubne izjavne formule vežemo med seboj s konjunkcijo, disjunkcijo ... in tako dobimo sestavljene izjavne formule. — Vzemimo zdaj poljubno logično pravilno izjavo, npr.: $(\alpha \vee \beta) \wedge \neg \alpha \Rightarrow \beta$, in v njej nadomestimo osnovne izjave s poljubnimi izjavnimi formulami, npr.: $((x = 0) \vee (x < 0)) \wedge (x \neq 0) \Rightarrow x < 0$. Tako dobljena sestavljena izjavna formula je tudi logično pravilna — in sicer v tem pomenu, da je pravilna pri vsaki zamenjavi (vrednosti) spremenljivk(e). (Pri vsaki zamenjavi namreč očitno dobimo logično pravilno izjavo.) Torej lahko vse ugotovitve izjavnega računa uporabimo tudi pri delu z izjavnimi formulami.

Kvantifikatorji. Marsikdaj ugotovimo, da je neka izjavna formula $\alpha(x)$ pravilna za vsako (ali vsaj eno ali natanko eno) vrednost spremenljivke x (pri čemer dopuščamo vrednosti iz dane množice $\mathscr{M}$). Spomnimo se na identične enačbe in na enačbe z vsaj (ali natanko) eno rešitvijo, pa tudi na razne izreke (V vsakem trikotniku je...; ...obstaja vsaj ena vzporednica...). Za izraze »vsak«, »vsaj eden«, »natanko eden« vpeljemo v začetku 4. razreda znake — kvantifikatorje: $\forall$, $\exists$, $\exists^*$ (glej [4], str. 5, 6). Zapis $\forall x \in \mathscr{M} : \alpha(x)$ pomeni: Izjavna formula $\alpha(x)$ je pravilna za vsak $x \in \mathscr{M}$ (to je pri vsaki vrednosti za x iz množice $\mathscr{M}$). Omenjeni zapis je očitno izjava, pravilna natanko tedaj, če $\alpha(x)$ res velja za vsak $x \in \mathscr{M}$. — Analogno velja za rabo kvantifikatorjev $\exists$ in $\exists^*$. — Iz izjavnih formul torej dobivamo izjave ne le z vstavljanjem konstant, ampak tudi z »vezavo« spremenljivk s kvantifikatorji.

** Spremenljivka je prosta, če ni vezana s kakšnim kvantifikatorjem; primerjaj [10], str. 90.

Rabo kvantifikatorjev utrdimo s prevajanjem primerno izbranih izjav iz matematike in iz vsakdanjega življenja v logični jezik (glej [10], str. 93...). Ob tem ugotovimo med drugim, da vrstnega reda znakov $\forall$ in $\exists$ (oziroma $\exists^*$) ne smemo kar obrniti — sicer se pomen izjave spremeni. Vloga kvantifikatorjev je še posebej izrazita v definiciji zgornje meje in natančne zgornje meje ([4], str. 57, 58) ter v definiciji limite funkcije (oziroma zaporedja) in zveznosti funkcije ([4], str. 59, 61—63, 80). Omenjene definicije je seveda treba tudi prevesti v običajni jezik, jih povedati na več načinov in jih podkrepiti s primeri. (Pri ugotavljanju zveznosti, npr. za linearno funkcijo, skušamo k poljubno izbranemu $\varepsilon > 0$ poiskati ustrezen δ v odvisnosti od ε; za ε vzamemo tudi konkretne vrednosti.)

Med logičnimi ekvivalencami predikatnega računa se pogosto rabita tile dve: $\neg\,(\forall x \in \mathscr{M} : a(x)) \Leftrightarrow (\exists x \in \mathscr{M} : \neg\, a(x))$, $\neg\,(\exists x \in \mathscr{M} : a(x)) \Leftrightarrow (\forall x \in \mathscr{M} : \neg\, a(x))$. Njuna logična pravilnost očitno sledi iz samega pomena kvantifikatorjev in jo v šoli utemeljimo čim nazorneje, ob primerih iz vsakdanjega življenja. Da npr. neko število a ni zgornja meja dane množice $\mathscr{M}$, povemo takole: $\neg\,(\forall x \in \mathscr{M} : x \leqq a)$ ali v ekvivalentni obliki: $\exists x \in \mathscr{M} : x > a$.

4. Aksiomatična metoda

Formalna aksiomatika. V razdelku *O aksiomatični metodi* v [10] je med drugim izčrpno opisan prehod od nazorne aksiomatike, ki ima precej pomanjkljivosti, k formalni aksiomatiki. Nekoč so pojmovali aksiome kot razvidne resnice, danes pa jih rajši gledamo kot nekakšen dogovor. Za osnovo posamezne matematične teorije vzamemo neko množico $\mathscr{U}$, znotraj katere poteka naša obravnava in jo zato imenujemo *univerzum*. Pri tem nič ne govorimo, *kaj* naj bi bili njeni elementi. Tem elementom nato z *aksiomi* predpišemo določene lastnosti in odnose med njimi. Pogosto pa se aksiomi ne nanašajo le na elemente, ampak tudi na podmnožice** univerzuma $\mathscr{U}$. — Pravimo, da smo z danim sistemom aksiomov vpeljali neko *matematično strukturo* v univerzumu $\mathscr{U}$.

Izjave v zvezi z univerzumom $\mathscr{U}$, ki jih lahko izpeljemo iz aksiomov z logičnim sklepanjem, imenujemo *izreke* dane teorije. Izreki so torej logično odvisni od aksiomov in so s tem dejansko že vsebovani v aksiomih. — Pri izpeljavi posameznih izrekov je koristno, če kdaj pa kdaj podrobno analiziramo opravljeno logično sklepanje in navedemo uporabljene logične ekvivalence oziroma implikacije. Ob tem tudi vidimo, kako je izpeljava izrekov neodvisna od tega, kaj si pod elementi našega univerzuma predstavljamo. Univerzum $\mathscr{U}$ in njegovi elementi so lahko karkoli, da je le zadoščeno vsem aksiomom. — Seveda pa so pri našem delu vendarle zelo koristne tudi nazorne predstave; le-te sicer ne sodijo v samo teorijo, uspešno pa nam pomagajo pri iskanju domnev za nove izreke.

