Logika in množice
NEDOKONČANI ZAPISKI

Andrej Bauer

4. november 2019

Kazalo

1 Uvod **5**

2 Logika in pravila sklepanja **7**
2.1 Kaj je matematični dokaz? 7
2.2 Simbolni zapis matematičnih izjav 10
2.3 Kako beremo in pišemo simbolni zapis 13
2.4 Definicije 15
2.5 Pravila sklepanja in dokazi 16
2.6 Izjavni račun 17
2.6.1 Konjunkcija 17
2.6.2 Implikacija 17
2.6.3 Disjunkcija 18
2.6.4 Resnica in neresnica 20
2.6.5 Ekvivalenca 20
2.6.6 Negacija 21
2.6.7 Aksiom o izključenem tretjem 22
2.7 Predikatni račun 25
2.7.1 Proste in vezane spremenljivke 26
2.7.2 Substitucija 27
2.7.3 Univerzalni kvantifikator 28
2.7.4 Eksistenčni kvantifikator 30
2.7.5 Enakost in reševanje enačb 31

Poglavje 1

Uvod

Glavni namen predmet Logika in množice v prvem letniku študija matematike je študente naučiti, kaj je matematični dokaz, kako se dokaze bere, zapiše in kako analizira. To je področje, s katerim se ukvarja matematična logika. Poleg tega pri predmetu spoznamo osnove teorije množic in diskretne matematike.

Za semesterski predmet z dvema urama predavanj in dvema urama vaj je to zelo ambiciozen program. Najučinkovitejši recept za uspeh je tisti, ki ga študenti ne marajo: učite se sproti, sprašujte predavatelja in asistente, trkajte na vrata njihovih pisarn tudi takrat, ko nimajo govorilnih ur.

Ti zapiski bodo nastajali sproti. Opozarjam vas, da je vsebujejo napake. Odkrivanje napak je sestavni del učnega procesa. Zelo vam bomo hvaležni, če nam boste odkrite napake sporočili, da jih popravimo. Matiji Pretnarju se zahvaljujem za skrbno odpravljanje napak. Vse ki so ostale, so moja last.

Andrej Bauer

Poglavje 2

Logika in pravila sklepanja

2.1 Kaj je matematični dokaz?

V srednji šoli se dijaki pri matematiki učijo, *kako* se kaj izračuna. Na univerzi imajo študentje matematike pred seboj zahtevnejšo nalogo: poleg *kako* morajo vedeti tudi *zakaj*. Od njih se pričakuje, da bodo računske postopke znali tudi utemeljiti, ne pa samo slediti pravilom, ki jih je predpisal učitelj. Razumeti morajo dokaze znamenitih izrekov in sami poiskati dokaze preprostih izjav. Da bi se lažje spopadli s temi novimi nalogami, bomo prvi del predmeta Logika in množice posvetili matematični infrastrukturi: izjavam, pravilom sklepanja in dokazom. Učili se bomo, kako pišemo dokaze, kako jih analiziramo in kako jih sami poiščemo.

Osrednji pojem matematične aktivnosti je *dokaz*. Namen dokaza je s pomočjo točno določenih in vnaprej dogovorjenih *pravil sklepanja* utemeljiti neko matematično *izjavo*. Načeloma mora dokaz vsebovati vse podrobnosti in natanko opisati posamezne korake sklepanja, ki privedejo do želene matematične izjave. Ker bi bili taki dokazi zelo dolgi in bi vsebovali nezanimive podrobnosti, matematiki običajno predstavijo samo oris ali glavno zamisel dokaza. Izkušenemu matematiku to zadošča, saj zna oris sam dopolniti do pravega dokaza. Matematik začetnik seveda potrebuje več podrobnosti. Poglejmo si primer.

Izrek 2.1 *Za vsako naravno število n je $n^3 - n$ deljivo s 3.*

Po kratkem premisleku bi izkušeni matematik zapisal:

Dokaz. Očitno. ∎

To ni dokaz, izkušeni matematik nam le dopoveduje, da je (zanj) izrek zelo lahek in da nima smisla izgubljati časa s pisanjem dokaza. Začetnik, ki težko razume že sam izrek, bo ob takem "dokazu" seveda zgrožen. Verjetno bo najprej preizkusil izrek na nekaj primerih:

$$1^3 - 1 = 0,$$
$$2^3 - 2 = 8 - 2 = 6,$$
$$3^3 - 3 = 27 - 4 = 24,$$
$$4^3 - 4 = 64 - 4 = 60.$$

Res dobivamo večkratnike števila 3. Ali smo izrek s tem dokazali? Seveda ne! Preizkusili smo le štiri primere, ostane pa jih še neskončno mnogo. Kdor misli, da lahko iz nekaj primerov sklepa na splošno veljavnost, naj v poduk vzame naslednjo nalogo.

Naloga 2.2 Ali je $n^2 - n + 41$ praštevilo za vsako naravno število n?

Ko izkušenega matematika prosimo, da naj nam vsaj pojasni idejo dokaza, zapiše:

> *Dokaz.* Število $n^3 - n$ je zmnožek treh zaporednih naravnih števil. ∎

To še vedno ni dokaz, ampak samo namig. Starejši študenti matematike pa bi iz namiga morali znati sestaviti naslednji dokaz:

> *Dokaz.* Ker je $n^3 - n = (n-1) \cdot n \cdot (n+1)$, je $n^3 - n$ zmnožek treh zaporednih naravnih števil, od katerih je eno deljivo s 3, torej je tudi $n^3 - n$ deljivo s 3. ∎

Mimogrede, znak ∎ označuje konec dokaza. Čeprav bi bila večina matematikov s tem dokazom zadovoljna, bi morali za popoln dokaz preveriti še nekaj podrobnosti:

1. Ali res velja $n^3 - n = (n-1) \cdot n \cdot (n+1)$?
2. Ali je res, da je izmed treh zaporednih naravnih števil eno vedno deljivo s 3?
3. Ali je res, da je zmnožek treh števil deljiv s 3, če je eno od števil deljivo s 3?

S srednješolskim znanjem algebre ugotovimo, da je odgovor na prvo vprašanje pritrdilen. Tudi odgovora na drugo in tretje vprašanje sta očitno pritrdilna, mar ne? To pa ne pomeni, da ju ni treba dokazati. Nasprotno, zgodovina matematike nas uči, da moramo prav "očitne" izjave še posebej skrbno preveriti.

Naloga 2.3 Kakšno je tvoje mnenje o resničnosti naslednjih izjav? Vprašaj starejše kolege, asistente in učitelje, kaj menijo oni. Ali znajo svoje mnenje utemeljiti z dokazi?

1. Sodih števil je manj kot naravnih števil.
2. Kroglo je mogoče razdeliti na pet delov tako, da lahko iz njih sestavimo dve krogli, ki sta enako veliki kot prvotna krogla.
3. Sklenjena krivulja v ravnini, ki ne seka same sebe, razdeli ravnino na dve območji, eno omejeno in eno neomejeno.
4. S krivuljo ne moremo prekriti notranjosti kvadrata.
5. Če ravnino razdelimo na tri območja, potem zagotovo obstaja točka, ki je dvomeja in ni tromeja med območji.

Vrnimo s k izreku 2.1. Če dokaz zapišemo preveč podrobno, postane dolgočasen in nerazumljiv:

Dokaz. Naj bo n poljubno naravno število. Tedaj velja

$$\begin{aligned} n^3 - n = n \cdot n^2 - n \cdot 1 = n(n^2 - 1) = n(n^2 + 0 - 1) \\ = n(n^2 + (n - n) - 1) = n(n^2 + (1 \cdot n - n \cdot 1) - 1) \\ = n(n^2 - n \cdot 1 + 1 \cdot n - 1) = n(n \cdot n - n \cdot 1 + 1 \cdot n - 1 \cdot 1) \\ = n(n(n-1) + 1 \cdot (n-1)) = n((n+1)(n-1)) \\ = n((n-1)(n+1)) = (n(n-1))(n+1) = (n-1)n(n+1). \end{aligned}$$

Vidimo, da je $n^3 - n$ zmnožek treh zaporednih naravnih števil. Dokažimo, da je eno od njih deljivo s 3. Število n lahko enolično zapišemo kot $n = 3k + r$, kjer je k naravno število in $r = 0$, $r = 1$ ali $r = 2$. Obravavajmo tri primere:

- če je $r = 0$, je $n = 3k$, zato je n deljiv s 3,
- če je $r = 1$, je $n - 1 = (3k + 1) - 1 = 3k + (1 - 1) = 3k + 0 = 3k$, zato je $n - 1$ deljiv s 3,
- če je $r = 2$, je $n + 1 = (3k + 2) + 1 = 3k + (2 + 1) = 3k + 3 = 3k + 3 \cdot 1 = 3(k + 1)$, zato je $n + 1$ deljiv s 3.

Vemo torej, da je $n - 1$, n ali $n + 1$ deljiv s 3. Obravnavamo tri primere:

- Če je $n - 1$ deljiv s 3, tedaj obstaja naravno število k, da je $n - 1 = 3k$. V tem primeru je $(n - 1)n(n + 1) = (3k)n(n + 1) = 3(kn(n + 1))$, zato je $(n - 1)n(n + 1)$ deljivo s 3.
- Če je n deljiv s 3, tedaj obstaja naravno število k, da je $n = 3k$. V tem primeru je $(n - 1)n(n + 1) = (n - 1)(3k)n(n + 1) = (3k)(n - 1)(n + 1) = 3(k(n - 1)(n + 1))$, zato je $(n - 1)n(n + 1)$ deljivo s 3.
- Če je $n + 1$ deljiv s 3, tedaj obstaja naravno število k, da je $n + 1 = 3k$. V tem primeru je $(n - 1)n(n + 1) = (n - 1)n(3k) = (n - 1)(3k)n = (3k)(n - 1)n = 3(k(n - 1)n)$, zato je $(n - 1)n(n + 1)$ deljivo s 3.

V vsakem primeru je $(n - 1)n(n + 1)$ deljivo s 3. Ker smo dokazali, da je $n^3 = n = (n - 1)n(n + 1)$, je tudi $n^3 - n$ deljivo s 3. ∎

Naloga 2.4 S kolegi se igraj naslednjo igro.[1] Prvi igralec v zgornjem dokazu poišče korak, ki ga je treba še dodatno utemeljiti. Drugi igralec ga utemelji. Nato prvi igralec poišče nov korak, ki ga je treba še dodatno utemeljiti in igra se ponovi. Drugi igralec zmaga, če zna vse korake utemeljiti, v nasprotnem primeru zmaga prvi igralec. Ali lahko igra traja neskončno dolgo?

