DISKRETNE STRUKTURE

***

– TEHNIKE DOKAZIVANJA –

I DEO

Matematičke teorije

Organizacija svih matematičkih teorija zasniva se na nekim zajedničkim polaznim principima.

Te principe postavio je još 300. godina pre Hrista antički matematičar Euklid, koji je u svom delu nazvanom Elementi izložio geometriju kao aksiomatsku teoriju.

Sa neznatnim izmenama ti principi i dalje važe i koriste se.

Prilikom izgradnje bilo koje aksiomatske teorije najpre činimo sledeće:

* jedan broj pojmova teorije proglašavamo za osnovne ili primitivne pojmove – pojmove koji se ne definišu;
* jedan broj tvrđenja teorije proglašavamo za aksiome – tvrđenja koja se ne dokazuju;
* navodimo pravila logičkog zaključivanja – pravila koja smemo da koristimo pri dokazivanju raznih tvrđenja u toj teoriji.

Zašto se osnovni pojmovi ne definišu, a aksiome ne dokazuju?

Razlog je vrlo jednostavan:

* Nije moguće sve definisati, pa se nešto mora ostaviti nedefinisano, i to su osnovni pojmovi.
* Nije moguće sve dokazati, pa se nešto mora ostaviti nedokazanim, i to su aksiome.

Na primer, svaki pokušaj da se sve dokaže doveo bi do pojave

* poročnog kruga, latinski circulus viciosus, gde bi u dokaz nekog tvrđenja neposredno ili posredno bilo uključeno i ono samo, ili
* beskonačnog regresa – beskonačne hijerarhije novih i novih tvrđenja neophodnih za dokazivanje onih prethodnih.

Matematičke teorije

Osnovni pojmovi se ne definišu, ali o njima obično postoji jasna intuitivna predstava.

Na primer, skup je osnovni pojam u teoriji skupova, tačka i prava su osnovni pojmovi u elementarnoj geometriji, itd.

Ukoliko je teorija aksiomatska, moglo bi se reći i da se osnovni pojmovi ne definišu eksplicitno, ali da su imlicitno definisani sistemom aksioma.

Ostali pojmovi se uvode definicijama.

Definicijama se značenje tih pojmova objašnjava uz pomoć osnovnih pojmova i već ranije definisanih pojmova.

Matematičke teorije

Sa druge strane, teorija se razvija tvrđenjima koja nazivamo teoreme.

Teoreme se dokazuju na osnovu pravila zaključivanja, i u dokazima se koriste samo aksiome i već ranije dokazane teoreme.

U dokazivanju se ne koristi iskustvo ili ubeđenje ma koje vrste, već isključivo logička pravila.

To znači da je navedeni metod razvijanja teorije deduktivan:

> Novi pojmovi i tvrdnje se izvode ili deduciraju iz već usvojenih, a na osnovu logičkih zakona.

Uvođenje i upotreba navedenih pojmova i postupaka u matematici se proučava u okviru matematičke logike.

Matematičke teorije

Dakle, kada se odaberu polazni stavovi - aksiome neke matematičke teorije, onda se iz njih izvode nova tvrđenja – teoreme.

U terminološkom smislu, teorema, tvrđenje, stav, propozicija, činjenica ili rezultat imaju isto značenje, dok je lema pomoćno tvrđenje tehničkog karaktera.

Tvrđenje koje neposredno sledi iz nekog drugog naziva se posledica.

Dokaz neke teoreme može se definisati kao konačan niz tvrđenja čiji je svaki član ili aksioma, ili tvrđenje koje je ranije dokazano, ili se dobija iz prethodnih članova niza uz pomoć nekog pravila zaključivanja.

Poslednji član u tom nizu je upravo teorema koje dokazujemo.

Zaključivanje se zasniva na zakonima logičkog mišljenja i raznim logičkim i matematičkim pravilima izvođenja, kojima se bavimo u daljem radu.

Metodi dokazivanja teorema

Dokazivanje teorema može biti veoma teško.

Zbog toga su nam neophodna sva sredstva koja je moguće upotrebiti u dokazivanju različitih teorema, i ovde ćemo prikazati čitavu paletu različitih metoda dokazivanja.

Ti metodi treba da postanu deo našeg repertoara koji ćemo koristiti u dokazivanju teorema.

Većina teorema u matematici ima oblik implikacije ili ekvivalencije, što se takođe svodi na implikacije.

Zbog toga su tehnike za dokazivanje implikacija veoma važne, i one će biti jedna od najvažnijih tema u našem daljem radu.

Direktni dokazi

Implikacija $p \Rightarrow q$ može se dokazati na taj način što se pokazuje da ako je p tačno, onda i q mora biti tačno.

To dokazuje da se ne može desiti da je p tačno, a q netačno.

Dokaz ovakvog tipa naziva se direktan dokaz.

Dakle, da bi se izveo direktan dokaz, uzima se da je p tačno i upotrebom odgovarajućih pravila zaključivanja i teorema koje su ranije dokazane utvrđuje se da q takođe mora biti tačno.

Pre no što damo primer direktnog dokaza, dajemo sledeću definiciju:

Definicija 1: Celi broj n je paran ako postoji ceo broj k takav da je $n = 2k$, a n je neparan ako postoji ceo broj k takav da je $n = 2k + 1$.

Direktni dokazi

Primer 1: Dati direktan dokaz teoreme: "Ako je n neparan ceo broj, tada je n^2 neparan ceo broj".

Dokaz: Uzmimo da je pretpostavka implikacije tačna, odnosno da je n neparan ceo broj.

Tada postoji ceo broj k takav da je $n = 2k + 1$, odakle je

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 = 2m + 1,$$

gde je $m = 2k^2 + 2k$, i prema tome, n^2 je neparan broj. $\square$

Napomena 1: Oznaka "$\square$" koju smo upotrebili na kraju dokaza prethodnog primera, je matematička oznaka za "kraj dokaza".

Indirektni dokazi

Kako je implikacija $p \Rightarrow q$ ekvivalentna svojoj kontrapoziciji $\neg q \Rightarrow \neg p$, to se tačnost implikacije $p \Rightarrow q$ može dokazati tako što se dokaže da je tačna njena kontrapozicija $\neg q \Rightarrow \neg p$.

Obično se implikacija $\neg q \Rightarrow \neg p$ dokazuje direktno, ali može se koristiti i bilo koja druga tehnika dokazivanja.

Dokaz ovog tipa naziva se indirektan dokaz.

Primer 2: Dati indirektan dokaz teoreme: "Ako je $3n + 2$ neparan broj, tada je n neparan broj".

Dokaz: Pretpostavimo da je zaključak ove implikacije pogrešan, naime da broj n nije neparan, odnosno da je broj n paran.

Tada je $n = 2k$, za neki ceo broj k, odakle je

$$3n + 2 = 6k + 2 = 2(3k + 1),$$

pa je u tom slučaju $3n+2$ paran broj, i dakle, $3n+2$ nije neparan broj.

Ovim smo dokazali tačnost kontrapozicije originalne implikacije, što znači da je i originalna implikacija tačna. □

Prazni i trivijalni dokazi

Uzmimo da je pretpostavka p implikacije $p \Rightarrow q$ netačna.

Tada je implikacija $p \Rightarrow q$ tačna, jer je ili oblika $0 \Rightarrow 1$ ili oblika $0 \Rightarrow 0$, a obe ove implikacije su tačne.

Prema tome, ako se može dokazati da je p netačno, tada to daje i dokaz implikacije $p \Rightarrow q$, koji se naziva prazan dokaz.

Na primer, prazni dokazi se često koriste da bi se dokazali specijalni slučajevi teorema koje tvrde da je implikacija tačna za sve pozitivne ili ne-negativne cele brojeve.

