

Uvod u matematičku logiku

– predavanja –

Slavko Moconja

Sadržaj

1	Iskazi, promenljive i predikati	2
2	Iskazna logika	4
2.1	Izgradnja iskazne formule	4
2.2	Semantika iskazne logike	5
	<i>Digresija: Princip potpune indukcije</i>	6
	Semantika iskazne logike (nastavak)	8
2.3	Lema o smeni	10
2.4	Logička ekvivalentnost i normalne forme	11
2.5	Prirodna dedukcija	15
2.6	Izvedena pravila prirodne dedukcije	18
2.7	Logička posledica i teorema saglasnosti	21
2.8	Slaba teorema potpunosti	23
2.9	Teorema kompaktnosti	24
	<i>Digresija: Aksioma izbora</i>	26
	Teorema kompaktnosti (nastavak)	26
2.10*	Primeri primene teoreme kompaktnosti	27
2.10.1	Uređenja racionalnih brojeva	27
2.10.2	Linearizacija parcijalnih uređenja	29
2.10.3	4-objivost planarnih grafova	30
2.10.4	Remzijeva teorema	31
2.11	Teorema potpunosti	33
3	Skupovi	34
3.1	Podskup	35
3.2	Osnovne skupovne operacije	35
3.3	Veza za iskaznom logikom	39
3.4	Algebarska normalna forma	42
3.5	Partitivni skup	43
3.6	Dekartov proizvod	44
4	Relacije	47
4.1	Podrelacija i skupovne operacije sa relacijama	48
4.2	Inverzna relacija	49
4.3	Kompozicija relacija	51
4.4	Osobine binarnih relacija na skupu S	54
4.5	Ekvivalencije	55
4.6	Uređenja	58

4.7*	Vitalijev skup	63
5	Funkcije	64
5.1	Funkcionalne relacije	64
5.2	Funkcije	65
5.3	1-1 i na funkcije, bijekcije	66
5.4	Egzistencija inverzne funkcije	67
5.5	Direktna i inverzna slika skupa	68
6	Kardinalnost	69
6.1	Definicija i osnovne osobine	69
6.2	Neke opšte (ne)jednakosti	70
6.3	Prebrojivi skupovi	72
6.4	Skupovi moći kontinuuma	74
6.5	Kardinalnost skupa $\mathcal{P}(\mathbb{N})$	74
6.6	Kantorov dijagonalni argument	75
6.7	Dokaz KŠB teoreme	76
6.8*	Dokaz Bernštajnovе teoreme	77

1 Iskazi, promenljive i predikati

Iskaz je rečenica ili matematički izraz koji ima *istinitosnu vrednost*, tj. tačan je ili netačan.¹ Npr. rečenica „Površina kvadrata stranice a jednaka je a^2 .” je primer tačnog iskaza, „Svaki prvougaonik je kvadrat.” je primer netačnog iskaza, „Izračunati obim kvadrata stranice a .” nije iskaz. Slično, izraz „ $\sin \frac{\pi}{4} = \frac{\sqrt{2}}{2}$ ” je primer tačnog iskaza, „ $\sin \frac{\pi}{4} = 5$ ” je primer netačnog iskaza, dok „ $\sin x = \frac{\sqrt{2}}{2}$ ” nije iskaz.

Tačnost iskaza često zavisi od (matematičkog) konteksta, pa je tako iskaz „Ako su u ravni π date prava p i tačka P van nje, onda u π postoji jedinstvena prava koja prolazi kroz P i ne seče p .” tačan u euklidskoj geometriji (geometrija sa kojom smo upoznati), ali je netačan u hiperboličkoj geometriji. Takođe, ponekad je jasno da je neka rečenica iskaz, ali njeova tačnost nije poznata. Npr. „Svaki paran prirodan broj veći od dva je zbir dva prosta broja.” očigledno jeste iskaz (ovo bi trebalo da je ili tačno ili netačno), međutim tačnost ovog iskaza nije poznata (u pitanju je čuvena Goldbahova hipoteza).

U matematici postoji nekoliko standardnih konstrukcija kojima polazeći od prostijih iskaza gradimo složenije.

Negacija iskaza φ je iskaz „Ne važi φ .” koji obeležavamo sa $\neg\varphi$ (čitamo „ne φ ”). Tačnost iskaza $\neg\varphi$ suprotna je tačnosti iskaza φ (ako je φ tačan, $\neg\varphi$ je netačan, i ako je φ netačan, $\neg\varphi$ je tačan). To najčešće zapisujemo sledećom istinitosnom tablicom:

φ	$\neg\varphi$
T	N
N	T

Konjunkcija iskaza φ i ψ je iskaz „Važe oba φ i ψ .” koji obeležavamo sa $\varphi \wedge \psi$ (čitamo „ φ i ψ ”). Konjunkcija $\varphi \wedge \psi$ je tačna samo u slučaju da su oba iskaza φ i ψ tačni:

φ	ψ	$\varphi \wedge \psi$
T	T	T
T	N	N
N	T	N
N	N	N

¹U ovom tekstu tačno obeležavamo sa T , a netačno sa N .

(*Inkluzivna*) *disjunkcija* iskaza φ i ψ je iskaz „Važi bar jedan od φ i ψ .“ koji obeležavamo sa $\varphi \vee \psi$ (najčešće čitamo „ φ ili ψ “). Disjunkcija $\varphi \vee \psi$ je netačna samo u slučaju da su oba iskaza φ i ψ netačni:

φ	ψ	$\varphi \vee \psi$
T	T	T
T	N	T
N	T	T
N	N	N

(*Ekskluzivna*) *disjunkcija* iskaza φ i ψ je iskaz „Važi tačno jedan od φ i ψ .“ koji obeležavamo sa $\varphi \underline{\vee} \psi$ (najčešće čitamo „ili φ ili ψ “²). Ekskluzivna disjunkcija $\varphi \underline{\vee} \psi$ je tačna samo kada je jedan od iskaza φ i ψ tačan a drugi netačan:

φ	ψ	$\varphi \underline{\vee} \psi$
T	T	N
T	N	T
N	T	T
N	N	N

(*Materijalna*) *implikacija* iskaza φ i ψ je iskaz „Ako važi φ , onda važi ψ .“ koji obeležavamo sa $\varphi \rightarrow \psi$ (čitamo „ako φ , onda ψ “, ili „iz φ sledi ψ “, ili „ φ povlači ψ “, ili „ ψ , ako φ “, ili „ φ , samo ako ψ “, ili „ φ je dovoljan uslov za ψ “, ili „ ψ je potreban uslov za φ “). Iskaz $\varphi \rightarrow \psi$ je netačan samo u slučaju da je φ tačan i ψ netačan:

φ	ψ	$\varphi \rightarrow \psi$
T	T	T
T	N	N
N	T	T
N	N	T

(*Ekvivalencija*) iskaza φ i ψ je iskaz „Iskazi φ i ψ su jednake tačnosti.“ koji obeležavamo sa $\varphi \leftrightarrow \psi$ (čitamo „ φ ako i samo ako ψ “, ili „ φ je ekvivalentno sa ψ “, ili „ φ je potreban i dovoljan uslov za ψ “). Ekvivalencija je tačna samo kada su φ i ψ jednake tačnosti:

φ	ψ	$\varphi \leftrightarrow \psi$
T	T	T
T	N	N
N	T	N
N	N	T

Promenljiva je simbol koji koristimo da predstavimo matematičke objekte. *Univerzum diskursa* neke promenljive je skup čije objekte ona predstavlja (tj. skup u kome ona uzima vrednosti). Univerzum diskursa je najčešće jasan iz konteksta. Univerzum diskursa promenljive x ćemo obeležavati sa $\mathcal{U}_x$. Npr. ako posmatramo izraz „ $\sin x = \frac{\sqrt{2}}{2}$ “, dosadašnje matematičko obrazovanje nam kaže da x uzima vrednosti u skupu $\mathbb{R}$, tj. $\mathcal{U}_x = \mathbb{R}$. Slično, ako posmatramo izraz „ $p \parallel q$ “, najverovatnije govorimo o paralelnosti dve prave, tj. promenljive p i q predstavljaju prave, pa je $\mathcal{U}_p = \mathcal{U}_q$ neki skup pravih. Nekada nam je univerzum diskursa promenljive eksplicitno rečen u tekstu. Npr. u zadatku: „Naći realna rešenja jednačine $x + \sqrt{3 + \sqrt{x}} = 3$.“, eksplicitno nam je rečeno da je $\mathcal{U}_x = \mathbb{R}$.

Predikat je rečenica ili matematički izraz u kome figuriše jedna ili više promenljivih, a koji postaje iskaz (tačan ili netačan) kada svaka promenljiva uzme konkretnu vrednost iz svog univerzuma diskursa. Tako je npr. „ x je prost broj“ predikat u kome figuriše promenljiva x čiji je univerzum diskursa najverovatnije skup prirodnih brojeva. Ako prethodni predikat obeležimo sa $P(x)$, vidimo da je $P(3)$ tačan iskaz, a da je $P(4)$ netačan iskaz.

²Primitite razliku, $\varphi \vee \psi$ se čita „ φ ili ψ “, a $\varphi \underline{\vee} \psi$ se čita „ili φ ili ψ “.

Ako sa $Q(x, a, b, c)$ obeležimo predikat „ $ax^2 + bx + c = 0$ “, gde je $\mathcal{U}_x = \mathbb{C}$ i $\mathcal{U}_a = \mathcal{U}_b = \mathcal{U}_c = \mathbb{R}$, lako vidimo da je npr. $Q(i, 1, 0, 1)$ tačan iskaz, a da je npr. $Q(-1, 2, 1, 1)$ netačan iskaz.

Neka je $P(x)$ predikat. Iskaz „Za svaki objekat t (odgovarajućeg univerzuma diskursa $\mathcal{U}_x$) iskaz $P(t)$ je tačan.“ obeležavamo sa $(\forall x) P(x)$, i čitamo „Za svako x važi $P(x)$.“ Dakle, iskaz $(\forall x) P(x)$ je tačan ako je iskaz $P(t)$ tačan za sve $t \in \mathcal{U}_x$. Npr. iskaz $(\forall x) x^2 \geq 0$, gde je $\mathcal{U}_x = \mathbb{R}$, jeste tačan jer je kvadrat svakog realnog broja nenegativan; iskaz $(\forall x) x^2 > 0$, gde je ponovo $\mathcal{U}_x = \mathbb{R}$, je netačan jer kvadrat nule nije pozitivan. Simbol $\forall$ se zove *univerzalni kvantifikator*, a za iskaz $(\forall x) P(x)$ kažemo da je dobijen *univerzalnom kvantifikacijom*.

Standardne iskazne konstrukcije (negacija, konjunkcija, itd.) mogu da se primenjuju i na predikate, pri čemu dobijamo komplikovanije predikate. Vrednosti takvih predikata se računaju kao i u slučaju iskaza.

Neka je i dalje $P(x)$ predikat. Iskaz „Za neki (bar jedan) objekat t (odgovarajućeg univerzuma diskursa $\mathcal{U}_x$) iskaz $P(t)$ je tačan.“ obeležavamo sa $(\exists x) P(x)$, i čitamo „Postoji x tako da važi $P(x)$.“, ili „Za neko x važi $P(x)$.“ Iskaz $(\exists x) P(x)$ je tačan ako je iskaz $P(t)$ tačan za bar jedan objekat $t \in \mathcal{U}_x$. Npr. iskaz $(\exists x) x^2 \leq 0$, $\mathcal{U}_x = \mathbb{R}$, je tačan jer je kvadrat nule jednak nuli; iskaz $(\exists x) x^2 < 0$, $\mathcal{U}_x = \mathbb{R}$, je netačan. Simbol $\exists$ se zove *egzistencijalni kvantifikator*, a za iskaz $(\exists x) P(x)$ kažemo da je dobijen *egzistencijalnom kvantifikacijom*.

Kvantifikaciju možemo da primenimo i na predikate sa više promenljivih, ali u tom slučaju ne dobijamo iskaz nego novi predikat. Neka je $P(x, y_1, \dots, y_n)$ predikat. Tada je $(\forall x) P(x, y_1, \dots, y_n)$ novi predikat čije su promenljive $y_1, \dots, y_n$ određen na sledeći način: za objekte $t_1 \in \mathcal{U}_{y_1}, \dots, t_n \in \mathcal{U}_{y_n}$ iskaz $(\forall x) P(x, t_1, \dots, t_n)$ je tačan ako je za sve objekte $s \in \mathcal{U}_x$ iskaz $P(s, t_1, \dots, t_n)$ tačan. Slično, $(\exists x) P(x, y_1, \dots, y_n)$ je novi predikat čije su promenljive $y_1, \dots, y_n$ određen sa: za objekte $t_1 \in \mathcal{U}_{y_1}, \dots, t_n \in \mathcal{U}_{y_n}$ iskaz $(\exists x) P(x, t_1, \dots, t_n)$ je tačan ako je za neki (bar jedan) objekat $s \in \mathcal{U}_x$ iskaz $P(s, t_1, \dots, t_n)$ tačan. Na ovako dobijene predikate ponovo možemo da primenimo postupak kvantifikacije, pa npr. možemo da dobijemo iskaz $(\forall x)(\exists y) P(x, y)$ ili $(\exists x)(\exists y) P(x, y)$, itd.

Neka je $P(x)$ predikat i $S \subseteq \mathcal{U}_x$. *Ograničenja kvantifikatora na skup S* su iskazi $(\forall x \in S) P(x)$ i $(\exists x \in S) P(x)$ definisani sa:

$$(\forall x \in S)(x \in S \rightarrow P(x)) \quad \text{i} \quad (\exists x \in S)(x \in S \wedge P(x)).$$

Primetimo da $(\forall x \in S) P(x)$ ima značenje „za sve $t \in S$ važi iskaz $P(t)$ “, i da $(\exists x \in S) P(x)$ ima značenje „za bar jedan $t \in S$ važi iskaz $P(t)$ “. Na isti način definišemo ograničenja kvantifikatora $(\forall x \in S) Q(x, y_1, \dots, y_n)$ i $(\exists x \in S) Q(x, y_1, \dots, y_n)$.

Primetimo, specijalno, da je iskaz $(\forall x \in \emptyset) P(x)$ uvek logički tačan, a iskaz $(\exists x \in \emptyset) P(x)$ uvek logički netačan. Zaista, za svako $t \in \mathcal{U}_x$ imamo:

$$\underbrace{t \in \emptyset \rightarrow P(t)}_T \quad \text{i} \quad \underbrace{t \in \emptyset \wedge P(t)}_N.$$

Slično, predikat $(\forall x \in \emptyset) Q(x, y_1, \dots, y_n)$ je tačan nezavisno od izbora vrednosti za promenljive $y_1, \dots, y_n$, a predikat $(\exists x \in \emptyset) Q(x, y_1, \dots, y_n)$ je netačan nezavisno od izbora vrednosti za promenljive $y_1, \dots, y_n$.

2 Iskazna logika

2.1 Izgradnja iskazne formule

Definicija 2.1. *Iskazne formule* su konačni nizovi sledećih simbola:

- *iskaznih slova* koje obično zapisujemo malim latiničnim slovima $p, q, r, \dots$, moguće sa indeksima; skup iskaznih slova obeležavamo sa P ;
- *logičkih konstanti*: $\perp$ (*kontradikcija*) i $\top$ (*tautologija*);
- *logičkih veznika*: $\neg$ (*negacija*), $\wedge$ (*konjunkcija*), $\vee$ (*disjunkcija*), $\underline{\vee}$ (*ekskluzivna disjunkcija*), $\rightarrow$ (*implikacija*) i $\leftrightarrow$ (*ekvivalencija*);

- pomoćnih simbola zagrada.

Iskazne formule gradimo primenom sledećih pravila u konačno mnogo koraka:

- iskazna slova i konstante su iskazne formule;
- ako su φ i ψ (već izgrađene) iskazne formule, onda su i $\neg\varphi$, $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $(\varphi \underline{\vee} \psi)$, $(\varphi \rightarrow \psi)$ i $(\varphi \leftrightarrow \psi)$ iskazne formula.

Skup svih iskaznih formula obeležavamo sa Φ .

Ako je nedvosmisleno jasno o kojoj formuli je reč, brisaćemo višak zagrada (npr. spoljne zagrade). Pri tome podrazumevamo da veznik $\neg$ ima najviši prioritet, $\vee$ i $\wedge$ srednji prioritet, a $\underline{\vee}$, $\rightarrow$ i $\leftrightarrow$ najniži prioritet, pa tako sa $\neg p \vee q \rightarrow r \wedge \neg s$ je kraće zapisana formula $((\neg p) \vee q) \rightarrow (r \wedge (\neg s))$.

Komentar 2.2. Primetimo da je u svakoj formuli broj pojavljivanja iskaznih slova i broj pojavljivanja veznika konačan. Konačan skup iskaznih slova koja se pojavljuju u formuli φ obeležavamo sa $P(\varphi)$, a broj pojavljivanja veznika u formuli φ obeležavamo sa $sl(\varphi)$ i zovemo ga *složenost* formule φ .

Komentar 2.3. Ako je $sl(\varphi) = 0$, onda je φ konstanta ili slovo. Ako je $sl(\varphi) > 0$, onda je φ oblika $\neg\psi$, ili oblika $\psi * \theta$ za neki veznik $*$ $\in \{\wedge, \vee, \underline{\vee}, \rightarrow, \leftrightarrow\}$. Ako je φ oblika $\neg\psi$, primetimo da je $sl(\psi) = sl(\varphi) - 1 < sl(\varphi)$ (zaista, φ ima jedan veznik $\neg$ više od ψ); ako je φ oblika $\psi * \theta$, primetimo da je $sl(\psi) + sl(\theta) = sl(\varphi) - 1$ (zaista, φ ima jedan veznik $*$ više od ψ i θ zajedno), odakle sledi $sl(\psi) < sl(\varphi)$ i $sl(\theta) < sl(\varphi)$.

Takođe, $P(\perp) = P(\top) = \emptyset$ i $P(p) = \{p\}$. Ako je φ oblika $\neg\psi$, primetimo da je $P(\varphi) = P(\psi)$. Ako je φ oblika $\psi * \theta$, primetimo da je $P(\varphi) = P(\psi) \cup P(\theta)$; specijalno, $P(\psi) \subseteq P(\varphi)$ i $P(\theta) \subseteq P(\varphi)$.

2.2 Semantika iskazne logike

Definicija 2.4. *Valuacija* je bilo koje dodeljivanje tačnosti iskaznim slovima: $v : P \rightarrow \{T, N\}$. Skup svih valuacija obeležavamo sa $\mathcal{V}$.

Za fiksiranu valuaciju v određujemo istinitosnu vrednost svake formule φ pri valuaciji v , u oznaci $\hat{v}(\varphi)$, rekurentno po izgradnji formule na sledeći način:

- $\hat{v}(\perp) = N$ i $\hat{v}(\top) = T$;
- $\hat{v}(p) = v(p)$ za svako slovo $p \in P$;
- $\hat{v}(\neg\varphi)$ računamo po tablici za negaciju:

$\hat{v}(\varphi)$	$\hat{v}(\neg\varphi)$
T	N
N	T

- $\hat{v}(\varphi \wedge \psi)$, $\hat{v}(\varphi \vee \psi)$, $\hat{v}(\varphi \underline{\vee} \psi)$, $\hat{v}(\varphi \rightarrow \psi)$ i $\hat{v}(\varphi \leftrightarrow \psi)$ računamo po tablicama:

$\hat{v}(\varphi)$	$\hat{v}(\psi)$	$\hat{v}(\varphi \wedge \psi)$	$\hat{v}(\varphi \vee \psi)$	$\hat{v}(\varphi \underline{\vee} \psi)$	$\hat{v}(\varphi \rightarrow \psi)$	$\hat{v}(\varphi \leftrightarrow \psi)$
T	T	T	T	N	T	T
T	N	N	T	T	N	N
N	T	N	T	T	T	N
N	N	N	N	N	T	T

Ako je $\hat{v}(\varphi) = T$ (formula φ je tačna pri valuaciji v), to još zapisujemo sa $v \models \varphi$ i čitamo v *zadovoljava* formulu φ . Ako je $\hat{v}(\varphi) = N$ (formula φ je netačna pri valuaciji v), to još zapisujemo sa $v \not\models \varphi$ i čitamo v *poriče* (ili *ne zadovoljava*) formulu φ .

Intuitivno je jasno da vrednost formule pri valuaciji v zavisi samo od vrednosti konačno mnogo slova koja se u toj formuli pojavljuju. To ćemo strogo i da dokažemo.

Teorema 2.5. Neka $\varphi \in \Phi$ i $v \in \mathcal{V}$. Vrednost $\hat{v}(\varphi)$ zavisi samo od vrednosti valuacije v na skupu slova $P(\varphi)$.

Dokazi teorema koje govore o formulama (kao što je prethodna teorema) najčešće se izvode koristeći princip potpune indukcije.