Matematični dokaz ima dvojno vlogo. Po eni strani je utemeljitev matematične izjave, zato mora biti čim bolj podroben. V idealnem primeru bi bil dokaz zapisan tako, da bi lahko njegovo pravilnost preverili mehansko, z računalnikom. Po drugi strani je dokaz sredstvo za komunikacijo idej med matematiki, zato mora vsebovati ravno pravo mero podrobnosti. Mera pa je odvisna od tega, komu je dokaz namenjen. Te socialne komponente se študenti učijo skozi prakso v toku študija. Dokazu kot povsem matematičnemu

[1] Igranje odsvetujemo zunaj prostorov Fakultete za matematiko in fiziko.

pojmu pa se bomo posvetili prav pri predmetu Logika in množice. Pojasnili bomo, kaj je dokaz kot matematični konstrukt in kako ga zapišemo tako podrobno, da je res mehansko preverljiv. Naučili se bomo tudi nekaj preprostih tehnik iskanja dokazov, ki pa še zdaleč ne bodo zadostovale za reševanje zares zanimivih matematičnih problemov, ki zahtevajo poglobljeno znanje, vztrajnost, kanček talenta in nekaj sreče.

2.2 Simbolni zapis matematičnih izjav

Matematična *izjava* je smiselno besedilo, ki izraža kako lastnost ali razmerje med matematičnimi objekti (števili, liki, funkcijami, množicami itn.). Primeri matematičnih izjav:

- $2 + 2 = 5$.
- Točke P, Q in R so kolinearne.
- Enačba $x^2 + 1 = 0$ nima realnih rešitev.
- $a > 5$.
- $\phi \vee \psi \Rightarrow (\neg\phi \Rightarrow \psi)$.

Vidimo, da je lahko izjava resnična, neresnična, ali pa je resničnost izjave *odvisna* od vrednosti spremenljivk, ki nastopajo v njej. Primeri besedila, ki niso matematične izjave:

- Ali je $2 + 2 = 5$?
- Za vsak $x > 5$.
- Študenti bi morali znati reševati diferencialne enačbe.
- Od nekdaj lepe so Ljubljanke slovele, al lepše od Urške bilo ni nobene.
- $\phi\vee)\psi \Rightarrow \psi$.

Matematične izjave običajno pišemo kombinirano v naravnem jeziku in z matematični simboli, saj so tako najlažje razumljive ljudem. Za potrebe matematične logike pa izjave pišemo *samo* z matematičnimi simboli. Tako zapisani izjavi pravimo *logična formula*. V ta namen moramo nadomestiti osnovne gradnike izjav, kot so "in", "ali" in "za vsak", z *logičnimi operacijami*. Le-te delimo na tri sklope. V prvi sklop sodita *logični konstanti*:

- resnica $\top$,
- neresnica $\bot$.

V računalništvu resnico $\top$ pogosto označimo z 1 ali `True` in neresnico $\bot$ z 0 ali `False`. Naslednji sklop so *logični vezniki*, s katerimi sestavljamo nove izjave iz že danih:

- konjunkcija $\phi \wedge \psi$, beremo "ϕ in ψ",
- disjunkcija $\phi \vee \psi$, beremo "ϕ ali ψ",
- implikacija $\phi \Rightarrow \psi$, beremo "če ϕ potem ψ",

- ekvivalenca $\phi \Leftrightarrow \psi$, beremo "$\phi$ če, in samo če, ψ" ali pa "ϕ natanko tedaj, kadar ψ",
- negacija $\neg\phi$, beremo "ne ϕ",

V tretji sklop sodita *logična kvantifikatorja*:

- univerzalni kvantifikator $\forall\, x \in S\,.\,\phi$, beremo "za vse x iz S velja ϕ",
- eksistenčni kvantifikator $\exists\, x \in S\,.\,\phi$, beremo "obstaja x v S, da velja ϕ",

Pri tem je S množica, razred[2] ali tip spremenljivke x. V praksi se uporablja več inačic zapisa za kvantifikatorje, kot so "$\forall x : S.\, \phi$", "$\forall x \in S : \phi$" in "$(\forall x \in S)\phi$". Srečamo tudi zapis "$\phi, \forall x \in S$", ki pa ga odsvetujemo.

Neomejena kvantifikatorja $\forall\, x\,.\,\phi$ in $\exists\, x\,.\,\phi$ se uporabljata, kadar je vnaprej znana množica S, po kateri teče spremenljivka x. V matematičnem besedilu je običajno razvidna iz spremnega besedila, včasih pa je treba upoštevati ustaljene navade: n je naravno ali celo število, x realno, f je funkcija ipd.

V uporabi so nekatere ustaljene okrajšave:

$\exists\, x, y \in S\,.\,\phi,$	pomeni	$\exists\, x \in S\,.\,\exists\, y \in S\,.\,\phi,$
$\forall\, x \in S, y \in T\,.\,\phi,$	pomeni	$\forall\, x \in S\,.\,\forall\, y \in T\,.\,\phi,$
$\phi \Leftrightarrow \psi \Leftrightarrow \rho \Leftrightarrow \sigma$	pomeni	$(\phi \Leftrightarrow \psi) \wedge (\psi \Leftrightarrow \rho) \wedge (\rho \Leftrightarrow \sigma),$
$f(x) = g(x) = h(x) = i(x)$	pomeni	$f(x) = g(x) \wedge g(x) = h(x) \wedge h(x) = i(x),$
$a \le b < c \le d$	pomeni	$a \le b \wedge b < c \wedge c \le d.$

Nekatere okrajšave odsvetujemo. V nizu neenakosti naj gredo vse primerjave v isto smer. Torej ne pišemo $a \le b < c \ge d$, ker se zlahka zmotimo in mislimo, da velja $a \ge d$. To bi morali zapisati ločeno kot $a \le b < c$ in $c \ge d$. Prav tako ne nizamo neenakosti, saj premnogi iz $f(x) \ne g(x) \ne h(x)$ "sklepajo" $f(x) \ne h(x)$, čeprav neenakost *ni* tranzitivna relacija. Zapis $f(x) = g(x) \ne h(x) = i(x)$ je v redu, saj ena sama neenakost ne povzroči težav.

Naloga 2.5 Zapiši $f(x) = g(x) \ne h(x) = i(x)$ brez okrajšav.

Povejmo še nekaj o pisanju oklepajev. Oklepaji povedo, katera operacija ima prednost. Kadar manjkajo, moramo poznati dogovorjeno *prioriteto* operacij. Na primer, ker ima množenje višjo prioriteto kot seštevanje, je $5 \cdot 3 + 8$ enako $(5 \cdot 3) + 8$ in ne $5 \cdot (3 + 8)$. Tudi logične operacije imajo svoje prioritete, ki pa niso tako splošno znane kot prioritete aritmetičnih operacij. Zato bodite pazljivi, ko berete tuje besedilo.

Mi bomo privzeli naslednje prioritete logičnih operacij:

- negacija $\neg$ ima prednost pred
- konjunkcijo $\wedge$, ki ima prednost pred
- disjunkcijo $\vee$, ki ima prednost pred
- implikacijo $\Rightarrow$, ki ima prednost pred

[2] V poglavju **??** bomo spoznali razliko med množicami in razredi, zaenkrat si S predstavljamo kot množico.

- kvantifikatorjema $\forall$ in $\exists$.

Na primer:

- $\neg\phi \vee \psi$ je isto kot $(\neg\phi) \vee \psi$,
- $\neg\neg\phi \Rightarrow \phi$ je isto kot $(\neg(\neg\phi)) \Rightarrow \phi$,
- $\phi \vee \psi \wedge \rho$ je isto kot $\phi \vee (\psi \wedge \rho)$,
- $\phi \wedge \psi \Rightarrow \phi \vee \psi$ je isto kot $(\phi \wedge \psi) \Rightarrow (\phi \vee \psi)$,
- $\forall\, x \in S\,.\, \phi \Rightarrow \psi$ je isto kot $\forall\, x \in S\,.\, (\phi \Rightarrow \psi)$,
- $\exists\, x \in S\,.\, \phi \wedge \psi$ je isto kot $\exists\, x \in S\,.\, (\phi \wedge \psi)$.

V aritmetiki poznamo poleg prioritete operacij tudi *levo* in *desno asociativnost*. Denimo, seštevanje je levo asociativno, ker beremo $5 + 3 + 7$ kot $(5 + 3) + 7$, saj najprej izračunamo $5 + 3$ in nato $8 + 7$. Pri seštevanju to sicer ni pomembno in bi lahko seštevali tudi $3 + 7$ in nato $5 + 10$. Drugače je z odštevanjem, kjer $5 - 3 - 7$ pomeni $(5 - 3) - 7$ in ne $5 - (3 - 7)$. Tudi za logične operacije velja dogovor o asociativnosti. Konjunkcija in disjunkcija sta levo asociativni:

$$\begin{array}{lll} \phi \wedge \psi \wedge \rho & \text{pomeni} & (\phi \wedge \psi) \wedge \rho, \\ \phi \vee \psi \vee \rho & \text{pomeni} & (\phi \vee \psi) \vee \rho. \end{array}$$

Za disjunkcijo in konjunkcijo sicer ni pomembno, kako postavimo oklepaje, ker sta obe možnosti med seboj ekvivalentni, vendar je prav, da natančno določimo, katera od njiju je mišljena. V logiki je implikacija desno asociativna:

$$\phi \Rightarrow \psi \Rightarrow \rho \qquad \text{pomeni} \qquad \phi \Rightarrow (\psi \Rightarrow \rho).$$

Tu *ni* vseeno, kako postavimo oklepaje, saj $\phi \Rightarrow (\psi \Rightarrow \rho)$ in $(\phi \Rightarrow \psi) \Rightarrow \rho$ v splošnem nista ekvivalentna. Vendar pozor! Ko matematiki, ki niso logiki, v matematičnem besedilu zapišejo

$$\phi \Rightarrow \psi \Rightarrow \rho,$$

s tem skoraj vedno mislijo

$$(\phi \Rightarrow \psi) \wedge (\psi \Rightarrow \rho).$$

Zakaj? Zato ker je to priročen zapis, ki nakazuje zaporedje sklepov "iz ϕ sledi ψ in nato iz ψ sledi ρ", še posebej, če je zapisan v več vrsticah. Recimo, za nenegativni števili x in y bi takole zapisali utemeljitev neenakosti med aritmetično in geometrijsko sredino:

$$\begin{array}{ll} (x-y)^2 \geq 0 \Rightarrow & \\ x^2 - 2xy + y^2 \geq 0 \Rightarrow & \text{(razstavimo)} \\ x^2 + 2xy + y^2 \geq 4xy \Rightarrow & \text{(prištejemo } 4xy\text{)} \\ (x+y)^2 \geq 4xy \Rightarrow & \text{(faktoriziramo)} \\ \dfrac{(x+y)^2}{4} \geq xy \Rightarrow & \text{(delimo s 4)} \\ \dfrac{x+y}{2} \geq \sqrt{xy}. & \text{(korenimo)} \end{array}$$

Matematiki radi celo spustijo znak $\Rightarrow$ in preprosto vsak naslednji sklep napišejo v svojo vrstico. Ker torej velja tak ustaljen način pisanja zaporedja sklepov, je varneje pisati $\phi \Rightarrow (\psi \Rightarrow \rho)$ brez oklepajev, da ne povzročamo zmede.