Prazni i trivijalni dokazi

Primer 3: Dokazati da je tačno tvrđenje $P(0)$, gde je za prirodan broj n sa $P(n)$ označeno tvrđenje: "Ako je $n > 1$, tada je $n^2 > n$".

Dokaz: Kako $P(0)$ zapravo znači

$$\text{Ako je } 0 > 1, \text{ onda je } 0^2 > 0,$$

i pretpostavka $0 > 1$ ove implikacije je netačna, to je implikacija automatski tačna, odnosno $P(0)$ je tačno. $\square$

Prazni i trivijalni dokazi

Dalje, neka je zaključak q implikacije $p \Rightarrow q$ tačan.

Tada je implikacija $p \Rightarrow q$ tačna, jer je ili oblika $1 \Rightarrow 1$ ili oblika $0 \Rightarrow 1$, a obe ove implikacije su tačne.

Prema tome, ako se može dokazati da je q tačno, tada to daje i dokaz implikacije $p \Rightarrow q$, koji se naziva **trivijalan dokaz**.

Trivijalni dokazi su često važni kada se dokazuju specijalni slučajevi teorema, na primer kada se koristi metod razlikovanja slučajeva, ili kod dokaza matematičkom indukcijom.

Prazni i trivijalni dokazi

Primer 4: Neka je $P(n)$ oznaka za "Ako su a i b pozitivni celi brojevi takvi da je $a \geqslant b$, onda je $a^n \geqslant b^n$". Dokazati da je tačno $P(0)$.

Dokaz: Imamo da $P(0)$ znači

Ako je $a \geqslant b$, onda je $a^0 \geqslant b^0$.

Kako je $a^0 = b^0 = 1$, to je zaključak ove implikacije tačan, i prema tome, $P(0)$ je tačno. $\square$

Ovo je bio primer trivijalnog dokaza.

Primetimo da pretpostavku $a \geqslant b$ ovde uopšte nismo koristili.

Osnovno o strategiji dokazivanja

U prethodnim razmatranjima upoznali smo se da direktnim i indirektnim dokazima implikacija, i na primerima smo videli kako se ova dva metoda koriste.

Kada se suočimo sa nekom implikacijom koju treba dokazati, nameće se pitanje koji od ta dva metoda koristiti?

Strategija bi mogla da bude sledeća.

Najpre prvo proceniti da li direktan dokaz izgleda obećavajuće.

Treba početi sa rastumačivanjem značenja pojmova koji se javljaju u hipotezama, a onda to treba upotrebiti u zaključivanju, zajedno sa aksiomama i ranije dokazanim teoremama koje bi nam mogle biti od pomoći.

Ako se bude učinilo da direktan dokaz ne vodi nikuda, onda treba pokušati sve to isto sa indirektnim dokazom.

Setimo se da u indirektnom dokazu uzimamo da je zaključak implikacije netačan, a onda koristimo direktan dokaz da dokažemo da i pretpostavka te implikacije mora biti netačna.

Ponekad, kada ne postoji očigledan način da se primeni direktan dokaz, indirektan dokaz može dati dobre rezultate.

Pre no što damo primere koji oslikavaju ovo o čemu smo govorili, daćemo definiciju koja nam je potrebna:

Definicija 2: Realan broj r je racionalan ako postoje celi brojevi p i q takvi da je $q \neq 0$ i $r = \frac{p}{q}$.

Realan broj koji nije racionalan naziva se iracionalan.

Primer 5: Dokazati da zbir dva racionalna broja jeste racionalan broj.

Dokaz: Prvo probamo sa direktnim dokazom.

Neka su r i s racionalni brojevi. To znači da postoje celi brojevi p i q takvi da je $q \neq 0$ i $r = \frac{p}{q}$, i celi brojevi u i v takvi da je $v \neq 0$ i $s = \frac{u}{v}$.

Da li možemo da iskoristimo tu informaciju da bi dokazali da je $r + s$ racionalan broj?

Očigledan način je da saberemo $r = \frac{p}{q}$ i $s = \frac{u}{v}$, čime dobijamo

$$r + s = \frac{p}{q} + \frac{u}{v} = \frac{pv + qu}{qv},$$

i kako je $q \neq 0$ i $v \neq 0$, to je $qv \neq 0$. Ovim smo izrazili $r + s$ kao razlomak celih brojeva $pv + qu$ i qv, pri cemu je $qv \neq 0$, što znači da je $r + s$ racionalan broj. □

Osnovno o strategiji dokazivanja

U prethodnom primeru smo videli da je pokušaj sa direktnim dokazom bio uspešan. U sledećem primeru takav pokušaj neće biti ispešan.

Primer 5: Dokazati da ako je n ceo broj i n^2 je neparan, onda je i n neparan.

Dokaz: Najpre probamo sa direktnim dokazom.

Pretpostavimo da je n ceo broj i n^2 je neparan broj. Tada postoji ceo broj k takav da je $n^2 = 2k + 1$.

Da li možemo iskoristiti tu informaciju da dokažemo da je n neparan broj?

Izgleda da nema očiglednog načina da se dokaže da je n neparan, jer rešavanje jednačine $n^2 = 2k + 1$ po n daje $n = \pm\sqrt{2k+1}$, što nije preterano korisno.

Pošto pokušaj sa direktnim dokazom nije dao rezultata, probamo sa indirektnim dokazom.

Pretpostavimo da n nije neparan broj, odnosno da je n paran. To znači da postoji ceo broj k takav da je $n = 2k$.

Da bi dokazali teoremu upotrebom indirektnog dokaza, treba dokazati da n^2 nije neparan broj, odnosno da je n^2 paran broj.

Sada je očigledno da nam jednakost $n = 2k$ daje dovoljno informacija da zaključimo da je n^2 paran broj. Naime,

$$n^2 = (2k)^2 = 4k^2 = 2(2k^2) = 2m,$$

gde je $m = 2k^2$, pa je n^2 zaista paran broj.

Prema tome, naš pokušaj da pronađemo indirektan dokaz je uspeo. □

Dokaz svođenjem na kontradikciju

U slučaju da ni direktan ni indirektan dokaz ne daju rezultat, postoje i neke dodatne tehnike dokazivanja koje možemo upotrebiti.

Pretpostavimo kada je moguće pronaći neku kontradikciju q, na primer $r \wedge \neg r$, takvu da je moguće dokazati da je tačna implikacija $\neg p \Rightarrow q$.

U tom slučaju tvrđenje $\neg p$ mora biti netačno, i prema tome, tvrđenje p je tačno.

Dakle, na taj način što smo dokazali da je tačna implikacija $\neg p \Rightarrow q$, gde je q kontradikcija, zapravo smo dokazali i da je tačno tvrđenje p.

Ovakva vrsta dokaza naziva se dokaz svođenjem na kontradikciju.

Dokaz svođenjem na kontradikciju

Definicija 3: Za razlomak $\frac{a}{b}$, gde su a i b celi brojevi i $b \neq 0$, kažemo da je nesvodljiv ili neskrativ ako a i b nemaju zajedničkih delitelja većih od 1.

Primer 6: Dokazati da se svaki racionalan broj r može predstaviti u obliku nesvodljivog razlomka.

Dokaz: Prema definiciji racionalnog broja, r se može predstaviti u obliku $r = \frac{a}{b}$, gde su a i b celi brojevi i $b \neq 0$.

Ako a i b nemaju zajedničkih delitelja većih od 1, onda je dokaz završen.

Pretpostavimo da postoji zajednički delitelj brojeva a i b veći od 1. U tom slučaju postoji i najveći zajednički delitelj d tih brojeva.