Digresija: Princip potpune indukcije

Skup prirodnih brojeva je $\mathbb{N} = \{0, 1, 2, 3, 4, \dots\}$.

Princip matematičke indukcije je jedan od osnovnih postupaka za dokazivanje u matematici. U pitanju je sledeće tvrđenje:

Aksioma 2.6 (Princip matematičke indukcije). Neka je $P(n)$, $n \in \mathbb{N}$, predikat. Ako su tačni iskazi:

- $P(0)$, i (baza indukcije)
- $(\forall n)(P(n) \rightarrow P(n+1))$, (indukcijski korak)

onda je i iskaz $(\forall n) P(n)$ tačan.

Primetimo da je princip matematičke indukcije intuitivno jasan. Naime, baza indukcije kaže da je $P(0)$ tačan iskaz. Iz koraka znamo da je $P(0) \rightarrow P(1)$ tačan iskaz, pa kako je $P(0)$ tačan, zaključujemo i da je $P(1)$ tačan. Ponovo iz koraka znamo da je $P(1) \rightarrow P(2)$ tačan iskaz, pa kako je $P(1)$ tačan, zaključujemo i da je $P(2)$ tačan. Nastavljajući ovaj postupak zaključujemo da je $(\forall n) P(n)$ tačan iskaz.

Dokaz iskaza $(\forall n) P(n)$ koristeći princip matematičke indukcije svodi se na dokaz baze indukcije (iskaza $P(0)$) i induksijskog koraka (iskaza $(\forall n)(P(n) \rightarrow P(n+1))$). Baza indukcije obično je stvar lake provere. Za dokaz induksijskog koraka uočavamo proizvoljno $n \in \mathbb{N}$ i dokazujemo implikaciju $P(n) \rightarrow P(n+1)$. Za dokaz poslednje implikacije obično koristimo postupak dedukcije: pretpostavljamo da važi $P(n)$, što je pretpostavka koju nazivamo *indukcijska hipoteza* i obeležavamo sa (IH), i cilj je da dokažemo $P(n+1)$ pogodno koristeći (IH).

Sam zapis dokaza indukcijom obično je sledećeg oblika:

Dokažimo $(\forall n) P(n)$ indukcijom po n .

Baza indukcije. Proveravamo da važi $P(0)$.

Indukcijski korak. Neka je $n \in \mathbb{N}$ proizvoljno.

Pretpostavimo $P(n)$ (IH), i dokažimo $P(n+1)$.

Sada pišemo dokaz za $P(n+1)$ pogodno koristeći (IH).

Navedimo nekoliko primera primene principa matematičke indukcije.

Primer 2.7. Dokazati $64 \mid 3^{2n+2} - 8n - 9$ za sve $n \in \mathbb{N}$.

Rešenje. Dokažimo $(\forall n) 64 \mid 3^{2n+2} - 8n - 9$ indukcijom po n .

Baza indukcije. Za $n = 0$ proveravamo $64 \mid 3^{2 \cdot 0 + 2} - 8 \cdot 0 - 9$, tj. $64 \mid 0$, što je trivijalno tačno.

Indukcijski korak. Neka je $n \in \mathbb{N}$ proizvoljno. Pretpostavimo $64 \mid 3^{2n+2} - 8n - 9$ (IH), i dokažimo $64 \mid 3^{2(n+1)+2} - 8(n+1) - 9$. Imamo sledeći račun:

$$\begin{aligned} 3^{2(n+1)+2} - 8(n+1) - 9 &= 9 \cdot 3^{2n+2} - 8n - 17 \\ &= 9 \cdot (3^{2n+2} - 8n - 9) + 64n + 64 \quad \text{nameštamo na (IH).} \end{aligned}$$

Po (IH) 64 deli prvi sabirak, dok su drugi i treći očigledno deljivi sa 64 . Prema tome, 64 deli ceo zbir, tj. $64 \mid 3^{2(n+1)+2} - 8(n+1) - 9$, što smo i želeli da dokažemo. $\square$

Princip matematičke indukcije možemo da koristimo i za iskaze oblika $(\forall n \geq n_0) P(n)$. U tom slučaju baza je iskaz $P(n_0)$, a korak je iskaz $(\forall n \geq n_0)(P(n) \rightarrow P(n+1))$.

Primer 2.8. Dokazati $2^n > n^2$ za sve $n \geq 5$.

Rešenje. Dokažimo $(\forall n \geq 5) 2^n > n^2$ indukcijom po n .

Baza indukcije. Za $n = 5$ proveravamo $2^5 > 5^2$, tj. $32 > 25$ što jeste tačno.

Indukcijski korak. Neka je $n \geq 5$ proizvoljno, pretpostavimo $2^n > n^2$ (IH), i dokažimo $2^{n+1} > (n+1)^2$.

Izvodimo sledeći račun:

$$\begin{aligned} 2^{n+1} &= 2 \cdot 2^n \\ &> 2 \cdot n^2 && \text{po (IH)} \\ &= n^2 + n^2 \\ &> n^2 + 2n + 1 && \text{jer } n^2 > 2n + 1 \text{ za } n \geq 5 \\ &= (n+1)^2. \end{aligned}$$

(U pretposlednjem koraku smo koristili $n^2 > 2n + 1$ ako i samo ako $(n-1)^2 > 2$, što za $n \geq 5$ jeste tačno jer je tada $n-1 \geq 4$, pa je $(n-1)^2 \geq 16 > 2$.) Prema tome, dokazali smo $2^{n+1} > (n+1)^2$, kao što smo i želeli. $\square$

Ponekad u dokazima iskaza $(\forall n) P(n)$ ili $(\forall n \geq n_0) P(n)$ nije lako ustanoviti indukcijski korak, ali je moguće ustanoviti implikacije oblika $P(n) \wedge P(n+1) \rightarrow P(n+2)$ ili $P(n) \wedge P(n+1) \wedge P(n+2) \rightarrow P(n+3)$, ili opštije $P(n) \wedge P(n+1) \wedge \dots \wedge P(n+(k-1)) \rightarrow P(n+k)$ za neko fiksirano $k \geq 2$. U tom slučaju takođe je moguće iskoristiti princip indukcije, pri čemu je baza iskaz $P(n_0) \wedge P(n_0+1) \wedge \dots \wedge P(n_0+k)$, a korak je iskaz $(\forall n \geq n_0)(P(n) \wedge P(n+1) \wedge \dots \wedge P(n+k-1) \rightarrow P(n+k))$.

Primer 2.9. Niz (a_n) definisan je sa $a_0 = 0$, $a_1 = 1$, $a_2 = 4$ i $a_{n+3} = 3a_{n+2} - 3a_{n+1} + a_n$ za sve $n \in \mathbb{N}$. Dokazati $a_n = n^2$ za sve $n \in \mathbb{N}$.

Rešenje. Dokaz izvodimo indukcijom po n sa tri indukcijske hipoteze.

Baza indukcije. Za $n = 0$, $n = 1$ i $n = 2$ imamo $a_0 = 0 = 0^2$, $a_1 = 1 = 1^2$ i $a_2 = 4 = 2^2$ direktno po definiciji.

Indukcijski korak. Neka je $n \in \mathbb{N}$ proizvoljno, pretpostavimo $a_n = n^2$, $a_{n+1} = (n+1)^2$ i $a_{n+2} = (n+2)^2$ (IH), i dokažimo $a_{n+3} = (n+3)^2$. Krenimo s leve strane:

$$\begin{aligned} a_{n+3} &= 3a_{n+2} - 3a_{n+1} + a_n && \text{po definiciji} \\ &= 3(n+2)^2 - 3(n+1)^2 + n^2 && \text{po (IH)} \\ &= 3n^2 + 12n + 12 - 3n^2 - 6n - 3 + n^2 \\ &= n^2 + 6n + 9 \\ &= (n+3)^2, \end{aligned}$$

kao što smo i želeli. $\square$

Iskaz $(\forall n) P(n)$ moguće je zaključiti ako znamo da za svako $n \in \mathbb{N}$ možemo zaključiti $P(n)$ koristeći sve $P(m)$ za $m < n$ kao hipoteze. Odgovarajući princip će nam posebno biti koristan:

Teorema 2.10 (Princip potpune indukcije). Neka je $P(n)$, $n \in \mathbb{N}$, predikat. Ako je tačan iskaz:

- $(\forall n)((\forall m < n) P(m) \rightarrow P(n))$,

onda je i iskaz $(\forall n) P(n)$ tačan.

Dokaz. Uočimo predikat $Q(n): (\forall m < n) P(m)$; pretpostavka teoreme tada glasi $(\forall n)(Q(n) \rightarrow P(n))$. Primećimo da je dovoljno da dokažemo $(\forall n) Q(n)$. Zaista, tada je za proizvoljno k iskaz $Q(k+1)$ tačan, pa je specijalno tačan i iskaz $P(k)$, odakle zaključujemo $(\forall n) P(n)$ (jer je k bilo proizvoljno). Tačnost iskaza $(\forall n) Q(n)$ dokazujemo koristeći princip matematičke indukcije.

Baza indukcije. Iskaz $Q(0): (\forall m < 0) P(m)$ je logički tačan jer je $(\forall m < 0)$ ograničenje univerzalnog kvantifikatora na prazan skup.

Indukcijski korak. Neka je k proizvoljno, i pretpostavimo da je iskaz $Q(k) := (\forall m < k) P(m)$ tačan. Primećimo da je $Q(k+1)$ logički ekvivalentan sa $Q(k) \wedge P(k)$, prema tome dovoljno je da dokažemo da je $P(k)$ tačan. Međutim to sledi iz pretpostavke teoreme $(\forall n)(Q(n) \rightarrow P(n))$ i indukcijske hipoteze $Q(k)$. $\square$

Da bismo potpunom indukcijom dokazali $(\forall n) P(n)$, postupamo na sledeći način: za proizvoljno $n \in \mathbb{N}$ pretpostavljamo $(\forall m < n) P(k)$, i cilj nam je da dokažemo $P(n)$. Primećimo da princip potpune indukcije ne zahteva bazni korak, međutim u praksi je obično potrebno razmotriti nekoliko specijalnih slučajeva koje možemo smatrati bazom.

Primer 2.11. Niz (a_n) definisan je sa $a_0 = 0$ i $a_n = a_{\lfloor \frac{n}{3} \rfloor} + 1$ za $n \geq 1$. Dokazati $\log_3(n+1) \leq a_n$ za sve $n \in \mathbb{N}$.

Rešenje. Dokaz izvodimo potpunom indukcijom po n . Neka je $n \in \mathbb{N}$ proizvoljno, pretpostavimo $(\forall m < n) \log_3(m+1) \leq a_m$ (IH), i dokažimo $\log_3(n+1) \leq a_n$. S obzirom na definiciju niza, razmotrićemo dva slučaja.

1° $n=0$: Treba da proverimo $\log_3 1 \leq a_0$, tj. $0 \leq 0$, što je očigledno tačno.

2° $n \geq 1$: Imamo sledeći račun:

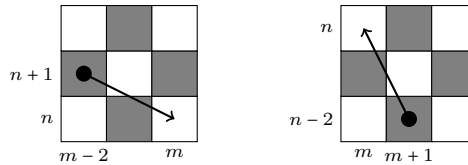
$$\begin{aligned} a_n &= a_{\lfloor \frac{n}{3} \rfloor} + 1 && \text{po definiciji} \\ &\geq \log_3\left(\left\lfloor \frac{n}{3} \right\rfloor + 1\right) + 1 && \text{po (IH) jer } \left\lfloor \frac{n}{3} \right\rfloor < n \text{ za } n \geq 1 \\ &\geq \log_3 \frac{n+1}{3} + 1 && \text{jer } \left\lfloor \frac{n}{3} \right\rfloor + 1 \geq \frac{n+1}{3} \\ &= \log_3(n+1). \end{aligned}$$

(Iskorišćena nejednakost $\left\lfloor \frac{n}{3} \right\rfloor + 1 \geq \frac{n+1}{3}$ ekvivalentna je sa $\frac{n}{3} - \left\lfloor \frac{n}{3} \right\rfloor \leq \frac{2}{3}$, koju lako dokazujemo ako razmotrimo slučajeve $n = 3m$, $n = 3m + 1$ i $n = 3m + 2$, za $m \in \mathbb{N}$.) Dokazali smo željenu nejednakost. $\square$

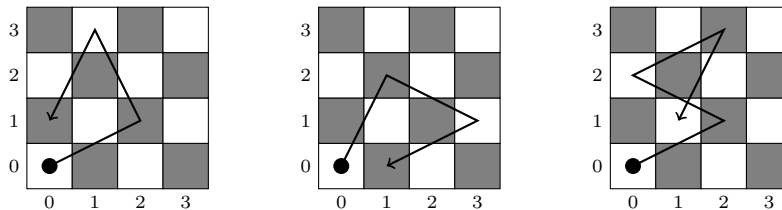
Primer 2.12. Data je šahovska tabla koja je beskonačna „u desno“ i „na gore“. U donjem levom uglu nalazi se skakač. Dokazati da skakač može da pređe na bilo koje drugo polje u konačno mnogo poteza.

Rešenje. Numerišimo polje u n -tom redu i m -toj koloni sa (m, n) , $m, n \geq 0$. Prema tome, skakač je na početku na polju $(0, 0)$ i mi želimo da dokažemo da skakač može da pređe u konačno mnogo koraka na polje (m, n) za proizvoljne m i n . Dokaz ćemo izvesti potpunom indukcijom po $k = m + n$.

Neka je $k \in \mathbb{N}$ proizvoljno, pretpostavimo da skakač može da dođe na polje (m', n') za $m' + n' < k$ (IH), i dokažimo da skakač može da dođe na polje (m, n) za $m + n = k$. Ako je $m \geq 2$, $m-2 \in \mathbb{N}$ i $(m-2) + (n+1) < m+n = k$, pa po (IH) skakač može da dođe na polje $(m-2, n+1)$. Odatle u jednom skoku dolazimo na polje (m, n) . Slično, ako je $n \geq 2$, po (IH) skakač može da dođe na polje $(m+1, n-2)$, odakle u jednom skoku dolazi na polje (m, n) .



Prema tome imamo samo nekoliko specijalnih slučajeva da proverimo. Treba da dokažemo da možemo da dođemo na polja (m, n) za $m, n < 2$, tj. do polja $(0, 0)$, $(0, 1)$, $(1, 0)$ i $(1, 1)$. Za $(0, 0)$ nemamo šta da dokažemo (već se nalazimo na tom polju). Nizom skokova $(0, 0) \mapsto (2, 1) \mapsto (1, 3) \mapsto (0, 1)$ dolazimo do $(0, 1)$, simetričnim nizom $(0, 0) \mapsto (1, 2) \mapsto (3, 1) \mapsto (1, 0)$ dolazimo do $(1, 0)$, a nizom $(0, 0) \mapsto (2, 1) \mapsto (0, 2) \mapsto (2, 3) \mapsto (1, 1)$ dolazimo do $(1, 1)$.



$\square$

Semantika iskazne logike (nastavak)

Dokažimo sada teoremu 2.5:

Dokaz teorema 2.5. Uočimo predikat $P(n)$, $n \in \mathbb{N}$: Za svaku formulu φ složenosti n , vrednost $\hat{v}(\varphi)$ zavisi samo od vrednosti valuacije v na skupu slova $P(\varphi)$. Primetimo da je dovoljno da dokažemo iskaz $(\forall n) P(n)$. To ćemo da uradimo potpunom indukcijom po n .

Neka je $n \in \mathbb{N}$ proizvoljno, pretpostavimo da gornje tvrđenje važi za formule složenosti $m < n$ (IH), i dokažimo ga za formulu φ složenosti n . U skladu sa definicijom 2.1, razmatramo sledeće slučajeve:

1° φ je konstanta: Ako $\varphi = \perp$, po definiciji 2.4, $\hat{v}(\varphi) = \hat{v}(\perp) = N$ nezavisno od v . Slično, ako je $\varphi = \top$, $\hat{v}(\varphi) = T$ nezavisno od v .

2° φ je slovo: Neka je $\varphi = p$; tada $P(\varphi) = \{p\}$. Po definiciji 2.4 imamo $\hat{v}(\varphi) = \hat{v}(p) = v(p)$; vrednost na desnoj strani očigledno zavisi samo od vrednosti valuacije v na skupu $P(\varphi)$.

3° $\varphi = \neg\psi$: Primitimo $sl(\psi) = n - 1 < n$ i $P(\psi) = P(\varphi)$. Po (IH) imamo da $\hat{v}(\psi)$ zavisi samo od vrednosti valuacije v na skupu $P(\psi)$, a po definiciji 2.4, $\hat{v}(\varphi)$ zavisi samo od vrednosti $\hat{v}(\psi)$; dakle, $\hat{v}(\varphi)$ zavisi samo od vrednosti valuacije v na skupu $P(\psi) = P(\varphi)$.

4° $\varphi = \psi * \theta$, $*$ $\in \{\wedge, \vee, \underline{\vee}, \rightarrow, \leftrightarrow\}$: Primitimo $sl(\psi), sl(\theta) < sl(\varphi) = n$ i $P(\varphi) = P(\psi) \cup P(\theta)$. Po (IH) znamo da $\hat{v}(\psi)$ i $\hat{v}(\theta)$ zavise samo od vrednosti valuacije v redom na skupovima $P(\psi)$ i $P(\theta)$, a po definiciji 2.4, $\hat{v}(\varphi)$ zavisi samo od vrednosti $\hat{v}(\psi)$ i $\hat{v}(\theta)$; dakle, $\hat{v}(\varphi)$ zavisi samo od vrednosti valuacije v na skupu $P(\psi) \cup P(\theta) = P(\varphi)$.

Završili smo dokaz. □

Definicija 2.13. Formula φ je:

- *zadovoljiva* ako za neku valuaciju v važi $\hat{v}(\varphi) = T$ (pišemo i $v \models \varphi$ i čitamo „ v zadovoljava φ “, ili „ v je model za φ “);
- *poreciva* ako za neku valuaciju v važi $\hat{v}(\varphi) = N$ (pišemo i $v \not\models \varphi$ i čitamo „ v ne zadovoljava (poriče) φ “, ili „ v je kontramodel za φ “);
- *tautologija*, u oznaci $\models \varphi$, ako za sve valuacije v važi $\hat{v}(\varphi) = T$ (tj. nije poreciva);
- *kontradikcija* ako za sve valuacije v važi $\hat{v}(\varphi) = N$ (tj. nije zadovoljiva).

Primitimo da $\not\models \varphi$ znači da je φ poreciva (ne da je kontradikcija).

Primer 2.14. Ispitati da li je formula $(p \wedge \neg r) \vee (q \wedge \neg r) \rightarrow (p \vee q \rightarrow r)$ zadovoljiva/poreciva?

Rešenje. Zapišimo tablicu date formule u svim valuacijama njenih slova:

p	q	r	$((p \wedge \neg r) \vee (q \wedge \neg r)) \rightarrow ((p \vee q) \rightarrow r)$
T	T	T	T
T	T	N	N
T	N	T	T
T	N	N	N
N	T	T	T
N	T	N	N
N	N	T	T
N	N	N	T

Iz tablice je jasno da je formula i zadovoljiva i poreciva (pa nije ni tautologija ni kontradikcija). □

Primer 2.15. Dokazati da je formula $(p \wedge (\neg q \rightarrow \neg p)) \wedge (\neg q \vee \neg r) \rightarrow (r \rightarrow \neg p)$ tautologija.

Rešenje. Pretpostavimo suprotno, formula je poreciva, tj. postoji valuacija v takva da je formula netačna. Tada je $\hat{v}((p \wedge (\neg q \rightarrow \neg p)) \wedge (\neg q \vee \neg r)) = T$ i $\hat{v}(r \rightarrow \neg p) = N$, odakle $\hat{v}(p \wedge (\neg q \rightarrow \neg p)) = T$, $\hat{v}(\neg q \vee \neg r) = T$, $\hat{v}(r) = T$ i $\hat{v}(\neg p) = N$. Iz prve jednakosti imamo $\hat{v}(\neg q \rightarrow \neg p) = T$, pa kako je $\hat{v}(\neg p) = N$ mora biti i $\hat{v}(\neg q) = N$. Odatle i $\hat{v}(\neg q \vee \neg r) = T$ je $\hat{v}(\neg r) = T$, što je u kontradikciji sa $\hat{v}(r) = T$.