2.3 Kako beremo in pišemo simbolni zapis

Izjave, zapisane v simbolni obliki, ni težko prebrati. Na primer,

$$\forall\, x, y \in \mathbb{R}\,.\,\big(x^2 = 4 \wedge y^2 = 4 \Rightarrow x = y\big)\,,$$

preberemo:

> "Za vse realne x in y, če je x^2 enako 4 in y^2 enako 4, potem je x enako y."

Več izkušenj pa je potrebnih, da *razumemo* matematični pomen take izjave, v tem primeru:

> "Enačba $x^2 = 4$ ima največ eno realno rešitev."

Začetnik potrebuje nekaj vaje, da se navadi brati simbolni zapis. Tudi prevod v obratno smer, iz besedila v simbolno obliko, ni enostaven, zato povejmo, kako se prevede nekatere standardne fraze.

"ϕ je zadosten pogoj za ψ."

To pomeni, da zadošča dokazati ϕ zato, da dokažemo ψ, ali v simbolni obliki

$$\phi \Rightarrow \psi.$$

"ϕ je potreben pogoj za ψ."

To pomeni, da ψ ne more veljati, ne da bi veljal ϕ. Z drugimi besedami, če velja ψ, potem velja tudi ϕ, kar se v simbolni obliki zapiše

$$\psi \Rightarrow \phi.$$

"ϕ je zadosten in potreben pogoj za ψ."

To je kombinacija prejšnjih dveh primerov, ki trdi, da iz ϕ sledi ψ in iz ψ sledi ϕ, kar pa je ekvivalenca:

$$\phi \Leftrightarrow \psi.$$

Naloga 2.6 Je "n je sod in $n > 2$" *potreben* ali *zadosten* pogoj za "n ni praštevilo"?

"Naslednje izjave so ekvivalentne: ϕ, ψ, ρ in σ."

To pomeni, da sta vsaki dve izmed danih izjav ekvivalentni, se pravi

$$(\phi \Leftrightarrow \psi) \wedge (\phi \Leftrightarrow \rho) \wedge (\phi \Leftrightarrow \sigma) \wedge (\psi \Leftrightarrow \rho) \wedge (\psi \Leftrightarrow \sigma) \wedge (\rho \Leftrightarrow \sigma).$$

Ker je ekvivalenca tranzitivna relacija, ni treba obravnavati vseh kombinacij, zadostujejo že tri, ki dane izjave "povežejo" med seboj:

$$(\phi \Leftrightarrow \psi) \wedge (\psi \Leftrightarrow \rho) \wedge (\rho \Leftrightarrow \sigma).$$

To pišemo krajše kar kot

$$\phi \Leftrightarrow \psi \Leftrightarrow \rho \Leftrightarrow \sigma,$$

čeprav je formalno gledano tako zapis nepravilen. V razdelku 2.6.5 bomo spoznali, kako se tako zaporedje ekvivalenc dokaže s ciklom implikacij $\phi \Rightarrow \psi \Rightarrow \rho \Rightarrow \sigma \Rightarrow \phi$.

Naloga 2.7 Podaj konkretne primere izjav ϕ, ψ in ρ, iz katerih je razvidno, da izjava $(\phi \Leftrightarrow \psi) \wedge (\psi \Leftrightarrow \rho)$ *ni* ekvivalentna niti $(\phi \Leftrightarrow \psi) \Leftrightarrow \rho$ niti $\phi \Leftrightarrow (\psi \Leftrightarrow \rho)$.

"Za vsak x is S, za katerega velja ϕ, velja tudi ψ."

To lahko preberemo tudi kot "Za vsak x iz S, če zanj velja ϕ, potem velja ψ," kar je v simbolni obliki

$$\forall\, x \in S\,.\,(\phi \Rightarrow \psi)\,.$$

Tudi izjave oblike "vsi ϕ-ji so ψ-ji" so te oblike, denimo "vsa od dva večja praštevila so liha" zapišemo

$$\forall\, n \in \mathbb{N}\,.\,(n > 2 \wedge n \text{ je praštevilo} \Rightarrow n \text{ je lih})\,.$$

Naloga 2.8 V simbolni obliki zapiši "n je lih" in "n je praštevilo". Namig: n je lih, kadar obstaja naravno število k, za katerega velja $n = 2k + 1$, in n je praštevilo, kadar *ni* zmnožek dveh naravnih števil, ki sta obe večji od 1.

"Enačba $f(x) = g(x)$ nima realne rešitve."

To lahko povemo takole: ni res, da obstaja $x \in \mathbb{R}$, za katerega bi veljalo $f(x) = g(x)$. S simboli zapišemo

$$\neg \exists\, x \in \mathbb{R}\,.\,f(x) = g(x).$$

Opozoriti velja, da iz same enačbe ne moremo vedno sklepati, kaj je neznanka. V enačbi $ax^2 + bx + c = 0$ bi za neznanko lahko načeloma imeli katerokoli od štirih spremenljivk a, b, c in x, ali pa kar vse. Večina matematikov bi sicer uganila, da je najverjetneje neznanka x, vendar se v splošnem ne moremo zanašati na običaje in uganjevanje, ampak moramo točno povedati, kateri simboli so *neznanke* in kateri *parametri*.

Naloga 2.9 Zapiši v simbolni obliki: "Sistem enačb

$$\begin{aligned} a_1 x + b_1 y &= c_1, \\ a_2 x + b_2 y &= c_2 \end{aligned}$$

nima pozitivnih realnih rešitev x, y."

Naloga 2.10 Zapiši v simbolni obliki:

1. "Enačba $f(x) = g(x)$ ima največ eno realno rešitev."
2. "Enačba $f(x) = g(x)$ ima več kot eno realno rešitev."
3. "Enačba $f(x) = g(x)$ ima natanko dve realni rešitvi."

"Brez izgube za splošnost."

V matematičnih besedilih najdemo frazo "brez izgube za splošnost" kot v naslednjem primeru.

Izrek 2.11 *Za vsa cela števila a, b in c je $|a-b|+|b-c|+|c-a|$ sodo število.*

Dokaz. Brez izgube za splošnost smemo predpostaviti $a \geq b \geq c$. Tedaj velja

$$|a-b|+|b-c|+|c-a| = (a-b)+(b-c)-(c-a) = 2(a-c),$$

kar je sodo število. ∎

Fraza "brez izgube za splošnost" nakazuje, da dokaz obravnava le eno od večih možnosti. Načeloma bi morali obravnavati tudi ostale možnosti, ki pa jih je pisec dokaza opustil, ker so bodisi zelo lahke bodisi zelo podobne tisti, ki jo dokaz obravnava. Za začetnika je najtežje dognati, katere so preostale možnosti in zakaj se je pisec dokaza pravzaprav odločil zanje. Avtor zgornjega dokaza je verjetno opazil, da števila a, b in c v izrazu $|a-b|+|b-c|+|c-a|$ nastopajo *simetrično*: če jih premešamo, se izraz ne spremeni. Denimo, ko zamenjamo a in b, dobimo $|b-a|+|a-c|+|c-b|$, kar je enako prvotnemu izrazu $|a-b|+|b-c|+|c-a|$. Torej lahko izmed šestih možnosti

$$\begin{array}{lll} a \geq b \geq c, & a \geq c \geq b, & b \geq a \geq c, \\ b \geq c \geq a, & c \geq a \geq b, & c \geq b \geq a \end{array}$$

obravnavamo le eno. Seveda pisanje dokazov, pri katerih večji del dokaza opustimo, zahteva pazljivost in nekaj izkušenj.

Naloga 2.12 Dokaži izrek 2.11 tako, da obravnavaš samo možnost $b \geq c \geq a$ in zraven dopišeš "brez izgube za splošnost".

2.4 Definicije

Poznamo tri vrste definicij. Prva in najpreprostejša je definicija, ki služi kot *okrajšava* za daljši izraz. To smemo vedno nadomestiti s prvotnim izrazom. Na primer, funkcija "hiperbolični tangens" $\tanh(x)$ je definirana kot

$$\tanh(x) = \frac{e^{2x}-1}{e^{2x}+1}.$$

Lahko bi shajali tudi brez zapisa $\tanh(x)$, vendar bi morali potem povsod pisati daljši izraz $\frac{e^{2x}-1}{e^{2x}+1}$, kar bi bilo nepregledno.

Druga vrsta definicije je vpeljava novega matematičnega pojma. Študenti prvega letnika matematike spoznajo celo vrsto novih pojmov (grupa, vektorski prostor, limita, stekališče, metrika itn.), s katerimi si razširijo sposobnost matematičnega razmišljanja. Matematiki cenijo dobre definicije in vpeljavo novih matematičnih pojmov vsaj toliko, kot dokaze težkih izrekov.

Tretja vrsta definicije je *konstrukcija* matematičnega objekta s pomočjo dokaza o enoličnem obstoju. O tem bomo povedali več v razdelku 2.7.4.

2.5 Pravila sklepanja in dokazi

Povedali smo že, da je dokaz utemeljitev neke matematične izjave. V razdelku 2.1 smo govorili o tem, da so dokazi mešanica besedila in simbolov, ki jih matematiki uporabljajo tako za utemeljitev matematičnih izjav, kakor tudi za razlago in podajanje matematičnih idej. V tem razdelku se posvetimo *formalnim dokazom*, ki so logične konstrukcije namenjene mehanskemu preverjanju pravilnosti izjav.