Modeli. Naš univerzum $\mathscr{U}$ ter lastnosti njegovih elementov in odnose med njimi pogosto predstavimo (interpretiramo) s kako množico konkretnih reči ter njihovimi lastnostmi in odnosi med njimi. Če pri teh konkretnih rečeh veljajo — ustrezno prevedeni — vsi aksiomi naše teorije, pravimo, da smo dobili model naše teorije. — Zelo znan je npr. model evklidske geometrije v fizikalnem svetu (glej razdelek *Geometrija in fizika* v [13] ter *Uvod* v [5]).

Izraz »model« v ožjem pomenu pa označuje takšen model dane teorije, ki je vzet iz matematike same. Končni kolobarji na strani 18 v [1] so modeli splošnega kolobarja; njegovi nadaljnji modeli so npr. kolobar celih števil, obseg racionalnih ali realnih števil (ki je seveda tudi kolobar), kolobarji polinomov ([2], str. 129...) itd. V knjigah [1] do [4] pogosto srečujemo modele algebrskih struktur (še posebej glej prvo poglavje v [4]).

** V geometriji radi pojmujemo točke kot elemente, premice in ravnine pa kot podmnožice univerzuma — trirazsežnega prostora.

Za prvo skupino aksiomov evklidske geometrije obstaja zelo preprost model: množico s štirimi elementi proglasimo za prostor, njene elemente za točke, njene podmnožice z dvema elementoma (oziroma s tremi elementi) pa za premice (oziroma ravnine). Veljavnost aksiomov I/1 do I/6 pri tej interpretaciji je prav lahko ugotoviti. — Model za celotno evklidsko geometrijo pa je analitična geometrija (ki jo v ta namen zasnujemo popolnoma neodvisno od običajne geometrije, le na podlagi realnih števil).

Neprotislovnost sistema aksiomov. Pravimo, da je sistem aksiomov dane teorije neprotisloven, če iz njega ni mogoče izpeljati kako trditev in hkrati njeno negacijo. Neprotislovnost aksiomov (ki je za teorijo življenjskega pomena) dokažemo, brž ko najdemo za teorijo kak model, ki je sam v sebi neprotisloven. (Iz protislovja v teoriji bi namreč sledilo ustrezno protislovje v modelu.) Tako nam npr. model kolobarja z edinima elementoma 0 in 1 zagotavlja neprotislovnost aksiomov za kolobar. Z analitično geometrijo pa prevedemo vprašanje o neprotislovnosti evklidske geometrije na vprašanje o neprotislovnosti aritmetike realnih števil; žal pa za neprotislovnost aritmetike še nimamo popolnoma zadovoljivega dokaza, v strogem smislu logike (glej [13], 106—113 in [10], str. 136—138).

Neodvisnost sistema aksiomov. Pravimo, da je sistem aksiomov dane teorije neodvisen, če noben aksiom ni odvisen od drugih aksiomov, to je, če ga ni mogoče izpeljati iz njih kot izrek. Odvisnost aksiomov je bolj lepotna napaka in jo npr. v šoli celo zavestno dopuščamo, kadar si s tem obravnavo poenostavimo. — Če je kak aksiom odvisen od drugih aksiomov, nas njegova negacija — skupaj z drugimi aksiomi — privede v protislovje. Z upoštevanjem tega so matematiki skušali dokazati odvisnost aksioma o vzporednicah od drugih geometrijskih aksiomov. Vendar z negacijo tega aksioma niso prišli do protislovja, temveč do nove, *neevklidične geometrije* (glej [10], str. 140, [13], str. 114..., [5], str. 167, 168 in *Uvod* v [12]).

5. Teorija množic

Osnovni pojmi o množicah predstavljajo — skupaj z osnovami logike — uvod v pouk matematike (glej *Uvod* v [1]). Obravnavo množic povežemo z izkustvom in jo spremljamo s primeri iz vsakdanjega življenja, aritmetike in geometrije. Operacije: unijo, presek in komplement naslonimo na ustrezne logične operacije: disjunkcijo, konjunkcijo in negacijo. Odnos podmnožice je v tesni zvezi z implikacijo, enakost dveh množic pa z ekvivalenco (po definiciji sta množici enaki, kadar imata natanko iste elemente).

Temu uvodu v množice je koristno dodati kakšno preprosto ugotovitev, npr.: $\mathscr{A} \cup \mathscr{B} = \mathscr{B} \cup \mathscr{A}$, $\mathscr{A} \cap \mathscr{B} = \mathscr{B} \cap \mathscr{A}$, $\mathscr{A} \subset \mathscr{A} \cup \mathscr{B}$, $\mathscr{A} \cap \mathscr{B} \subset \mathscr{A}$ ... Takšne trditve utemeljimo z logičnimi ekvivalencami oziroma implikacijami. Če npr. v logični implikaciji $\alpha \Rightarrow \alpha \vee \beta$ vstavimo »$a \in \mathscr{A}$« za α in »$a \in \mathscr{B}$« za β, vidimo, da velja za poljuben element a: $a \in \mathscr{A} \Rightarrow (a \in \mathscr{A}) \vee (a \in \mathscr{B})$, oziroma: $a \in \mathscr{A} \Rightarrow a \in \mathscr{A} \cup \mathscr{B}$, kar pomeni: $\mathscr{A} \subset \mathscr{A} \cup \mathscr{B}$. (Pri tem smo za $\mathscr{A}$ in $\mathscr{B}$ vzeli poljubni množici). Formalno sklepanje je seveda treba povezati z našim razmišljanjem in s slikami ravninskih množic; te slike tudi prispevajo k boljšemu dojemanju logičnih ekvivalenc in implikacij. — Pozneje lahko še marsikdaj omenimo — v povezavi z logiko — kakšen izrek iz *Algebre množic* v [3], in sicer brž ko ga pri matematiki rabimo.