To znači da je $a = da'$ i $b = db'$, za neke cele brojeve a' i b', pri čemu je $b' \neq 0$, jer je $b \neq 0$, pa je

$$r = \frac{a}{b} = \frac{da'}{db'} = \frac{a'}{b'}.$$

Dokazaćemo da a' i b' nemaju zajedničkih delitelja većih od 1.

To ćemo dokazati svođenjem na kontradikciju. Naime, pretpostavimo suprotno, da postoji zajednički delitelj d' brojeva a' i b' veći od 1.

Tada je $a' = d'a''$ i $b' = d'b''$, za neke cele brojeve a'' i b'', pa je

$$a = da' = dd'a'' \quad \text{i} \quad b = db' = dd'b'',$$

odakle je dd' zajednički delitelj brojeva a i b veći od d, što je u suprotnosti sa činjenicom da je d najveći zajednički delitelj brojeva a i b.

Ovim smo dokazali da a' i b' nemaju zajedničkih delitelja većih od 1. □

Dokaz svođenjem na kontradikciju

Primer 7: Dokazati da je $\sqrt{2}$ iracionalan broj.

Dokaz: Označimo sa p tvrđenje "$\sqrt{2}$ je iracionalan broj".

Uzmimo da je tvrđenje $\neg p$ tačno, odnosno da je $\sqrt{2}$ racionalan broj.

Tada se $\sqrt{2}$ može predstaviti u obliku nesvodljivog razlomka dva cela broja a i b, tj.

$$\sqrt{2} = \frac{a}{b}$$

pri čemu je $b \neq 0$ i a i b nemaju zajedničkih delitelja većih od 1.

Kvadriranjem obe strane gornje jednačine dobijamo da je $2 = \frac{a^2}{b^2}$, što povlači da je $2b^2 = a^2$. Odatle sledi da je a^2 paran broj, i na osnovu Primera 5, i a je paran broj, odnosno $a = 2c$, za neki ceo broj c.

Dalje, iz $2b^2 = a^2$ i $a = 2c$ dobijamo da je $2b^2 = 4c^2$, odnosno da je $b^2 = 2c^2$, odakle na isti način kao i za a dobijamo da je b paran broj, tj. $b = 2d$, za neki ceo broj d.

Dakle, imamo da je $a = 2c$ i $b = 2d$, što znači da je 2 zajednički delitelj brojeva a i b. Sa druge strane, a i b smo izabrali tako da nemaju zajedničkih delitelja većih od 1.

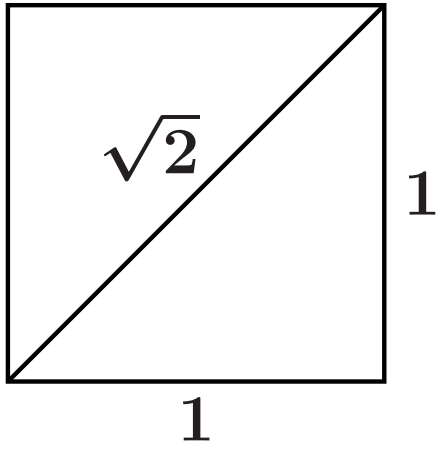
Time smo došli do kontradikcije.

Prema tome, pretpostavka da je $\neg p$ tačno dovela nas je do kontradikcije, pa zaključujemo da je p tačno.

Dakle, $\sqrt{2}$ je iracionalan broj. $\square$

Napomena 2: Činjenica da je $\sqrt{2}$ iracionalan broj bila je poznata još u antičkoj Grčkoj, koji su to nazivali nesamerljivošću dijagonale kvadrata.

Naime, ako imamo kvadrat sa stranicama dužine 1, onda je prema Pitagorinoj teoremi dužina dijagonale jednaka $\sqrt{2}$.



Još u antičkoj Grčkoj je ustanovljeno da se dužina dijagonale ovog kvadrata ne može predstaviti razlomkom, i tada su praktično uvedeni iracionalni, odnosno realni brojevi.

Dokaz svođenjem na kontradikciju

Primer 8: Svođenjem na kontradikciju dokazati teoremu: "Ako je $3n + 2$ neparan broj, onda je n neparan broj".

Dokaz: Pretpostavimo da je $3n + 2$ neparan broj, a da n nije neparan broj, odnosno da je n paran broj.

Tada je $n = 2k$, za neki ceo broj k, odakle je

$$3n + 2 = 6k + 2 = 2(3k + 1),$$

pa dobijamo da je $3n + 2$ paran broj.

Dakle, imamo da je $3n + 2$ i neparan i paran broj, čime smo došli do kontradikcije.

Odatle zaključujemo da pretpostavka da n nije neparan broj nije tačna, što znači da je tačno da je n neparan broj. $\square$

Dokaz podelom na slučajeve

O dokazu podelom na slučajeve, kao pravilu zaključivanja, već smo govorili ranije. Ovde dajemo još jednu verziju tog istog metoda dokazivanja.

Osnova ovog metoda je tautologija

$$\big[(p_1 \vee p_2 \vee \cdots \vee p_n) \Rightarrow q\big] \Leftrightarrow \big[(p_1 \Rightarrow q) \wedge (p_2 \Rightarrow q) \wedge \cdots \wedge (p_n \Rightarrow q)\big].$$

Naime, ako dokazujemo implikaciju $p \Rightarrow q$, pri čemu premisu p možemo "podeliti na slučajeve" p_1, p_2, $\ldots$, p_n, odnosno $p \equiv p_1 \vee p_2 \vee \cdots \vee p_n$, tada se dokaz implikacije $p \Rightarrow q$ svodi na dokaz implikacije

$$p_1 \vee p_2 \vee \cdots \vee p_n \Rightarrow q,$$

a ovo se, prema gornjoj tautologiji, svodi na dokaz da važi

$$(p_1 \Rightarrow q) \wedge (p_2 \Rightarrow q) \wedge \cdots \wedge (p_n \Rightarrow q),$$

tj. na dokaz svake od n implikacija $p_i \Rightarrow q$, za $i = 1, 2, \ldots, n$.

Dokaz podelom na slučajeve

Primer 9: Podelom na slučajeve dokazati da je $|xy| = |x||y|$, gde su x i y realni brojevi, pri čemu je, potsetimo se, apsolutna vrednost $|x|$ broja x definisana sa

$$|x| = \begin{cases} x & \text{ako je } x \geqslant 0 \\ -x & \text{ako je } x < 0 \end{cases}.$$

Dokaz: Kako je apsolutna vrednost definisana pomoću slučajeva, to je prirodno da se i tvrđenja koja se tiču apsolutnih vrednosti dokazuju podelom na slučajeve.

Označimo sa p i q sledeća tvrđenja:

p: "x i y su realni brojevi"

q: "$|xy| = |x||y|$"

Ono što imamo zadatak da dokažemo je implikacija $p \Rightarrow q$.

Dokaz podelom na slučajeve

Možemo razlikovati četiri slučaja:

p_1 : "$x \geqslant 0 \ \wedge \ y \geqslant 0$"

p_2 : "$x \geqslant 0 \ \wedge \ y < 0$"

p_3 : "$x < 0 \ \wedge \ y \geqslant 0$"

p_4 : "$x < 0 \ \wedge \ y < 0$"

odnosno, imamo da je $p \equiv p_1 \vee p_2 \vee p_3 \vee p_4$.