Alternativno, možemo da napišemo tablicu formule:

p	q	r	$((p \wedge (\neg q \rightarrow \neg p)) \wedge (\neg q \vee \neg r)) \rightarrow (r \rightarrow \neg p)$										
T	T	T	T	N	T	N	N	N	N	N	T	N	N
T	T	N	T	N	T	N	T	N	T	T	T	T	N
T	N	T	N	T	N	N	N	T	T	N	T	N	N
T	N	N	N	T	N	N	N	T	T	T	T	T	N
N	T	T	N	N	T	T	N	N	N	N	T	T	T
N	T	N	N	N	T	T	N	N	T	T	T	T	T
N	N	T	N	T	T	T	N	T	T	N	T	T	T
N	N	N	N	T	T	T	N	T	T	T	T	T	T

iz koje vidimo da je formula tautologija. □

Zadatak 2.16 (Spisak osnovnih tautologija). Dokazati da su sledeće formule tautologije:

- 1° $p \vee \neg p$; 2° $\neg(p \wedge \neg p)$; 3° $p \rightarrow p$; 4° $\neg\neg p \leftrightarrow p$;
- 5° $p \wedge p \leftrightarrow p$; 6° $p \vee p \leftrightarrow p$; 7° $p \wedge \top \leftrightarrow p$; 8° $p \wedge \perp \leftrightarrow \perp$;
- 9° $p \vee \top \leftrightarrow \top$; 10° $p \vee \perp \leftrightarrow p$; 11° $p \wedge (p \vee q) \leftrightarrow p$; 12° $p \vee (p \wedge q) \leftrightarrow p$;
- 13° $p \wedge q \leftrightarrow q \wedge p$; 14° $p \vee q \leftrightarrow q \vee p$; 15° $(p \leftrightarrow q) \leftrightarrow (q \leftrightarrow p)$;
- 16° $p \wedge (q \wedge r) \leftrightarrow (p \wedge q) \wedge r$; 17° $p \vee (q \vee r) \leftrightarrow (p \vee q) \vee r$;
- 18° $(p \leftrightarrow (q \leftrightarrow r)) \leftrightarrow ((p \leftrightarrow q) \leftrightarrow r)$;
- 19° $p \wedge (q \vee r) \leftrightarrow (p \wedge q) \vee (p \wedge r)$; 20° $p \vee (q \wedge r) \leftrightarrow (p \vee q) \wedge (p \vee r)$;
- 21° $\neg(p \wedge q) \leftrightarrow \neg p \vee \neg q$; 22° $\neg(p \vee q) \leftrightarrow \neg p \wedge \neg q$;
- 23° $(p \rightarrow q) \leftrightarrow (\neg q \rightarrow \neg p)$; 24° $(p \rightarrow q) \leftrightarrow (p \wedge \neg q \rightarrow \perp)$;
- 25° $p \wedge (p \rightarrow q) \rightarrow q$; 26° $(p \rightarrow q) \wedge \neg q \rightarrow \neg p$;
- 27° $(p \vee q) \wedge \neg p \rightarrow q$; 28° $(p \rightarrow q) \wedge (q \rightarrow r) \rightarrow (p \rightarrow r)$.

Komentar 2.17. Tautologija 1 naziva se *zakon isključenja trećeg* (*tertium non datur*). Tautologija 4 je *zakon duple negacije*. Tautologije 5 i 6 nazivaju se *zakoni idempotencije* za konjunkciju i disjunkciju. Tautologije 11 i 12 su *zakoni apsorpcije*. Tautologije 13–14 su *komutativni zakoni*, a 16–18 *asocijativni zakoni* za konjunkciju, disjunkciju i ekvivalenciju. Tautologije 19 i 20 su *distributivni zakoni* konjunkcije prema disjunkciji i disjunkcije prema konjunkciji. Tautologije 21 i 22 su De Morganovi zakoni. Tautologija 23 je *zakon kontrapozicije*. Tautologija 24 je *zakon svodenja na protivrečnost* (*reductio ad absurdum*). Tautologija 25 je *modus ponens*, a 26 je *modus tollens*. Tautologija 27 naziva se *disjunktivni silogizam*, a 28 *hipotetički silogizam*.

2.3 Lema o smeni

Komentar 2.18. Zapisom $\varphi = \varphi(p_1, p_2, \dots, p_k)$ ističemo da su sva slova koja se pojavljuju u formuli φ neka (i možda ne sva) od $p_1, p_2, \dots, p_k$, tj. da je $P(\varphi) \subseteq \{p_1, p_2, \dots, p_k\}$. Pa tako ako je φ formula $p \rightarrow q$, možemo da pišemo $\varphi = \varphi(p, q)$ ili $\varphi = \varphi(p, q, r)$, ali nećemo da pišemo $\varphi = \varphi(p)$ ili $\varphi = \varphi(q, r)$.

Definicija 2.19. Neka su $\varphi = \varphi(p_1, p_2, \dots, p_k)$, $\psi_1, \psi_2, \dots, \psi_k$ formule. Označavamo sa $\varphi(\psi_1, \psi_2, \dots, \psi_k)$ formulu φ u kojoj smo sva pojavljivanja slova p_i zamenili sa ψ_i za sve $i = 1, \dots, k$. (Npr. ako je $\varphi = \varphi(p, q)$ formula $p \rightarrow q \wedge p$, onda je $\varphi(p \vee q, s \rightarrow r)$ formula $p \vee q \rightarrow (s \rightarrow r) \wedge (p \vee q)$.)

Lema 2.20 (Lema o smeni). Neka su $\varphi = \varphi(p_1, p_2, \dots, p_k)$, $\psi_1, \psi_2, \dots, \psi_k$ formule i v valuacija. Tada je:

$$\hat{v}(\varphi(\psi_1, \psi_2, \dots, \psi_k)) = \hat{w}(\varphi),$$

gde je w bilo koja valuacija takva da $w(p_i) = \hat{v}(\psi_i)$ za sve $i = 1, \dots, k$.

Dokaz. Dokaz izvodimo potpunom indukcijom po složenosti formule φ . Neka je $n \in \mathbb{N}$ proizvoljno, pretpostavimo da tvrđenje važi za formule složenosti $m < n$ (IH), i dokažimo da tvrđenje važi za formulu φ složenosti n . Razmatramo sledeće slučajeve:

1° φ je konstanta: Pretpostavimo $\varphi = \perp$. Primitimo da je $\varphi(\psi_1, \dots, \psi_k) = \perp$, pa direktno po definiciji 2.4 imamo:

$$\hat{v}(\varphi(\psi_1, \dots, \psi_k)) = \hat{v}(\perp) = N = \hat{w}(\perp) = \hat{w}(\varphi).$$

Slično postupamo ako je $\varphi = \top$.

2° φ je slovo: Kako su slova formule φ po pretpostavci među $p_1, \dots, p_k$, mora biti $p = p_i$ za neko $i = 1, \dots, k$: $\varphi = p_i$. Tada je $\varphi(\psi_1, \dots, \psi_k) = \psi_i$, pa kako po pretpostavci imamo $w(p_i) = \hat{v}(\psi_i)$ računamo:

$$\hat{v}(\varphi(\psi_1, \dots, \psi_k)) = \hat{v}(\psi_i) = w(p_i) = \hat{w}(p_i) = \hat{w}(\varphi).$$

3° $\varphi = \neg\sigma$: Formula σ je složenosti $n - 1 < n$, i jasno je da je $\sigma = \sigma(p_1, \dots, p_k)$, pa možemo da primenimo (IH):

$$\hat{v}(\sigma(\psi_1, \dots, \psi_k)) = \hat{w}(\sigma).$$

Kako je $\varphi(\psi_1, \dots, \psi_k) = \neg\sigma(\psi_1, \dots, \psi_k)$, prema prethodnoj jednakosti važi:

$$\hat{v}(\varphi(\psi_1, \dots, \psi_k)) = \hat{w}(\varphi).$$

4° $\varphi = \sigma * \theta$, $* \in \{\wedge, \vee, \underline{\vee}, \rightarrow, \leftrightarrow\}$: Formule σ i θ su jasno složenosti manje od n , i takođe je jasno da možemo da pišemo $\sigma = \sigma(p_1, \dots, p_k)$ i $\theta = \theta(p_1, \dots, p_k)$, pa možemo da primenimo (IH) na formule σ i θ , tj.:

$$\hat{v}(\sigma(\psi_1, \dots, \psi_k)) = \hat{w}(\sigma) \quad \text{i} \quad \hat{v}(\theta(\psi_1, \dots, \psi_k)) = \hat{w}(\theta).$$

Kako je još očigledno $\varphi(\psi_1, \dots, \psi_k) = \sigma(\psi_1, \dots, \psi_k) * \theta(\psi_1, \dots, \psi_k)$, po definiciji 2.4 prema prethodnim jednakostima imamo:

$$\hat{v}(\varphi(\psi_1, \dots, \psi_k)) = \hat{w}(\varphi).$$

Dokazali smo lemu. □

Imamo direktnu posledicu leme o smeni:

Tvrđenje 2.21. Neka su $\varphi = \varphi(p_1, \dots, p_k)$, $\psi_1, \dots, \psi_k$ formule i neka je $\models \varphi$. Tada je $\models \varphi(\psi_1, \dots, \psi_k)$.

Dokaz. Neka je v proizvoljna valuacija i neka je w valuacija takva da $w(p_i) = \hat{v}(\psi_i)$ za sve $i = 1, \dots, k$. Tada je:

$$\begin{aligned} \hat{v}(\varphi(\psi_1, \dots, \psi_k)) &= \hat{w}(\varphi) \quad \text{po lemi 2.20} \\ &= T \quad \text{jer je } \models \varphi. \end{aligned}$$

Kako je $\varphi(\psi_1, \dots, \psi_k)$ tačna za proizvoljnu valuaciju v , važi $\models \varphi(\psi_1, \dots, \psi_k)$. □

Primer 2.22. Dokazati da je formula $(p \leftrightarrow q \vee r) \wedge ((p \leftrightarrow q \vee r) \rightarrow (q \vee r \rightarrow s)) \rightarrow (q \vee r \rightarrow s)$ tautologija.

Rešenje. Naša formula jednaka je $\varphi(p \leftrightarrow q \vee r, q \vee r \rightarrow s)$, gde je $\varphi(a, b) = a \wedge (a \rightarrow b) \rightarrow b$ tautologija modus ponens. Prema tvrđenju 2.21 i naša formula je tautologija. □

2.4 Logička ekvivalentnost i normalne forme

Definicija 2.23. Formule φ i ψ su *logički ekvivalentne*, u oznaci $\varphi \equiv \psi$, ako za sve valuacije v važi $\hat{v}(\varphi) = \hat{v}(\psi)$, tj. ako je formula $\varphi \leftrightarrow \psi$ tautologija.

Primer 2.24. Neke od osnovnih tautologija iz zadatka 2.16 nam daju sledeće ekvivalentne formule:

$$\begin{array}{lll} 4^\circ \neg\neg p \equiv p; & 5^\circ p \wedge p \equiv p; & 6^\circ p \vee p \equiv p; \\ 7^\circ p \wedge \top \equiv p; & 8^\circ p \wedge \perp \equiv \perp; & 9^\circ p \vee \top \equiv \top; \quad 10^\circ p \vee \perp \equiv p; \\ 11^\circ p \wedge (p \vee q) \equiv p; & 12^\circ p \vee (p \wedge q) \equiv p; & \\ 13^\circ p \wedge q \equiv q \wedge p; & 14^\circ p \vee q \equiv q \vee p; & 15^\circ p \leftrightarrow q \equiv q \leftrightarrow p; \end{array}$$

$$\begin{array}{lll}
16^\circ & p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r; & 17^\circ & p \vee (q \vee r) \equiv (p \vee q) \vee r; & 18^\circ & p \leftrightarrow (q \leftrightarrow r) \equiv (p \leftrightarrow q) \leftrightarrow r; \\
19^\circ & p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r); & 20^\circ & p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r); & & \\
21^\circ & \neg(p \wedge q) \equiv \neg p \vee \neg q; & 22^\circ & \neg(p \vee q) \equiv \neg p \wedge \neg q; & & \\
23^\circ & p \rightarrow q \equiv \neg q \rightarrow \neg p; & 24^\circ & p \rightarrow q \equiv p \wedge \neg q \rightarrow \perp. & &
\end{array}$$

Tvrđenje 2.25. Neka su $\varphi_1 = \varphi_1(p_1, \dots, p_k)$, $\varphi_2 = \varphi_2(p_1, \dots, p_k)$, $\psi_1, \dots, \psi_k$ i $\theta_1, \dots, \theta_k$ formule i pretpostavimo $\varphi_1 \equiv \varphi_2$ i $\psi_i \equiv \theta_i$ za sve $i = 1, \dots, k$. Tada je:

$$\varphi_1(\psi_1, \dots, \psi_k) \equiv \varphi_2(\theta_1, \dots, \theta_k).$$

Dokaz. Neka je v proizvoljna valuacija i neka je w valuacija takva da $w(p_i) = \hat{v}(\psi_i)$ za sve $i = 1, \dots, k$. Kako je $\psi_i \equiv \theta_i$ za sve $i = 1, \dots, k$, važi i $w(p_i) = \hat{v}(\theta_i)$ za sve $i = 1, \dots, k$. Sada imamo:

$$\begin{aligned}
\hat{v}(\varphi_1(\psi_1, \dots, \psi_k)) &= \hat{w}(\varphi_1) && \text{po lemi 2.20} \\
&= \hat{w}(\varphi_2) && \text{jer } \varphi_1 \equiv \varphi_2 \\
&= \hat{v}(\varphi_2(\theta_1, \dots, \theta_k)) && \text{po lemi 2.20.}
\end{aligned}$$

Kako je v proizvoljna valuacija, zaključujemo $\varphi_1(\psi_1, \dots, \psi_k) \equiv \varphi_2(\theta_1, \dots, \theta_k)$. $\square$

Primer 2.26. Dokazati da su formule $(\neg p \vee q) \rightarrow (r \leftrightarrow s)$ i $\neg(p \rightarrow q) \vee (s \leftrightarrow r)$ logički ekvivalentne.

Rešenje. Uočimo formule $\varphi_1 = \varphi_1(a, b) = a \rightarrow b$ i $\varphi_2 = \varphi_2(a, b) = \neg a \vee b$, i primetimo $\varphi_1 \equiv \varphi_2$. Sada imamo:

$$\begin{aligned}
(\neg p \vee q) \rightarrow (r \leftrightarrow s) &= \varphi_1(\neg p \vee q, r \leftrightarrow s) \\
&\equiv \varphi_2(p \rightarrow q, s \leftrightarrow r) && \text{po tvrđenju 2.25} \\
&= \neg(p \rightarrow q) \vee (s \leftrightarrow r),
\end{aligned}$$

gde u drugom koraku možemo da primenimo tvđenje 2.25 jer $\varphi_1 \equiv \varphi_2$, $\neg p \vee q \equiv p \rightarrow q$ i $r \leftrightarrow s \equiv s \leftrightarrow r$. $\square$

Primer 2.27. Dokazati da je $(p \rightarrow r) \wedge (q \rightarrow r) \leftrightarrow (p \vee q \rightarrow r)$ tautologija.

Rešenje. Izvodimo niz ekvivalentnih zamena, implicitno koristeći tvrđenje 2.25, a detaljnije objašnjenje primene tvrđenja ostavljamo za kasnije:

$$\begin{aligned}
(p \rightarrow r) \wedge (q \rightarrow r) \leftrightarrow (p \vee q \rightarrow r) &\equiv (\neg p \vee r) \wedge (\neg q \vee r) \leftrightarrow \neg(p \vee q) \vee r \\
&\equiv (\neg p \wedge \neg q) \vee r \leftrightarrow (\neg p \wedge \neg q) \vee r \\
&\equiv \top.
\end{aligned}$$

U prvom koraku smo izvršili ekvivalentne zamene $p \rightarrow r \equiv \neg p \vee r$, $q \rightarrow r \equiv \neg q \vee r$ i $p \vee q \rightarrow r \equiv \neg(p \vee q) \vee r$. Formalno, primenili smo tvrđenje 2.25 na formule $\varphi_1(a, b, c) = \varphi_2(a, b, c) = a \wedge b \leftrightarrow c$ i zaključili $\varphi_1(p \rightarrow r, q \rightarrow r, p \vee q \rightarrow r) \equiv \varphi_2(\neg p \vee r, \neg q \vee r, \neg(p \vee q) \vee r)$.

U drugom koraku izvršili smo ekvivalentne smene $(\neg p \vee r) \wedge (\neg q \vee r) \equiv (\neg p \wedge \neg q) \vee r$ (distributivan zakon) i $\neg(p \vee q) \equiv \neg p \wedge \neg q$ (De Morganov zakon). Formalno, uočimo formule $\varphi_1(a, b, c) = \varphi_2(a, b, c) = a \leftrightarrow b \vee c$ i po tvrđenju 2.25 zaključimo $\varphi_1((\neg p \vee r) \wedge (\neg q \vee r), \neg(p \vee q), r) \equiv \varphi_2((\neg p \wedge \neg q) \vee r, \neg p \wedge \neg q, r)$.

U trećem koraku koristimo tautologiju $\varphi(a) = a \leftrightarrow a$ i tvrđenje 2.21 da zaključimo da je $\varphi((\neg p \wedge \neg q) \vee r)$ tautologija.

Kako smo polaznu formulu ekvivalentnim smenama sveli na tautologiju, i polazna formula je tautologija. $\square$

Definicija 2.28. a) *Literal* je iskazno slovo ili negacija iskaznog slova.

b) *(Disjunktivna) klauza* je disjunkcija literala.

c) *Konjunktivna klauza* je konjunkcija literala.

d) Formula je u *disjunktivnoj normalnoj formi (DNF)* ako je disjunkcija konjunktivnih klauza.

e) Formula je u *konjunktivnoj normalnoj formi (KNF)* ako je konjunkcija klauza.

Teorema 2.29 (Teorema o normalnim formama). Svaka formula logički je ekvivalentna formuli u DNF i formuli u KNF.

Dokaz. Svaka formula se svodi na formulu u DNF i na formulu u KNF koristeći tvrđenje 2.25 sledećim algoritmom.

Prvi korak. Zamenimo pojavljivanja veznika $\vee$, $\leftrightarrow$ i $\rightarrow$ koristeći ekvivalencije:

$$\begin{aligned} p \vee q &\equiv (p \wedge \neg q) \vee (\neg p \wedge q) & \text{ili} & & p \vee q &\equiv (p \vee q) \wedge (\neg p \vee \neg q), \\ p \leftrightarrow q &\equiv (p \wedge q) \vee (\neg p \wedge \neg q) & \text{ili} & & p \leftrightarrow q &\equiv (p \vee \neg q) \wedge (\neg p \vee q), \text{ i} \\ p \rightarrow q &\equiv \neg p \vee q & \text{ili} & & p \rightarrow q &\equiv \neg(p \wedge \neg q). \end{aligned}$$

Nakon prvog koraka formula je zapisana koristeći veznike $\neg$, $\wedge$ i $\vee$.

Drugi korak. Sve negacije „ubacimo“ u zagrade koristeći De Morganove zakone:

$$\neg(p \wedge q) \equiv \neg p \vee \neg q \quad \text{i} \quad \neg(p \vee q) \equiv \neg p \wedge \neg q,$$

pri čemu dvostruke negacije brišemo koristeći zakon $\neg\neg p \equiv p$.

Nakon drugog koraka formula je zapisana koristeći veznike $\neg$, $\wedge$ i $\vee$ pri čemu se $\neg$ nalaze samo uz slova.

Treći korak. Sređujemo formulu na DNF/KNF koristeći distributivne zakone:

$$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r) \quad \text{i} \quad p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r).$$

Četvrti korak. Uprostimo izraze koristeći:

$$\begin{aligned} p \wedge p &\equiv p, & p \vee p &\equiv p, & p \wedge \neg p &\equiv \perp, & p \vee \neg p &\equiv \top, \\ p \wedge \top &\equiv p, & p \vee \top &\equiv \top, & p \wedge \perp &\equiv \perp, & p \vee \perp &\equiv p. \end{aligned}$$

□

Primer 2.30. Nađimo DNF i KNF formule $(p \leftrightarrow q) \rightarrow r$. Pratimo algoritam:

$$\begin{aligned} (p \leftrightarrow q) \rightarrow r &\equiv ((p \vee \neg q) \wedge (\neg p \vee q)) \rightarrow r - \text{eliminacija } \leftrightarrow \\ &\equiv \neg((p \vee \neg q) \wedge (\neg p \vee q)) \vee r - \text{eliminacija } \rightarrow \\ &\equiv (\neg p \wedge q) \vee (p \wedge \neg q) \vee r - \text{ubacivanje } \neg \text{ i brisanje } \neg\neg \end{aligned}$$

Dobijena formula je već u DNF, tako da tu možemo da stanemo. Da bismo našli KNF, nastavljamo sa distributivnim zakonima:

$$\begin{aligned} (p \leftrightarrow q) \rightarrow r &\equiv (\neg p \wedge q) \vee (p \wedge \neg q) \vee r - \text{dobijena formula gore} \\ &\equiv (\neg p \vee p \vee r) \wedge (\neg p \vee \neg q \vee r) \wedge (q \vee p \vee r) \wedge (q \vee \neg q \vee r) \\ &\quad - \text{distributivnost „svaki sa svakim“} \\ &\equiv (\top \vee r) \wedge (\neg p \vee \neg q \vee r) \wedge (q \vee p \vee r) \wedge (\top \vee r) - \text{sređivanje} \\ &\equiv \top \wedge (\neg p \vee \neg q \vee r) \wedge (q \vee p \vee r) \wedge \top - \text{sređivanje} \\ &\equiv (\neg p \vee \neg q \vee r) \wedge (q \vee p \vee r) - \text{sređivanje.} \end{aligned}$$

Dobijena formula je u KNF.