Po vpeljavi pojma spremenljivke v 1. razredu (glej 3. razdelek) lahko že rabimo oznako: $\{x \in \mathscr{U};\ \alpha(x)\}$ za množico vseh tistih x iz univerzuma $\mathscr{U}$, ki zadoščajo pogoju $\alpha(x)$ (natančneje: za množico vseh tistih vrednosti za x, pri katerih je izjavna formula $\alpha(x)$ pravilna). Primer: $\{x \in \mathscr{R};\ a < x < b\}$ (ali kar $\{x;\ a < x < b\}$, če že vemo za izbrani univerzum).

Poljubni točki T v ravnini priredimo — pri izbranem koordinatnem sistemu — urejen par realnih števil (x, y). Vsej ravnini priredimo s tem množico vseh parov (x, y), to je $\{(x, y);\ (x \in \mathscr{R}) \wedge (y \in \mathscr{R})\}$, ki jo imenujemo *kartezični produkt* $\mathscr{R} \times \mathscr{R}$. Ob tem je koristno definirati kartezični produkt poljubnih dveh množic $\mathscr{A}$ in $\mathscr{B}$: $\mathscr{A} \times \mathscr{B} = \{(x, y);\ (x \in \mathscr{A}) \wedge$

$\wedge (y \in \mathscr{B})\}$ (pri tem x in y nista nujno števili). — Po preslikavi $(x, y) \to T(x, y)$ je ravnina slika produkta $\mathscr{R} \times \mathscr{R}$; za vajo naj dijaki upodobijo v ravnini še kakšne podmnožice iz $\mathscr{R} \times \mathscr{R}$, ki so tudi same produkti, npr.: $\mathscr{R}^+ \times \mathscr{R}^+$, $\mathscr{R} \times \mathscr{Z}$, $[a, b] \times [c, d]$... Seveda so slike teh množic odvisne od preslikave $(x, y) \to T(x, y)$ in s tem od izbire koordinatnega sistema. Tako je npr. slika produkta $[a, b] \times [c, d]$ zaprt pravokotnik, če smo izbrali pravokoten koordinatni sistem, oziroma zaprt romboid, če smo izbrali poševnokoten koordinatni sistem. — Znanje o kartezičnem produktu poglobimo v 4. razredu (glej [4], str. 6, 7).

Algebra množic. Razdelek s tem naslovom v [3] podaja zaokroženo obravnavo operacij in relacij med množicami. Izreki o množicah sledijo iz ustreznih logično pravilnih izjav (ki imajo tudi analogno obliko). Pri naši obravnavi še posebej upoštevamo, da sta dve množici $\mathscr{A}$ in $\mathscr{B}$ enaki natanko tedaj, ko je hkrati $\mathscr{A} \subset \mathscr{B}$ in $\mathscr{A} \supset \mathscr{B}$, oziroma ko velja za poljuben element x: $x \in \mathscr{A} \Leftrightarrow x \in \mathscr{B}$. Tako je npr. enakost $\mathscr{A} \cap (\mathscr{B} \cup \mathscr{C}) = (\mathscr{A} \cap \mathscr{B}) \cup (\mathscr{A} \cap \mathscr{C})$ utemeljena z naslednjo ekvivalenco, ki velja za vsak x (in ki sledi iz definicij preseka in unije ter iz distributivnosti v logiki):

$$x \in \mathscr{A} \cap (\mathscr{B} \cup \mathscr{C}) \Leftrightarrow (x \in \mathscr{A}) \wedge (x \in \mathscr{B} \cup \mathscr{C}) \Leftrightarrow (x \in \mathscr{A}) \wedge ((x \in \mathscr{B}) \vee (x \in \mathscr{C})) \Leftrightarrow$$
$$\Leftrightarrow ((x \in \mathscr{A}) \wedge (x \in \mathscr{B})) \vee ((x \in \mathscr{A}) \wedge (x \in \mathscr{C})) \Leftrightarrow$$
$$\Leftrightarrow (x \in \mathscr{A} \cap \mathscr{B}) \vee (x \in \mathscr{A} \cap \mathscr{C}) \Leftrightarrow x \in (\mathscr{A} \cap \mathscr{B}) \cup (\mathscr{A} \cap \mathscr{C})$$

Da postane ta dokaz še razumljivejši, ga povemo tudi z besedami kakor v [3], str. 114. — Podobno lahko obdelamo še druge izreke v algebri množic.

Vse podmnožice danega univerzuma $\mathscr{U}$ sestavljajo — glede na operacije med njimi — *Boolovo algebro* (glej [4], str. 29). Podmnožice iz $\mathscr{U}$ so elementi potenčne množice $\mathscr{P}\mathscr{U}$; tako lahko rečemo, da je množica $\mathscr{P}\mathscr{U}$ model Boolove algebre.

Dijaki, ki jih zanima aksiomatična teorija množic, pa naj vsekakor preberejo II. poglavje v [11].