Dakle, da bi dokazali implikaciju $p \Rightarrow q$, **treba da dokažemo implikacije**

$$p_1 \Rightarrow q, \quad p_2 \Rightarrow q, \quad p_3 \Rightarrow q, \quad p_4 \Rightarrow q.$$

(1) Ako važi p_1, **tj. ako je** $x \geqslant 0$ **i** $y \geqslant 0$, **tada je i** $xy \geqslant 0$, **pa imamo da je** $|x| = x$, $|y| = y$ **i** $|xy| = xy$, **odakle sledi da je**

$$|xy| = xy = |x||y|.$$

Dokaz podelom na slučajeve

(2) Ako važi p_2, tj. ako je $x \geqslant 0$ i $y < 0$, tada je $xy < 0$, pa imamo da je $|x| = x$, $|y| = -y$ i $|xy| = -xy$, odakle sledi da je

$$|xy| = -xy = x(-y) = |x||y|.$$

(3) Ako važi p_3, tj. ako je $x < 0$ i $y \geqslant 0$, tada je $xy < 0$, pa imamo da je $|x| = -x$, $|y| = y$ i $|xy| = -xy$, odakle sledi da je

$$|xy| = -xy = (-x)y = |x||y|.$$

(4) Ako važi p_4, tj. ako je $x < 0$ i $y < 0$, tada je $xy > 0$, pa imamo da je $|x| = -x$, $|y| = -y$ i $|xy| = xy$, odakle sledi da je

$$|xy| = xy = (-x)(-y) = |x||y|.$$

Dakle, dokazali smo da su tačne sve četiri implikacije, što znači da je tačna i implikacija $p \Rightarrow q$. $\square$

Produžena implikacija

U praksi se veoma retko srećemo sa dokazima koji se svode na dokaz tačnosti jednostavne implikacije $p \Rightarrow q$.

Mnogo češće srećemo se sa dokazima koji se svode na niz implikacija

$$p_1 \Rightarrow p_2, \quad p_2 \Rightarrow p_3, \ \cdots \ , \ p_{n-1} \Rightarrow p_n, \tag{1.1}$$

koji koristimo da bi dokazali implikaciju $p_1 \Rightarrow p_n$, odnosno da prvi član tog niza povlači poslednji.

Ovakav niz implikacija nazivamo produžena implikacija.

Dakle, tačnost implikacije $p_1 \Rightarrow p_n$ možemo dokazati na taj način što ćemo dokazati tačnost svake implikacije u nizu (1.1).

Ovaj metod zasniva se na svojstvu tranzitivnosti implikacije, odnosno na tautologiji

$$\big[(p_1 \Rightarrow p_2) \wedge (p_2 \Rightarrow p_3) \wedge \cdots \wedge (p_{n-1} \Rightarrow p_n)\big] \Rightarrow (p_1 \Rightarrow p_n).$$

Produžena implikacija

Primer 10: **Dokazati teoremu: "Ako je ceo broj n deljiv sa 2 i sa 5, onda je n deljiv sa 10".**

Dokaz: **Za cele brojeve a i b, umesto "a deli b" pišemo kraće "$a \mid b$".**

Implikaciju $\big[(2 \mid n) \wedge (5 \mid n)\big] \Rightarrow (10 \mid n)$ dokazujemo sledećim nizom implikacija:

$$
\begin{aligned}
(2 \mid n) \wedge (5 \mid n) &\Rightarrow \big[(\exists k)(n = 2k)\big] \wedge \big[(\exists m)(n = 5m)\big] \\
&\Rightarrow (\exists k)(\exists m)(n = 2k \wedge n = 5m) \\
&\Rightarrow (\exists k)(\exists m)(5n = 10k \wedge 4n = 20m) \\
&\Rightarrow (\exists k)(\exists m)\big[n = 10(k - 2m)\big] \\
&\Rightarrow (\exists l)(n = 10l) \\
&\Rightarrow 10 \mid n
\end{aligned}
$$

Dokazi ekvivalencija

Kada dokazujemo teoreme koje imaju oblik ekvivalencije, tj. teoreme oblika $p \Leftrightarrow q$, gde su p i q neka tvrđenja, obično koristimo tautologiju

$$(p \Leftrightarrow q) \Leftrightarrow \big[(p \Rightarrow q) \wedge (q \Rightarrow p)\big].$$

Na osnovu ove tautologije, umesto da dokažemo da je tačno $p \Leftrightarrow q$, možemo dokazati da su tačne obe implikacije $p \Rightarrow q$ i $q \Rightarrow p$.

U mnogim slučajevima to može biti jednostavnije nego direktno dokazivati $p \Leftrightarrow q$.

Naravno, kada krenemo da dokazujemo ekvivalenciju $p \Leftrightarrow q$, najpre treba pokušati da se to dokaže direktno.

Međutim, ako uočimo da bi možda bilo jednostavnije da se ta ekvivalenciija razbije u dve implikacije, treba probati i to.

Dokazi ekvivalencija

Primer 11: Dokazati teoremu: "Ceo broj n je neparan ako i samo ako je broj n^2 neparan".

Dokaz: Označimo sa p i q tvrđenja

p: "n je neparan broj"

q: "n^2 je neparan broj"

Ne postoji očigledan način da se ekvivalencija $p \Leftrightarrow q$ dokaže direktno. Naime

$$n \text{ je neparan broj} \Leftrightarrow (\exists k)\, n = 2k + 1;$$

$$n^2 \text{ je neparan broj} \Leftrightarrow (\exists m)\, n^2 = 2m + 1;$$

i ne postoji očigledan način da se dirtektno dokaže da je

$$(\exists k)(n = 2k + 1) \Leftrightarrow (\exists m)(n^2 = 2m + 1).$$

Dokazi ekvivalencija

Zbog toga ekvivalenciju $p \Leftrightarrow q$ razbijamo u implikacije $p \Rightarrow q$ i $q \Rightarrow p$, i dokazujemo svaku od te dve implikacije.

Setimo se da smo implikaciju $p \Rightarrow q$ dokazali u Primeru 1, upotrebom direktnog dokaza.

Implikaciju $q \Rightarrow p$ smo dokazali u Primeru 5, gde smo videli da direktan dokaz ne daje rezultat, pa smo je dokazali upotrebom indirektnog dokaza.

Činjenica da se implikacije $p \Rightarrow q$ i $q \Rightarrow p$ dokazuju na različite načine, još jedna je potvrda da smo dobro uradili što nismo direktno dokazivali $p \Leftrightarrow q$, jer to zaista ne bi dalo rezultat. $\square$

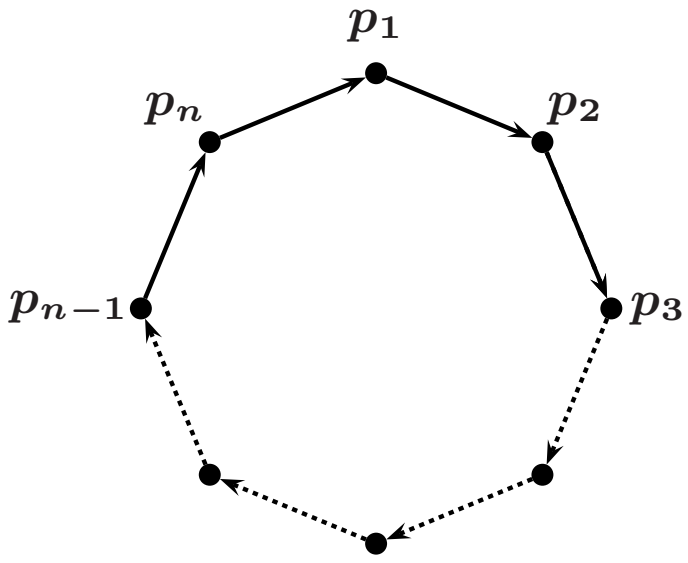
Ciklična implikacija

Mnoge teoreme u matematici tvrde da su neka tvrđenja $p_1, p_2, \ldots, p_n$ međusobno ekvivalentna, tj. da je $p_i \Leftrightarrow p_j$, za sve $i, j = 1, 2, \ldots, n$, $i \neq j$.