Sledeća teorema će nam reći kako da DNF i KNF formule pročitamo iz njene tablice. Za $p \in P$ i $v \in \mathcal{V}$ definišemo oznake p^v i $\overline{p^v}$ sa:

$$p^v := \begin{cases} p & \text{ako } v(p) = T, \\ \neg p & \text{ako } v(p) = N, \end{cases} \quad \text{i} \quad \overline{p^v} := \begin{cases} \neg p & \text{ako } v(p) = T, \\ p & \text{ako } v(p) = N. \end{cases}$$

Teorema 2.31 (Teorema o kanonskim normalnim formama). Neka je $\varphi \in \Phi$, $P(\varphi) = \{p_1, \dots, p_n\}$, i neka je $\mathcal{V}_0$ skup svih valuacija slova $p_1, \dots, p_n$.

a) Ako $\varphi \neq \perp$, onda:

$$\varphi \equiv \bigvee_{\substack{v \in \mathcal{V}_0 \\ v \models \varphi}} (p_1^v \wedge p_2^v \wedge \cdots \wedge p_n^v).$$

b) Ako $\varphi \neq \top$, onda:

$$\varphi \equiv \bigwedge_{\substack{v \in \mathcal{V}_0 \\ v \not\models \varphi}} (\overline{p_1^v} \vee \overline{p_2^v} \vee \cdots \vee \overline{p_n^v}).$$

Dokaz. Dokazaćemo deo a), dokaz za b) je sličan. Najpre primetimo da je $\hat{w}(p^v) = T$ ako i samo ako $w(p) = v(p)$; specijalno, $\hat{v}(p^v) = T$. Neka je w proizvoljna valuacija.

Prepostavimo najpre $w \models \varphi$. Tada w učestvuje u disjunkciji na desnoj strani, tj. formula $p_1^w \wedge \cdots \wedge p_n^w$ je jedna od disjunkata na desnoj strane. Kako je $\hat{w}(p_i^w) = T$, to $w \models p_1^w \wedge \cdots \wedge p_n^w$, pa w zadovoljava formulu na desnoj strani.

Prepostavimo sada da w zadovoljava formulu na desnoj strani. To znači da postoji $v \models \varphi$ tako da $w \models p_1^v \wedge \cdots \wedge p_n^v$. Iz $w \models p_i^v$ sledi $w(p_i) = v(p_i)$, pa kako se v i w poklapaju na slovima formule φ , imamo da $\hat{w}(\varphi) = \hat{v}(\varphi)$. Kako $v \models \varphi$, to i $w \models \varphi$.

Dakle, u svim valuacijama leva i desna strana imaju iste vrednosti, te smo završili dokaz. $\square$

Primer 2.32. Zapišimo KDNF i KKNF formule $\varphi = \varphi(p, q, r)$ čija je tablica:

p	q	r	φ
T	T	T	T
T	T	N	N
T	N	T	T
T	N	N	T
N	T	T	N
N	T	N	T
N	N	T	N
N	N	N	N

Prema prethodnoj, da bismo zapisali KDNF treba da izdvojimo sve valuacije u kojima je φ tačna:

p	q	r	φ
T	T	T	T
T	N	T	T
T	N	N	T
N	T	N	T

Prvoj valuaciji odgovara disjunkt $p \wedge q \wedge r$, drugoj $p \wedge \neg q \wedge r$, trećoj $p \wedge \neg q \wedge \neg r$ i četvrtoj $\neg p \wedge q \wedge \neg r$, pa je KDNF:

$$(p \wedge q \wedge r) \vee (p \wedge \neg q \wedge r) \vee (p \wedge \neg q \wedge \neg r) \vee (\neg p \wedge q \wedge \neg r).$$

Da bismo zapisali KKNF treba da izdvojimo sve valuacije u kojima je φ netačna:

p	q	r	φ
T	T	N	N
N	T	T	N
N	N	T	N
N	N	N	N

Prvoj valuaciji odgovara konjunkt $\neg p \vee \neg q \vee r$, drugoj $p \vee \neg q \vee \neg r$, trećoj $p \vee q \vee \neg r$, i četvrtoj $p \vee q \vee r$, pa je

KKNF:

$$(\neg p \vee \neg q \vee r) \wedge (p \vee \neg q \vee \neg r) \wedge (p \vee q \vee \neg r) \wedge (p \vee q \vee r).$$

Na kraju ovog odeljka naglasimo i sledeće opažanje:

Tvrđenje 2.33. Svaka formula logički je ekvivalentna formuli koja je zapisana koristeći samo slova, konstantu $\perp$ i veznik $\rightarrow$.

Dokaz. Za dokaz dovoljno je da primetimo sledeće ekvivalencije:

- $\top \equiv \perp \rightarrow \perp$;
- $\neg p \equiv p \rightarrow \perp$;
- $p \wedge q \equiv \neg(p \rightarrow \neg q)$ (što je zapisivo na jeziku $\perp$ i $\rightarrow$ prema prethodnoj tački);
- $p \vee q \equiv \neg p \rightarrow q$ (ista napomena);
- $p \underline{\vee} q \equiv (\neg p \rightarrow q) \wedge (q \rightarrow \neg p)$ (ista napomena);
- $p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$ (ista napomena).

□

2.5 Prirodna dedukcija

Videli smo da je skup simbola $\{\perp, \rightarrow\}$ dovoljan da se do na ekvivalentnost izraze svi ostali simboli (tvrđenje 2.33). Sada ćemo pretpostaviti da smo od samog početka formule gradili koristeći samo simbole $\{\perp, \rightarrow\}$. To znači da je odgovarajuća definicija formule sledeća:

- iskazna slova i konstanta $\perp$ su formule;
- ako su φ i ψ (već) izgrađene formule, onda je i $(\varphi \rightarrow \psi)$ formula;
- svaka formula se gradi koristeći prethodna dva pravila u konačno mnogo koraka.

Sada možemo da kažemo da su preostali simboli definisani sledećim skraćenicama:

- $\top := \perp \rightarrow \perp$,
- $\neg \varphi := \varphi \rightarrow \perp$,
- $\varphi \wedge \psi := \neg(\varphi \rightarrow \neg \psi)$,
- $\varphi \vee \psi := \neg \varphi \rightarrow \psi$, i
- $\varphi \leftrightarrow \psi := (\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi)$.

Prirodna dedukcija je sistem za formalno dokazivanje formula iz polaznih premisa koji se bazira na uobičajenim deduktivnim postupcima matematičkog dokaza. Osnovna pravila zaključivanja su sledeća četiri:

$$\frac{\varphi}{\varphi} \text{R} \quad \frac{\varphi \quad \varphi \rightarrow \psi}{\psi} \text{MP} \quad \frac{\begin{array}{c} \varphi \quad \text{pp} \\ \vdots \\ \psi \end{array}}{\varphi \rightarrow \psi} \text{D} \quad \frac{\begin{array}{c} \neg \varphi \quad \text{pp} \\ \vdots \\ \perp \end{array}}{\varphi} \text{RAA}$$

Zovemo ih redom *reiteracija*, *modus ponens*, pravilo *dedukcije* i *reductio ad absurdum*. Pravilo R kaže: iz formule φ možemo da zaključimo φ . Pravilo MP kaže: iz φ i $\varphi \rightarrow \psi$ možemo da zaključimo ψ . Pravilo D kaže: ako pod pretpostavkom φ dokažemo ψ možemo da zaključimo $\varphi \rightarrow \psi$. Pravilo RAA kaže: ako pod pretpostavkom $\neg \varphi$ dokažemo kontradikciju možemo da zaključimo φ .

Neka su φ formula i Σ skup formula. *Dokaz* u prirodnoj dedukciji formule φ iz premisa Σ je konačan niz koraka u kojem koristeći premise (formule iz Σ) i poštujući navedena pravila dolazimo do zaključka φ . Preciznije, u svakom koraku možemo ili da konstatujemo neku od premisa ili da primenimo neko od gornjih pravila na prethodno izvedene formule u dokazu kako bismo izveli novu formulu. Poslednja formula u dokazu treba da bude baš formula φ .

Pravila R i MP direktno se odnose na jednu, odnosno dve prethodne formule u dokazu. Pogledajmo sledeći primer:

Primer 2.34. Iz premisa $\varphi, \varphi \rightarrow \psi, \psi \rightarrow \theta$ može se dokazati θ .

Rešenje. Zapišimo najpre dokaz, pa ćemo ga prokomentarisati.

- | | | |
|---|----------------------------|---------|
| 1 | φ | premise |
| 2 | $\varphi \rightarrow \psi$ | premise |
| 3 | $\psi \rightarrow \theta$ | premise |
| 4 | ψ | MP(1,2) |
| 5 | θ | MP(3,4) |

Svaki korak u dokazu numerišemo kako bismo lakše pratili postupak. Takođe sa desne strane pišemo opravdanje date formule. U prva tri koraka smo konstatovali date premise. U koraku četiri primenili smo pravilo modus ponens na formule iz prvog i drugog koraka kako bismo zaključili formulu ψ . Konačno u petom koraku još jednom primenjujemo pravilo modus ponens na formule iz trećeg i četvrtog koraka i zaključujemo formulu θ . S obzirom da je cilj i bio da izvedemo formulu θ , ovim korakom smo i završili dokaz. $\square$

Pravila D i RAA zahtevaju da u okviru dokaza napišemo određen poddokaz koji započinjemo odgovarajućom dodatnom pretpostavkom (pp). Treba voditi računa da datu pretpostavku nemamo kao premisu, tako da poddokaz u kojem je koristimo naglašavamo pisanjem linije s leve strane poddokaza koja nam govori dokle traje važenje date pretpostavke. Sama pretpostavka i formule dobijene u okviru poddokaza ne smeju se koristiti van samog poddokaza. Poslednja formula dokaza ne sme da bude unutar poddokaza, tj. sve poddokaze moramo da završimo do tog trenutka.

Pogledajmo još dva primera:

Primer 2.35. Iz premisa $\varphi \rightarrow \psi, \psi \rightarrow \theta$ može se dokazati $\varphi \rightarrow \theta$.

Rešenje. Ponovo zapišimo dokaz, pa ćemo ga prokomentarisati:

- | | | |
|---|------------------------------|---------|
| 1 | $\varphi \rightarrow \psi$ | premise |
| 2 | $\psi \rightarrow \theta$ | premise |
| 3 | φ | pp |
| 4 | ψ | MP(1,3) |
| 5 | θ | MP(2,4) |
| 6 | $\varphi \rightarrow \theta$ | D(3–5) |

U prva dva koraka smo konstatovali premise. S obzirom da treba da dokažemo formulu koja je u obliku implikacije, idemo na pravilo dedukcije, pa u trećem koraku otvaramo poddokaz sa odgovarajućom pretpostavkom. U koracima četiri i pet koristimo modus ponens. Kako smo u petom koraku došli do željenog zaključka, zatvaramo poddokaz i koristimo pravilo dedukcije u šestom koraku. $\square$

Primer 2.36. Bez premisa može se dokazati $(\varphi \rightarrow (\psi \rightarrow \theta)) \rightarrow ((\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow \theta))$.

Rešenje. Zapišimo dokaz:

1	$\varphi \rightarrow (\psi \rightarrow \theta)$	pp
2	$\varphi \rightarrow \psi$	pp
3	φ	pp
4	ψ	MP(2,3)
5	$\psi \rightarrow \theta$	MP(1,3)
6	θ	MP(4,5)
7	$\varphi \rightarrow \theta$	D(3-6)
8	$(\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow \theta)$	D(2-7)
9	$(\varphi \rightarrow (\psi \rightarrow \theta)) \rightarrow ((\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow \theta))$	D(1-8)

Kako dokazujemo formulu u obliku implikacije, idemo na pravilo dedukcije i započinjemo poddokaz sa odgovarajućom pretpostavkom $\varphi \rightarrow (\psi \rightarrow \theta)$, sa željom da dokažemo formulu $(\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow \theta)$. S obzirom da je i ova formula u obliku implikacije, ponovo idemo na pravilo dedukcije i započinjemo novi poddoka sa pretpostavkom $\varphi \rightarrow \psi$ i zadatko da dokažemo $\varphi \rightarrow \theta$. Ponovo, kao je i ovo implikacije, u trećem koraku otvaramo još jedan poddokaz sa pretpostavkom φ i zadatkom da dokažemo θ . To radimo koristeći MP u sledeća tri koraka. Na kraju zatvaramo poddokaze po pravilu dedukcije u poslednja tri koraka. $\square$

Definicija 2.37. Ako se iz premisa Σ može dokazati formula φ , to ćemo zapisivati sa $\Sigma \vdash \varphi$ (čitamo „ Σ dokazuje φ “, „ Σ izvodi φ “, ili „*sekvent* $\Sigma \vdash \varphi$ je dokaziv“).

Ako je Σ konačan, umesto $\{\psi_1, \dots, \psi_n\} \vdash \varphi$ pišemo $\psi_1, \dots, \psi_n \vdash \varphi$. Takođe, umesto $\emptyset \vdash \varphi$ pišemo samo $\vdash \varphi$ i u tom slučaju za φ kažemo da je *teorema*.

U primeru 2.34 dokazali smo sekvent $\varphi, \varphi \rightarrow \psi, \psi \rightarrow \theta \vdash \theta$, u primeru 2.35 dokazali smo $\varphi \rightarrow \psi, \psi \rightarrow \theta \vdash \varphi \rightarrow \theta$, a u primeru 2.36, $\vdash (\varphi \rightarrow (\psi \rightarrow \theta)) \rightarrow ((\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow \theta))$, tj. ova formula je teorema.

Odmah ćemo da dokažemo jednu jednostavnu, ali korisnu teoremu:

Teorema 2.38 (Teorema dedukcije). $\Sigma, \varphi \vdash \psi \iff \Sigma \vdash \varphi \rightarrow \psi$.

Dokaz. ($\Rightarrow$) Pretpostavimo $\Sigma \vdash \varphi \rightarrow \psi$ i uočimo jedan dokaz ovog sekventa (dokaz levo):

1		1	
$\vdots$	$\vdots$	$\vdots$	$\vdots$
n	$\varphi \rightarrow \psi$	$\rightsquigarrow$	n $\varphi \rightarrow \psi$
			(n+1) φ premisa
			(n+2) ψ MP(n,n+1)

Od premisa u ovom dokazu koristimo samo formule iz Σ . Pogledajmo dokaz na desnoj strani. Prepišimo prethodni dokaz, dodajmo premisu φ u koraku (n+1) i pozivajući se na modus ponens zaključujemo ψ . Time smo konstruisali dokaz za $\Sigma, \varphi \vdash \psi$.

($\Leftarrow$) Pretpostavimo $\Sigma, \varphi \vdash \psi$. Uočimo jedan dokaz ovog sekventa (dokaz levo):

		0	φ	premise	0	φ	pp
1		1			1		
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\rightsquigarrow$	$\vdots$	$\vdots$	
n	ψ	n	ψ		n	ψ	
					(n+1)	$\varphi \rightarrow \psi$	D(0-n)

U ovom dokazu se od premisa javljaju formule iz Σ i φ . Prepravimo dokaz na sledeći način (dokaz u sredini). Dodajmo ispred celog dokaza nultu formulu φ koju opravdamo kao premisa, a u koracima 1 – n svako pojavljivanje premise φ opravdamo kao R(0). Primetimo da je i ovo dokaz sekventa $\Sigma, \varphi \vdash \psi$, premisa φ javlja se jedino u koraku 0, a u koracima 1 – n jedine premise su iz Σ . Sada ovakav dokaz prepravimo na sledeći način (dokaz desno). Prograsimo formulu φ u koraku 0 za pretpostavku i pretvorimo ceo dokaz 0 – n u poddokaz sa ovom pretpostavkom. U koraku (n+1) iskoristimo pravilo dedukcije da se rešimo poddokaza. Od premisa u ovom dokazu su samo formule iz Σ , tj. zapisali smo dokaz sekventa $\Sigma \vdash \varphi \rightarrow \psi$. $\square$

2.6 Izvedena pravila prirodne dedukcije

Sekvent dokazan u primeru 2.35 možemo da koristimo i kao pravilo:

$$\frac{\varphi \rightarrow \psi \quad \psi \rightarrow \theta}{\varphi \rightarrow \theta} \text{HS}$$

Zovemo ga *hipotetički silogizam*.

U sledećim primerima dokazujemo izvestan broj izvedenih pravila.

Primer 2.39 (Eliminacija i uvođenje negacije). Dokazati sledeća dva pravila:

$$\frac{\varphi \quad \neg\varphi}{\perp} \neg_E \quad \text{i} \quad \frac{\begin{array}{c|c} \varphi & \text{pp} \\ \vdots & \\ \perp & \end{array}}{\neg\varphi} \neg_U$$

Rešenje. Ako se setimo da je $\neg\varphi$ po definiciji zamena za $\varphi \rightarrow \perp$, zamenom ψ sa $\perp$ u pravilima MP i D, Dobijamo $\neg_E$ i $\neg_U$ kao njihove specijalne slučajeve. □

Primer 2.40 (*Ex falso quodlibet*). Dokazati $\perp \vdash \varphi$, tj. pravilo:

$$\frac{\perp}{\varphi} \text{EFQ}$$

Rešenje. Dokaz je:

1	$\perp$	premise		1	$\neg\varphi$	pp
2	$\neg\varphi$	pp		2	$\perp$	premise
3	$\perp$	R(1)	ili kraće	3	φ	RAA(1-2)
4	φ	RAA(2-3)				

□

Primer 2.41 (Eliminacija i uvođenje duple negacije). Dokazati $\neg\neg\varphi \vdash \varphi$ i $\varphi \vdash \neg\neg\varphi$, tj. pravila:

$$\frac{\neg\neg\varphi}{\varphi} \neg\neg_E \quad \text{i} \quad \frac{\varphi}{\neg\neg\varphi} \neg\neg_U$$

Rešenje. Dokazi su:

1	$\neg\neg\varphi$	premise		1	φ	premise
2	$\neg\varphi$	pp		2	$\neg\varphi$	pp
3	$\perp$	$\neg_E(1,2)$	i	3	$\perp$	$\neg_E(1,2)$
4	φ	RAA(2-3)		4	$\neg\neg\varphi$	$\neg_U(2-3)$

Primetimo da ovde, zarad kraćeg dokaza, koristimo već dokazana pravila eliminacije i uvođenja negacije. □

Primer 2.42 (*Modus tollens*). Dokazati $\varphi \rightarrow \psi, \neg\psi \vdash \neg\varphi$, tj. pravilo:

$$\frac{\varphi \rightarrow \psi \quad \neg\psi}{\neg\varphi} \text{MT}$$

Rešenje. Dokaz je:

1	$\varphi \rightarrow \psi$	premise
2	$\neg\psi$	premise
3	φ	pp
4	ψ	MP(1,3)
5	$\perp$	$\neg_E(2,4)$
6	$\neg\varphi$	$\neg_U(3-5)$

□

Primer 2.43 (Kontrapozicija). Dokazati $\varphi \rightarrow \psi \vdash \neg\psi \rightarrow \neg\varphi$ i $\neg\psi \rightarrow \neg\varphi \vdash \varphi \rightarrow \psi$, tj. pravila:

$$\frac{\varphi \rightarrow \psi}{\neg\psi \rightarrow \neg\varphi} K \quad \text{i} \quad \frac{\neg\psi \rightarrow \neg\varphi}{\varphi \rightarrow \psi} K$$

Rešenje. Dokazi su:

1	$\varphi \rightarrow \psi$	premise	1	$\neg\psi \rightarrow \neg\varphi$	premise
2	$\neg\psi$	pp	2	φ	pp
3	$\neg\varphi$	MT(1,2)	3	$\neg\neg\varphi$	$\neg\neg_U(2)$
4	$\neg\psi \rightarrow \neg\varphi$	D(2-3)	4	$\neg\neg\psi$	MT(1,3)
			5	ψ	$\neg\neg_E(4)$
			6	$\varphi \rightarrow \psi$	D(2-5)

□

Primer 2.44 (Eliminacija i uvođenje disjunkcije). Dokazati $\varphi \vdash \varphi \vee \psi$, $\psi \vdash \varphi \vee \psi$ i $\varphi \vee \psi, \varphi \rightarrow \theta, \psi \rightarrow \theta \vdash \theta$, tj. pravila:

$$\frac{\varphi}{\varphi \vee \psi} \vee_U \quad \frac{\psi}{\varphi \vee \psi} \vee_U \quad \frac{\varphi \vee \psi \quad \varphi \rightarrow \theta \quad \psi \rightarrow \theta}{\theta} \vee_E$$

Rešenje. Setimo se da je $\varphi \vee \psi$ po definiciji zamena za formulu $\neg\varphi \rightarrow \psi$. Dokazi su:

1	φ	premise	1	ψ	premise	1	$\neg\varphi \rightarrow \psi$	premise
2	$\neg\varphi$	pp	2	$\neg\varphi$	pp	2	$\varphi \rightarrow \theta$	premise
3	$\perp$	$\neg_E(1,2)$	3	ψ	R(1)	3	$\psi \rightarrow \theta$	premise
4	ψ	EFQ(3)	4	$\neg\varphi \rightarrow \psi$	D(2-3)	4	$\neg\theta$	pp
5	$\neg\varphi \rightarrow \psi$	D(2-4)				5	$\neg\varphi$	MT(2,4)
						6	ψ	MP(1,5)
						7	θ	MP(3,6)
						8	$\perp$	$\neg_E(4,7)$
						9	θ	RAA(4-8)

□

Komentar 2.45. Imajući u vidu pravilo dedukcije, pravilo $\vee_E$ možemo da formulišemo i na sledeći način:

$$\frac{\varphi \vee \psi \quad \begin{array}{c|c} \varphi & \text{pp} \\ \vdots & \\ \theta & \end{array} \quad \begin{array}{c|c} \psi & \text{pp} \\ \vdots & \\ \theta & \end{array}}{\theta} \vee_E$$

Primer 2.46 (Disjunktivni silogizmi). Dokazati $\varphi \vee \psi, \neg\psi \vdash \varphi$ i $\varphi \vee \psi, \neg\varphi \vdash \psi$, tj. pravila:

$$\frac{\varphi \vee \psi \quad \neg\psi}{\varphi} DS \quad \text{i} \quad \frac{\varphi \vee \psi \quad \neg\varphi}{\psi} DS$$

Rešenje. Kako je $\varphi \vee \psi$ zamena za $\neg\varphi \rightarrow \psi$, prvo pravilo sledi iz MT i $\neg\neg_E$, a drugo direktno iz MP. □

Primer 2.47 (*Tertium non datur*). Dokazati $\vdash \varphi \vee \neg\varphi$, tj. pravilo:

$$\frac{}{\varphi \vee \neg\varphi} TND$$

Rešenje. Kako je $\varphi \vee \neg\varphi$ zamena za $\neg\varphi \rightarrow \neg\varphi$, dokaz je:

1	$\neg\varphi$	pp
2	$\neg\varphi \rightarrow \neg\varphi$	D(1-1)

□

Primer 2.48 (Eliminacija i uvođenje konjunkcije). Dokazati $\varphi \wedge \psi \vdash \varphi$, $\varphi \wedge \psi \vdash \psi$ i $\varphi, \psi \vdash \varphi \wedge \psi$, tj. pravila:

$$\frac{\varphi \wedge \psi}{\varphi} \wedge_E \quad \frac{\varphi \wedge \psi}{\psi} \wedge_E \quad \frac{\varphi \quad \psi}{\varphi \wedge \psi} \wedge_U$$

Rešenje. Kako je $\varphi \wedge \psi$ po definiciji zamena za $\neg(\varphi \rightarrow \neg\psi)$, dokazi su:

1	$\neg(\varphi \rightarrow \neg\psi)$	premisa	1	$\neg(\varphi \rightarrow \neg\psi)$	premisa
2	$\neg\varphi$	pp	2	$\neg\psi$	pp
3	φ	pp	3	φ	pp
4	$\perp$	$\neg_E(2,3)$	4	$\neg\psi$	R(2)
5	$\neg\psi$	EFQ(4)	5	$\varphi \rightarrow \neg\psi$	D(3-4)
6	$\varphi \rightarrow \neg\psi$	D(3-5)	6	$\perp$	$\neg_E(1,5)$
7	$\perp$	$\neg_E(1,6)$	7	ψ	RAA(2-6)
8	φ	RAA(2-7)			

i:

1	φ	premisa
2	ψ	premisa
3	$\varphi \rightarrow \neg\psi$	pp
4	$\neg\psi$	MP(1,3)
5	$\perp$	$\neg_E(2,4)$
6	$\neg(\varphi \rightarrow \neg\psi)$	$\neg_U(3-5)$

□

Primer 2.49 (Eliminacija i uvođenje ekvivalencije). Dokazati $\varphi \leftrightarrow \psi \vdash \varphi \rightarrow \psi$, $\varphi \leftrightarrow \psi \vdash \psi \rightarrow \varphi$ i $\varphi \rightarrow \psi, \psi \rightarrow \varphi \vdash \varphi \leftrightarrow \psi$, tj. pravila:

$$\frac{\varphi \leftrightarrow \psi}{\varphi \rightarrow \psi} \leftrightarrow_E \quad \frac{\varphi \leftrightarrow \psi}{\psi \rightarrow \varphi} \leftrightarrow_E \quad \frac{\varphi \rightarrow \psi \quad \psi \rightarrow \varphi}{\varphi \leftrightarrow \psi} \leftrightarrow_U$$

Rešenje. Kako je po definiciji $\varphi \leftrightarrow \psi$ zamena za $(\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi)$, ova pravila su specijalni slučajevi $\wedge_E$ i $\wedge_U$. □

Primer 2.50 (De Morganova pravila). Dokazati $\neg(\varphi \wedge \psi) \vdash \neg\varphi \vee \neg\psi$, $\neg\varphi \vee \neg\psi \vdash \neg(\varphi \wedge \psi)$, $\neg(\varphi \vee \psi) \vdash \neg\varphi \wedge \neg\psi$ i $\neg\varphi \wedge \neg\psi \vdash \neg(\varphi \vee \psi)$, tj. pravila:

$$\frac{\neg(\varphi \wedge \psi)}{\neg\varphi \vee \neg\psi} \text{DM} \quad \frac{\neg\varphi \vee \neg\psi}{\neg(\varphi \wedge \psi)} \text{DM} \quad \frac{\neg(\varphi \vee \psi)}{\neg\varphi \wedge \neg\psi} \text{DM} \quad \frac{\neg\varphi \wedge \neg\psi}{\neg(\varphi \vee \psi)} \text{DM}$$

Rešenje. Dokazi prva dva pravila su:

1	$\neg(\varphi \wedge \psi)$	premisa	1	$\neg\varphi \vee \neg\psi$	premisa
2	$\varphi \rightarrow \neg\psi$	$\neg\neg_E(1)$ po def. $\wedge$	2	φ	pp
3	$\neg\neg\varphi$	pp	3	$\neg\neg\varphi$	$\neg\neg_U(2)$
4	φ	$\neg\neg_E(3)$	4	$\neg\psi$	MP(1,3) po def. $\vee$
5	$\neg\psi$	MP(2,4)	5	$\varphi \rightarrow \neg\psi$	D(2-4)
6	$\neg\varphi \vee \neg\psi$	D(3-5) po def. $\vee$	6	$\neg(\varphi \wedge \psi)$	$\neg\neg_U(5)$ po def. $\wedge$

Dokazi preostala dva pravila su:

1	$\neg(\varphi \vee \psi)$	premisa	1	$\neg\varphi \wedge \neg\psi$	premisa
2	$\neg\varphi \rightarrow \neg\neg\psi$	pp	2	$\neg\varphi \rightarrow \psi$	pp
3	$\neg\varphi$	pp	3	$\neg\varphi$	pp
4	$\neg\neg\psi$	MP(2,3)	4	ψ	MP(3,2)
5	ψ	$\neg\neg_E(4)$	5	$\neg\neg\psi$	$\neg\neg_U(4)$
6	$\neg\varphi \rightarrow \psi$	D(3-5)	6	$\neg\varphi \rightarrow \neg\neg\psi$	D(3-5)
7	$\perp$	$\neg_E(1,6)$ po def. $\vee$	7	$\perp$	$\neg_E(1,6)$ po def. $\wedge$
8	$\neg\varphi \wedge \neg\psi$	RAA(2-7) po def. $\wedge$	8	$\neg(\varphi \vee \psi)$	RAA(2-7) po def. $\vee$

□

2.7 Logička posledica i teorema saglasnosti

Definicija 2.51. Neka $\Sigma \subseteq \Phi$ i $\varphi \in \Phi$.

- a) Valaucija v zadovoljava skup formula Σ , u oznaci $v \models \Sigma$, ako za sve formule $\sigma \in \Sigma$ važi $\hat{v}(\sigma) = T$.
- b) Skup formula Σ je *zadovoljiv* ako postoji valuacija v takva da $v \models \Sigma$.
- c) Formula φ je *logička posledica* skupa formula Σ , u oznaci $\Sigma \models \varphi$, ako za sve valuacije v važi implikacija $v \models \Sigma$ povlači $\hat{v}(\varphi) = T$.

Lema 2.52. Skup formula Σ je zadovoljiv ako i samo ako $\Sigma \not\models \perp$.

Dokaz. ($\Rightarrow$) Pretpostavimo Σ je zadovoljiv, tj. postoji valuacija v takva da $v \models \Sigma$. Kako je svakako $\hat{v}(\perp) = N$, zaključujemo $\Sigma \not\models \perp$.

($\Leftarrow$) Pretpostavimo $\Sigma \not\models \perp$. To znači da postoji valuacija v takva da $v \models \Sigma$, ali $\hat{v}(\perp) = N$, specijalno neka valuacija zadovoljava Σ , tj. Σ je zadovoljiv. $\square$

Lema 2.53. Neka je φ formula. Tada $\emptyset \models \varphi$ ako i samo ako $\models \varphi$.

Dokaz. Primetimo da $\emptyset \models \varphi$ znači $(\forall v)(v \models \emptyset \rightarrow \hat{v}(\varphi) = T)$. Takođe $v \models \emptyset$ znači $(\forall \sigma \in \emptyset) \hat{v}(\sigma) = T$, što je logički tačan iskaz jer je dobijen ograničenjem univerzalnog kvantifikatora na prazan skup. Kako je $v \models \emptyset$ logički tačan, implikacija $v \models \emptyset \rightarrow \hat{v}(\varphi) = T$ ekvivalentna je sa $\hat{v}(\varphi) = T$, pa $\emptyset \models \varphi$ svodi se na $(\forall v) \hat{v}(\varphi) = T$, što sa druge strane znači $\models \varphi$. $\square$

Teorema 2.54 (Teorema saglasnosti). Neka je $\Sigma \subseteq \Phi$ i $\varphi \in \Phi$. Ako $\Sigma \vdash \varphi$, onda $\Sigma \models \varphi$.

Za sekvent $\Sigma \vdash \varphi$, označimo sa $d(\Sigma \vdash \varphi)$ dužinu najkraćeg dokaza u prirodnoj dedukciji (koji koristi samo osnovna pravila) ovog sekventa ako je on dokaziv; ako nije dokaziv možemo da definišemo $d(\Sigma \vdash \varphi) = \infty$. Dakle, $\Sigma \vdash \varphi$ je dokaziv ako i samo ako $d(\Sigma \vdash \varphi) \in \mathbb{N}^+$.

Dokaz teoreme 2.54. Dovoljno je da dokažemo sledeće za sve $n \geq 1$: Za svaki sekvent $\Sigma \vdash \varphi$, ako je $d(\Sigma \vdash \varphi) = n$, onda $\Sigma \models \varphi$. Dokaz izvodimo potpunom indukcijom po n . Neka je $n \geq 1$ proizvoljno, pretpostavimo da tvrdjenje važi za sekvente čija je dužina najkraćeg dokaza k , $1 \leq k < n$ (IH), i dokažimo tvrdjenje za sekvente čija je dužina najkraćeg dokaza jednaka n . Pretpostavimo da imamo sekvent $\Sigma \vdash \varphi$ takav da $d(\Sigma \vdash \varphi) = n$. Uočimo neki najkraći dokaz ovog sekventa:

$$\begin{array}{ccc} 1 & & \\ \vdots & \vdots & \\ n & \varphi & \text{opravdanje} \end{array}$$

u kome se od premisa javljaju samo formule iz Σ . Diskutovaćemo po opravdanju, tj. imamo sledećih pet slučajeva.

1° opravdanje=premise: Ako je φ premise, to znači da $\varphi \in \Sigma$, pa očigledno važi $\Sigma \models \varphi$. (Primetimo jednu činjenicu koja nije bila bitna u dokazu. Naime, ako je opravdanje premise, mora biti $n = 1$ jer smo uočili najkraći dokaz.)

2° opravdanje=R: Dokažaćemo da ovaj slučaj nije moguć. Ako je opravdanje reiteracija, mora biti oblika $R(m)$, gde je $m < n$ i u koraku m je formula φ , tj. dokaz je sledećeg oblika:

$$\begin{array}{ccc} 1 & & \\ \vdots & \vdots & \\ m & \varphi & \\ \vdots & \vdots & \\ n & \varphi & R(m) \end{array}$$

Ako bismo prekinuli prethodni dokaz nakon prvog koraka, takođe bismo imali dokaz za $\Sigma \vdash \varphi$, koji je kraći od n . Kako ovo nije moguće, zaključujemo da ovaj slučaj nije moguć. (Zapravo smo dokazali da se najkraći dokaz ne može završiti reiteracijom.)

3° opravdanje=MP: Ako je opravdanje modus ponens, mora biti oblika $MP(k, m)$, gde $k < m < n$, formula u k -tom koraku je ψ i formula u m -tom koraku je $\psi \rightarrow \varphi$ (ili obratno). (Takođe možemo zaključiti i da je $m = n - 1$ jer smo uočili najkraći dokaz, što neće biti bitno.) Dakle, dokaz je sledećeg oblika:

$$\begin{array}{ll}
1 & \\
\vdots & \vdots \\
k & \psi \\
\vdots & \vdots \\
m & \psi \rightarrow \varphi \\
\vdots & \vdots \\
n & \varphi \quad \quad MP(k, m)
\end{array}$$

Primetimo da ako prekinemo dokaz posle k -tog, odnosno m -tog koraka, dobijamo dokaze za sekvente $\Sigma \vdash \psi$ i $\Sigma \vdash \psi \rightarrow \varphi$ dužine $k < n$, odnosno $m < n$. Prema tome $d(\Sigma \vdash \psi), d(\Sigma \vdash \psi \rightarrow \varphi) < n$, pa možemo da primenimo (IH) i zaključujemo $\Sigma \models \psi$ i $\Sigma \models \psi \rightarrow \varphi$. Dokažimo sada $\Sigma \models \varphi$. Neka je v valuacija takva da $v \models \Sigma$. Iz $\Sigma \models \psi$ i $\Sigma \models \psi \rightarrow \varphi$ imamo $\hat{v}(\psi) = T$ i $\hat{v}(\psi \rightarrow \varphi) = T$, odakle sledi $\hat{v}(\varphi) = T$. Dakle, $\Sigma \models \varphi$.

4° opravdanje=D: Ako je opravdanje pravilo dedukcije, mora biti oblika $D(k - m)$, gde $k < m < n$, formula φ je oblika $\psi \rightarrow \theta$, u k -tom koraku je pretpostavka ψ i formula u m -tom koraku je θ . (Takođe možemo zaključiti i da je $m = n - 1$ jer smo uočili najkraći dokaz, što neće biti bitno.) Dakle, dokaz je sledećeg oblika (levo):

$$\begin{array}{ll}
1 & 1 \\
\vdots & \vdots \\
k & \psi \quad \quad pp \\
\vdots & \vdots \\
m & \theta \\
\vdots & \vdots \\
n & \psi \rightarrow \theta = \varphi \quad D(k - m)
\end{array}
\quad \rightsquigarrow \quad
\begin{array}{ll}
1 & \\
\vdots & \vdots \\
k & \psi \quad \quad \text{premise} \\
\vdots & \vdots \\
m & \theta
\end{array}$$

Prepravimo ovaj dokaz na sledeći način (dokaz desno). Prekinimo dokaz posle m -tog koraka i proglasimo pretpostavku ψ u k -tom koraku za premisu, pri čemu poddokaz od k -tog do m -tog koraka postaje glavni deo dokaza (sklanjamo crtu poddokaza s leve strane). Time dobijamo dokaz za sekvent $\Sigma, \psi \vdash \theta$ dužine $m < n$ (ψ je s leve strane sekventa jer smo je proglasili za premisu). Prema tome $d(\Sigma, \psi \vdash \theta) < n$, pa možemo da primenimo (IH) i zaključujemo $\Sigma, \psi \models \theta$. Dokažimo sada $\Sigma \models \varphi$, tj. $\Sigma \models \psi \rightarrow \theta$. Neka je v valuacija takva da $v \models \Sigma$. Ako je $\hat{v}(\psi) = N$, važi $\hat{v}(\psi \rightarrow \theta) = T$. Ako je $\hat{v}(\psi) = T$, tada $v \models \Sigma, \psi$, pa kako $\Sigma, \psi \models \theta$, dobijamo $\hat{v}(\theta) = T$, odakle ponovo važi $\hat{v}(\psi \rightarrow \theta) = T$. Dakle, $\Sigma \models \varphi$.

5° opravdanje=RAA: Ako je opravdanje reductio ad absurdum, mora biti oblika $RAA(k - m)$, gde $k < m < n$, u k -tom koraku je pretpostavka $\neg \varphi$ i formula u m -tom koraku je $\perp$. (Takođe možemo zaključiti i da je $m = n - 1$ jer smo uočili najkraći dokaz, što neće biti bitno.) Dakle, dokaz je sledećeg oblika (levo):

$$\begin{array}{ll}
1 & 1 \\
\vdots & \vdots \\
k & \neg \varphi \quad \quad pp \\
\vdots & \vdots \\
m & \perp \\
\vdots & \vdots \\
n & \varphi \quad \quad RAA(k - m)
\end{array}
\quad \rightsquigarrow \quad
\begin{array}{ll}
1 & \\
\vdots & \vdots \\
k & \neg \varphi \quad \quad \text{premise} \\
\vdots & \vdots \\
m & \perp
\end{array}$$

Ponovo prepravljamo ovaj dokaz na sledeći način (dokaz desno). Prekinimo dokaz posle m -tog koraka i proglasimo pretpostavku $\neg \varphi$ u k -tom koraku za premisu, pri čemu poddokaz od k -tog do m -tog koraka postaje glavni deo dokaza (sklanjamo crtu poddokaza s leve strane). Time dobijamo dokaz za sekvent $\Sigma, \neg \varphi \vdash \perp$ dužine

$m < n$. Prema tome $d(\Sigma, \neg\varphi \vdash \perp) < n$, pa možemo da primenimo (IH) i zaključujemo $\Sigma, \neg\varphi \models \perp$. Dokažimo sada $\Sigma \models \varphi$. Neka je v valuacija takva da $v \models \Sigma$. Ako je $\hat{v}(\neg\varphi) = T$, važi $v \models \Sigma, \neg\varphi$, pa kako $\Sigma, \neg\varphi \models \perp$, dobijamo $\hat{v}(\perp) = T$, što je besmisleno. Prema tome mora biti $\hat{v}(\neg\varphi) = N$, tj. $\hat{v}(\varphi) = T$. Dakle, $\Sigma \models \varphi$.

Završili smo dokaz. □

Definicija 2.55. Skup formula Σ je *konzistentan* ako $\Sigma \not\models \perp$.

Još jedna verzija teoreme saglasnosti je:

Posledica 2.56 (Teorema saglasnosti). Ako je skup Σ zadovoljiv, Σ je konzistentan.

Dokaz. Dokažimo kontrapoziciju. Ako Σ nije konzistentan, tj. $\Sigma \vdash \perp$ po teoremi 2.54, $\Sigma \models \perp$, pa Σ nije zadovoljiv po lemi 2.52. □

2.8 Slaba teorema potpunosti

Prema teoremi saglasnosti za sve $\varphi \in \Phi$ specijalno važi:

$$\vdash \varphi \implies \models \varphi.$$

Cilj ovog odeljka je da dokažemo da važi i obratna implikacija:

Teorema 2.57 (Slaba teorema potpunosti). Za sve $\varphi \in \Phi$ važi:

$$\vdash \varphi \iff \models \varphi.$$

Za dokaz nam je potrebna kratka priprema.

Lema 2.58. Neka $\Sigma \subseteq \Phi$, $\varphi, \psi \in \Phi$.

- a) Važi $\varphi \rightarrow \psi, \neg\varphi \rightarrow \psi \vdash \psi$.
- b) Ako $\Phi, \varphi \vdash \psi$ i $\Phi, \neg\varphi \vdash \psi$, onda $\Phi \vdash \psi$.

Dokaz. a) Dokaz sekventa je:

1	$\varphi \rightarrow \psi$	premise
2	$\neg\varphi \rightarrow \psi$	premise
3	$\neg\psi$	pretpostavka
4	$\neg\varphi$	MT(1,3)
5	$\neg\neg\varphi$	MT(2,3)
6	$\perp$	$\neg E(4,5)$
7	ψ	RAA(3–6)

b) Prema teoremi dedukcije $\Phi, \varphi \vdash \psi$ i $\Phi, \neg\varphi \vdash \psi$ povlače $\Phi \vdash \varphi \rightarrow \psi$ i $\Phi \vdash \neg\varphi \rightarrow \psi$; prema a), $\Phi \vdash \psi$. □

Neka $v \in \mathcal{V}$ i $\varphi \in \Phi$. Definišemo $\varphi^v \in \Phi$ sa:

$$\varphi^v := \begin{cases} \varphi & \hat{v}(\varphi) = T, \\ \neg\varphi & \hat{v}(\varphi) = N. \end{cases}$$

Lema 2.59. Neka $\varphi, \psi \in \Phi$, $v \in \mathcal{V}$. Važi: $\varphi^v, \psi^v \vdash (\varphi \rightarrow \psi)^v$.