Vloga množic pri pouku matematike. Z množicami se, zaradi njihovega temeljnega pomena, srečujemo povsod v matematiki; tu bom navedel le nekaj značilnih primerov takšnih srečanj. — Pouk algebre začnemo s pojmom *algebrske strukture*: imamo poljubno množico, v kateri so definirane operacije z določenimi lastnostmi. Pozneje se ukvarjamo z raznimi množicami na realni osi in v koordinatni ravnini, ki so določene z enačbami oziroma neenačbami. Množica rešitev razcepne enačbe $f(x)g(x) = 0$ je unija rešitev enačbe $f(x) = 0$ in enačbe $g(x) = 0$. Pri sistemu enačb $(f(x, y) = 0) \wedge (g(x, y) = 0)$ pa moramo vzeti presek rešitev za $f(x, y) = 0$ in za $g(x, y) = 0$; če morda iz $f(x, y) = 0$ sledi $g(x, y) = 0$, rešijo dani sistem kar vse rešitve enačbe $f(x, y) = 0$ (upoštevamo, da je $\mathscr{A} \cap \mathscr{B} = \mathscr{A}$, če je $\mathscr{A} \subset \mathscr{B}$). Ob sistemu: $(f(x) = 0) \wedge (|x - a| > b)$ naletimo hkrati na presek in unijo množic; uporabimo ustrezni distributivnostni zakon. Pri iracionalnih enačbah upoštevamo, da se po kvadriranju obeh strani množica rešitev v splošnem poveča (velja le implikacija: $f(x) = g(x) \Rightarrow [f(x)]^2 = [g(x)]^2$).

V geometriji radi pojmujemo premice, ravnine in prostor kot množice točk, saj nas že sam odnos »leži na (v)« s svojimi lastnostmi navaja k temu, da ga interpretiramo kot odnos pripadnosti oziroma podmnožice. Pri tem pojmujemo premice, ravnine in prostor še vedno kot celote, saj tudi nasploh pod množico elementov ne razumemo teh elementov samih, ampak nov objekt, ki te elemente vsebuje. — Poljubno ravnino lahko izrazimo kot unijo dveh zaprtih polravnin; zaprte (oziroma odprte) kote, trikotnike in mnogokotnike pa dobimo kot preseke zaprtih (oziroma odprtih) polravnin. — Tudi v geometriji marsikdaj rabimo kak račun iz algebre množic, npr.: če vzporedni ravnini Π in Φ sekata ravnino Σ, sta presečnici vzporedni: $(\Pi \cap \Sigma) \cap (\Phi \cap \Sigma) = (\Pi \cap \Phi) \cap \Sigma = \emptyset \cap \Sigma = \emptyset$.

6. Relacije in funkcije

Dvomestne relacije. Že v 1. razredu imamo pogosto opraviti s to ali ono dvomestno relacijo, to je z odnosom med dvema elementoma a in b neke množice $\mathscr{M}$. Zapis kakor »$a = b$« ali »$a < b$« je izjava, ki govori o dveh elementih iz $\mathscr{M}$ (ta je npr. kak kolobar) in ki je pravilna le tedaj, če sta a in b res v zapisanem odnosu.

Ob posameznih relacijah v algebri in v geometriji ($=$, $<$, $\leqq$, $|$, $\subset$, $||$, $\perp$ ...) navajamo posebne lastnosti relacij (refleksivnost, simetričnost, tranzitivnost, asimetričnost, antisimetričnost...), ki jih formuliramo tudi za splošno relacijo aRb; definicije iz [11], str. 74—76 povemo z besedami in jih utrdimo ob primerih.

Ko že srečamo grafe realnih funkcij, se lahko ustavimo še pri grafih relacij med realnimi števili. Graf ali slika neke relacije R je množica točk $T(x, y)$, ki v izbranem koordinatnem sistemu ustrezajo pogoju: xRy. (Natančneje vzeto, je graf relacije R množica urejenih parov $(x, y) \in \mathscr{R} \times \mathscr{R}$, ki ustrezajo pogoju: xRy*. Relacijo R razlagamo tudi kot lastnost urejenega para (x, y).) Na grafih relacij se lepo odražajo posebne lastnosti relacij (refleksivnost, simetričnost...). — Nasploh predstavlja vsaka množica točk v koordinatni ravnini relacijo med realnimi števili. Poljubno funkcijo $f: \mathscr{R} \to \mathscr{R}$ pa lahko označimo kot takšno relacijo med realnimi števili, katere graf seka poljubno navpičnico le v eni točki.

Ekvivalenčne relacije so vse tiste dvomestne relacije, ki so hkrati refleksivne, simetrične in tranzitivne. Takšna je npr. relacija enakosti (identitete) v poljubni množici $\mathscr{M}$ (trditev »$a = b$« pomeni, da a in b označujeta isti element). Pri drugih ekvivalenčnih relacijah pa sta lahko ekvivalentna tudi dva različna elementa; primeri: enakost ulomkov** ([1], str. 52), ekvivalenca enačb ([1], str. 105), kongruenca celih števil ([4], str. 24), lega točk na istem bregu dane premice ([5], str. 25), skladnost (oziroma podobnost) geometrijskih likov, vzporednost premic v prostoru ([5], str. 102), enakost vektorjev ([6], str. 40) — tu gre prvotno za ekvivalenco usmerjenih daljic.

Pri ekvivalenčnih relacijah je primerno vpeljati pojem ekvivalenčnega razreda ([11], str. 78) in potem upoštevati, da sta dva elementa ekvivalentna (po dani relaciji) natanko tedaj, ko sta v istem ekvivalenčnem razredu. Primere ekvivalenčnih razredov najdemo v [11], str. 82, 83. Dodajmo še, da so vektorji ekvivalenčni razredi usmerjenih daljic glede na že omenjeno ekvivalenco med njimi.