Jedan od načina da to dokažemo je da se dokaže niz implikacija

$$p_1 \Rightarrow p_2, \quad p_2 \Rightarrow p_3, \quad \ldots \ , \ p_{n-1} \Rightarrow p_n, \quad p_n \Rightarrow p_1 \tag{1.2}$$

koji nazivamo ciklična implikacija, jer je poslednjom implikacijom u nizu zatvoren krug:



Ciklična implikacija

Pretpostavimo da smo dokazali tačnost svih implikacija u nizu (1.2).

To je sasvim dovoljno da bi se dokazala tačnost ekvivalencije $p_i \Leftrightarrow p_j$, za sve $i, j = 1, 2, \ldots, n$, $i \neq j$, jer njena tačnost sledi iz tačnosti svih implikacija u nizu (1.2).

Naime, ako uzmemo da je $i < j$, tada iz tačnosti implikacija

$$p_i \Rightarrow p_{i+1}, \quad p_{i+1} \Rightarrow p_{i+2}, \quad \ldots \ , p_{j-2} \Rightarrow p_{j-1}, \quad p_{j-1} \Rightarrow p_j,$$

dobijamo da je tačna implikacija $p_i \Rightarrow p_j$ (na osnovu metoda produžene implikacije), a iz tačnosti implikacija

$$p_j \Rightarrow p_{j+1}, \ \ldots \ , \ p_{n-1} \Rightarrow p_n, \ p_n \Rightarrow p_1, \ p_1 \Rightarrow p_2, \ \ldots \ , \ p_{i-1} \Rightarrow p_i,$$

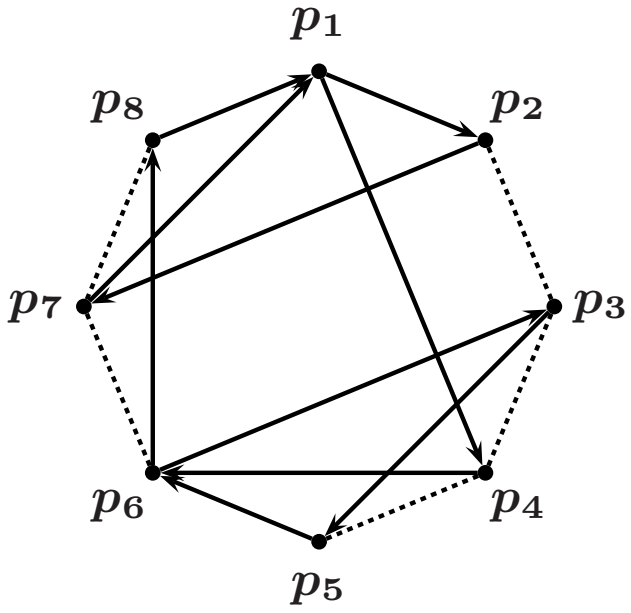
dobijamo da je tačna implikacija $p_j \Rightarrow p_i$.

Prema tome, iz tačnosti implikacija $p_i \Rightarrow p_j$ i $p_j \Rightarrow p_i$ zaključujemo da je tačna ekvivalencija $p_i \Leftrightarrow p_j$.

Ciklična implikacija

Primetimo da redosled dokazivanja implikacija ne mora biti isti kao u (1.2). Naime, možemo ići bilo kojim redom, jedino je bitno da zatvorimo krug.

Takođe, ciklus možemo podeliti u nekoliko manjih ciklusa, ali tako da ti manji ciklusi budu međusobno povezani, da bi se zatvorio veliki ciklus, na primer, kao na sledećoj slici:



Ciklična implikacija

Primer 12: Dokazati da su za proizvoljan prirodan broj n sledeća tvrđenja ekvivalentna:

(i) n je deljiv sa 30;

(ii) n je deljiv sa 6 i sa 5;

(iii) zbir cifara broja n deljiv je sa 3 i cifra jedinica mu je 0.

Pre no što pređemo na dokaz, uvedimo sledeću oznaku.

Za cele brojeve a, b i k, sa $a \equiv b (\mathrm{mod}\, k)$ se označava da a i b daju isti ostatak pri deljenju sa k.

Dokaz: Ekvivalentnost ovih tvrđenja dokazujemo cikličnim nizom implikacija

$$\text{(i)} \Rightarrow \text{(ii)} \Rightarrow \text{(iii)} \Rightarrow \text{(i)}.$$

(i)⇒(ii). Neka je n deljiv sa 30, tj. $n = 30k$, za neki $k \in \mathbb{N}$.

Tada je $n = (5k) \cdot 6$ i $n = (6k) \cdot 5$, pa je n deljiv i sa 6 i sa 5.

(ii)⇒(iii). Neka je n deljiv sa 6 i sa 5.

Neka je $x_k x_{k-1} \dots x_1 x_0$ desetični zapis broja n, tj.

$$n = 10^k x_k + 10^{k-1} x_{k-1} + \cdots + 10 x_1 + x_0. \tag{1.3}$$

Primetimo da broj deljiv sa 5 može imati cifru jedinice samo 0 ili 5, dok broj deljiv sa 6 može imati cifru jedinice 6, 2, 8, 4 ili 0.

Odavde zaključujemo da n ima cifru jedinice 0, tj. $x_0 = 0$.

Dalje, primetimo da je $10^i \equiv 4 \pmod 6$, za svaki $i \in \mathbb{N}$.

Naime, jasno je da je $10 \equiv 4 \pmod 6$.

Ciklična implikacija

Ako je $10^i \equiv 4 \pmod 6$, za neki $i \in \mathbb{N}$, onda

$$10 \equiv 4 \pmod 6 \ \wedge \ 10^i \equiv 4 \pmod 6 \ \Rightarrow \ 10^i \cdot 10 \equiv 4 \cdot 4 \pmod 6,$$

odnosno $10^{i+1} \equiv 16 \pmod 6$, pa je

$$10^{i+1} \equiv 16 \pmod 6 \ \wedge \ 16 \equiv 4 \pmod 6 \ \Rightarrow \ 10^{i+1} \equiv 4 \pmod 6.$$

Dakle, matematičkom indukcijom zaključujemo da je $10^i \equiv 4 \pmod 6$, za svaki $i \in \mathbb{N}$, i na osnovu (1.3) dobijamo da je

$$n \equiv 4(x_k + x_{k-1} + \cdots + x_2 + x_1) \pmod 6,$$

i kako je n deljiv sa 6, to je i $4(x_k + x_{k-1} + \cdots + x_2 + x_1)$ deljiv sa 6, odnosno, $2(x_k + x_{k-1} + \cdots + x_2 + x_1)$ je deljiv sa 3, odakle sledi da je $x_k + x_{k-1} + \cdots + x_2 + x_1$ deljiv sa 3.

Kako je $x_0 = 0$, to je i zbir svih cifara broja n deljiv sa 3.

(iii)⇒(i). Neka je zbir cifara broja n deljiv je sa 3 i cifra jedinica mu je 0. To znači da je

$$n = 10^k x_k + 10^{k-1} x_{k-1} + \cdots + 10 x_1$$

pri čemu je broj $x_k + x_{k-1} + \cdots + x_1$ deljiv sa 3.

Na isti način kao u (i)⇒(ii), matematičkom indukcijom dokazujemo da je $10^i \equiv 10 \pmod{10}$, za svaki $i \in \mathbb{N}$.