Za vsako logično operacijo bomo podali *formalna pravila sklepanja*, ki jih smemo uporabljati v formalnem dokazu. Pravilo sklepanja shematsko zapišemo

$$\frac{\phi \qquad \psi \qquad \rho}{\sigma}$$

in ga preberemo: "Če smo dokazali ϕ, ψ in ρ, smemo sklepati σ." Izjavam nad črto pravimo *hipoteze*, izjavi pod črto pa *sklep*. Hipotez je lahko nič ali več, sklep mora biti natanko en. Pravilo sklepanja brez hipotez se imenuje *aksiom*.

Da bomo lahko pojasnili, kaj je dokaz, podajmo pravila sklepanja za $\top$ in $\wedge$, ki jih bomo v naslednjem razdelku še enkrat bolj pozorno obravnavali:

$$\frac{}{\top} \qquad \frac{\phi \qquad \psi}{\phi \wedge \psi} \qquad \frac{\phi \wedge \psi}{\phi} \qquad \frac{\phi \wedge \psi}{\psi}$$

Po vrsti beremo:

- Velja $\top$.
- Če velja ϕ in ψ, smemo sklepati $\phi \wedge \psi$.
- Če velja $\phi \wedge \psi$, smemo sklepati ϕ.
- Če velja $\phi \wedge \psi$, smemo sklepati ψ.

Formalni dokaz ima drevesno obliko in prikazuje, kako iz danih *hipotez* dokažemo neko *sodbo*. Pri dnu je zapisana izjava, ki jo dokazujemo, nad njo pa dokaz. Vsako vejišče je eno od pravil sklepanja. Vsaka veja se mora zaključiti z aksiomom ali s hipotezo. Oglejmo si dokaz izjave $(\alpha \wedge \alpha) \wedge (\top \wedge \beta)$ iz hipoteze $\beta \wedge \alpha$:

$$\dfrac{\dfrac{\dfrac{\beta \wedge \alpha}{\alpha} \qquad \dfrac{\beta \wedge \alpha}{\alpha}}{\alpha \wedge \alpha} \qquad \dfrac{\dfrac{}{\top} \qquad \dfrac{\beta \wedge \alpha}{\beta}}{\top \wedge \beta}}{(\alpha \wedge \alpha) \wedge (\top \wedge \beta)}$$

Dokaz se razveji na dve veji, vsaka od njiju pa še na dve veji. Tako pri vrhu dobimo štiri liste, od katerih se trije izjava $\beta \wedge \alpha$ in en aksiom za $\top$.

Naloga 2.13 Preveri, da je vsako vejišče v zgornjem dokazu res uporaba enega od zgoraj podanih pravil sklepanja.

V praksi matematično besedilo bolj ali manj odraža strukturo formalnega dokaza, le da se besedilo ne veji, ampak so sestavni kosi dokaza zloženi v zaporedje. Formalni dokazi so uporabni, kadar želimo preveriti veljavnost najbolj osnovnih logičnih dejstev. Ni mišljeno, da bi matematiki pisali ali preverjali velike formalne dokaze pomembnih matematičnih izrekov, to je delo za računalnike. Formalna pravila sklepanja in formalni dokazi so za matematike pomembni, ker nam omogočajo, da natančno in v celoti povemo, kakšna so "pravila igre" v matematiki.

2.6 Izjavni račun

Izjavni račun je tisti del logike, ki govori o logičnih konstantah $\bot$, $\top$ in o logičnih operacijah $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$, $\neg$. Za vsako od njih podamo formalna pravila sklepanja, ki so dveh vrst. Pravila *vpeljave* povedo, kako se izjave dokaže, pravila *uporabe* pa povedo, kako se že dokazane izjave uporabi.

2.6.1 Konjunkcija

Konjunkcija ima eno pravilo vpeljave in dve pravili uporabe:

$$\frac{\phi \qquad \psi}{\phi \wedge \psi} \qquad\qquad \frac{\phi \wedge \psi}{\phi} \qquad\qquad \frac{\phi \wedge \psi}{\psi}$$

Pravilo vpeljave pove, da konjunkcijo $\phi \wedge \psi$ dokažemo tako, da dokažemo posebej ϕ in posebej ψ. Pravili uporabe pa povesta, da lahko $\phi \wedge \psi$ "razstavimo" na izjavi ϕ in ψ.

V matematičnem besedilu je dokaz konjunkcije $\phi \wedge \psi$ zapisan kot zaporedje dveh poddokazov:

Dokazujemo $\phi \wedge \psi$:

1. *(Dokaz ϕ)*
2. *(Dokaz ψ)*

Dokazali smo $\phi \wedge \psi$.

Manj podroben dokaz ne vsebuje začetnega in končnega stavka, ampak samo dokaza za ϕ in ψ. Bralec mora sam ugotoviti, da je s tem dokazana izjava $\phi \wedge \psi$.

2.6.2 Implikacija

Preden zapišemo pravila sklepanja za implikacijo, si oglejmo primer neformalnega dokaza.

Izrek 2.14 *Če je $x > 2$, potem je $x^3 + x + 7 > 16$.*

Dokaz. Predpostavimo, da velja $x > 2$. Tedaj je $x^3 > 2^3 = 8$, zato velja

$$x^3 + x + 7 > 8 + 2 + 7 = 17 > 16.$$

Dokazali smo $x > 2 \Rightarrow x^3 + x + 7 > 16$. ∎

Prvi stavek dokaza z besedico "predpostavimo" uvede *začasno hipotezo* $x > 2$, iz katere nato izpeljemo posledico $x^3 + x + 7 > 16$. Implikacijo $\phi \Rightarrow \psi$ torej dokažemo tako, da začasno predpostavimo ϕ in dokažemo ψ. Tako pravilo vpeljave zapišemo

$$\frac{\begin{array}{c}[\phi]\\ \vdots \\ \psi\end{array}}{\phi \Rightarrow \psi}$$

Zapis $[\phi]$ z oglatimi oklepaji pomeni, da ϕ ni prava, ampak samo začasna hipoteza. Zapis

$$\begin{array}{c}[\phi]\\ \vdots \\ \psi\end{array}$$

pomeni "dokaz izjave ϕ s pomočjo začasne hipoteze ϕ."

Pravilo uporabe za implikacijo se imenuje *modus ponens* in se glasi

$$\frac{\phi \Rightarrow \psi \qquad \phi}{\psi}$$

V matematičnem besedilu se modus ponens pojavi kot uporaba že prej dokazanega izreka izreka oblike $\phi \Rightarrow \psi$.

2.6.3 Disjunkcija

Disjunkcija ima dve pravili vpeljave in eno pravilo uporabe:

$$\frac{\phi}{\phi \vee \psi} \qquad \frac{\psi}{\phi \vee \psi} \qquad \frac{\phi \vee \psi \qquad \begin{array}{c}[\phi]\\ \vdots \\ \rho\end{array} \qquad \begin{array}{c}[\psi]\\ \vdots \\ \rho\end{array}}{\rho}$$

Pravili sklepanja povesta, da lahko dokažemo disjunkcijo $\phi \vee \psi$ tako, da dokažemo enega od disjunktov.

Pojasnimo še pravilo uporabe. Denimo, da bi radi dokazali ρ, pri čemer že vemo, da velja $\phi \vee \psi$. Pravilo uporabe pravi, da je treba obravnavati dva primera: iz začasne hipoteze ϕ je treba dokazati ρ in iz začasne hipoteze ψ je treba dokazati ρ.

Ponazorimo pravilo uporabe v dokazu izjave $(\alpha \vee \gamma) \wedge (\beta \vee \gamma)$ iz hipoteze $(\alpha \wedge \beta) \vee \gamma$. Dokazno drevo je precej veliko, v njem pa se dvakrat pojavi uporaba disjunkcije:

$$\dfrac{\dfrac{(\alpha \wedge \beta) \vee \gamma \qquad \dfrac{\dfrac{[\alpha \wedge \beta]}{\alpha}}{\alpha \vee \gamma} \qquad \dfrac{[\gamma]}{\alpha \vee \gamma}}{\alpha \vee \gamma} \qquad \dfrac{(\alpha \wedge \beta) \vee \gamma \qquad \dfrac{\dfrac{[\alpha \wedge \beta]}{\beta}}{\beta \vee \gamma} \qquad \dfrac{[\gamma]}{\beta \vee \gamma}}{\beta \vee \gamma}}{(\alpha \vee \gamma) \wedge (\beta \vee \gamma)}$$

Poglejmo na primer levo vejo tega dokaza, desna je podobna:

$$\dfrac{(\alpha \wedge \beta) \vee \gamma \qquad \dfrac{\dfrac{[\alpha \wedge \beta]}{\alpha}}{\alpha \vee \gamma} \qquad \dfrac{[\gamma]}{\alpha \vee \gamma}}{\alpha \vee \gamma}$$

Res je to uporaba disjunkcije $\phi \vee \psi$, kjer smo vzeli $\phi = \alpha \wedge \beta$ in $\psi = \gamma$, dokazali pa smo izjavo $\rho = \alpha \vee \gamma$.

Naloga 2.15 Iz hipoteze $(\alpha \vee \gamma) \wedge (\beta \vee \gamma)$ dokaži $(\alpha \wedge \beta) \vee \gamma$.

V besedilu dokažemo disjunkcijo s pravilom za vpeljavo takole:

Dokazujemo $\phi \vee \psi$. Zadostuje dokazati ϕ:

(Dokaz ϕ.)

Dokazali smo $\phi \vee \psi$.

Pravilo uporabe disjunkcije se v besedilu zapiše kot obravnava primerov:

Dokazujemo ρ. To bomo dokazali z obravnavo primerov ϕ in ψ:

1. *(Dokaz $\phi \vee \rho$)*
2. *Predpostavimo, da velja ϕ. (Dokaz ρ)*
3. *Predpostavimo, da velja ψ. (Dokaz ρ)*

Dokazali smo ρ.

Še primer konkretnega dokaza, ki je tako napisan.