Splošni pojem funkcije $f: \mathscr{A} \to \mathscr{B}$ najdemo v [3], str. 116, in [4], str. 7, 8. (Primerjaj še [11], str. 84—87, kjer je funkcija strogo definirana kot enolična binarna relacija.) Pojem funkcije (preslikave) med poljubnima množicama $\mathscr{A}$ in $\mathscr{B}$ lahko omenimo tudi že v drugem ali celo v prvem razredu. V splošni okvir $f: \mathscr{A} \to \mathscr{B}$ sodijo poleg realnih funkcij ene spremenljivke še funkcije več spremenljivk, funkcije med končnimi množicami (kombinatorika!), razne geometrijske preslikave (zrcaljenja, projekcije...), vse algebrske operacije (glej [4], str. 9)... Če utegnemo, vpeljemo v 2. razredu še pojme *surjektivnosti*, *injektivnosti* in *bijektivnosti* poljubne funkcije $f: \mathscr{A} \to \mathscr{B}$ ter jih uporabljamo v konkretnih primerih. V [2], str. 19 srečamo pojem slike dane množice $\mathscr{M}$ pri transformaciji (funkciji) F: $\mathscr{M}' = F(\mathscr{M}) = \{F(T);\ T \in \mathscr{M}\}$.

Funkcija $f: \mathscr{A} \to \mathscr{B}$ ni določena le s predpisom f, ampak tudi z množicama $\mathscr{A}$ in $\mathscr{B}$. Tako npr. neka surjektivna funkcija izgubi svojo surjektivnost, če povečamo množico $\mathscr{B}$. Če pa definicijsko območje $\mathscr{A}$ zmanjšamo, dobimo zožitev prvotne funkcije; primer: zožitev kvadratne funkcije z množice kompleksnih števil na množico realnih števil.

---

* Enako definiramo graf relacije v poljubni množici $\mathscr{M}$; le namesto $\mathscr{R} \times \mathscr{R}$ imamo tedaj $\mathscr{M} \times \mathscr{M}$.

** Pri enakosti $a/b = c/d$ sta ulomka a/b in c/d kot para celih števil lahko različna.

Ekvipolenca množic je primer ekvivalenčne relacije med množicami ([3], str. 117, 118); lastnosti te relacije sledijo iz lastnosti bijektivnih funkcij. Obstoj ustreznih ekvivalenčnih razredov v splošnem ni zagotovljen ([11], str. 201), pač pa ti razredi obstajajo npr. pri končnih množicah in pri podmnožicah nekega danega univerzuma. — Zanimivo je priti do ugotovitev, kot npr.: $\mathcal{N} \sim \mathcal{Z}$, $\mathcal{N} \sim \mathcal{Q}$ ([14], str. 112), $(-1, 1) \sim \mathcal{R}$ (vzamemo funkcijo $y = \operatorname{tg}(\pi x/2)$), pa tudi do spoznanja, da množica $\mathcal{N}$ ni ekvipolentna intervalu $(0, 1]$ ([11], str. 193—195). — Neskončno množico lahko opredelimo kot takšno, ki je ekvipolentna neki svoji pravi podmnožici (primer: množica $\mathcal{N}$ je ekvipolentna množici vseh sodih števil). Poljubni dve neskončni množici seveda nista nujno ekvipolentni (primer: $\mathcal{N}$ in $\mathcal{R}$).

7. Razne miselne naloge

Naloge iz logike navadno zahtevajo, da iz danih predpostavk izvedemo razne posledice, ki naj bodo čim zanimivejše oziroma uporabnejše. Primer takšne naloge:

Kaj lahko povemo o Andreju, če vemo naslednje. Andrej bo kupil avto ali hišo. Če bo kupil avto, ne bo kupil hiše. Če bo kupil hišo, bo kupil avto.

Če označimo z α izjavo »Andrej bo kupil avto«, z β pa »Andrej bo kupil hišo«, se konjunkcija predpostavk izraža takole: $(\alpha \vee \beta) \wedge (\alpha \Rightarrow \neg \beta) \wedge (\beta \Rightarrow \alpha)$. Ta sestavljena izjava je pravilna le, če je α pravilen, β pa ne (to lahko ugotovimo npr. s tabelo pravilnosti). Odgovor je torej: Andrej bo kupil avto, ne pa hiše. — K rešitvi te naloge nam je pripomogla ugotovitev prostora pravilnosti za konjunkcijo predpostavk. Pogosto pa tudi uporabljamo dobro znane logične ekvivalence oziroma implikacije ([10], str. 40, 41, 71); za primer vzemimo reševanje naslednje naloge.

Vemo, da Tone ni kriv ali da Jaka ne govori resnice. Če pa je Tone kriv, Jaka govori resnico. Kaj lahko sklepamo iz tega?

Naj α pomeni »Tone je kriv«, β pa »Jaka govori resnico«. Konjunkcija predpostavk: $(\neg \alpha \vee \neg \beta) \wedge (\alpha \Rightarrow \beta)$ je logično ekvivalentna izjavi: $(\neg \alpha \vee \neg \beta) \wedge (\neg \alpha \vee \beta)$ oziroma: $\neg \alpha \vee (\neg \beta \wedge \beta)$ in s tem izjavi: $\neg \alpha$. Naš sklep se glasi: Tone ni kriv; ta sklep je celo ekvivalenten konjunkciji predpostavk.

V področje izjavnega računa spada tudi zanimiva naloga o ujetniku ljudožercev ([10], str. 47—49); tam je treba sestaviti izjavo s predpisanim prostorom pravilnosti.

Pri logičnem sklepanju je pogosto treba upoštevati predikatni račun, posebej še razne silogizme ([8], str. 100—117). V takšnem primeru lahko delamo tudi z množicami, saj skriva teorija množic v sebi ugotovitve predikatnega računa. — Naslednjo nalogo najdemo na strani 229 v [9].