Odavde sledi da je

$$n \equiv 10(x_k + x_{k-1} + \cdots + x_2 + x_1) \pmod{30},$$

i kako je $x_k + x_{k-1} + \cdots + x_1$ deljiv sa 3, to je n deljiv sa 30. □

Produžena ekvivalencija

Dokaz može imati i strukturu produžene ekvivalencije

$$p_1 \Leftrightarrow p_2, \quad p_2 \Leftrightarrow p_3, \quad \cdots \ , \ p_{n-1} \Leftrightarrow p_n,$$

odnosno, dokazivanjem tačnosti tih ekvivalencija dokazujemo i tačnost ekvivalencije $p_1 \Leftrightarrow p_n$.

Ispravnost ovog metoda zasnovana je na tautologiji

$$\big[(p_1 \Leftrightarrow p_2) \wedge (p_2 \Leftrightarrow p_3) \wedge \cdots \wedge (p_{n-1} \Leftrightarrow p_n)\big] \Leftrightarrow (p_1 \Leftrightarrow p_n).$$

Ovaj metod se često koristi, na primer, kod rešavanja jednačina.

Naime, jednačina (formula) se zamenjuje ekvivalentnom sve do one u kojoj se rešenje neposredno nalazi, što ćemo videti u narednom primeru.

Takođe, ovaj metod se često koristi u dokazivanju skupovnih jednakosti, što ćemo pokazati kada se budemo bavili skupovima.

Primer 13: Koristeći metod produžene ekvivalencije rešiti jednačinu

$$\frac{2x+3}{7} = 3x,$$

Rešenje: Imamo sledeći niz ekvivalencija:

$$\begin{aligned} \frac{2x+3}{7} = 3x \quad &\Leftrightarrow \quad 2x+3 = 21x \\ &\Leftrightarrow \quad 3 = 19x \\ &\Leftrightarrow \quad x = \frac{3}{19}. \end{aligned}$$

Prema tome, rešenje jednačine je broj $\frac{3}{19}$. $\square$

Teoreme sa kvantifikatorima

Mnoge teoreme su formulisane tako da uključuju i kvantifikatore.

Postoje brojni metodi koji se koriste pri dokazivanju teorema sa kvantifikatorima, i možemo ih podeliti u četiri opšte kategorije:

(1) Metodi dokazivanja tvrđenja sa egzistencijalnim kvantifikovanjem, među kojima su najznačajniji
   * Metodi dokazivanja egzistencije;
   * Metodi dokazivanja jedinstvenosti;

(2) Metodi dokazivanja tvrđenja sa univerzalnim kvantifikovanjem, među kojima su najznačajniji
   * Metod iscrpljivanja;
   * Metod generalizacije iz generičkog primerka;

(3) Metodi opovrgivanja tvrđenja sa egzistencijalnim kvantifikovanjem;

(4) Metodi opovrgivanja tvrđenja sa univerzalnim kvantifikovanjem.

Dokazi egzistencije

Mnoge teoreme tvrde da postoje objekti određenog tipa.

Takve teoreme mogu se predstaviti u obliku $(\exists x)\, P(x)$, gde je $P(x)$ neki predikat.

Dokaz tvrđenja oblika $(\exists x)\, P(x)$ nazivamo dokaz egzistencije.

Često se takav dokaz izvodi tako što se eksplicitno odredi neki element a za koji je $P(a)$ tačno.

Takav dokaz naziva se konstruktivni dokaz egzistencije.

Međutim, moguće je dokazati da je $(\exists x)\, P(x)$ tačno i na neki drugi način, bez eksplicitnog pronalaženja elementa a za koji je $P(a)$ tačno.

Takav dokaz naziva se nekonstruktivni dokaz egzistencije.

Na primer, jedan od najčešće korišćenih načina da se tvrđenje $(\exists x)\, P(x)$ dokaže na nekonstruktivan način je da se iz negacije tog tvrđenja izvede kontradikcija.

Primer 14: **Konstruktivni dokaz egzistencije**

Dokazati da postoji prirodan broj koji se može na dva različita načina predstaviti kao zbir kubova dva prirodna broja.

Dokaz: **Posle puno izračunavanja, na primer, posle pretraživanja računarom, možemo utvrditi da je**

$$1729 = 10^3 + 9^3 = 12^3 + 1^3.$$

Prema tome, pronašli smo prirodan broj koji se može na dva različita načina predstaviti kao zbir kubova dva prirodna broja. □

Dokazi egzistencije

Zanimljivost: Kada je čuveni engleski matematičar Hardy u bolnici posetio bolesnog kolegu, isto tako čuvenog Indijskog matematičara Ramanujan-a, primetio je da je broj njegove sobe, 1729, prilično nezanimljiv.

Međutim, Ramanujan je odgovorio da je to veoma zanimljiv broj, jer je to najmanji prirodan broj koji se može na dva različita načina predstaviti kao zbir kubova dva prirodna broja.

Primer 15: **Nekonstruktivni dokaz egzistencije**

Dokazati da postoje iracionalni brojevi x i y takvi da je broj x^y racionalan.

Dokaz: Kao što smo bvideli, broj $\sqrt{2}$ je iraciuonalan.

Ako je broj $\sqrt{2}^{\sqrt{2}}$ racionalan, onda smo pronašli dva iracionalna broj x i y takva da je broj x^y raciuonalan, naime $x = \sqrt{2}$ i $y = \sqrt{2}$.

Sa druge strane, ako je $\sqrt{2}^{\sqrt{2}}$ iracionalan broj, onda možemo uzeti da je $x = \sqrt{2}^{\sqrt{2}}$ i $y = \sqrt{2}$, i u tom slučaju su x i y iracionalni brojevi i

$$x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{(\sqrt{2}\cdot\sqrt{2})} = \sqrt{2}^{2} = 2,$$

i dakle, x^y je racionalan broj. $\square$

Dokazi egzistencije

Ovaj dokaz je primer nekonstruktivnog dokaza egzistencije jer smo dokazali da postoje iracionalni brojevi x i y takvi da je broj x^y racionalan, ali ih nismo eksplicitno pronašli.

Naime, utvrdili smo da jedan od parova $x = \sqrt{2}$ i $y = \sqrt{2}$, odnosno $x = \sqrt{2}^{\sqrt{2}}$ i $y = \sqrt{2}$, sigurno zadovoljava taj uslov, ali nismo utvdili koji od njih to zadovoljava.

Dokazi jedinstvenosti

U nekim teoremama tvrdi se postojanje tačno jednog (jedinstvenog) elementa sa izvesnim svojstvom.

Dokazi takvih teorema nazivaju se dokazi jedinstvenosti, i sastoje se iz dve celine

dokaz egzistencije: dokazuje se da postoji element x sa datim svojstvom;

dokaz jedinstvenosti: dokazuje se da ako je y element različit od x, onda y nema to svojstvo, odnosno, dokazuje se da ako je y bilo koji drugi element sa tim svojstvom, onda mora biti $y = x$.

Dokazi jedinstvenosti

Primer 16: Dokazati da za svaki celi broj x postoji jedinstven celi broj y takav da je $x + y = 0$.

Dokaz: Najpre dokazujemo da takav broj postoji.

Zaista, za proizvoljan celi broj x, broj $-x$ ispunjava gornji uslov, odnosno $x + (-x) = x - x = 0$.

Dalje, dokazujemo da za x postoji tačno jedan celi broj koji ispunjava gornji uslov.

Pretpostavimo da postoje celi brojevi y i z takvi da važi $x + y = 0$ i $x + z = 0$.

Tada imamo da je

$$y = y + 0 = y + (x + z) = (y + x) + z = (x + y) + z = 0 + z = z,$$

čime smo dokazali jedinstvenost. □

Metod iscrpljivanja

Uzmimo da treba dokazati teoremu oblika $(\forall x)\, P(x)$, pri čemu je univerzum razmatranja konačan skup.

