Dokazovanje z metodo supozicije

1. Osnovna dejavnost v matematiki je dokazovanje. Pri dokazovanju izhajamo iz že znanih izrekov in nato izpeljujemo nove in nove matematične resnice. V tej smeri seveda ni konca, vedno se da formulirati novo trditev, ki jo je treba dokazati. Kaj pa v obratni smeri? Pri dokazu vsakega izreka se sklicujemo na že dokazane izreke in teh je seveda le končno mnogo. Tako pridemo do prvega dokazanega izreka. V tem prvem dokazu se lahko sklicujemo le na trditve, ki smo jih privzeli brez dokaza – to so *aksiomi*. Naslednja stvar, ki jo je treba omeniti, pa so pravila sklepanja, ki jih pri izpeljevanju uporabljamo. Le-ta imajo obliko

$$\frac{A_1 \ldots . A_n}{B}$$

uporabljamo pa jih takole: če smo že dokazali izreke A_1, ..., A_n, potem lahko k teoriji dodamo nov izrek B.

Seveda pa se vse, kar je v zvezi z dokazovanjem, tudi zapisuje, to je, dogaja se v okviru nekega jezika.

Če torej želimo opredeliti pojem dokaza ali pojem dokazane trditve, moramo:
– opisati jezik, v katerem bomo izrazili našo teorijo,
– našteti vsa pravila sklepanja, ki jih smemo uporabljati,
– izmed trditev izbrati nekatere za aksiome,
– če imamo tudi definicije, moramo formulirati njihovo konstruiranje.

Vse, kar smo do sedaj našteli, nam že namiguje, da ne bo mogoče opredeliti najbolj splošnega pojma dokaza v matematiki, pač pa bomo skušali opredeliti pojem dokaza za kakšen majhen del matematike, to je, za kakšno enostavno matematično teorijo.

2. V tem sestavku se bomo ukvarjali z lastnostmi negacije in implikacije ter z njunimi medsebojnimi odnosi. Tej teoriji bomo rekli izjavni račun.

Da bi lahko opisali jezik, moramo najprej našteti znake, ki jih lahko uporabljamo:
– znaki za izjavne spremenljivke so: p, q, r, s, t, u, v
– znak za negacijo: N
– znak za implikacijo: C

Vsakemu končnemu zaporedju znakov pravimo *izraz*. Med izrazi bomo izbrali nekatere, rekli jim bomo formule, ki ustrezajo stavkom v pogovornem jeziku:
a) Vsaka izjavna spremenljivka je formula.
b) Če je izraz A formula, potem je tudi izraz NA formula.
c) Če sta izraza A in B formuli, potem je tudi izraz CAB formula.
d) Izraz je formula, če je dobljen po končnem številu uporab točk *a)*, *b)* in *c)*.

To, da pišemo znak za povezavo pred obema argumentoma, imenujemo *poljska notacija*, ki jo je prvi uporabljal Lukasiewicz. Formulo "Np" preberemo "*ni res, da p*" ali "*ni p*". Formulo "Cpq" preberemo "*če p, potem q*".

Zdaj želimo doseči, da bo možno dokazovati v naši teoriji formulo $CpCCpqq$ takole:

Recimo, da velja p. Pri tej predpostavki privzemimo še, da velja Cpq. Od tod sklepamo, da velja q. Ker pri predpostavki Cpq velja q, velja $CCpqq$. Iz p torej sledi $CCpqq$, zato velja $CpCCpqq$.

Ta dokaz bomo v formalizmu zapisali takole:

1	$. p$	PR (predpostavka)
2	$. . Cpq$	PR
3	$. . q$	EC 1, 2 (vrstica 3 sledi iz vrstic 1 in 2 z opustitvijo – Eliminacijo – znaka C)
4	$. CCpqq$	IC 2, 3 (vrstica 4 sledi iz vrstic 2 in 3 po pravilu uvedbe – Introdukcije – znaka C)
5	$CpCCpqq$	IC 1, 4

Pika (oziroma pike) pred formulo zaznamuje odvisnost formule od predpostavke, ki to piko uvaja. Formule, ki nimajo nobene pike, so dokazane; formule, pred katerimi je ena pika, veljajo pri pogoju, da velja predpostavka, ki to piko uvaja. Formule, pred katerimi je n pik, veljajo pri pogoju, da veljajo vse predpostavke, ki uvajajo 1, 2, ..., n pik. Formule, ki imajo pred seboj n pik, imenujemo *domena predpostavke*, ki prva uvaja n pik. Formule, ki imajo $n-1$ pik pred seboj, sestavljajo *neposredno naddomeno*, formule z $n+1$ pikami pred seboj pa *neposredno poddomeno* formule, ki uvaja n pik. Izraz poddomena (oz. naddomena) je rezerviran za množico formul, pred katerimi je večje (manjše) število pik kot pri dani predpostavki. Formula, ki velja v naddomeni, velja tudi v poddomeni.

V zvezi z negacijo bomo uporabljali še naslednjo obliko pravila *reductio ad absurdum*: če v domeni predpostavke NA veljata formuli B in NB, potem izjava A velja v neposredni naddomeni predpostavke NA.