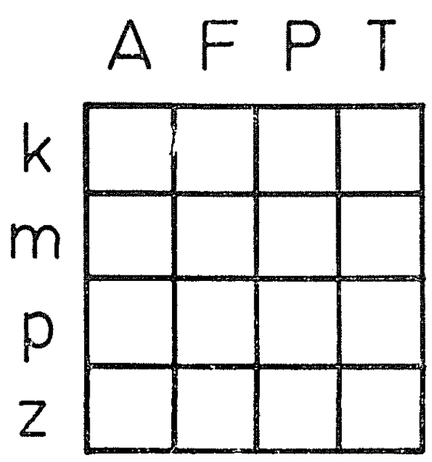
Iz naslednjih predpostavk izvedi sklep, pri katerem uporabiš vse predpostavke. — Vsi pravniki so premožni. Vsi pesniki so čustveni. Marko je pravnik. Noben čustven človek ni premožen.

Naj bo $\mathcal{A}$ množica pravnikov, $\mathcal{B}$ množica premožnih ljudi, $\mathcal{C}$ množica pesnikov, $\mathcal{D}$ množica čustvenih ljudi. Predpostavke nam povedo, da je $\mathcal{A} \subset \mathcal{B}$, $\mathcal{C} \subset \mathcal{D}$ in $\mathcal{B} \cap \mathcal{D} = \emptyset$; od tod sledi: $\mathcal{A} \cap \mathcal{C} = \emptyset$. Ker Marko spada v $\mathcal{A}$, ne spada v $\mathcal{C}$; torej Marko ni pesnik.

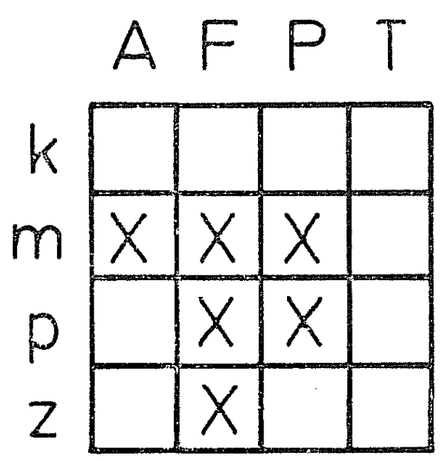
Naloge z bijektivnimi preslikavami končnih množic. Pri osnovni nalogi te vrste sta dani končni množici z istim številom elementov; treba je poiskati takšno bijektivno preslikavo med njima, ki zadošča določenim pogojem. (Teh pogojev je dovolj za enolično določitev preslikave.) Več naj pove naslednji primer.

Štirje možje: Andrej, France, Peter in Tone so po poklicu: kmet, mehanik, poštar in zdravnik (vendar ne nujno v tem vrstnem redu). O njih vemo med drugim naslednje. Mehanik je pred časom popravil Petrov avto in Andrejev motor. Zdravnik pozna Franceta že dve leti. Poštar se pogosteje oglasi pri Petru kakor pri Francetu. France je mehanikov bratranec. — Kaj je kdo po poklicu?

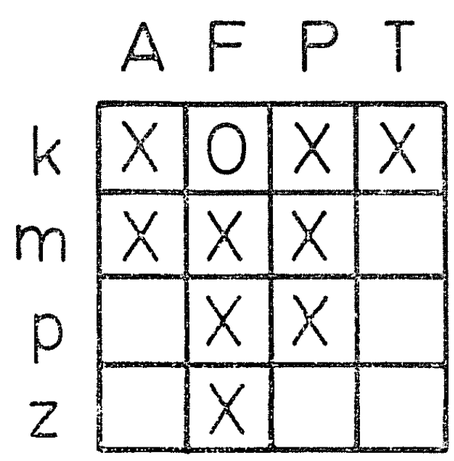
Treba je poiskati bijektivno preslikavo (priredbo) med množico imen: {A., F., P., T.} in množico poklicev: {k., m., p., z.}, pri kateri bodo izpolnjene navedene predpostavke. Graf iskane preslikave je pravzaprav neka (za sedaj neznana) množica štirih kvadratkov v velikem kvadratu na sl. 1.



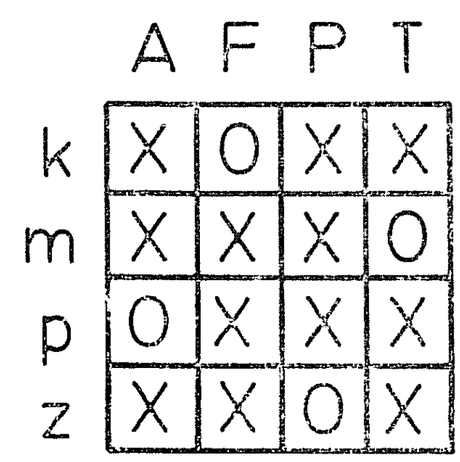
Sl. 1



Sl. 2



Sl. 3



Sl. 4

S križcem: × označimo na sl. 2 tiste kvadratke, ki ne morejo pripadati grafu. Iz navedenih predpostavk namreč sledi: niti Andrej niti Peter ni mehanik; France ni zdravnik; niti France niti Peter ni poštar; France ni mehanik. — Za Franceta ostane le ena možnost: po poklicu je kmet (na sl. 3 označimo to s krogcem: ○). Potem seveda nobeden od drugih treh mož ne more biti kmet (injektivnost naše preslikave!); tako imamo še tri nove križce na sl. 3. Peter je zdaj lahko le zdravnik. Ker potem niti Andrej niti Tone ne more biti zdravnik, je Andrej nujno poštar, Tone (ki ne more biti poštar) pa je mehanik. Krogci na sl. 4 podajajo rešitev naloge.

Mnogo nalog s tega oziroma širšega področja (večinoma precej težjih od naše) najdemo v zbirki [7], kjer so sistematično obdelane tudi metode reševanja.