Dokaz. Dokaz leme se svodi na dokazivanje sledeća četiri sekventa:

$$\varphi, \psi \rightarrow \varphi \rightarrow \psi, \quad \varphi, \neg\psi \vdash \neg(\varphi \rightarrow \psi), \quad \neg\varphi, \psi \vdash \varphi \rightarrow \psi \quad \text{i} \quad \neg\varphi, \neg\psi \vdash \varphi \rightarrow \psi.$$

Prva dva dokaza pokazuju prvi, treći i četvrti sekvent, treći dokaz pokazuje drugi sekvent:

1	ψ	premissa	1	$\neg\varphi$	premissa	1	φ	premissa
2	φ	pretpostavka	2	φ	pretpostavka	2	$\neg\psi$	premissa
3	ψ	R(1)	3	$\perp$	$\neg_E(1,2)$	3	$\varphi \rightarrow \psi$	pretpostavka
4	$\varphi \rightarrow \psi$	D(2-3)	4	ψ	EFQ(3)	4	ψ	MP(1,3)
			5	$\varphi \rightarrow \psi$	D(2-4)	5	$\perp$	$\neg_E(2,4)$
						6	$\neg(\varphi \rightarrow \psi)$	$\neg_U(3-5)$

□

Tvrđenje 2.60. Neka $\varphi = \varphi(p_1, \dots, p_n) \in \Phi$ i $v \in \mathcal{V}$. Važi: $p_1^v, \dots, p_n^v \vdash \varphi^v$.

Dokaz. Dokaz izvodimo potpunom indukcijom po $sl(\varphi)$. Neka je najpre $sl(\varphi) = 0$. Ako je $\varphi = \perp$, dokazujemo $p_1^v, \dots, p_n^v \vdash \neg\perp$ jer $\perp^v = \neg\perp$ za sve $v \in \mathcal{V}$. To sledi iz $\vdash \neg\perp$, a dokaz je:

1	$\perp$	pretpostavka
2	$\neg\perp$	RAA(1-1)

Ako je $\varphi = p_i$, treba da dokažemo $p_1^v, \dots, p_n^v \vdash p_i^v$, što je očigledno.

Neka je $sl(\varphi) > 0$. Tada je $\varphi = \psi \rightarrow \theta$ za neke $\psi, \theta \in \Phi$, $\psi = \psi(p_1, \dots, p_n)$, $\theta = \theta(p_1, \dots, p_n)$ i $sl(\psi), sl(\theta) < sl(\varphi)$. Prema indukcijskoj hipotezi $p_1^v, \dots, p_n^v \vdash \psi^v$ i $p_1^v, \dots, p_n^v \vdash \theta^v$, pa prema lemi 2.59, $p_1^v, \dots, p_n^v \vdash \varphi^v$. □

Dokaz teoreme 2.57. Kao što smo već rekli smer ($\Rightarrow$) je specijalan slučaj teoreme saglasnosti. Za ($\Leftarrow$) pretpostavimo $\models \varphi$. Neka je $P(\varphi) = \{p_1, \dots, p_n\}$; tada je $\varphi = \varphi(p_1, \dots, p_n)$. Neka je v proizvoljna valuacija slova $p_1, \dots, p_{n-1}$. Ako dodefinišemo $v(p_n) = T$, prema tvrđenju 2.60 važi:

$$p_1^v, \dots, p_{n-1}^v, p_n \vdash \varphi,$$

a ako dodefinišemo $v(p_n) = N$, prema tvrđenju 2.60 važi:

$$p_1^v, \dots, p_{n-1}^v, \neg p_n \vdash \varphi.$$

(U oba slučaja, na desnoj strani sekventa je $\varphi^v = \varphi$ jer $\models \varphi$.) Iz prethodna dva sekventa, prema lemi 2.58, sledi:

$$p_1^v, \dots, p_{n-1}^v \vdash \varphi. \quad (*)$$

Neka je sada v proizvoljna valuacija slova $p_1, \dots, p_{n-2}$. Ako dodefinišemo $v(p_{n-1}) = T$, prema (*) važi:

$$p_1^v, \dots, p_{n-2}^v, p_{n-1} \vdash \varphi,$$

a ako dodefinišemo $v(p_{n-1}) = N$, prema (*) važi:

$$p_1^v, \dots, p_{n-2}^v, \neg p_{n-1} \vdash \varphi.$$

Iz prethodna dva sekventa, prema lemi 2.58, sledi:

$$p_1^v, \dots, p_{n-2}^v \vdash \varphi. \quad (**)$$

Nastavljajući ovaj postupak zaključujemo $\vdash \varphi$. □

2.9 Teorema kompaktnosti

Podsetimo se pojma zadovoljivosti, i definišimo pojam konačne zadovoljivosti.

Definicija 2.61. Neka je $\Sigma \subseteq \Phi$ skup formula.

- a) Σ je *zadovoljiv* ako postoji valuacija v takva da $v \models \Sigma$ (tj. takva da $(\forall \varphi \in \Sigma) \hat{v}(\varphi) = T$).
- b) Σ je *konačno zadovoljiv* ako je svaki konačan podskup od Σ zadovoljiv.

Cilj ovog poglavlja je da dokažemo teoremu kompaktnosti:

Teorema 2.62 (Teorema kompaktnosti). Neka je $\Sigma \subseteq \Phi$. Tada:

$$\Sigma \text{ je zadovoljiv} \iff \Sigma \text{ je konačno zadovoljiv.}$$

Smer ($\Rightarrow$) je očigledan (naime svaka valuacija koja zadovoljava Σ zadovoljava i sve njegove podskupove, pa i sve njegove konačne podskupove). Za dokaz ($\Leftarrow$) potrebna nam je priprema. Najpre ćemo da dokažemo specijalan slučaj smera ($\Leftarrow$) (teorema o kanonskoj valuaciji), na koji ćemo kasnije da svedemo dokaz same teoreme kompaktnosti.

Definicija 2.63. Neka je $\Sigma \subseteq \Phi$. Skup Σ je *zatvoren za slova* ako za svako slovo $p \in P$ važi $p \in \Sigma$ ili $\neg p \in \Sigma$.

Teorema 2.64 (Teorema o kanonskoj valuaciji). Neka je $\Sigma \subseteq \Phi$ konačno zadovoljiv skup formula koji je zatvoren za slova. Tada postoji jedinstvena valuacija v_Σ takva da $v_\Sigma \models \Sigma$.

Specijalno, Σ je zadovoljiv.

Dokaz. Kako je Σ zatvoren za slova, za svako slovo $p \in P$ važi $p \in \Sigma$ ili $\neg p \in \Sigma$, međutim kako je Σ konačno zadovoljiv i kako skup $\{p, \neg p\}$ nije zadovoljiv, ne mogu da važe oba $p \in \Sigma$ i $\neg p \in \Sigma$; dakle, za svako slovo $p \in P$ važi tačno jedno od $p \in \Sigma$ i $\neg p \in \Sigma$. Definišimo valuaciju v_Σ sa:

$$v_\Sigma(p) := \begin{cases} T & p \in \Sigma, \\ N & \neg p \in \Sigma; \end{cases}$$

prema prethodnoj napomeni, v_Σ je dobro definisana valuacija. Primetimo da po samoj definiciji v_Σ , za svako $p \in P$ važi $p^{v_\Sigma} \in \Sigma$.³

Dokažimo $v_\Sigma \models \Sigma$. Neka je $\varphi \in \Sigma$ proizvoljna formula, i neka je $P(\varphi) = \{p_1, \dots, p_n\}$. Tada $\Pi = \{\varphi, p_1^{v_\Sigma}, \dots, p_n^{v_\Sigma}\} \subseteq \Sigma$, pa po konačnoj zadovoljivosti postoji valuacija v takva da $v \models \Pi$. Iz $v \models p_i^{v_\Sigma}$ sledi $v(p_i) = v_\Sigma(p_i)$ za sve $i = 1, \dots, n$, tj. valuacije v i v_Σ se poklapaju na slovima formule φ . Odatle $\hat{v}_\Sigma(\varphi) = \hat{v}(\varphi) = T$, tj. $v_\Sigma \models \varphi$. Dakle, $v_\Sigma \models \Sigma$.

Ako je v valuacija takva da $v \models \Sigma$, zbog zatvorenosti za slova, $v \models p$ ako i samo ako $p \in \Sigma$, tj. ako i samo ako $v_\Sigma \models p$. Dakle, $v = v_\Sigma$, što dokazuje željenu jedinstvenost valuacije v_Σ . Završili smo dokaz. $\square$

Sada je ideja da svedemo dokaz teoreme kompaktnosti na prethodnu teoremu tako što ćemo dokazati da se svaki konačno zadovoljiv skup formula može proširiti do konačno zadovoljivog skupa formula koji je zatvoren za slova. Potrebne su nam dve leme.

Lema 2.65. Neka je $\Sigma \subseteq \Phi$ i $\varphi \in \Phi$. Ako je Σ konačno zadovoljiv, bar jedan od skupova $\Sigma \cup \{\varphi\}$ i $\Sigma \cup \{\neg\varphi\}$ je konačno zadovoljiv.

Dokaz. Pretpostavimo Σ je konačno zadovoljiv, i pretpostavimo suptorno, $\Sigma \cup \{\varphi\}$ i $\Sigma \cup \{\neg\varphi\}$ nisu konačno zadovoljivi. Tada postoje konačni podskupovi $\Sigma_1, \Sigma_2 \subseteq \Sigma$ takvi da $\Sigma_1 \cup \{\varphi\}$ i $\Sigma_2 \cup \{\neg\varphi\}$ nisu zadovoljivi. Skup $\Sigma_1 \cup \Sigma_2$ je konačan podskup od Σ , pa postoji valuacija v takva da $v \models \Sigma_1 \cup \Sigma_2$. Iz $v \models \Sigma_1$ i $v \not\models \Sigma_1 \cup \{\varphi\}$ sledi $\hat{v}(\varphi) = N$, dok iz $v \models \Sigma_2$ i $v \not\models \Sigma_2 \cup \{\neg\varphi\}$ sledi $\hat{v}(\varphi) = T$; kontradikcija. $\square$

Lema 2.66. Neka je $\Sigma_0 \subseteq \Sigma_1 \subseteq \Sigma_2 \subseteq \dots \subseteq \Phi$ rastući niz skupova formula. Ako su svi skupovi Σ_n konačno zadovoljivi, onda je i $\Sigma^* := \bigcup_{n=0}^{\infty} \Sigma_n$ konačno zadovoljiv.

Dokaz. Neka je $\Pi \subseteq \Sigma^*$ proizvoljan konačan podskup; treba da dokažemo da je Π zadovoljiv. Neka je $\Pi = \{\varphi_1, \dots, \varphi_k\}$. Po definiciji Σ^* , za svako $i = 1, \dots, k$ važi da $\varphi_i \in \Sigma_{n_i}$ za neko n_i , pa kako je niz rastući za sve $i = 1, \dots, k$ važi $\varphi_i \in \Sigma_N$, gde je $N = \max\{n_1, \dots, n_k\}$, tj. $\Pi \subseteq \Sigma_N$. Dakle, Π je konačan podskup konačno zadovoljivog skupa Σ_N , odakle sledi da je Π zadovoljiv. $\square$

³Setimo se da je $p^{v_\Sigma} = \begin{cases} p & v_\Sigma(p) = T, \\ \neg p & v_\Sigma(p) = N. \end{cases}$

Sledeća teorema je glavni korak u svođenju teoreme kompaktnosti na teoremu o kanonskoj valuaciji.

Teorema 2.67 (Lindenbaumova teorema). Neka je $\Sigma \subseteq \Phi$ konačno zadovoljiv skup formula. Tada postoji konačno zadovoljiv skup formula Σ^* takav da $\Sigma^* \supseteq \Sigma$ i Σ^* je zatvoren za slova.

U opštem slučaju dokaz Lindenbaumove teoreme koristi aksiomu izbora (malo kasnije ćemo diskutovati o ovome), pa ćemo za početak da dokažemo specijalan slučaj.

Dokaz teoreme 2.67 ako je P prebrojiv. Pretpostavimo da je skup slova P prebrojiv. O prebrojivim skupovima ćemo kasnije pričati, za sada je dovoljno da znamo da možemo da pretpostavimo da je:

$$P = \{p_0, p_1, p_2, \dots\}.$$

Definišimo rastući niz konačno zadovoljivih skupova $\Sigma_0 \subseteq \Sigma_1 \subseteq \Sigma_2 \subseteq \dots$ rekurzijom na sledeći način:

- $\Sigma_0 = \Sigma$; po pretpostavci Σ_0 je konačno zadovoljiv.
- Pretpostavimo da smo definisali konačno zadovoljiv skup Σ_n , definišemo:

$$\Sigma_{n+1} := \begin{cases} \Sigma_n \cup \{p_n\} & \text{ako je } \Sigma_n \cup \{p_n\} \text{ zadovoljiv,} \\ \Sigma_n \cup \{\neg p_n\} & \text{inače.} \end{cases}$$

Skup Σ_{n+1} je konačno zadovoljiv prema lemi 2.65, i očigledno $\Sigma_{n+1} \supseteq \Sigma_n$.

Prema konstrukciji skup $\Sigma^* := \bigcup_{n=0}^{\infty} \Sigma_n$ je zatvoren za slova i $\Sigma^* \supseteq \Sigma$, a prema lemi 2.66, skup Σ^* je konačno zadovoljiv. $\square$

Sada možemo da dokažemo teoremu kompaktnosti:

Dokaz teoreme 2.62. Već smo rekli, smer $(\Rightarrow)$ je očigledan, pa dokazujemo $(\Leftarrow)$. Neka je Σ konačno zadovoljiv skup formula. Prema teoremi 2.67 proširimo Σ do konačno zadovoljivog skupa formula Σ^* koji je zatvoren za slova. Prema teoremi 2.64, Σ^* je zadovoljiv, pa je i Σ zadovoljiv kao njegov podskup. $\square$

Prethodni dokaz oslanja se na Lindenbaumovu teoremu koju smo dokazali samo u specijalnom slučaju. Opšti slučaj zavisi od aksiome izbora, pa ćemo sada reći nekoliko reči o tome.

Digresija: Aksioma izbora

Definicija 2.68. Neka je $\mathcal{F}$ familija skupova.

- Familija $\mathcal{F}$ je *lanac skupova* ako za svaka dva skupa $X, Y \in \mathcal{F}$ važi $X \subseteq Y$ ili $Y \subseteq X$.
- Skup $A \in \mathcal{F}$ je *maksimalan* element familije $\mathcal{F}$ ako za svaki skup $X \in \mathcal{F}$ važi $A \not\subseteq X$.

Aksioma 2.69 (Cordova lema). Neka je $\mathcal{F}$ neprazna familija skupova. Pretpostavimo da za svaki neprazan lanac $\mathcal{L} \subseteq \mathcal{F}$ važi $\bigcup \mathcal{L} \in \mathcal{F}$.⁴ Tada $\mathcal{F}$ ima maksimalan element.

Teorema kompaktnosti (nastavak)

Da bismo dokazali teoremu kompaktnosti u opštem slučaju, dovoljno je da dokažemo Lindenbaumovu teoremu u opštem slučaju. U dokazu ćemo iskoristiti Cornovu lemu, i za dokaz će nam biti potrebna nešto opštija verzija leme 2.66 (sa suštinski istim dokazom):

Lema 2.70. Ako je $\mathcal{L}$ lanac konačno zadovoljivih skupova formula, onda je i $\bigcup \mathcal{L}$ konačno zadovoljiv.

⁴ $\bigcup \mathcal{L}$ je oznaka za uniju $\bigcup_{X \in \mathcal{L}} X$.

Dokaz. Neka je $\Pi \subseteq \bigcup \mathcal{L}$ proizvoljan konačan podskup; treba da dokažemo da je Π zadovoljiv. Neka je $\Pi = \{\varphi_1, \dots, \varphi_k\}$. Za svako $i = 1, \dots, k$ važi da $\varphi_i \in \Sigma_i$ za neko $\Sigma_i \in \mathcal{L}$, pa kako je $\mathcal{L}$ lanac za sve $i = 1, \dots, k$ važi $\varphi_i \in \Sigma$, gde je Σ najveći od skupova $\Sigma_1, \dots, \Sigma_k$. Dakle, $\Pi \subseteq \Sigma$, tj. Π je konačan podskup konačno zadovoljivog skupa Σ , odakle sledi da je Π zadovoljiv. $\square$

Sada možemo da dokažemo Lindenbaumovu teoremu.

Dokaz teoreme 2.67 u opštem slučaju. Neka je Σ konačno zadovoljiv, i neka je:

$$\mathcal{F} := \{\Pi \subseteq \Phi : \Sigma \subseteq \Pi \text{ i } \Pi \text{ je konačno zadovoljiv}\}.$$

Familija $\mathcal{F}$ je neprazna jer očigledno $\Sigma \in \mathcal{F}$. Takođe, prema lemi 2.70 za svaki neprazan lanac $\mathcal{L} \subseteq \mathcal{F}$ važi $\bigcup \mathcal{L} \in \mathcal{F}$. Prema Cornovoj lemi (aksioma 2.69), $\mathcal{F}$ ima maksimalni element Σ^* . Očigledno $\Sigma \subseteq \Sigma^*$ i Σ^* je konačno zadovoljiv jer $\Sigma^* \in \mathcal{F}$. Ostaje da proverimo da je Σ^* zatvoren za slova.

Neka je $p \in P$ proizvoljno slovo. Pretpostavimo $p \notin \Sigma^*$. Tada je $\Sigma^* \cup \{p\} \not\subseteq \Sigma^*$, pa zbog maksimalnosti Σ^* u $\mathcal{F}$ sledi da $\Sigma^* \cup \{p\} \notin \mathcal{F}$, odakle $\Sigma^* \cup \{p\}$ nije konačno zadovoljiv. Prema lemi 2.65, $\Sigma^* \cup \{-p\}$ mora biti konačno zadovoljiv, tj. $\Sigma^* \cup \{-p\} \in \mathcal{F}$, pa kako je $\Sigma^* \subseteq \Sigma^* \cup \{-p\}$ i kako je Σ^* maksimalan u $\mathcal{F}$, mora biti $\Sigma^* = \Sigma^* \cup \{-p\}$, odakle $-p \in \Sigma^*$. Završili smo dokaz. $\square$

2.10* Primeri primene teoreme kompaktnosti

Daćemo nekoliko primera primene teoreme 2.62. Generalna ideja je da polazni problem, koji se odnosi na neku beskonačnu konfiguraciju, pametno pretvorimo u problem zadovoljivosti nekog skupa iskaznih formula. Samu zadovoljivost skupa dokazujemo koristeći kompaktnost tako što proverimo da su svi njegovi konačni podskupovi zadovoljivi. Za poslednje je obično potrebno da rešimo polazni problem za konačne konfiguracije, što je ponekad mnogo lakše nego rešiti polazni problem.

2.10.1 Uređenja racionalnih brojeva

Problem 2.71. Dokazati da se racionalni brojevi mogu poredati tako da ne postoji rastući (u smislu uočenog poretka) aritmetički niz dužine tri. Drugim rečima, moguće je definisati linearni poredak $<$ na $\mathbb{Q}$ tako da kadgod $a < b < c$, niz (a, b, c) nije aritmetički niz (tj. $b - a \neq c - b$).

Prethodni problem ćemo rešiti koristeći kompaktnost, za šta će nam biti potrebna sledeća (konačna) lema.

Lema 2.72. Za svako $n \in \mathbb{N}$, elementi $0, 1, 2, \dots, 2^n - 1$ se mogu poredati tako da u ovom poretku ne postoji rastući aritmetički niz dužine tri.

Dokaz. Dokaz izvodimo indukcijom po n .