Takvu teoremu je moguće dokazati tako što ćemo proveriti sve elemente a konačnog univerzuma razmatranja i utvrditi da je $P(a)$ tačno.

Međutim, ta mogućnost je teorijska, jer čak i ako univerzum razmatranja ima konačan broj elemenata, taj broj može biti toliko veliki da čak i najbržim računarom, provera svih elemenata tog skupa može biti praktično neizvodljiva.

Ovakav metod dokazivanja nazivamo metod iscrpljivanja, jer se njime iscrpljuju svi mogući slučajevi, ili metod prostog nabrajanja.

Primer 17: Dokazati da je svaki paran broj između 4 i 32 zbir dva prosta broja.

Dokaz: Proverom svih parnih brojeva između 4 i 32 dobijamo da je

$$4 = 1 + 3 = 2 + 2$$
$$6 = 1 + 5 = 3 + 3$$
$$8 = 1 + 7 = 3 + 5$$
$$10 = 3 + 7 = 5 + 5$$
$$12 = 5 + 7 = 1 + 11$$
$$14 = 1 + 13 = 3 + 11 = 7 + 7$$
$$16 = 3 + 13 = 5 + 11$$
$$18 = 5 + 13 = 7 + 11$$
$$20 = 1 + 19 = 3 + 17 = 7 + 13$$
$$22 = 3 + 19 = 5 + 17 = 11 + 11$$
$$24 = 1 + 23 = 5 + 19 = 7 + 17 = 11 + 13$$
$$26 = 3 + 23 = 7 + 19 = 13 + 13$$
$$28 = 5 + 23 = 11 + 17$$
$$30 = 1 + 29 = 11 + 19 = 13 + 17$$
$$32 = 1 + 31 = 3 + 29 = 13 + 19$$

Ovim je tvrđenje dokazano. □

Metod generalizacije iz generičkog primerka

Najmoćnija tehnika za dokazivanje teorema oblika $(\forall x)\, P(x)$, koja ne zavisi od veličine univerzuma razmatranja, je metod generalizacije iz generičkog primerka.

Ovaj metod je baziran na pravilu zaključivanja o kome smo ranije govorili i koje smo zvali univerzalna generalizacija.

Dakle, da bi dokazali da svaki element univerzuma razmatranja ima izvesno svojstvo, pretpostavljamo da je x neki poseban, ali proizvoljno izabran element univerzuma razmatranja, i dokazujemo da x ima zadato svojstvo.

Iz toga, na osnovu pravila univerzalne generalizacije, zaključujemo da svi elementi univerzuma razmatranja imaju zadato svojstvo.

Metod generalizacije iz generičkog primerka

Proizvoljan izbor elementa x znači da o tom elementu ne pretpostavljamo ništa drugo što ne važi za sve elemente iz univerzuma razmatranja.

Proizvoljno izabrani element x je generički primerak, pri čemu termin "generički" znači da on "ima sve zajedničke karakteristike elemenata iz datog univerzuma razmatranja".

Dakle, sve što možemo zaključiti o generičkom primerku x uzetom iz univerzuma razmatranja jednako važi i za sve ostale elemente univerzuma razmatranja.

Metod generalizacije iz generičkog primerka

Primer 18: Dokazati teoremu: "Zbir svaka dva parna broja je paran broj."

Dokaz: Neka su m i n [posebni, ali proizvoljno izabrani] parni brojevi.

[Sada treba dokazati da je zbir $m+n$ paran] Prema definiciji parnog broja, postoje celi brojevi r i s takvi da je $m = 2r$ i $n = 2s$. Tada je

$$\begin{aligned} m+n &= 2r+2s && \text{[na osnovu pravila zamene]} \\ &= 2(r+2) && \text{[na osnovu zakona distributivnosti].} \end{aligned}$$

Neka je $k = r+s$. Tada je k ceo broj, jer je zbir dva cela broja. Dakle

$$m+n = 2k, \qquad \text{gde je } k \text{ ceo broj.}$$

Sada opet na osnovu definicije parnog broja zaključujemo da je $m+n$ paran broj. [To je ono što samo i trebali dokazati] $\square$

Opovrgivanje kontraprimerom

Već smo ranije rekli da se za tvrđenje oblika $(\forall x)\, P(x)$ može dokazati da nije tačno ako se pronađe element a univerzuma razmatranja takav da $P(a)$ nije tačno.

Za takav element smo rekli da se naziva **kontraprimer** za to tvrđenje, i kažemo da on **opovrgava** to tvrđenje.

Kada se sretnemo sa tvrđenjem oblika $(\forall x)\, P(x)$, za koje verujemo da nije tačno, ili su nam brojni pokušaji da pronađemo dokaz tog tvrđenja bili bezuspešni, onda ćemo pokušati da pronađemo kontraprimer za to tvrđenje.

Primer 19: Dokazati da sledeće tvrđenje nije tačno: "Svaki prirodan broj je zbir kvadrata tri prirodna broja".

Dokaz: Za ovo tvrđenje se može dokazati da nije tačno ako pronađemo kontraprimer za njega, odnosno ako nađemo prirodan broj koji nije zbir kvadrata tri prirodna broja.

Da bi pronašli kontraprimer, razmatramo jedan po jedan prirodan broj i proveravamo da li oni predstavljaju zbir kvadrata tri prirodna broja:

$$0 = 0^2 + 0^2 + 0^2 \qquad 1 = 0^2 + 0^2 + 1^2 \qquad 2 = 0^2 + 1^2 + 1^2$$
$$3 = 1^2 + 1^2 + 1^2 \qquad 4 = 0^2 + 0^2 + 2^2 \qquad 5 = 0^2 + 1^2 + 2^2$$
$$6 = 1^2 + 1^2 + 2^2$$

i kada dođemo do broja 7, videćemo da se on ne može predstaviti kao zbir kvadrata tri prirodna broja.

Opovrgivanje kontraprimerom

Naime, jedini kvadrati prirodnih brojeva koje možemo koristiti da bi dobili zbir 7 su oni koji su manji od 7, i to su samo 0, 1 i 4.

Jasno je da nijedna moguća trojka tih brojeva ne daje zbir 7.

Prema tome, broj 7 je kontraprimer polaznog tvrđenja, odakle zaključujemo da polazno tvrđenje nije tačno. $\square$

Opovrgivanje kontraprimerom

Primer 20: Opovrgnuti tvrđenje: "Za sve realne brojeve a i b, iz $a^2 = b^2$ sledi $a = b$".

Dokaz: Da bi opovrgli ovo tvrđenje, treba pronaći realne brojeve a i b takve da je $a^2 = b^2$ i $a \neq b$.

Ono što će nam biti od velike pomoći je činjenica da i pozitivni i negativni brojevi imaju pozitivne kvadrate, tako da se prirodno nameće da uzmemo neki pozitivni broj a i njemu suprotni broj $-a$.

Na primer, imamo da je $1^2 = 1 = (-1)^2$, a da je $1 \neq -1$.

Isto to možemo učiniti i sa 2 i -2, 0.5 i -0.5, itd. $\square$

Opovrgivanje tvrđenja o egzistenciji

Neka je dato neko tvrđenje oblika $(\exists x)\, P(x)$, odnosno ono koje tvrdi da postoji objekat sa izvesnim svojstvom.

Negacija takvog tvrđenja je oblika $(\forall x)\, \neg P(x)$, što znači da se tvrđenje $(\exists x)\, P(x)$ može opovrgnuti dokazivanjem tvrđenja $(\forall x)\, \neg P(x)$, na način kako se inače dokazuju tvrđenja sa univerzalnim kvantifikatorom.