Izrek 2.16 *Naj bo x realno število. Če je $|x-3| > 5$, potem je $x^4 > 15$.*

Dokaz. Dokazujemo $|x-3| > 5 \Rightarrow x^4 > 15$. Predostavimo $|x-3| > 5$ in dokažimo $x^4 > 15$. To bomo dokazali z obravavo primerov $x \leq 3$ in $x \geq 3$:

1. $x \leq 3 \vee x \geq 3$ velja, ker so realna števila linearno urejena z relacijo $\leq$.
2. Predpostavimo $x \leq 3$. Tedaj je $x - 3 \leq 0$ in zato $|x-3| = 3 - x$, od koder sledi $3 - x = |x-3| > 5$, oziroma $x < -2$. Tako dobimo
$$x^4 > (-2)^4 = 16 > 15.$$
3. Predpostavimo $x \geq 3$. Tedaj je $x - 3 \geq 0$ in zato$|x-3| = x - 3$, od koder sledi $x - 3 = |x-3| > 5$, oziroma $x > 8$. Tako dobimo
$$x^4 > 8^4 = 4096 > 15.$$

Iz predpostavke $|x-3| > 5$ smo izpeljali $x^4 > 15$. S tem smo dokazali $|x-3| > 5 \Rightarrow x^4 > 15$. ∎

Težji del tega dokaza se skriva v izbiri disjunkcije. Kako je pisec uganil, da je treba obravnavati primera $x \leq 3$ in $x \geq 3$? Zakaj ni raje obravnaval $x < 3$ in $x \geq 3$, ali morda $x \leq 17$ in $x \geq 17$? Odgovor se skriva v definiciji absolutne vrednosti:

$$|a| = \begin{cases} a & \text{če je } a \geq 0, \\ -a & \text{če je } a \leq 0. \end{cases}$$

Ker v izreku nastopa izraz $|x-3|$, bo obravnava primerov $x-3 \geq 0$ in $x-3 \leq 0$ omogočila, da $|x-3|$ poenostavimo enkrat v $x-3$ in drugič v $3-x$. Seveda pa je $x-3 \geq 0$ ekvivalentno $x \geq 3$ in $x-3 \leq 0$ ekvivalentno $x \leq 3$.

Naloga 2.17 Ali bi lahko izrek 2.16 dokazali tudi z obravnavo primerov $x < 3$ in $x \geq 3$?

2.6.4 Resnica in neresnica

Logična konstanta $\top$ označuje resnico. Kar je res, je res, in tega ni treba posebej dokazovati. To dejstvo izraža aksiom

$$\frac{}{\top}$$

Logična konstanta $\top$ nima pravila uporabe, ker iz $\top$ ne moremo sklepati nič koristnega.

Logična konstanta $\bot$ označuje neresnico. Ker se tega, kar ni res, ne more dokazati, $\bot$ nima pravila vpeljave. Pravilo uporabe je

$$\frac{\bot}{\phi}$$

se imenuje *ex falso (sequitur) quodlibet*, kar pomeni "iz neresnice sledi karkoli".

V matematičnem besedilu se $\top$ in $\bot$ ne pojavljata pogosto, ker matematiki izraze, v katerih se $\top$ in $\bot$ pojavita, vedno poenostavijo s pomočjo ekvivalenc:

$$\top \wedge \phi \Leftrightarrow \phi \qquad \top \vee \phi \Leftrightarrow \phi \qquad \bot \wedge \phi \Leftrightarrow \bot \qquad \bot \vee \phi \Leftrightarrow \phi$$

$$(\top \Rightarrow \phi) \Leftrightarrow \phi \qquad (\bot \Rightarrow \phi) \Leftrightarrow \top \qquad (\phi \Rightarrow \top) \Leftrightarrow \top$$

2.6.5 Ekvivalenca

Logična ekvivalenca $\phi \Leftrightarrow \psi$ je okrajšava za

$$(\phi \Rightarrow \psi) \wedge (\psi \Rightarrow \phi).$$

Ker je to konjunkcija (dveh implikacij), so pravila za vpeljavo in uporabo ekvivalence samo poseben primer pravil sklepanja za konjunkcijo:

$$\frac{\phi \Rightarrow \psi \qquad \psi \Rightarrow \phi}{\phi \Leftrightarrow \psi} \qquad \frac{\phi \Leftrightarrow \psi}{\phi \Rightarrow \psi} \qquad \frac{\phi \Leftrightarrow \psi}{\psi \Rightarrow \phi}$$

V matematičnem besedilu ekvivalenco dokažemo takole:

Dokazujemo $\phi \Leftrightarrow \psi$:

1. *(Dokaz $\phi \Rightarrow \psi$)*
2. *(Dokaz $\psi \Rightarrow \phi$)*

Dokazali smo $\phi \Leftrightarrow \psi$.

Če sta izjavi ϕ in ψ logično ekvivalentni, lahko eno zamenjamo z drugo. To matematiki s pridom uporabljajo pri dokazovanju izjav, čeprav pogosto sploh ne omenijo, katero ekvivalenco so uporabili.

Kadar dokazujemo medsebojno ekvivalenco večih izjav ϕ_1, ϕ_2, ..., ϕ_n, zadostuje dokazati cikel implikacij

$$\phi_1 \Rightarrow \phi_2 \Rightarrow \cdots \Rightarrow \phi_{n-1} \Rightarrow \phi_n \Rightarrow \phi_1.$$

(Ne spreglejte zadnje implikacije $\phi_n \Rightarrow \phi_1$, ki zaključi cikel). V besedilu to dokažemo:

Dokazujemo, da so izjave $\phi_1, \phi_2, \ldots, \phi_n$ ekvivalentne:

1. *(Dokaz $\phi_1 \Rightarrow \phi_2$)*
2. *(Dokaz $\phi_2 \Rightarrow \phi_3$)*
3. *...*
4. *(Dokaz $\phi_{n-1} \Rightarrow \phi_n$)*
5. *(Dokaz $\phi_n \Rightarrow \phi_1$)*

Seveda smemo pred samim dokazovanjem izjave $\phi_1, \ldots, \phi_n$ preurediti tako, da je zahtevane implikacije kar najlažje dokazati. Dokaz lahko tudi razdelimo na dva ločena cikla implikacij

$$\phi_1 \Rightarrow \cdots \Rightarrow \phi_k \Rightarrow \phi_1$$

in

$$\phi_{k+1} \Rightarrow \cdots \Rightarrow \phi_n \Rightarrow \phi_{k+1}$$

in nato dokažemo še eno ekvivalenco $\phi_i \Leftrightarrow \phi_j$, pri čemer je ϕ_i iz prvega in ϕ_j iz drugega cikla.

2.6.6 Negacija

Negacija $\neg\phi$ je definirana kot okrajšava za $\phi \Rightarrow \bot$. Iz pravil sklepanja za $\Rightarrow$ in $\bot$ tako izpeljemo pravili sklepanja za negacijo:

$$\frac{\begin{array}{c}[\phi] \\ \vdots \\ \bot\end{array}}{\neg\phi} \qquad\qquad \frac{\neg\phi \qquad \phi}{\psi}$$

V besedilu dokazujemo $\neg\phi$ takole:

Dokazujemo $\neg\phi$.

Predpostavimo ϕ.
(Dokaz $\bot$.)

Dokazali smo $\neg\phi$.

Tu "Dokaz $\bot$" pomeni, da iz danih predpostavk izpeljemo protislovje. Mnogi matematiki menijo, da se takemu dokazu reče "dokaz s protislovjem", vendar to ni res. To je samo navaden dokaz negacije. Dokazovanje s protislovjem bomo obravnavali v razdelku 2.6.7.

Pravilo uporabe za $\neg\phi$ v besedilu ni eksplicitno vidno, ampak ga matematiki uporabijo, ko sredi dokaza, da velja ψ, izpeljejo protislovje:

Dokazujemo ψ.

(Dokaz ϕ.)

(Dokaz $\neg\phi$.)

To je nesmisel, in ker iz nesmisla sledi karkoli, sledi ψ.

2.6.7 Aksiom o izključenem tretjem

Aksiom o izključenem tretjem se glasi

$$\frac{}{\phi \vee \neg\phi}$$

Povedano z besedami, vsaka izjava je bodisi resnična bodisi neresnična. Torej ni "tretje možnosti" za resničnostno vrednost izjave ϕ, od koder izhaja tudi ime aksioma.

Aksiom o izključenem tretjem omogoča *posredne* dokaze izjav, od katerih je najbolj znano *dokazovanje s protislovjem*: pri tem ne utemeljimo izjave ϕ, ampak utemeljimo, zakaj $\neg\phi$ *ne* velja. Natančneje povedano, izjavo ϕ zamenjamo z njej ekvivalentno izjavo $\neg\neg\phi$ in dokažemo $\neg\neg\phi$. Dokaz ekvivalence $\phi \Leftrightarrow \neg\neg\phi$ sestoji iz dokazov dveh implikacij:

$$\dfrac{\dfrac{\dfrac{[\neg\phi] \qquad [\phi]}{\bot}}{\neg\neg\phi}}{\phi \Rightarrow \neg\neg\phi} \qquad\qquad \dfrac{\dfrac{\dfrac{}{\phi \vee \neg\phi} \qquad [\phi] \qquad \dfrac{\dfrac{[\neg\neg\phi] \qquad [\neg\phi]}{\bot}}{\phi}}{\phi}}{\neg\neg\phi \Rightarrow \phi}$$

V dokazu $\neg\neg\phi \Rightarrow \phi$ smo uporabili aksiom o izključenem tretjem. V matematičnem besedilu se dokaz s protislovjem glasi:

Dokažimo ϕ s protislovjem.

Predpostavimo, da bi veljalo $\neg\phi$.

(Dokaz neresnice $\bot$.)

Ker torej $\neg\phi$ pripelje do protislovja, velja ϕ.

Praviloma izvemo o vsebini matematične izjave ϕ več, če jo dokažemo neposredno. Dokazovanja s protislovjem zato ni smiselno uporabljati vsepovprek, ampak le takrat, ko je zares potreben ali ko nam zelo olajša dokazovanje.

Ostali načini za sestavljanje posrednih dokazov slonijo na ekvivalencah

$$(\phi \vee \psi) \Leftrightarrow \neg(\neg\phi \wedge \neg\psi), \qquad (\phi \vee \psi) \Leftrightarrow (\neg\phi \Rightarrow \psi), \qquad (\phi \Rightarrow \psi) \Leftrightarrow (\neg\psi \Rightarrow \neg\phi),$$

$$(\forall\, x \in S\,.\,\phi) \Leftrightarrow \neg\exists\, x \in S\,.\,\neg\phi, \qquad (\exists\, x \in S\,.\,\phi) \Leftrightarrow \neg\forall\, x \in S\,.\,\neg\phi.$$

V vseh petih primerih implikacija $\Rightarrow$ iz leve na desno velja brez uporabe aksioma o izključenem tretjem. Za dokaz implikacij $\Leftarrow$ is desne na levo pa potrebujemo aksiom o izključenem tretjem.