LITERATURA

[1]—[4] F. Križanič, *Aritmetika, algebra in analiza za gimnazije I—IV*, Ljubljana, Državna založba Slovenije 1968—1971.

[1a]—[4a] I. Štalec (in drugi), *Zbirka vaj iz aritmetike, algebre in analize za I.—IV. razred gimnazije*, Ljubljana, Državna založba Slovenije 1975—1977.

[5] I. Pucelj-I. Štalec, *Geometrija za I. razred gimnazije*, Maribor, Založba Obzorja 1970.

[6] I. Pucelj-I. Štalec, *Geometrija za II. razred gimnazije*, Maribor, Založba Obzorja 1970.

[7] G. Bizám-J. Herczeg, *Logik macht Spass*, Budapest, Akadémiai Kiadó 1976.

[8] L.A. Kalužnin, *Što je matematička logika*, Zagreb, Školska knjiga 1971.

[9] S. Lipschutz, *Theory and Problems of Set Theory and Related Topics*, Schaum's Outline Series, New York, Mc Graw-Hill 1964.

[10] N. Prijatelj, *Uvod v matematično logiko*, Ljubljana, Mladinska knjiga 1973 (Knjižnica Sigma; 3b).

[11] N. Prijatelj, *Matematične strukture I*, Ljubljana, Mladinska knjiga 1971 (Knjižnica Sigma; 9a).

[12] I. Pucelj, *Neevklidične geometrije*, Ljubljana, Mladinska knjiga 1969 (Knjižnica Sigma; 18).

[13] I. Vidav, *Števila in matematične teorije*, Ljubljana, Mladinska knjiga 1975 (Knjižnica Sigma; 11a).

[14] I. Vidav, *Rešeni in nerešeni problemi matematike*, Ljubljana, Mladinska knjiga 1975 (Knjižnica Sigma; 1b).

Za nadaljnje branje so primerne še tele knjige:

[15] G. Polya, *Kako rešujemo probleme*, Ljubljana, DDU Univerzum 1976.

[16] R. Stoll, *Sets, Logic and Axiomatic Theories*, San Francisco, W.H. Freeman and comp. 1961.

[17] P. Suppes, *Introduction to Logic*, Princeton, D. Van Nostrand comp. 1957.

PREJELI SMO V OCENO

W. Krabs, Optimierung und Approximation. (Teubner Studienbücher), B. G. Teubner, Stuttgart, 1975, 208 strani.

Knjižica uvaja bralca v teorijo optimizacije, hkrati pa tej teoriji podreja teorijo aproksimacije. Sestavljajo jo tri neodvisna poglavja, posvečena linearnim, konveksnim in nelinearnim nalogam, v dodatku pa so zbrani nekateri pripomočki. Teorija je podprta s primeri, v zgledih iz uporabe iščejo poglavja tudi svoje iztočnice. Knjižica bo našla bralce med matematiki in med uporabniki.

M. Braun, Differential Equations and Their Applications. Applied Mathematical Sciences 15. Springer-Verlag. New York Heidelberg Berlin, 1975, 724 strani.

Ta zajetna skripta s preprostim in nenavadnim uvodom v teorijo in uporabo diferencialnih enačb so izšla v Springerjevi zbirki za uporabno matematiko. Naslovi poglavij: *Enačbe prvega reda*, *Enačbe drugega reda*, *Sistemi enačb prvega reda*, *Kvalitativna teorija diferencialnih enačb*, *Ločljive spremenljivke in Fourierove vrste* o posebnostih knjige ničesar ne povedo. Podrobnejši pregled pa pokaže, da je knjiga prav imenitno sestavljena. Preprosta je, ker ne terja posebnega predznanja, v poglavju o sistemih diferencialnih enačb razvije vso linearno algebro, kar je potrebuje, z determinantami vred. Elementarna je in v prvi vrsti namenjena uporabniku. Zaradi uporabnika, na katerega računa, pa je nenavadna. Pri uvodih te vrste smo pač navajeni na primere iz fizike in mehanike, ki spremljajo diferencialne enačbe od zibelke sem. M. Braun pa je v svojem delu zbral primere z vseh vetrov in opozoril, da je krog uporabnikov danes že mnogo širši. Pravzaprav je bil že pred vojno, pa nič zato. Na uporabnike ne bomo s prstom kazali, rajši naštejmo nekaj zgledov: ugotavljanje sladkorne bolezni, populacijska dinamika, teorija epidemij, širjenje kapavice, linearni model zunanje politike.

Za ilustracijo izberimo kar Richardsonov model vojne, ki je v knjigi povzet po njegovem članku Generalized foreign politics iz leta 1936. Medsebojne odnose dveh dežel ali dveh blokov opisuje v tem preprostem modelu sistem diferencialnih enačb

$$\dot{x} = ay - \alpha x + p \qquad \dot{y} = bx - \beta y + q$$

x meri vojaško moč prve, y druge države. Prvi člen na desni strani (z latinskim koeficientom) meri obrambno nujo, odgovor na potencial nasprotne strani, Drugi člen (z grškim koeficientom) meri gospodarsko moč države. Hitrost oboroževanja je pač tem večja, čim večja je obrambna nuja in čim manjši so stroški oboroževanja. Preprosti model privzema, da sta obe funkciji linearni. Desna stran vsake enačbe pa ima še konstantni člen, ta je na moč zanimiv in težko merljiv, izraža pa jezo, ki jo država kuha na nasprotno stranko. Kar vzemimo, da sta svobodna člena p in q pozitivna, v začetnem trenutku pa obe državi razoroženi ($x = y = 0$). Hitrosti oboroževanja sta kljub razorožitvi različni od 0 in oborožewalna tekma se nemudoma začne. Pa zanemarimo jezo in stroške, upoštevajmo le željo po obrambi. Iz sistema $\dot{x} = ay$, $\dot{y} = bx$, kaj hitro izvemo, da $x(t)$ in $y(t)$ naraščata čez vsako mejo. V splošnem ima sistem ravnovesno rešitev (točko mirovanja) s koordinatama $(aq + \beta p)/(\alpha\beta - ab)$, $(bp + \alpha q)/(\alpha\beta - ab)$. Točka je stabilna (stabilni vozel), če je $\alpha\beta - ab > 0$, nestabilna (sedlo), če je $\alpha\beta - ab < 0$.