Tako dokaz formule $CCNpNqCqp$ izgleda takole:

1	$. CNpNq$	PR
2	$. . q$	PR
3	$. . . Np$	PR
4	$. . . Nq$	EC 3, 1
5	$. . p$	EN 3, 2, 4 (vrstico 5 smo dobili iz vrstic 3,2 in 4 z eliminacijo negacije)
6	$. Cqp$	IC 2, 5
7	$CCNpNqCqp$	IC 1, 6

(Pri pravilu reductio ad absurdum sklepano z NP na p, to je, pri sklepu eliminiramo znak N, zato oznaka EN).

Pravili opustitve (eliminacije) in uvedbe (introdukcije) za implikacijo formuliramo takole:

a) Če veljata A in CAB, velja tudi B. Število pik pred formulo B je enako večjemu od števila pik pred formulama A oz. CAB.
b) Če v domeni predpostavke A velja formula B, potem lahko dodamo formulo CAB v neposredno naddomeno predpostavke A.

Sedaj lahko opredelimo pojem dokaza za našo teorijo: dokaz je zaporedje formul, vsaka

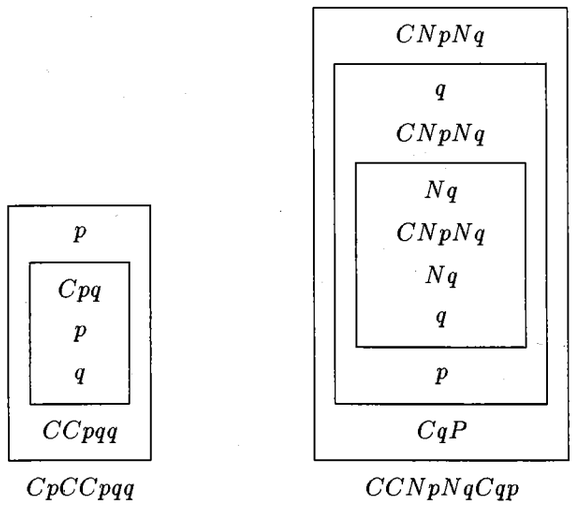
izmed njih je predpostavka ali pa je dobljena iz predhodnih formul z enim od treh opisanih pravil sklepanja.

Če je zadnja formula veljavna v ničelni domeni (v domeni brez pike), rečemo, da je dano zaporednje dokaz te zadnje formule. Formula je dokazljiva, če obstaja kakšen dokaz zanjo.

Analiza dokaza, označba vrstic in pike niso del dokaza, pač pa takšen zapis povečuje preglednost in razumljivost dokaza.

Zanimivost tega sistema je, da nima aksiomov.

Ta sistem je izdelal poljski logik Stanislaw Jaskowski leta 1926, katerega je na način sklepanja opozoril Jan Lukasiewicz. V prvotni obliki sta zgornji izpeljavi izgledali takole:



Nekateri izrazi, kot so 'p', 'q', '$CNpNq$', ki so zapisani zunaj nekega pravokotnika, so bili zapisani ponovno znotraj pravokotnika, kar se je z dopolnilom pravil pokazalo za odveč. Seveda pa pravokotniki lepo ponazarjajo domeno predpostavke.

Dopolnimo naslednje dokaze z analizo ali manjkajočimi formulami:

a)

1	$.\,NNp$	?
2	$..\,Np$	?
3	$..\,Np$	?
4	$CNNpp$	?

b)

1	?	PR
2	?	PR
3	?	PR
4	?	$EN\ 3,3,2$
5	?	$EN\ 2,1,4$
6	$CpNNp$	$IC\ 1,5$

a) Za prvo in drugo vrstico je razlaga PR, saj uvajata pike. V domeni predpostavke $Np(2)$ veljata tako $Np(2)$ kot $NNp(1)$, zato je razlaga za tretjo vrstico $EN\ 2,2,1$, četrta vrstica uvaja znak C, zato $IC\ 1,3$.

b) Šesta vrstica nam pove, da v prvi oz. peti vrstici manjkata "$.\,p$" oz. "$.\,NNp$". Peta vrstica nam pove, da imamo v drugi vrstici "$..\,NNNp$" in da je četrta vrstica negacija

prve, to je "$..\,Np$", mora pa imeti dve piki. Tretja vrstica ima tri pike, ker vsaka predpostavka uvaja dodatno piko, formulo pa dobimo iz formule druge vrstice, če ji odstranimo en "N": "$...\,NNp$".

V našem sistemu (sistem naravne dedukcije, ki ga je uvedel poljski logik Stanislaw Jaskovski) smo imeli tri pravila sklepanja, oziroma štiri, če računamo še uvedbo predpostavke. Lahko bi dodali še kakšno pravilo. To bi skrajšalo nekatere dokaze. Zanimivo pa je, da že s temi pravili lahko dokažemo vse tavtologije, v katerih nastopajo le negacije in implikacije. Temu pravimo, da je naš sistem *popoln*. Obratno, da lahko dokažemo le tavtologije, pomeni, da je naš sistem *zdrav* ali *konsistenten*.