Naloga 2.18 Sestavi formalne dokaze za zgornjih pet ekvivalenc. Pri dokazovanju ekvivalenc za $\forall$ in $\exists$ si pomagaj s pravili sklepanja iz razdelkov 2.7.3 in 2.7.4.

Povejmo, kako zgornje ekvivalence uporabimo v besedilu za posredni dokaz izjave:

- $(\phi \vee \psi) \Leftrightarrow \neg(\neg\phi \wedge \neg\psi)$ uporabimo takole:

  Dokazujemo $\phi \vee \psi$.

  Predpostavimo, da velja $\neg\phi$ in $\neg\psi$.
  (Dokaz neresnice $\bot$.)

  Ker torej nista ϕ in ψ oba neresnična, je eden od njiju resničen. Dokazali smo $\phi \vee \psi$.

- $(\phi \vee \psi) \Leftrightarrow (\neg\phi \Rightarrow \psi)$ uporabimo takole:

  Dokazujemo $\phi \vee \psi$.

  Predpostavimo $\neg\phi$.
  (Dokaz ψ.)

  Če torej ne velja $\neg\phi$, velja ψ. Torej velja vsaj eden, zato smo dokazali $\phi \vee \psi$.

- $(\phi \Rightarrow \psi) \Leftrightarrow (\neg\psi \Rightarrow \neg\phi)$ uporabimo takole:

  Dokazujemo $\phi \Rightarrow \psi$.

  1. *Predpostavimo $\neg\psi$.*
  2. *(Dokaz $\neg\psi$.)*

  Dokazali smo, da iz ϕ sledi ψ.

- $(\forall\, x \in S\,.\,\phi) \Leftrightarrow \neg\exists\, x \in S\,.\,\neg\phi$ uporabimo takole:

  Dokazujemo, da za vsak $x \in S$ velja ϕ.

  1. *Predpostavimo, da obstaja $x \in S$, za katerega ϕ* ne *velja.*
  2. *(Dokaz neresnice $\bot$.)*

  Predpostavka, da obstaja $x \in S$, za katerega ϕ ne velja, pripelje do protislovja. Torej za vsak $x \in S$ velja ϕ.

- $(\exists\, x \in S\,.\,\phi) \Leftrightarrow \neg\forall\, x \in S\,.\,\neg\phi$ uporabimo takole:

  Dokazujemo, da obstaja tak $x \in S$, za katerega velja ϕ.

1. *Predpostavimo, da bi veljalo $\neg\phi$ za vse $x \in S$.*
2. *(Dokaz neresnice $\bot$.)*

Predpostavka, da velja $\neg\phi$ za vse $x \in S$, pripelje do protislovja. Torej obstaja $x \in S$, za katerega velja ϕ.

Negacijo poljubne izjave ϕ tvorimo preprosto tako, da pred njo postavimo $\neg$. Vendar nam to ne pove dosti o matematični vsebini negirane izjave. V večini primerov je negacijo lažje razumeti, če simbol $\neg$ "porinemo" navznoter do osnovnih izjav z uporabo naslednjih ekvivalenc:

$$\begin{aligned}
\neg(\phi \wedge \psi) &\iff \neg\phi \vee \neg\psi \\
\neg(\phi \vee \psi) &\iff \neg\phi \wedge \neg\psi \\
\neg(\phi \Rightarrow \psi) &\iff \phi \wedge \neg\psi \\
\neg(\neg\phi) &\iff \phi \\
\neg(\forall\, x \in S\,.\,\phi) &\iff \exists\, x \in S\,.\,\neg\phi \\
\neg(\exists\, x \in S\,.\,\phi) &\iff \forall\, x \in S\,.\,\neg\phi
\end{aligned}$$

Primer 2.19 Denimo, da bi radi ovrgli izjavo

"Vsako zaporedje pozitivnih realnih števil ima limito 0."

Da izjavo ovržemo, moramo dokazati njeno negacijo. Načeloma lahko negacijo tvorimo tako, da pred izjavo napišemo "ni res, da velja ...", a nam to ne pove, kako bi negacijo dokazali. Zapišimo prvotno izjavo v delni simbolni obliki:

$$\forall\,(a_n)_n\,.\,((a_n)_n \text{ pozitivno zaporedje} \Rightarrow 0 \text{ je limita zaporedja } (a_n)_n)\,. \tag{2.1}$$

Zgornja pravila za računanje negacije nam povedo, da se $\neg\forall$ spremeni v $\exists\neg$ in da se nato implikacija oblike $\phi \Rightarrow \psi$ spremeni v $\phi \wedge \neg\psi$. Tako izrazimo negacijo izjave (2.1):

$$\exists\,(a_n)_n\,.\,((a_n)_n \text{ pozitivno zaporedje} \wedge \neg(0 \text{ je limita zaporedja } (a_n)_n))\,.$$

To preberemo z besedami:

"Obstaja tako zaporedje $(a_n)_n$, da je $(a_n)_n$ zaporedje pozitivnih števil in da 0 ni limita zaporedja $(a_n)_n$."

Če se še malo potrudimo, preberemo bolj razumljivo:

"Obstaja tako zaporedje pozitivnih realnih števil, da 0 ni njegova limita."

S tem še nismo končali, saj je tudi "Število 0 ni limita zaporedja $(a_n)_n$" negacija. Izjavo "0 je limita zaporedja $(a_n)_n$" najprej zapišemo simbolno:

$$\forall\,\epsilon > 0\,.\,\exists\,m \in \mathbb{N}\,.\,\forall\,n \geq m\,.\,|a_n - 0| < \epsilon. \tag{2.2}$$

Z zgornjimi pravili za negiranje izračunamo negacijo izjave (2.2). Operacijo $\neg$ postopoma "porivamo" navznoter:

$$\begin{aligned}
\neg\forall\,\epsilon>0\,.\,\exists\,m\in\mathbb{N}\,.\,\forall\,n\geq m\,.\,|a_n-0|<\epsilon &\iff\\
\exists\,\epsilon>0\,.\,\neg\exists\,m\in\mathbb{N}\,.\,\forall\,n\geq m\,.\,|a_n-0|<\epsilon &\iff\\
\exists\,\epsilon>0\,.\,\forall\,m\in\mathbb{N}\,.\,\neg\forall\,n\geq m\,.\,|a_n-0|<\epsilon &\iff\\
\exists\,\epsilon>0\,.\,\forall\,m\in\mathbb{N}\,.\,\exists\,n\geq m\,.\,\neg(|a_n-0|<\epsilon) &\iff\\
\exists\,\epsilon>0\,.\,\forall\,m\in\mathbb{N}\,.\,\exists\,n\geq m\,.\,|a_n-0|\geq\epsilon &\iff\\
\exists\,\epsilon>0\,.\,\forall\,m\in\mathbb{N}\,.\,\exists\,n\geq m\,.\,a_n\geq\epsilon &
\end{aligned}$$

V zadnjem koraku smo upoštevali, da za pozitivno število a_n velja $|a_n-0|=|a_n|=a_n$. Tako smo dobili podrobno zapisano negacijo prvotne izjave

> "Obstaja tako zaporedje pozitivnih števil $(a_n)_n$ in obstaja tak $\epsilon>0$, da za vsak $m\in\mathbb{N}$ obstaja $n\geq m$, za katerega velja $a_n>\epsilon$."

To izjavo pa znamo dokazati tako, da podamo konkreten primer zaporedja $(a_n)_n$ in konkretno vrednost ϵ, ki zadoščata pogoju, denimo $a_n=2+n$ in $\epsilon=1$. Res, če je $m\in\mathbb{N}$ poljuben, lahko vzamemo kar $n=m$, saj potem velja $a_n=a_m=2+m>1=\epsilon$.

Pričujoči primer smo zapisali zelo podrobno. Izkušeni matematik tega seveda ne bo pisal, saj bo izračunal negacijo prvotne izjave kar v glavi in takoj podal primer zaporedja, ki dokazuje, da prvotna izjava ne velja.

2.7 Predikatni račun

Predikatni račun je tisti del logike, ki obravnava predikate ter kvantifikatorja $\forall$ in $\exists$.

Predikate tvorimo z logičnimi operacijami in kvantifikatorji iz *osnovnih predikatov*. Katere osnovne predikate imamo na voljo, je odvisno od snovi, ki jo obravnavamo.[3] Vedno imamo na voljo tudi *enakost* $x=y$, ki jo bomo obravnavali v razdelku 2.7.5.

V osnovnih predikatih nastopajo *izrazi* ali *termi*. Katere izraze lahko tvorimo je spet odvisno od tega, katere konstante in operacije imamo na voljo. Na primer, če obravnavamo aritmetiko celih števil, so na voljo operacije $+$, $-$, $\times$, če pa obravnavamo realna števila, so na voljo operacije $+$, $-$, $\times$, $/$. V izrazih vedno lahko nastopajo *spremenljivke*. Kadar uporabimo spremenljivko, moramo povedati njen *tip* oziroma *množico* vrednosti, ki jih lahko zavzame spremenljivka. Pogosto je tip spremenljivke razviden iz spremnega besedila ali iz ustaljene uporabe: n se uporablja za naravno število, x za realno, f za funkcijo ipd.

Ponazorimo pravkar definirane pojme s primerom. Predikat

$$0<f(x)\wedge f(x)<\pi/4\Rightarrow\sin(2f(x))=1/3$$

je sestavljen s pomočjo logičnih operacij $\wedge$ in $\Rightarrow$ iz treh osnovnih predikatov, zgrajenih iz osnovnih relacij $<$ in $=$,

$$0<f(x)\qquad\qquad f(x)<\pi/4\qquad\qquad\sin(2f(x))=1/3,$$

[3] Na primer, če obravnavamo ravninsko geometrijo, potem so osnovni predikati "točka x leži na premici y", "premici p in q se sekata" itn.

v katerih nastopa pet izrazov:

$$0 \qquad f(x) \qquad \pi/4 \qquad \sin(2f(x)) \qquad 1/3$$

V teh izrazih nastopa spremenljivka x, katere tip je množica realnih števil (to moramo uganiti) in spremenljivka f, ki označuje funkcijo iz realnih v realna števila (tudi to moramo uganiti). Nadalje, v izrazih nastopajo konstante 0, π, 4, 2, 1 in 3, operacija sin in operacija množenja.