Numerične metode za reševanje diferencialnih enačb spremlja program, zapisan v preprostem programskem jeziku APL, semtertja pa v fortranu.

Knjiga bo zaradi svojih odlik dobrodošel priročnik tudi matematiku, preprosti jezik je mikaven tudi zanj, številni primeri pa ga bodo zanimali vsaj toliko kot uporabnike. Bralce bo prav gotovo našla tudi med nami. To in ono iz filozofiranja in iz zemljepisa (Fiume) ji bomo pa morali spregledati.

France Križanič

Amorphous Semiconductors '76, ed. by I. Kósza Somogyi, Proceedings of the International Conference, Balatonfüred, Hungary, 20—25 September 1976, Budapest, Akadémiai Kiadó, 1977, 565 str.

Amorfni polprevodniki so v zadnjih petnajstih letih postali zanimivi za znanstvene raziskave in za uporabo, na primer za spominske elemente. Značilnost amorfnih polprevodnikov je pomanjkanje ureditve dolgega dosega, kar otežuje teorijsko obravnavo, kot tudi velike težave pri reproducibilnosti materialov. Prav slaba reproducibilnost je ovira, da se amorfni polprevodniki niso bolj uveljavili.

Knjiga vsebuje vabljena predavanja in nekaj referatov z mednarodnega kongresa o amorfnih polprevodnikih, tretjega v vrsti vzhodnoevropskih kongresov s tega področja.

Vsebina knjige je razdeljena na dvanajst poglavij. Prvo opisuje osnovni mehanizem spominskih elementov, izdelanih iz raznih stekel, to je preklop iz stanja majhne prevodnosti v stanje velike prevodnosti. Drugo poglavje obravnava zapis optičnih informacij v halkogenidnih steklih. V tretjem poglavju je zbrana teorija amorfnih polprevodnikov. Dve poglavji podajata optične lastnosti amorfnih polprevodnikov, zlasti optično absorpcijo na elektronskih pasovih in fotoluminiscenco. Štiri poglavja so namenjena električnim lastnostim. Ta poglavja vsebujejo predvsem predavanja o frekvenčni odvisnosti prevodnosti, fotoprevodnosti, fotoefektu in prevodnosti pri velikih električnih poljih. V dveh poglavjih sta opisani še struktura amorfnih snovi in spremembe strukture pod vplivom svetlobe, električnega polja in nekaterih organskih spojin.

Kot vsi zapisi s konferenc je tudi ta knjiga namenjena le strokovnjakom, ki delajo na področju amorfnih polprevodnikov.

Igor Vilfan

Béla Andrásfai: Introductory graph theory, Akadémiai Kiadó, Budapest, 1977, 268 str.

V madžarskem jeziku je knjiga izšla že leta 1969 in je presenetljivo, šele prvi madžarski učbenik teorije grafov. Znano je, da so ravno madžarski matematiki razvili velik del te matematične veje, saj je na primer prva monografija teorije grafov v svetu, izpod peresa madžarskega matematika Dénesa Königa izšla že leta 1936, vendar v nemškem jeziku. Velika škoda je, da je knjiga Béle Andrásfaia tako pozno postala dostopna širšemu krogu bralcev.

Knjiga je razdeljena na sedem poglavij. V prvem so nanizani osnovni pojmi o grafih. V drugem poglavju avtor obravnava drevesa, predvsem vpeta drevesa grafov. Naslednji dve poglavji govorita o poteh in ciklih v grafih, tretje je posvečeno Eulerjevim, četrto pa Hamiltonovim grafom. V petem poglavju se seznanimo s faktorizacijo grafov in s problemom prirejanja. Seveda se pri slednjem avtor ne more izogniti znani »madžarski metodi«. Najobsežnejše je šesto poglavje, o ekstremalnih grafih, iz katerega kar izžareva izvrstna madžarska šola teorije grafov.

Knjigi daje nenavaden pečat tudi samosvoja notranja struktura. Lahko bi namreč nosila naslov: »334 rešenih nalog teorije grafov«, ravno toliko je v njej rešenih vaj, problemov in dokazanih izrekov. Avtor nenehno navaja bralca na samostojno razmišljanje. Z vajami in problemi vodi bralca do novih problemov in zanimivih izrekov. Bralec lahko sproti preverja svoje znanje z reševanjem problemov iz rekreacijske matematike. V veliko pomoč pa mu je preko 260 slik, ki skrbijo za nazorno predstavo.

Čeprav je večina nalog rešena že sproti, pa so na koncu vsakega poglavja zbrane dodatne naloge. Rešitve teh nalog pa sestavljajo zajetno sedmo poglavje.

Ravno zgradba te izvrstne knjige, predvsem pa dejstvo, da so vse naloge v njej tudi rešene, zasenči morebitne pomanjkljivosti. Očitali bi lahko kvečjemu nepopoln spisek literature na koncu knjige, v katerem iz razumljivih razlogov ni novejših del in ki je morebiti za dlako preveč madžarsko pobarvan. Drugi očitek, češ da je knjiga preozko usmerjena, pa spodbija avtor sam, ki v uvodu najavlja drugi del.

Učbenik je primeren za vsakogar, ki ima veselje in voljo, da se sam kaj nauči, posebej če rad rešuje težje naloge.

Tomaž Pisanski