Baza indukcije. Za $n = 0$ nemamo šta da dokažemo jer imamo samo jedan element. Za $n = 1$ imamo samo dva elementa 0 i 1, pa bilo da ih poredamo $0 < 1$ ili $1 < 0$, uslov je ispunjen. Prvi zanimljiv slučaj je $n = 2$, i treba da poredamo elemente 0, 1, 2, 3 tako da nemamo rastući aritmetički niz dužine tri. Jedan način da to uradimo je:

$$0 < 2 < 1 < 3.$$

Indukcijski korak. Pretpostavimo da smo poredali $0, 1, \dots, 2^n - 1$ u niz:

$$a_0 < a_1 < \dots < a_{2^n-1}$$

tako da u prethodnom nizu nemamo rastući aritmetički niz dužine tri. Sada ćemo poredati $0, 1, \dots, 2^{n+1} - 1$ u niz koji zadovoljava traženi uslov. Primetimo da je $\{0, 1, \dots, 2^{n+1} - 1\} = \{2a_0, 2a_1, \dots, 2a_{2^n-1}\} \cup \{2a_0 + 1, 2a_1 + 1, \dots, 2a_{2^n-1} + 1\}$. Trik je da ih poredamo na sledeći način:

$$2a_0 < 2a_1 < \dots < 2a_{2^n-1} < 2a_0 + 1 < 2a_1 + 1 < \dots < 2a_{2^n-1} + 1.$$

Primitimo da u prvoj polovini nemamo rastući aritmetički niz dužine tri jer za $i < j < k$, $(2a_i, 2a_j, 2a_k)$ je aritmetički niz ako i samo ako (a_i, a_j, a_k) je aritmetički niz, a poslednje ne važi po indukcijskoj hipotezi. Slično, u drugoj polovini nemamo rastući aritmetički niz dužine tri jer za $i < j < k$, $(2a_i + 1, 2a_j + 1, 2a_k + 1)$ je aritmetički niz ako i samo ako (a_i, a_j, a_k) je aritmetički niz. Za $i < j$ i k , niz $(2a_i, 2a_j, 2a_k + 1)$ nije aritmetički jer je razlika prva dva člana parna, a razlika druga dva neparna. Slično, za i i $j < k$, $(2a_i, 2a_j + 1, 2a_k + 1)$ nije aritmetički jer je razlika prva dva člana neparna, a razlika druga dva parna. Prema tome, poređali smo $0, 1, \dots, 2^{n+1} - 1$ na odgovarajući način. $\square$

Rešenje problema 2.71. Iskodirajmo sada naš problem u iskaznoj logici. Uočićemo skup slova $P = \{p_{a,b} : a, b \in \mathbb{Q}, a \neq b\}$ i sledeći skup iskaznih formula:

$$\begin{aligned} \Sigma &= \{p_{a,b} \vee p_{b,a} : a, b \in \mathbb{Q}, a \neq b\} \\ &\cup \{p_{a,b} \wedge p_{b,c} \rightarrow p_{a,c} : a, b, c \in \mathbb{Q}, a \neq b \neq c \neq a\} \\ &\cup \{\neg(p_{a,b} \wedge p_{b,c}) : (a, b, c) \in A\}, \end{aligned}$$

gde je A skup svih nekonstantnih, racionalnih, aritmetičkih nizova dužine tri. Primitimo da ako možemo da poređamo $\mathbb{Q}$ na željeni način, onda imamo sledeću valuaciju koja zadovoljava skup Σ :

$$v(p_{a,b}) := \begin{cases} T & \text{ako } a < b \\ N & \text{ako } b < a \end{cases}.$$

Zaista, formule $p_{a,b} \vee p_{b,a}$ su tačne jer važi ili $a < b$ ili $b < a$, formule $p_{a,b} \wedge p_{b,c} \rightarrow p_{a,c}$ su tačne jer $a < b$ i $b < c$ povlače $a < c$, i na kraju formule $\neg(p_{a,b} \wedge p_{b,c})$ su tačne jer ako $(a, b, c) \in A$, kako poredak zadovoljava željeni uslov, ne može važiti $a < b$ i $b < c$.

Sa druge strane, ako imamo valuaciju v koja zadovoljava Σ , na skupu $\mathbb{Q}$ možemo definisati željeni poredak na sledeći način:

$$a < b \quad :\Longleftrightarrow \quad v(p_{a,b}) = T, \text{ za različite } a, b \in \mathbb{Q}.$$

Ovo zaista jeste poredak jer v zadovoljava prva dva skupa formula, a takođe ako $(a, b, c) \in A$, kako je $p_{a,b} \wedge p_{b,c}$ netačna, niz (a, b, c) nije rastući.

Prema tome sveli smo problem na dokaz da je Σ zadovoljiv skup. Po kompaktnosti, tj. teoremi 2.62, dovoljno je da dokažemo da su konačni podskupovi od Σ zadovoljivi. Pa neka je Σ_0 proizvoljan konačan podskup od Σ . Samo konačno mnogo slova pojavljuje se u skupu Σ_0 , pa se i samo konačno mnogo racionalnih brojeva pojavljuje kao indeksi ovih slova. Neka je $Q_0 \subseteq \mathbb{Q}$ konačan podskup racionalnih brojeva koji se pojavljuju kao indeksi slova u skupu Σ_0 ; dakle, imamo:

$$\begin{aligned} \Sigma_0 &\subseteq \{p_{a,b} \vee p_{b,a} : a, b \in Q_0, a \neq b\} \\ &\cup \{p_{a,b} \wedge p_{b,c} \rightarrow p_{a,c} : a, b, c \in Q_0, a \neq b \neq c \neq a\} \\ &\cup \{\neg(p_{a,b} \wedge p_{b,c}) : (a, b, c) \in A \cap Q_0^3\}. \end{aligned}$$

Označimo sa Σ_1 skup na desnoj strani. Dovoljno je da dokažemo da je on zadovoljiv, jer je onda i manji skup Σ_0 jasno zadovoljiv. Kako je Q_0 konačan možemo da nađemo prirodan broj M takav da $Ma \in \mathbb{Z}$ za sve $a \in \mathbb{Q}$ (uzmimo M da bude NZS svih imenilaca brojeva iz Q_0 zapisanih u obliku skraćenog razlomka). Dalje nađemo prirodan broj K takav da $Ma + K \geq 0$ za sve $a \in Q_0$. Konačno izaberimo prirodan broj N takav da $Ma + K < 2^N$, za sve $a \in A$. Prema lemi 2.72, brojeve $0, 1, \dots, 2^N - 1$ možemo da poređamo tako da u ovom poretку nemamo rastući aritmetički niz dužine tri; označimo ovaj poredak sa $<$. Primitimo da su brojevi $Ma + K$, $a \in Q_0$, poređani u ovom poretку. Definišimo valuaciju v slova $p_{a,b}$, $a, b \in Q_0$, $a \neq b$ sa:

$$v(p_{a,b}) = \begin{cases} T & Ma + K < Mb + K \\ N & Mb + K < Ma + K \end{cases},$$

i primitimo da v zadovoljava Σ_1 . Zaista, formule $p_{a,b} \vee p_{b,a}$ i $p_{a,b} \wedge p_{b,c} \rightarrow p_{a,c}$ su tačne jer su $Ma + K$, $a \in Q_0$,

poređani u odnosu na $<$. Formule $p_{a,b} \wedge p_{b,c}$ za $(a,b,c) \in A \cap Q_0^3$ su netačne jer je niz (a,b,c) aritmetički ako i samo ako je niz $(Ma+K, Mb+K, Mc+K)$ aritmetički, pa ne važi $Ma+K < Mb+K < Mc+K$.

Dakle, Σ_1 je zadovoljiv i time smo rešili problem. $\square$

Zadatak 2.73. Dokazati da se realni brojevi mogu poređati tako da ne postoji rastući aritmetički niz dužine tri. ⁵

2.10.2 Linearizacija parcijalnih uređenja

Problem 2.74. Dokazati da postoji strogo linearno uređenje $<$ na $\mathcal{P}(\mathbb{N})$ tako da $A \not\subseteq B$ povlači $A < B$ za sve $A, B \subseteq \mathbb{N}$. (Tj. dokazati da se relacija podskupa na $\mathcal{P}(\mathbb{N})$ može dodefinisati do linearnog uređenja.)

Ponovo najpre dokazujemo odgovarajuću konačnu verziju problema.

Lema 2.75. Za proizvoljne $n \geq 1$ i $A_1, \dots, A_n \subseteq \mathbb{N}$, $A_1, \dots, A_n$ se mogu poređati tako da ako $A_i \not\subseteq A_j$, onda je i $A_i < A_j$, za sve $1 \leq i, j \leq n$.

Dokaz. Dokaz izvodimo indukcijom po n .

Baza indukcije. Ako je $n = 1$ nemamo šta da dokažemo. Razmotrimo i slučaj (što nije neophodno) $n = 2$. Ako imamo dva podskupa $A, B \subseteq \mathbb{N}$, postupamo na sledeći način. Ako je $A \not\subseteq B$, stavili bismo $A < B$, a ako je $B \not\subseteq A$, stavili bismo $B < A$. Ako nije ni $A \not\subseteq B$ ni $B \not\subseteq A$, možemo da definišemo bilo $A < B$ bilo $B < A$, u oba slučaja imamo zadovoljavajuće ređanje.

Indukcijski korak. Pretpostavimo da imamo sada podskupove $A_1, \dots, A_n, A_{n+1}$. Njih je samo konačno mnogo, pa možemo nađemo A_i tako da $A_j \not\subseteq A_i$ za sve $j \neq i$. (Zaista, ako nijedan A_i ne zadovoljava ovaj uslov, onda za svaki A_i možemo da nađemo A_j takav da $A_j \not\subseteq A_i$. Sada imamo $A_1 \not\subseteq A_{j_1}$ za neko j_1 , pa $A_{j_1} \not\subseteq A_{j_2}$ za neko j_2 , pa $A_{j_2} \not\subseteq A_{j_3}$, itd. U $n+1$ koraka nalazimo niz međusobno različitih $n+2$ podskupova:

$$A_1 \not\subseteq A_{j_1} \not\subseteq A_{j_2} \not\subseteq A_{j_3} \not\subseteq \dots \not\subseteq A_{j_{n+1}},$$

što nije moguće jer imamo samo $n+1$ skupova $A_1, \dots, A_n, A_{n+1}$.) Po induksijskoj hipotezi znamo da skupove $A_1, \dots, A_{i-1}, A_{i+1}, \dots, A_{n+1}$ možemo da poređamo tako da $A_j \subseteq A_k$ povlači $A_j \leq A_k$ za sve $j, k \neq i$. Sada je dovoljno da dodefinišemo ovo ređanje tako što skup A_i stavimo ispred svih. Željeni uslov očigledno je zadovoljen. $\square$

Rešenje probleme 2.74. Sada ćemo iskodirati naš problem u iskaznoj logici. Uočimo skup slova $P = \{p_{A,B} : A, B \subseteq \mathbb{N}, A \neq B\}$ i skup iskaznih formula:

$$\begin{aligned} \Sigma &= \{p_{A,B} \vee p_{B,A} : A, B \subseteq \mathbb{N}, A \neq B\} \\ &\cup \{p_{A,B} \wedge p_{B,C} \rightarrow p_{A,C} : A, B, C \subseteq \mathbb{N}, A \neq B \neq C \neq A\} \\ &\cup \{p_{A,B} : A \not\subseteq B \subseteq \mathbb{N}\}. \end{aligned}$$

Ako možemo da nađemo rešenje $<$ problema 2.74, primetimo da možemo da definišemo i valuaciju v koja zadovoljava Σ na sledeći način:

$$v(p_{A,B}) := \begin{cases} T & \text{ako } A < B \\ N & \text{ako } B < A \end{cases} \quad \text{za } A, B \in \mathbb{N}, A \neq B.$$

Sa druge strane, ako je Σ zadovoljiv i ako je v neka valuacija koja ga zadovoljava, možemo da definišemo željeno uređenje $<$ na sledeći način:

$$A < B \quad : \iff \quad v(p_{A,B}) = T, \text{ za } A, B \in \mathbb{N}, A \neq B.$$

⁵ Ovo je teži zadatak. Možete da pokušate da ga rešite na sledeći način. Skup $\mathbb{R}$ je vektorski prostor nad $\mathbb{Q}$, pa možemo da uočimo jednu njegovu bazu nad $\mathbb{Q}$. Koristeći rezultat problema 2.71 i zapis realnog broja u uočenoj bazi, pokušajte da konstruišete željeni poredak.

Zaista, kako su formule $p_{A,B} \vee p_{B,A}$ tačne, za svaka dva različita skupa A i B smo odredili da li je $A < B$ ili je $B < A$. Takođe, kako su formule $p_{A,B} \wedge p_{B,C} \rightarrow p_{A,C}$ tačne, definisana relacija je i tranzitivna, pa smo korektno definisali linearno uređenje. Konačno, za $A \not\subseteq B \subseteq \mathbb{N}$, tačna je formula $p_{A,B}$, pa zaista važi i $A < B$.

Prema tome, dovoljno je da dokažemo da je Σ zadovoljiv skup formula. Po kompaktnosti (teorema 2.62), dovoljno je da dokažemo da je svaki konačan podskup $\Sigma_0 \subseteq \Sigma$ zadovoljiv, pa uočimo proizvoljan konačan $\Sigma_0 \subseteq \Sigma$. Kako je Σ_0 konačan, samo konačno mnogo skupova $A_1, \dots, A_n \subseteq \mathbb{N}$ pojavljuju se kao indeksi slova u skupu Σ_0 . Dakle:

$$\begin{aligned} \Sigma_0 \subseteq & \{p_{A_i, A_j} \vee p_{A_j, A_i} : 1 \leq i, j \leq n, i \neq j\} \\ & \cup \{p_{A_i, A_j} \wedge p_{A_j, A_k} \rightarrow p_{A_i, A_k} : 1 \leq i, j, k \leq n, i \neq j \neq k \neq i\} \\ & \cup \{p_{A_i, A_j} : 1 \leq i, j \leq n, A_i \not\subseteq A_j\}. \end{aligned}$$

Označimo sa Σ_1 skup na desnoj strani i primetimo da je dovoljno da dokažemo da je on zadovoljiv. Prema lemi 2.75 možemo da uočimo linearno uređenje $<$ skupova $A_1, \dots, A_n$ koje proširuje relaciju podskupa. Sada definišemo valuaciju v sa:

$$v(p_{A_i, A_j}) = \begin{cases} T & \text{ako } A_i < A_j \\ N & \text{ako } A_j < A_i \end{cases} \quad \text{za } 1 \leq i, j \leq n, i \neq j.$$

Sada direktno vidimo da v zadovoljava skup Σ_1 , što završava rešenje problema 2.74. $\square$

Zadatak 2.76. Dokazati da se (bilo koje) parcijalno uređenje na (bilo kom) skupu S može dodefinisati do linearnog uređenja.

2.10.3 4-oboјivost planarnih grafova

Graf je (konačan ili beskonačan) skup tačaka (*čvorova* grafa) od kojih su neke povezane *ivicama*. Graf je *planaran* ako je moguće da ga nacrtamo u ravni tako da se nikoje dve ivice ne preseku. Graf je *k-oboјiv* ako svaki čvor grafa možemo da oboјimo u jednu od k boja tako da jednako oboјeni čvorovi nisu spojeni ivicom. (Pretpostavljamo da nijedan čvor nije povezan ivicom sam sa sobom.)

Problem 2.77. Dokazati da je planaran graf 4-oboјiv.

Konačni planarni grafovi jesu 4-oboјivi:

Teorema 2.78 (Teorema o četiri boje). Konačan planaran graf je 4-oboјiv.

Prethodna teorema je čuvena jer je prva teorema koja je dokazana uz pomoć računara 1976. godine.

Rešenje problema 2.77. Da bismo dokazali beskonačnu verziju teoreme, tj. u potpunosti rešili problem 2.77, iskoristićemo kompaktnost. Uočimo graf G koji je dat skupom čvorova V i skupom ivica E . Uočimo sledeći skup iskaznih slova:

$$P = \{p_v, c_v, z_v, b_v : v \in V\},$$

i skup iskaznih formula:

$$\begin{aligned} \Sigma = & \left\{ \begin{aligned} & (p_v \wedge \neg c_v \wedge \neg z_v \wedge \neg b_v) \vee (\neg p_v \wedge c_v \wedge \neg z_v \wedge \neg b_v) \vee \\ & \vee (\neg p_v \wedge \neg c_v \wedge z_v \wedge \neg b_v) \vee (\neg p_v \wedge \neg c_v \wedge \neg z_v \wedge b_v) \end{aligned} : v \in V \right\} \\ & \cup \left\{ \neg(p_v \wedge p_w) \wedge \neg(c_v \wedge c_w) \wedge \neg(z_v \wedge z_w) \wedge \neg(b_v \wedge b_w) : \begin{array}{l} v, w \in V \text{ su} \\ \text{povezani ivicom} \end{array} \right\}. \end{aligned}$$

Ako je graf G 4-oboјiv, npr. bojama plavom, crvenom, zelenom i belom, možemo da definišemo valuaciju u

koja zadovoljava Σ na sledeći način:

$$\begin{aligned} u(p_v) &:= \begin{cases} T & \text{ako je čvor } v \text{ plav} \\ N & \text{inače} \end{cases}, & u(c_v) &= \begin{cases} T & \text{ako je čvor } v \text{ crven} \\ N & \text{inače} \end{cases} \\ u(z_v) &= \begin{cases} T & \text{ako je čvor } v \text{ zelen} \\ N & \text{inače} \end{cases}, & u(b_v) &= \begin{cases} T & \text{ako je čvor } v \text{ beo} \\ N & \text{inače} \end{cases} \end{aligned}$$

za sve $v \in V$. Formule prvog skupa su tačne jer je svaki čvor obojen u tačno jednu boju. Formule drugog skupa su tačne jer dva povezana čvora nisu obojena istom bojom.

Sa druge strane, pretpostavimo da je Σ zadovoljiv i neka je u valuacija koja ga zadovoljava. Tada možemo da brojimo graf na sledeći način. Za čvor $v \in V$ obojimo:

$$\begin{aligned} v \text{ je plav} & : \iff u(p_v) = T, & v \text{ je crven} & : \iff u(c_v) = T, \\ v \text{ je zelen} & : \iff u(z_v) = T, & v \text{ je beo} & : \iff u(b_v) = T. \end{aligned}$$

Kako su formule prvog skupa tačne, za svako v tačno je tačno jedno od slova p_v, c_v, z_v, b_v , pa smo prethodnom definicijom svakom čvoru dodeli tačno jednu boju. Takođe, kako su formule drugog skupa tačne, dva povezana čvora nismo obojili istom bojom. Prema tome, dobili smo odgovarajuće bojenje.

Dakle, dovoljno je da dokažemo da je Σ zadovoljiv. Po kompaktnosti dovoljno je da dokažemo da su konačni podskupovi od Σ zadovoljivi. Neka je $\Sigma_0 \subseteq \Sigma$ proizvoljan konačan podskup. Kako je Σ_0 konačan, samo konačno mnogo $v \in V$ pojavljuje se kao indeks slova u Σ_0 , pa neka je $V_0 \subseteq V$ konačan podskup onih v koji se pojavljuju kao indeksi u Σ_0 . Dakle:

$$\begin{aligned} \Sigma_0 &\subseteq \left\{ \begin{aligned} &(p_v \wedge \neg c_v \wedge \neg z_v \wedge \neg b_v) \vee (\neg p_v \wedge c_v \wedge \neg z_v \wedge \neg b_v) \vee \\ &\vee (\neg p_v \wedge \neg c_v \wedge z_v \wedge \neg b_v) \vee (\neg p_v \wedge \neg c_v \wedge \neg z_v \wedge b_v) \end{aligned} : v \in V_0 \right\} \\ &\cup \left\{ \neg(p_v \wedge p_w) \wedge \neg(c_v \wedge c_w) \wedge \neg(z_v \wedge z_w) \wedge \neg(b_v \wedge b_w) : \begin{array}{l} v, w \in V_0 \text{ su} \\ \text{povezani ivicom} \end{array} \right\}. \end{aligned}$$

Neka je Σ_1 skup na desnoj strani; dovoljno je da dokažemo da je on zadovoljiv. Neka je G_0 konačan podgraf od G čiji su čvorovi V_0 . Graf G_0 jasno je konačan i planaran, pa prema teoremi o četiri boje možemo da ga 4-obojujemo (recimo u boje plava, crvena, zelena i bela). Sada defininišemo valuaciju u koja zadovoljava Σ_1 sa:

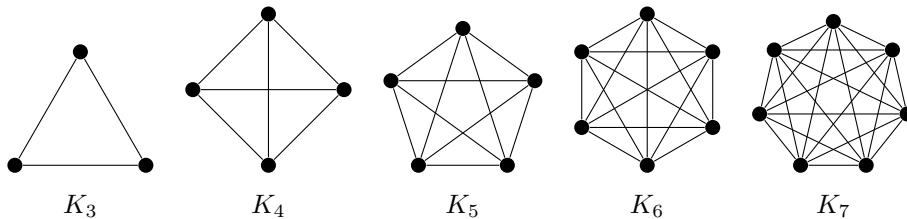
$$\begin{aligned} u(p_v) &= \begin{cases} T & \text{ako je čvor } v \text{ plav} \\ N & \text{inače} \end{cases}, & u(c_v) &= \begin{cases} T & \text{ako je čvor } v \text{ crven} \\ N & \text{inače} \end{cases} \\ u(z_v) &= \begin{cases} T & \text{ako je čvor } v \text{ zelen} \\ N & \text{inače} \end{cases}, & u(b_v) &= \begin{cases} T & \text{ako je čvor } v \text{ beo} \\ N & \text{inače} \end{cases} \end{aligned}$$

za sve $v \in V$. Kao i gore, lako vidimo da u zaista zadovoljava Σ_1 . Time smo završili rešenje problema. $\square$

Zadatak 2.79. Dokazati da je graf k -obojujiv ako i samo ako su svi njegovi konačni podgrafovi k -obojujivi.