2.7.1 Proste in vezane spremenljivke

V predikatih in izrazih se pojavljajo spremenljivke. Pri tem moramo ločiti med *prostimi* in *vezanimi* spremenljivkami. Oglejmo si naslednja izraza in predikat:

$$\sum_{i=0}^{n} a_i, \qquad \int_0^1 f(t)\,dt, \qquad \forall x \in A.\, \phi(x)\ .$$

V vsoti je vezana spremenljivka i, spremenljivki n in a sta prosti. To pomeni, da je i neke vrste "lokalna spremenljivka",[4] katere veljavnost je samo znotraj vsote, medtem ko sta spremenljiki n in a veljavni tudi zunaj samega izraza. Podobno je v integralu t vezana spremenljivka in f prosta, v izjavi na desni pa je vezana spremenljivka x, spremenljivki A in ϕ sta prosti.

Vezane spremenljivke so "nevidne" zunaj izraza in jih lahko vedno preimenujemo, ne da bi spremenili pomen izraza (seveda se novo ime ne sme mešati z ostalimi spremenljivkami, ki nastopajo v izrazu): izraza $\int_0^1 f(t)\,dt$ in $\int_0^1 f(x)\,dx$ štejemo za *enaka*, ker se razlikujeta le v imenu vezane spremenljivke. Spremenljivki, ki ni vezana, pravimo *prosta*. Izrazu, v katerem ni prostih spremenljivk, pravimo *zaprt izraz*. Zaprta logična izjava se imenuje *stavek*.

Pomembno se je zavedati, da vezana spremenljivka "zunaj" svojega območja ne obstaja. Matematiki so glede tega precej površni in na primer pišejo

$$\int x^2\,dx = x^3/3 + C,$$

kar je strogo gledano nesmisel. Na levi strani v integralu stoji vezana spremenljivka x, ki je na desni "pobegnila" iz integrala. Še več, če je $x \in \mathbb{R}$ in $C \in \mathbb{R}$, potem je izraz $x^3/3 + C$ *število* (odvisno od vrednosti x in C), saj je vsota dveh realnih števil. Na desni strani bi morala stati oznaka za *funkcijo*, recimo

$$\int x^2\,dx = (x \mapsto x^3/3 + C),$$

vendar tega v praksi nihče ne piše. Seveda pri vsem tem ostane še vprašanje, kakšno vlogo ima v zgornjem izrazu C. Pri analizi se učimo, da je C "poljubna konstanta". Poskusimo to razumeti natančno s stališča logike. Besedico "poljubno" ponavadi razumemo kot "za vsak", vendar to ne gre, saj je

$$\forall\, C \in \mathbb{R}\,.\ \int x^2\,dx = (x \mapsto x^3/3 + C)$$

[4] Podobnost z lokalnimi spremenljivkami v programskih jezikih ni zgolj naključje. Lokalna spremenljivka in števec v zanki sta tudi primera vezanih spremenljivk v teoriji programskih jezikov.

nesemisel. Če bi to bilo res, bi veljalo za $C = 1$ in za $C = 2$, od koder bi dobili

$$(x \mapsto x^3/3 + 1) = \int x^2\,dx = (x \mapsto x^3/3 + 2).$$

Potemtakem bi morali biti funkciji $(x \mapsto x^3/3+1)$ in $(x \mapsto x^3/3+1)$ enaki, od koder sledi nesmisel $1 = 2$. Težave nastopajo iz dejstva, da poskušamo nedoločeni integral razumeti kot operacijo, ki slika funkcije v funkcije, kar ni. Nedoločeni integral preslika funkcijo f v *množico* vseh funkcij F, za katere velja $F' = f$. Če bi to želeli zapisati zares pravilno, bi dobili

$$\int x^2\,dx = \left\{(x \mapsto x^3/3 + C) \;\middle|\; C \in \mathbb{R}\right\}.$$

Ali naj torej sklepamo, da so matematiki pravzaprav zelo površni pri pisanju integralov? Da, s stališča formalne logike prav gotovo. Vendar to ni nujno slabo: matematični zapis v praksi služi ljudem za sporazumevanje in prav je, da si izberejo tak zapis, s katerim najbolj učinkovito komunicirajo drug z drugim. Kljub temu pa se je treba zavedati, kdaj gredo matematiki "po bližnjici" in ne zapišejo ali povedo vsega dovolj natančno, da bi to bilo sprejemljivo za standarde, ki jih postavlja formalna logika.

2.7.2 Substitucija

Substitucija je osnovna sintaktična operacija, v kateri *proste* spremenljivke zamenjamo z izrazi. Zapis

$$e[x_1 \mapsto e_1, \ldots, x_n \mapsto e_n]$$

pomeni: "v izrazu e *hkrati* zamenjaj proste spremenljivke x_1 z e_1, x_2 z e_2, ... in x_n z e_n." Na primer,

$$(x^2 + y)[x \mapsto 3, y \mapsto 5, z \mapsto 12]$$

je enako $3^2 + 5$. Nič hudega ni, če se v substituciji omenja spremenljivko z, ki se v izrazu $x^2 + y$ ne pojavi.

Ko naredimo substitucijo, moramo paziti, da se proste spremenljivke ne "ujamejo". Denimo, da želimo v integralu

$$\int_0^1 \frac{x}{a - x^2}\,dx$$

parameter a zamenjati z y^2. To naredimo s substitucijo

$$\left(\int_0^1 \frac{x}{a - x^2}\,dx\right)[a \mapsto y^2] = \int_0^1 \frac{x}{y^2 - x^2}\,dx.$$

Vse lepo in prav. Kaj pa, če želimo a zamenjati z $1 + x$? Ker je spremenljivka x vezana v integralu, *ne smemo* delati takole:

$$\left(\int_0^1 \frac{x}{a - x^2}\,dx\right)[a \mapsto x^2] = \int_0^1 \frac{x}{x^2 - x^2}\,dx?!$$

Ker vstavljamo v integral spremenljivko x, moramo vezano spremenljivko x najprej preimenovati v kaj drugega, na primer t, šele nato vstavimo:

$$\left(\int_0^1 \frac{x}{a - x^2}\,dt\right)[a \mapsto x^2] = \left(\int_0^1 \frac{t}{a - t^2}\,dt\right)[a \mapsto x^2] = \int_0^1 \frac{t}{x^2 - t^2}\,dt.$$

Podajmo še nekaj primerov substitucij:

$$\begin{aligned}(x+y+1)[x\mapsto 2] &= 2+y+1\ ,\\ (x+y^2+1)[x\mapsto y, y\mapsto x] &= y+x^2+1\\ ((x+y^2+1)[x\mapsto y])[y\mapsto x] &= x+x^2+1\ ,\\ (x+\textstyle\int_0^1 x\cdot y\ ,dx)[x\mapsto 2] &= 2+\int_0^1 x\cdot y\ ,dx\ ,\\ (\textstyle\int_0^1 x\cdot y\ dx)[y\mapsto x^2] &= \int_0^1 t\cdot x^2\ dt\ .\end{aligned}$$

Ločiti je treba med hkratno in zaporedno substitucijo:

$$\begin{aligned}(x+y^2)[x\mapsto y, y\mapsto x] &= y+x^2\\ ((x+y^2)[x\mapsto y])[y\mapsto x] &= (y+y^2)[y\mapsto x] = x+x^2\\ ((x+y^2)[y\mapsto x])[x\mapsto y] &= (x+x^2)[x\mapsto y] = y+y^2.\end{aligned}$$

V nadaljevanju bomo obravnavali pravila sklepanja za univerzalne in eksistenčne kvantifkatorje, v katerih se pojavi substitucija. Ker je sam zapis za substitucijo nekoliko nepregleden, bomo uporabili nekoliko manj pravilen, a bolj praktičen zapis. Denimo, da imamo logično formulo ϕ, v kateri se morda pojavi spremenljivka x, ni pa to nujno. Tedaj pišemo $\phi(x)$. Če želimo zamenjati x z izrazom e, zapišemo $\phi(e)$. To je pravzaprav običajni zapis, kot ga uporabljajo matematiki za zapis funkcij, mi pa smo ga uporabili za zapis logičnih formul. Če bi uporabili zapis s substitucijo, bi formulo označili samo s ϕ namesto s $\phi(x)$ in zamenjavo s $\phi[x\mapsto e]$ namesto s $\phi(e)$. Zakaj je ta bolj priročen zapis hkrati manj pravilen? V formalni logiki strogo ločimo med *simbolnim zapisom* matematičnega pojma, ki je zaporedje znakov na papirju, in njegovim *pomenom*, ki je matematična abstrakcija. Substitucija $\phi[x\mapsto e]$ nam pove, kako niz znakov ϕ predelamo v novi niz znakov, torej deluje na novoju simbolnega zapisa. Ko pišemo $\phi(x)$ pa si že predstavljamo, da je ϕ matematična funkcija, ki deluje na argumentu x. S tem nastopi zmešnjava med simbolnim zapisom in pomenom. Dokler se zmešnjave zavedamo, je vse v redu.

2.7.3 Univerzalni kvantifikator

Univerzalna kvantifikacija $\forall\, x\in S\,.\,\phi$ se prebere "Za vse x iz S velja ϕ." Pravili sklepanja sta

$$\frac{\begin{array}{c}[x\in S]\\ \vdots\\ \phi(x)\end{array}}{\forall\, x\in S\,.\,\phi(x)}\ (x \text{ svež}) \qquad\qquad \frac{\forall\, x\in S\,.\,\phi(x) \qquad e\in S}{\phi(e)}$$

pri čemer je x spremenljivka, $\phi(x)$ logična formula in e poljuben izraz.