Rešimo še naslednjo nalogo: Imamo tri ljudi. Vemo, da je kvečjemu eden od njih lažnivec, to je, da se včasih tudi zlaže. Pokažimo, da lahko z vprašanjem *"Ali je prvi resničnik?"*, ki ga postavimo drugemu, najdemo človeka, ki vedno govori resnico.
Kako bi formulirali problem samo z negacijo in implikacijo? Najprej uvedimo okrajšave:

p = *Prva oseba je resničnik.*
q = *Druga oseba je resničnik.*
r = *Tretja oseba je resničnik.*

Kako bi zapisali dejstvo, da je kvečjemu eden lažnivec? Sestavili bi ga iz treh oz. šestih pogojev: *Če je i lažnivec, potem j $(i \neq j)$ ni lažnivec:*

$$CNpq,\ CNpr,\ CNqp,\ CNqr,\ CNrp,\ CNrq.$$

Če sedaj drugega človeka vprašamo, ali je prvi resničnik, imamo dve možnosti:

a) da reče "da", tedaj vemo še Cqp;
b) da reče "ne", tedaj vemo še $CqNp$.

Vse te formule imajo vlogo aksiomov in so veljavne v vsaki domeni.

1	Cqp	odgovor "da"
2	$CNpq$	eden od pogojev naloge
3	$.\,Np$	PR
4	$.\,q$	$EC\ 3,2$
5	$.\,p$	$EC\ 4,1$
6	p	$EN\ 3,5,3$

V tem primeru je prva oseba resničnik.

Sklepanje v drugem primeru je takole:

1	$CqNp$	odgovor "ne"
2	$CNrp$	pogoj naloge
3	$CNrq$	pogoj naloge
4	$.\,Nr$	PR
5	$.\,p$	$EC\ 4,2$
6	$.\,q$	$EC\ 4,3$
7	$.\,Np$	$EC\ 7,1$
8	r	$EN\ 4,5,7$

V tem primeru je tretja oseba resničnik.

Vaja: Zadnja dva dokaza prevedi v pogovorni jezik.

Naloge

1) Dopolni dokaze z analizo:

a)

1	$.p$	?
2	$..Cpq$	?
3	$..q$	?
4	$.CCpqq$	?
5	$CpCCpqq$	?

b)

1	$.p$	?
2	$..p$	?
3	$.Cqp$	?
4	$CpCqp$	?

c)

1	$.p$	?
2	$..Np$	?
3	$...Nq$	?
4	$..q$	?
5	$.CNpq$	?
6	$CpCNpq$	?

2) Dopolni dokaze

a)

1	$.Cpq$	PR
2	?	PR
3	?	PR
4	?	$EC\ 3,1$
5	?	$EC\ 2,4$
6	?	$IC\ 3,5$
7	?	$IC\ 2,6$
8	$CCpqCCqrCpr$	$IC\ 1,7$

b)

1	?	PR
2	?	PR
3	?	$EC\ 2,1$
4	?	$EN\ 2,3,2$
5	$CCNppp$	$IC\ 1,4$

c)

1	$.CNpNCrNNr$	PR
2	$..Np$	PR
3	?	$EC\ 2,1$
4	?	PR
5	?	PR
6	?	PR
7	?	$EN\ 6,6,5$
8	?	$EN\ 5,7,6$
9	?	$IC\ 4,8$
10	$.p$	$EN\ 2,9,3$
11	$CCNpNCrNNrp$	$IC\ 1,10$

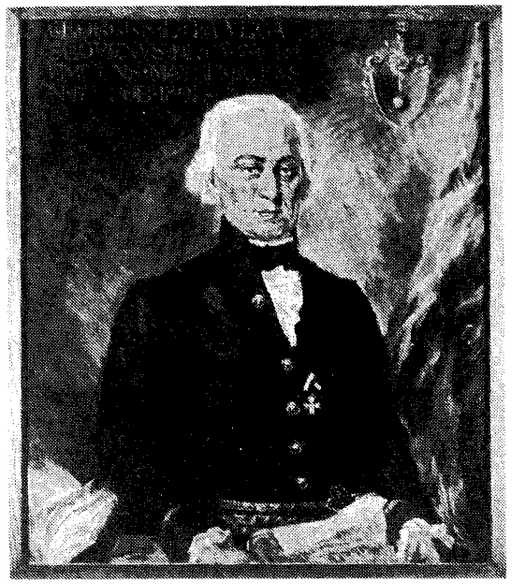
Izidor Hafner

DRUŠTVO MATEMATIKOV, FIZIKOV IN ASTRONOMOV SLOVENIJE

ZAVOD REPUBLIKE SLOVENIJE ZA ŠOLSTVO IN ŠPORT

BILTEN

31. tekmovanja za ZLATO VEGOVO PRIZNANJE v šolskem letu 1994/95



Ljubljana, Maribor, Celje,
Novo mesto, Koper, Nova Gorica,
20. 5. 1995