Primer 20: Opovrgnuti tvrđenje: "Postoji prirodan broj n takav da je $n^2 + 3n + 2$ prost broj".

Dokaz: Da bi opovrgnuli ovo tvrđenje, treba da dokažemo da je tačno sledeće tvrđenje:

"Za svaki prirodan broj n, broj $n^2 + 3n + 2$ nije prost".

Krećemo sa dokazom ovog tvrđenja.

Opovrgivanje tvrđenja o egzistenciji

Uzmimo da je n bilo koji [poseban, ali proizvoljno izabran] prirodan broj. [Dokazaćemo da $n^2 + 3n + 2$ nije prost broj]

Broj $n^2 + 3n + 2$ možemo predstaviti u obliku

$$n^2 + 3n + 2 = (n + 1)(n + 2),$$

i kako su $n + 1$ i $n + 2$ celi brojevi, i važi $n + 1 > 1$ i $n + 2 > 1$ (jer je $n \geqslant 1$), to smo dobili da je $n^2 + 3n + 2$ proizvod dva prirodna broja veća od 1.

To znači da $n^2 + 3n + 2$ nije prost broj. [Što je i trebalo dokazati] □

Greške u dokazivanju

Postoje mnoge opšte greške koje se sreću u matematičkim dokazima, i ovde ćemo ukazati na neke od njih.

Zaključivanje na osnovu primera

Ne tako retka greška u dokazivanju potiče od pogrešnog shvatanja da se tvrđenje oblika $(\forall x)\, P(x)$ može dokazati na osnovu jednog ili više primera koji potvrđuju da je $P(x)$ tačno.

Međutim, bez obzira na to koliko mnogo primera postoji da je $P(x)$ tačno, tvrđenje $(\forall x)\, P(x)$ i dalje može biti netačno.

Ovakva greška u dokazivanju naziva se zaključivanje na osnovu primera.

Korišćenje istog slova za označavanje dve različite stvari

Česta greška koju prave početnici u dokazivanju teorema je da se nova promenljiva koja se uvodi označi istim slovom kojim je već označena neka promenljiva, što može značajno promeniti smisao i rezultat dokaza.

Na primer, u dokazu u kome se razmatraju dva neparna broja m i n, neko bi rezonovao na sledeći način:

> Neka su m i n neparni brojevi. Prema definiciji neparnog broja, $m = 2k + 1$ i $n = 2k + 1$, za neki ceo broj k.

To nije korektno, jer korišćenje istog simbola k u izrazima i za m i za n dovodi do toga da je $m = 2k + 1 = n$.

Odatle bi sledilo da se ostatak dokaza odnosi samo na cele brojeve m i n koji su međusobno jednaki, a to nije saglasno polaznoj pretpostavci da su m i n proizvoljno izabrani neparni brojevi.

Skakanje na zaključak

Skakanje na zaključak znači da se potvrdi istinitost nečega, a da se pri tome ne da adekvatan razlog za to.

Na taj način može se doći do pogrešnog zaključka, ali čak i kada je krajnji zaključak ispravan, neophodno je detaljno obrazložiti svaki korak u zaključivanju kojim smo došli do njega.

Razmotrimo sledeći jednostavan primer:

> **Neka su m i n bilo koji parni brojevi. Prema definiciji parnog broja, $m = 2r$ i $n = 2s$, za neke cele brojeve r i s. Tada je $m + n = 2r + 2s$. Dakle, $m + n$ je paran broj.**

Ovde je zaključak ispravan, ali je ipak preskočen ključni korak, jednakost $2r + 2s = 2(r + s)$, iz koje se jasno vidi kako smo došli do zaključka.

Pozivanje na ono što se dokazuje (Begging the question)

Ovo je jedna varijanta skakanja na zaključak, gde u dokazu pretpostavljamo i pozivamo se na ono što zapravo treba dokazati.

Razmotrimo sledeći primer "dokaza" da je proizvod dva neparna broja neparan:

> Neka su m i n neparni brojevi. Ako je mn neparan, tada je $mn = 2k + 1$, za neki ceo broj k. Takođe, kako su m i n neparni, to je $m = 2r + 1$ i $n = 2s + 1$, za neke cele brojeve r i s. Tada je $mn = (2r + 1)(2s + 1) = (2k + 1)$, odakle zaključujemo da je mn neparan broj.

Ono što u ovom "dokazu" nije dobro je to što se na samom početku pretpostavlja, a kasnije i koristi, ono što treba dokazati, a to je da je mn neparan broj.

Greške u dokazivanju

Ispravno bi bilo da se kaže

> **Tada je**
>
> $$mn = (2r+1)(2s+1) = 4rs + 2r + 2s + 1 = 2(2rs + r + s) + 1,$$
>
> **i ako stavimo da je $k = 2rs + r + s$, tada je k ceo broj i $mn = 2k + 1$. Prema tome, mn je neparan broj.**

Naravno, u ovom slučaju greška može ispraviti, jer je tvrđenje koje dokazujemo tačno.

Međutim, greška ovog tipa može se napraviti i tako da zahvaljujući njoj "dokažemo" i tvrđenje koje nije tačno.

Zloupotreba reči ako (if)

Ova opšta greška nije tako ozbiljna, ali oslikava neprecizno razmišljanje koje kasnije u dokazu može da napravi probleme.

Greška se satoji u mpogrešnom korišćenju reči ako (if) na mestima gde bi trebalo da stoji zato što je, kako je ili pošto je (because, since).

Razmotrimo sledeći fragment dokaza:

> Uzmimo da je p prost broj. Ako je p prost, onda p ne može biti napisan kao proizvod dva manja prirodna broja.

Korišćenje reči "ako" u prethodnoj rečenici nije pogodno. Ono sugeriše da je činjenica da je p prost broj pod sumnjom. Međutim, znamo da je p prost na osnovu prethodne rečenice.

Greške u dokazivanju

Dakle, p ne može biti ne može biti napisan kao proizvod dva manja prirodna broja zato što je prost.

Ispravna verzija ovog fragmenta bi bila:

> **Uzmimo da je p prost broj. Kako je p prost, to se p ne može biti napisan kao proizvod dva manja prirodna broja.**

Greške u dokazivanju

Primer 22: Šta je pogrešno u sledećem "dokazu" da je $1 = 2$?

"Dokaz:" Neka su a i b dva jednaka prirodna broja. Tada imamo

(1) $a = b$	pretpostavka
(2) $a^2 = ab$	množimo obe strane u (1) sa a
(3) $a^2 - b^2 = ab - b^2$	oduzimamo b^2 od obe strane u (2)
(4) $(a - b)(a + b) = b(a - b)$	faktorišemo obe strane u (3)
(5) $a + b = b$	delimo obe strane u (4) sa $a - b$
(6) $2b = b$	zamenjujemo a sa b, jer je $a = b$
(7) $2 = 1$	delimo obe strane u (6) sa b

Gde je greška?

Greške u dokazivanju

Primer 22: Šta je pogrešno u sledećem "dokazu" da je $1 = 2$?

"Dokaz:" Neka su a i b dva jednaka prirodna broja. Tada imamo

(1) $a = b$	pretpostavka
(2) $a^2 = ab$	množimo obe strane u (1) sa a
(3) $a^2 - b^2 = ab - b^2$	oduzimamo b^2 od obe strane u (2)
(4) $(a - b)(a + b) = b(a - b)$	faktorišemo obe strane u (3)
(5) $a + b = b$	delimo obe strane u (4) sa $a - b$
(6) $2b = b$	zamenjujemo a sa b, jer je $a = b$
(7) $2 = 1$	delimo obe strane u (6) sa b

Gde je greška?

U koraku (5) nismo smeli da delimo sa $a - b$, jer je $a - b = 0$