V besedilu dokažemo se pravilo vpeljave zapiše:

Dokazujemo $\forall\, x\in S\,.\,\phi(x)$*:*

Naj bo $x\in S$ *poljuben.*

(Dokaz, da velja $\phi(x)$*).*

Dokazali smo $\forall\, x\in S\,.\,\phi(x)$*.*

Pravilo uporabe v besedilu ponavadi ni eksplicitno navedeno, če pa bi ga že zapisali, bi šlo takole:

Dokazujemo, da velja $\phi(e)$*:*

(Dokaz, da velja $\forall\, x \in S\,.\,\phi(x)$*.)*

(Dokaz, da velja $e \in S$*.)*

Torej velja $\phi(e)$*.*

Ob pravilu vpeljave stoji stranski pogoj, da mora biti spremenljivka x "sveža". To pomeni, da se x ne sme pojavljati drugje v dokazu, saj bi sicer lahko prišlo do zmešnjave med vezanimi in prostimi spremenljivkami. V besedilu se dejstvo, da je x svež izraža z besedico "poljuben" ali "katerikoli". Primer, kako gredo stvari narobe, če ne pazimo in pomešamo spremenljivke:

Izrek 2.20 (z napako v dokazu) *Če je* x *večji od* 42*, so vsa realna števila večja od* 23*.*

Dokaz. Denimo, da bi nekoliko nerodno zapisali izrek simbolno takole:

$$x > 42 \Rightarrow \forall\, x \in \mathbb{R}\,.\,x > 23.$$

To je sicer dovoljeno, saj se prosti x, ki stoji zunaj $\forall$ ni ujel, ni pa preveč smotrno, ker smo na dobri poti, da bomo zunanji prosti x in vezanega znotraj $\forall$ pomešali. Res, če ne upoštevamo pravila, da mora biti x svež, dobimo tale nepravi "dokaz":

$$\dfrac{\dfrac{\dfrac{[x > 42] \qquad 42 > 23}{x > 23}}{\forall\, x \in \mathbb{R}\,.\,x > 23}}{x > 42 \Rightarrow \forall\, x \in \mathbb{R}\,.\,x > 23}$$

Pri pravilu za vpeljavo $\forall$ smo uporabili spremenljivko x, ki pa je že nastopala v začasni hipotezi $x > 42$. Z besedilom bi se isti dokaz glasil takole:

> "Dokazujemo $x > 42 \Rightarrow \forall\, x \in \mathbb{R}\,.\,x > 23$. Predpostavimo, da velja $x > 42$ in dokažimo $\forall\, x \in \mathbb{R}\,.\,x > 23$. Naj bo $x \in \mathbb{R}$. Po predpostavki je $x > 42$ in ker je $42 > 23$, od tod sledi $x > 3$."

Če bi izrek zapisali bolje kot $x > 42 \Rightarrow \forall\, y \in \mathbb{R}\,.\,y > 23$, težav ne bi bilo, saj bi se prejšnji dokaz "zataknil":

> "Dokazujemo $x > 42 \Rightarrow \forall\, y \in \mathbb{R}\,.\,y > 23$. Predpostavimo, da velja $x > 42$ in dokažimo $\forall\, y \in \mathbb{R}\,.\,y > 23$. Naj bo $y \in \mathbb{R}$. (Kaj zdaj? Lahko sicer dokažemo $x > 23$, a zares bi morali dokazati $y > 23$, kar ne gre.)"

■

Pogoj, da mora biti spremenljivka x v pravilu za vpeljavo "sveža", se v praksi kaže v tem, da pri uvajanju nove spremenljivke izberemo zanjo novo ime, ki se še ni pojavilo v dokazu.

2.7.4 Eksistenčni kvantifikator

Eksistenčna kvantifikacija $\exists\, x \in S \,.\, \phi$ se prebere "obstaja x iz S, za katerega velja ϕ" ali "za neki x iz S velja ϕ." Pravili sklepanja za eksistenčni kvantifikator se glasita

$$\frac{\phi(e) \qquad e \in S}{\exists\, x \in S \,.\, \phi(x)} \qquad\qquad \frac{\exists\, x \in S \,.\, \phi(x) \qquad \begin{array}{c}[x \in S \wedge \phi(x)] \\ \vdots \\ \psi\end{array}}{\psi}\ (x \text{ svež})$$

kjer je e poljuben izraz in x spremenljivka. Pri tem mora biti x v pravilu uporabe svež. V besedilu pravilo vpeljave uporabimo takole:

Dokazujemo $\exists\, x \in S \,.\, \phi(x)$:

1. *(Skonstruiramo element $e \in S$.)*
2. *(Dokažemo, da velja $\phi(e)$.)*

Dokazali smo $\exists\, x \in S \,.\, \phi(x)$.

Pravilo uporabe pa se v besedilu izraža takole:

Dokazujemo ψ:

1. *(Dokaz izjave $\exists\, x \in S \,.\, \phi(x)$.)*
2. *Predpostavimo, da za $x \in S$ velja $\phi(x)$:*
   (Dokaz izjave ψ.)

Dokazali smo ψ.

Enolični obstoj

Poleg običajnega eksistenčnega kvantifikatorja $\exists$ poznamo tudi *enolični* eksistenčni kvantifikator $\exists!$. Izjavo $\exists!\, x \in S \,.\, (\phi)$ preberemo "obstaja natanko en $x \in S$, za katerega velja $\phi(x)$".

Enolični eksistenčni kvantifikator ni osnovni logični operator, ampak je $\exists!\, x \in S \,.\, (\phi)$ le okrajšava za

$$\exists\, x \in S \,.\, (\phi(x) \wedge (\forall\, y \in S \,.\, (\phi(y) \Rightarrow x = y))) \,. \tag{2.3}$$

Z besedami preberemo to izjavo takole: "obstaja x iz S, za katerega velja $\phi(x)$ in za vsak $y \in S$ za katerega velja $\phi(y)$ sledi $x = y$". To je samo zapleten način, kako povedati, da obstaja natanko en element množice S, ki zadošča pogoju ϕ.

Pravilo sklepanja za vpeljavo enoličnega obstoja izpeljemo iz (2.3):

$$\frac{e \in S \qquad \phi(e) \qquad \begin{array}{c}[y \in S \wedge \phi(y)] \\ \vdots \\ y = e\end{array}}{\exists!\, x \in S \,.\, (\phi)}$$

V besedilu dokažemo enolični obstoj takole:

Dokazujemo, da obstaja natanko en $x \in S$, za katerega velja $\phi(x)$:

1. *Obstoj: (Konstrukcija elementa $e \in S$ in dokaz, da velja $\phi(x)$.)*
2. *Enoličnost: denimo da za $y \in S$ velja $\phi(y)$:*
   (Dokaz, da je $e = y$).

Dokazali smo $\exists!\, x \in S \,.\, \phi(x)$.

Če dokažemo enolični obstoj $\exists!\, x \in S \,.\, \phi(x)$, lahko vpeljemo novo konstanto c, ki označuje tisti element iz S, ki zadošča pogoju ϕ, pri čemer moramo seveda paziti, da znaka c nismo že prej uporabili za kak drug pomen. Nova konstanta c je opredeljena s praviloma

$$\frac{}{\phi(c)} \qquad\qquad \frac{y \in S \qquad \phi(y)}{y = c}$$

Če v formuli ϕ poleg spremenljivke x nastopajo še druge proste spremenljivke, denimo $y_1, \ldots, y_n$, potem je nova konstanta c v resnici *funkcija* parametrov $y_1, \ldots, y_n$.

2.7.5 Enakost in reševanje enačb

Enakost $=$ je osnovna relacija, ki zadošča naslednjim aksiomom in pravilom sklepanja:

$$\frac{}{a = a} \qquad \frac{a = b}{b = a} \qquad \frac{a = b \qquad b = c}{a = c} \qquad \frac{\phi(a) \qquad a = b}{\phi(b)}$$

Po vrsti so so pravilo *refleksivnosti*, *simetrije*, *tranzitivnosti* in *zamenjave*. Zaenkrat enakosti ne bomo posvečali posebne pozornosti, saj jo v praksi študenti dobro obvladajo.

V osnovni is srednji šoli se učimo pravil za reševanje enačb: enačbi smemo na obeh straneh prišteti ali odšteti poljuben izraz, pomnožiti ali deliti smemo s poljubnim *neničelnim* izrazom, ipd. Od kod izhajajo ta pravila? Kaj sploh pomeni, da smo enačbo "rešili"? Ko rešimo kvadratno enačbo

$$x^2 - 5x + 6 = 0$$

običajno zapišemo rešitev takole:

$$x_1 = 2, \quad x_2 = 3.$$

Kako naj to razumemo iz stališča matematične logike? Treba je pojasniti dvoje: kaj pomenita x_1 in x_2, saj v prvotni enačbi nastopa spremenljivka x, ter kako naj razumemo vejico med izjavama $x_1 = 2$ in $x_2 = 3$. Z indeksoma 1 in 2 štejemo rešitve enačbe in sta v resnici nepotrebna,[5] na kar kaže tudi dejstvo, da pišemo $x = \ldots$ in ne $x_1 = \ldots$, kadar je rešitev ena sama. Torej bi lahko rešitev zapisali kot

$$x = 2, \quad x = 3.$$

Sedaj pa je tudi jasno, da bi namesto vejice morala stati disjunkcija, se pravi

$$x = 2 \vee x = 3.$$

[5] Kako pa bi zapisali rešitve enačbe $x_1^2 - 5x_1 + 6x = 0$?

Začetna enačba in tako zapisana rešitev sta logično ekvivalentni:

$$x^2 - 5x + 6 = 0 \iff x = 2 \vee x = 3.$$

Povzemimo: reševanje enačbe je postopek, s katerim dano enačbo $f(x) = g(x)$ prevedemo v njen *logično ekvivalentno* obliko $x = a_1 \vee x = a_2 \vee \cdots \vee x = a_n$, iz katere so neposredno razvidne rešitve enačbe.

Pravila za reševanje enačb torej niso nič drugega kot recepti, s pomočjo katerih enačbo predelamo v njen *ekvivalentno* obliko, ki je korak bližje končni obliki, v kateri bi radi zapisali rešitev. To pojasnjuje srednješolska pravila za reševanje enačb. Na primer, za realna števila $a, b, c \in \mathbb{R}$ vedno velja

$$a = b \Rightarrow c \cdot a = c \cdot b,$$

medtem ko obratna implikacija

$$c \cdot a = c \cdot b \Rightarrow a = b$$

za splošne a in b velja le v primeru, ko je $c \neq 0$. Ker pri reševanju enačb potrebujemo implikacijo v obe smeri, srednješolce učimo, da smejo enačbo množiti samo z od nič različnimi števili.

Naloga 2.21 Kako bi srednješolcem pojasnil, od kod izvira pravilo za množenje enačbe z neničelnim številom?

Naloga 2.22 Enačbo $f(x) = g(x)$ smo "rešili" z zaporedjem korakov

$$\begin{aligned} f(x) &= g(x) \Leftrightarrow \\ f_1(x) &= g_1(x) \Leftrightarrow \\ &\vdots \\ f_k(x) &= g_k(x) \Rightarrow \\ f_{k+1}(x) &= g_{k+1}(x) \Leftrightarrow \\ &\vdots \\ x = a_1 \vee \cdots \vee x &= a_n \end{aligned}$$

kjer smo v k-tem koraku namesto ekvivalence pomotoma naredili implikacijo. Smo s tem dobili preveč ali premalo rešitev prvotne enačbe?