2.10.4 Remzijeva teorema

Potpun graf K_n je graf sa n čvorova kod koga su svaka dva različita čvora povezana ivicom.

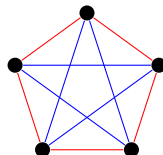


Teorema 2.80 (Remzijeva teorema). Za svaka dva prirodna broja $m, n \geq 1$ postoji prirodan broj N takav da za svako bojenje ivica potpunog grafa K_N u dve boje, crvenu i plavu, postoji podgraf koji je kopija K_m i čije su sve ivice crvene ili postoji podgraf koji je kopija K_n i čije su sve ivice plave.

Najmanji takav broj N obeležavamo sa $R(m, n)$ i zovemo ga Remzijev broj.

Primer 2.81. Dokažimo $R(3, 3) = 6$, tj. kako god obojimo ivice grafa K_6 u dve boje, crvenu i plavu, uvek će postojati ili crveni trougao ili plavi trougao. Izaberimo proizvoljno teme A . Iz A izlazi pet ivica, pa neke tri, nazovimo ih AB , AC i AD , su iste boje, recimo crvene. Ako je neka od ivica BC , BD i CD crvena, našli smo crveni trougao; u suprotnom, BCD je plavi trougao.

Ovo pokazuje da je $R(3, 3) \leq 6$. Sledeća slika pokazuje da $R(3, 3) \not\leq 6$, odakle $R(3, 3) = 6$:



Prethodni primer ima sledeću popularnu interpretaciju: u svakoj grupi od šest ljudi postoje tri osobe koje se međusobno poznaju ili tri osobe koje se međusobno ne poznaju. Zaista, ako zamislimo potpun graf između osoba, i obojimo ivicu između dve osobe crveno ako se one poznaju, odnosno plavo ako se one ne poznaju, prethodni primer nam kaže da postoje tri osobe koje se međusobno poznaju ili tri osobe koje se međusobno ne poznaju. Ovim jezikom Remzijeva teorema se može izraziti na sledeći način: Za svaka dva prirodna broja $m, n \geq 1$ postoji najmanji prirodan broj $R(m, n)$ takav da u svakoj grupi od $R(m, n)$ ljudi postoji m osoba koje se međusobno poznaju ili n osoba koje se međusobno ne poznaju.

Remzijevu teoremu dokazaćemo koristeći kompaktnost i njenu beskonačnu verziju (koja je lakša za dokaz):

Teorema 2.82 (Beskonačna Remzijeva teorema). Za svako bojenje ivica grafa K_ω u dve boje postoji podgraf koji je kopija K_ω i čije su sve ivice obojene istom bojom.⁶

(Ako želite, u svakoj grupi od beskonačno mnogo ljudi postoji beskonačno mnogo osoba koje se međusobno poznaju ili beskonačno mnogo osoba koje se međusobno ne poznaju.)

Dokaz. Neka je K_ω potpuni graf u kome su čvorovi indeksirani prirodnim brojevima, i neka je dato neko crveno/plavo bojenje ivica. Rekurentno definišemo opadajući niz beskonačnih podskupova prirodnih brojeva (S_n) i niz prirodnih brojeva (a_n) takav da $a_n \in S_n$ na sledeći način:

- Stavimo $S_0 = \mathbb{N}$ i $a_0 = 0$.
- Pretpostavimo da smo definisali beskonačan S_n i a_n tako da $a_n \in S_n$. Skup $S_n \setminus \{a_n\}$ podelimo na dva dela: $C := \{x \in S_n \setminus \{a_n\} : a_n - x \text{ je crvena}\}$ i $P := \{x \in S_n \setminus \{a_n\} : a_n - x \text{ je plava}\}$. Kako je $C \cup P = S_n \setminus \{a_n\}$, bar jedan od C i P je beskonačan, pa stavimo $S_{n+1} := C$ ako je C beskonačan i $S_{n+1} := P$ ako je C konačan (u kom slučaju je P beskonačan); jasno $S_{n+1} \subsetneq S_n$. U svakom slučaju izaberimo proizvoljno $a_{n+1} \in S_{n+1}$. Nastavimo postupak.

Primetimo da su po konstrukciji svi a_n međusobno različiti. Takođe, primetimo da za svako n imamo $a_m \in S_{n+1}$ za $m > n$, što znači da su ivice $a_n - a_m$ za $m > n$ sve iste boje. Podelimo sada skup $\{a_n : n \in \mathbb{N}\}$ na dva dela: $\{a_n : (\forall m > n) a_n - a_m \text{ je crvena}\}$ i $\{a_n : (\forall m > n) a_n - a_m \text{ je plava}\}$. Bar jedan od ovih skupova je beskonačan, npr. neka je $S = \{a_n : (\forall m > n) a_n - a_m \text{ je crvena}\}$ beskonačan. Sada je očigledno da su sve ivice podgraфа sa čvorovima iz skupa S crvene, pa je u pitanju željena kopija K_ω . Završili smo dokaz. $\square$

Dokažimo sada Remzijevu teoremu:

⁶Sa K_ω smo obeležili potpun graf sa prebrojivo mnogo čvorova (npr. čvorovi su označeni prirodnim brojevima).

Dokaz teoreme 2.80. Fiksirajmo $m, n \geq 1$. Uočimo graf K_ω u kome su čvorovi indeksirani prirodnim brojevima, i uočimo skup iskaznih slova $P := \{p_{i,j} : 0 \leq i < j\}$. Za $A, B \subseteq \mathbb{N}$, $|A| = m$ i $|B| = n$, označimo:

$$\rho_A := \bigwedge_{\substack{i,j \in A \\ i < j}} p_{i,j} \quad \text{ i } \quad \beta_B := \bigwedge_{\substack{i,j \in B \\ i < j}} \neg p_{i,j}.$$

Ako $p_{i,j}$ čitamo kao „ivica $i - j$ je crvena“, a $\neg p_{i,j}$ kao „ivica $i - j$ je plava“, onda ρ_A ima značenje „podgraf sa skupom temena A je crven“, a β_B ima značenje „podgraf sa skupom temena B je plav“. Neka je:

$$\Sigma := \{\neg \rho_A : A \subseteq \mathbb{N}, |A| = m\} \cup \{\neg \beta_B : B \subseteq \mathbb{N}, |B| = n\}.$$

Tvrdimo da Σ nije zadovoljiv. Pretpostavimo suprotno, $v \models \Sigma$. Obojimo K_ω na sledeći način:

$$\text{ivica } i - j \text{ je } \begin{cases} \text{crvena} & \text{ako } v(p_{i,j}) = T, \\ \text{plava} & \text{ako } v(p_{i,j}) = N. \end{cases}$$

Prema teoremi 2.82 postoji beskonačan skup $S \subseteq \mathbb{N}$ takav da su ivice grafa nad čvorovima iz skupa S ili crvene ili plave; bez umanjenja opštosti pretpostavimo da su crvene. Tada za bilo koji skup $A \subseteq S$, $|A| = m$, važi $v \models \rho_A$, što protivreči pretpostavci $v \models \Sigma$. Dakle, Σ nije zadovoljiv.

Po teoremi kompaktnosti, neki konačan podskup $\Sigma_0 \subseteq \Sigma$ nije zadovoljiv. Neka je N najveći broj koji se pojavljuje kao indeks nekog slova u skupu Σ_0 . Tada je $\Sigma_0 \subseteq \Sigma_1$, gde je Σ_1 skup:

$$\Sigma_1 := \{\neg \rho_A : A \subseteq \{0, 1, \dots, N\}, |A| = m\} \cup \{\neg \beta_B : B \subseteq \{0, 1, \dots, N\}, |B| = n\},$$

i očigledno Σ_1 nije zadovoljiv (jer sadrži nezadovoljiv podskup Σ_0).

Sada tvrdimo da za svako crveno/plavo bojenje ivica grafa K_{N+1} postoji crveno obojena kopija K_m ili plavo obojena kopija K_n . Obeležimo čvorove našeg grafa sa $0, 1, \dots, N$, i fiksirajmo neko bojenje. Definišimo valuaciju slova $p_{i,j}$, $0 \leq i < j \leq N$ sa:

$$v(p_{i,j}) := \begin{cases} T & \text{ako je ivica } i - j \text{ crvena,} \\ N & \text{ako je ivica } i - j \text{ plava.} \end{cases}$$

Kako $v \not\models \Sigma_1$ postoji $A \subseteq \{0, 1, \dots, N\}$ tako da $|A| = m$ i $v \not\models \neg \rho_A$, ili postoji $B \subseteq \{0, 1, \dots, N\}$ tako da $|B| = n$ i $v \not\models \neg \beta_B$. Ako postoji $A \subseteq \{0, 1, \dots, N\}$ tako da $|A| = m$ i $v \not\models \neg \rho_A$, tada $v \models \rho_A$ što znači da su sve ivice podgraфа na skupu A crvene, a ako postoji $B \subseteq \{0, 1, \dots, N\}$ tako da $|B| = n$ i $v \not\models \neg \beta_B$, tada $v \models \beta_B$ što znači da su sve ivice podgraфа na skupu B plave. Završili smo dokaz. $\square$

2.11 Teorema potpunosti

Cilj ovog odeljka je da dokažemo:

Teorema 2.83 (Teorema potpunosti). Neka je $\Sigma \subseteq \Phi$ i $\varphi \in \Phi$. Tada:

$$\Sigma \vdash \varphi \iff \Sigma \models \varphi.$$

Dokaz. Smer $(\Rightarrow)$ je teorema saglasnosti, pa dokazujemo $(\Leftarrow)$. Pretpostavimo $\Sigma \models \varphi$. To znači da $\Sigma \cup \{\neg \varphi\}$ nije zadovoljiv, pa po teoremi kompaktnosti nije ni konačno zadovoljiv, tj. postoje formule $\psi_1, \dots, \psi_n \in \Sigma$ takve da $\{\psi_1, \dots, \psi_n, \neg \varphi\}$ nije zadovoljiv. To znači da $\psi_1, \dots, \psi_n \models \varphi$, ili, ekvivalentno, važi $\models \psi_1 \wedge \dots \wedge \psi_n \rightarrow \varphi$. Po slaboj teoremi potpunosti imamo $\vdash \psi_1 \wedge \dots \wedge \psi_n \rightarrow \varphi$, odakle po teoremi dedukcije sledi $\psi_1 \wedge \dots \wedge \psi_n \vdash \varphi$. Imajući u vidu pravilo uvođenja konjunkcije zaključujemo da $\psi_1, \dots, \psi_n \vdash \varphi$. Kako $\psi_1, \dots, \psi_n \in \Sigma$, konačno zaključujemo $\Sigma \vdash \varphi$. Završili smo dokaz. $\square$

3 Skupovi

Pojam *skupa* je osnovni pojam u matematici. U uobičajenom formalnom zasnivanju matematike skup je prvi pojam, pojam koji nema definiciju, čije se osobine aksiomatski opisuju. Aksiomatsko zasnivanje skupova izlazi van okvira kursa za prvu godinu studija, tako da ćemo se zadržati na nečemu što je intuitivno objašnjenje skupa, uvodeći osnovne operacije za manipulaciju sa skupovima.

Definicija 3.1 (Intuitivna definicija skupa). *Skup* je celina koja okuplja određeni broj objekata koje nazivamo elementima tog skupa.

Činjenicu da je objekat x element skupa A zapisujemo sa $x \in A$ (čitamo „ x je element od A “ ili „ x pripada A “); u suprotnom, ako $\neg x \in A$, pišemo $x \notin A$ („ x nije element od A “ ili „ x ne pripada A “).

Ako je skup konačan, npr. skup koji sadrži brojeve 1, 2, 5 i 8, zapisujemo koristeći vitičaste zagrade između kojih navedemo njegove elemente: $\{1, 2, 5, 8\}$. Tada $2 \in \{1, 2, 5, 8\}$ znači da 2 jeste element skupa $\{1, 2, 5, 8\}$, dok $3 \notin \{1, 2, 5, 8\}$ znači da 3 nije element ovog skupa. Ako je skup konačan, ali ima previše elemenata da bi bilo racionalno sve ih navesti, možemo da ih nabrojimo koristeći ... ako je to moguće, tj. ako je jasan šablon po kome smo elemente nabrojali. Npr. $\{2, 3, 4, \dots, 17\}$ je skup prirodnih brojeva između 2 i 17 (uključujući ova dva broja), $\{1, 3, 5, \dots, 997, 999\}$ je skup svih neparnih brojeva prve hiljade. Takođe, ... možemo da koristimo i za zapis beskonačnih skupova koje je moguće nabrojati po nekom šablonu. Npr. $\{0, 2, 4, \dots\}$ je skup svih parnih prirodnih brojeva, $\{0, 1, 4, 9, 16, \dots\}$ je skup svih kvadrata prirodnih brojeva, $\{\dots, -3, -1, 1, 3, 5, \dots\}$ je skup svih neparnih celih brojeva, i sl.

Jedan od najčešćih načina za zapis skupa je zapis koji koristi tzv. *operator okupljanja*. To znači sledeće. Ako je $p(x)$ predikat gde x ima svoj univerzum diskursa, sa:

$$\{x: p(x)\} \quad \text{ili} \quad \{x \in \mathcal{U}_x: p(x)\}$$

obeležavamo skup svih elemenata univerzuma diskursa za koje važi predikat p . Npr. skup $\{n \in \mathbb{N}: 2 \mid n\}$ je skup svih prirodnih brojeva deljivih sa dva, tj. skup svih parnih prirodnih brojeva. Iako u praksi ovu vrstu zapisa koristimo vrlo slobodno bez bilo kakvih problema, formalno bi trebalo biti oprezan. Ako je naš predikat $X \notin X$, gde je univerzum diskursa promenljive X univerzum svih skupova, možemo da uočimo skup:

$$S = \{X: X \notin X\}.$$

Da li $S \in S$? Ako $S \in S$, onda S zadovoljava predikat koji ga opisuje, tj. $S \notin S$. Ako $S \notin S$, onda S zadovoljava predikat $X \notin X$, pa po definiciju skupa S imamo $S \in S$. Dakle, $S \in S$ ako i samo ako $S \notin S$. Ovo je kontradikcija. Ovaj primer zove se *Raselov paradoks*, koji je poslužio kao polazna motivacija za strogo zasnivanje koncepta skupa. Razrešenje Raselovog paradoksa je sledeće. Ne možemo da dozvolimo da je kolekcija S zapisana gore skup. Strogo zasnivanje dozvoljava formiranje skupa $\{x: p(x)\}$, pod uslovom da je poznato da univerzum diskursa promenljive x jeste skup. S tim u vezi, univerzum svih skupova ne može da postoji (tj. ne može da bude skup), kako bismo izbegli Raselov paradoks.

Još jedan od čistih načina zapisa skupa je i sledeći. Ako za elemente x skupa S imamo neki način f da izračunamo neku vrednost $f(x)$, sa $\{f(x): x \in S\}$ obeležavamo skup svih elemenata $f(x)$ kad x prođe skup S . Npr. $\{2n: n \in \mathbb{N}\}$ je još jedan način da zapišemo skup parnih brojeva.

Definicija 3.2. Skupovi A i B su jednaki, $A = B$, ako imaju iste elemente, tj. važi iskaz:

$$(\forall x)(x \in A \leftrightarrow x \in B).$$

Jednakost skupova ima očekivana svojstva:

- $(\forall A) A = A$;
- $(\forall A, B)(A = B \rightarrow B = A)$;

- $(\forall A, B, C)(A = B \wedge B = C \rightarrow A = C)$.

Definicija 3.3. *Prazan skup*, u oznaci $\emptyset$, je skup koji nema elemente, tj. $(\forall x) x \notin \emptyset$.

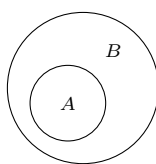
Po definiciji jednakosti dva skupa bez elemenata moraju biti jednaka, tako da je u redu da mu damo ime *prazan skup* i oznaku $\emptyset$.

3.1 Podskup

Definicija 3.4. Neka su A i B skupovi. Kažemo da je A *podskup od* B ili B *je nadskup od* A , u oznaci $A \subseteq B$, ako su svi elementi skupa A ujedno i elementi skupa B , tj. važi iskaz:

$$(\forall x)(x \in A \rightarrow x \in B).$$

Skupovi su često zgodni za skiciranje, što u velikoj meri pomaže u razumevanju problema. Pa tako činjenicu da je $A \subseteq B$ možemo da skiciramo sa:



Skupove A i B skicirali smo kao krugove, zamišljamo da su elementi skupa A unutar kruga A , elementi skupa B unutar kruga B , pa činjenicu da je $A \subseteq B$ skiciramo tako što je krug A ceo unutar kruga B .

Po definiciji je jasno kako obično dokazujemo da je $A \subseteq B$. Najčešće uočimo proizvoljan element x , pretpostavimo $x \in A$ i ciljamo da dokažemo $x \in B$ (kombinacija postupka generalizacije i dedukcije). Možemo da dokažemo $A \subseteq B$ i kombinacijom postupka generalizacije i dedukcije kontrapozicije: uočimo proizvoljan element x , pretpostavimo $x \notin B$ i ciljamo da dokažemo $x \notin A$. Konačno, možemo da koristimo i kombinaciju postupka generalizacije i svođenja na protivrečnost: uočimo proizvoljan element x , pretpostavimo $x \in A$ i $x \notin B$, i ciljamo da nađemo kontradikciju.

Direktno po definiciji vidimo nekoliko osobina relacije podskupa:

- $(\forall A) \emptyset \subseteq A$;
- $(\forall A) A \subseteq A$;
- $(\forall A, B)(A \subseteq B \wedge B \subseteq A \leftrightarrow A = B)$;
- $(\forall A, B, C)(A \subseteq B \wedge B \subseteq C \rightarrow A \subseteq C)$.

Treća osobina nam najčešće služi za dokaz jednakosti dva skupa. Naima, ako želimo da dokažemo $A = B$, najčešće ćemo dokazati $A \subseteq B$ i $B \subseteq A$.

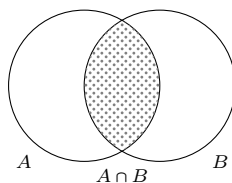
3.2 Osnovne skupovne operacije

Definicija 3.5. *Presek* skupova A i B je skup zajedničkih elemenata skupova A i B :

$$A \cap B = \{x: x \in A \wedge x \in B\},$$

tj. $x \in A \cap B$ akko $x \in A$ i $x \in B$.

Presek skupova A i B skiciramo sa (šrafiran deo):



Prethodna sličica, dva kruga koja se seku, zove se *Venov dijagram* za sva skupa. Na Venovom dijagramu možemo verno da predstavimo odnos dva skupa.

Po definiciji preseka lako vidimo nekoliko osnovnih osobina preseka:

- $(\forall A, B) A \cap B = B \cap A$;
- $(\forall A, B, C) A \cap (B \cap C) = (A \cap B) \cap C$;
- $(\forall A, B) (A \cap B = A \leftrightarrow A \subseteq B)$;
- specijalno, $(\forall A) \emptyset \cap A = \emptyset$ i $(\forall A) A \cap A = A$.

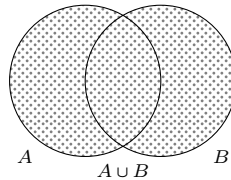
Zbog druge osobine, asocijativnosti preseka, zapis $A \cap B \cap C$, ili presek više od tri skupova, ima smisla i predstavlja skup zajedničkih elemenata svih skupova koji učestvuju u preseku.

Definicija 3.6. *Unija* skupova A i B je skup svih elemenata skupova A i B :

$$A \cup B = \{x: x \in A \vee x \in B\},$$

tj. $x \in A \cup B$ akko $x \in A$ ili $x \in B$.

Na Venovom dijagramu uniju skupova A i B skiciramo sa:



Po definiciji direktno imamo sledeće osnovne osobine unije:

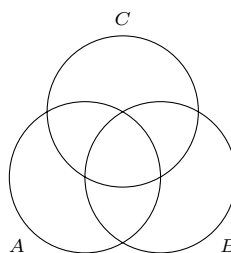
- $(\forall A, B) A \cup B = B \cup A$;
- $(\forall A, B, C) A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$;
- $(\forall A, B) (A \cup B = B \leftrightarrow A \subseteq B)$;
- specijalno, $(\forall A) \emptyset \cup A = A$ i $(\forall A) A \cup A = A$.

Zbog druge osobine, asocijativnosti unije, zapis $A \cup B \cup C$, ili unija više od tri skupova, ima smisla i predstavlja skup svih elemenata skupova koji učestvuju u uniji.

Zadatak 3.7. Dokazati sledeće osobine:

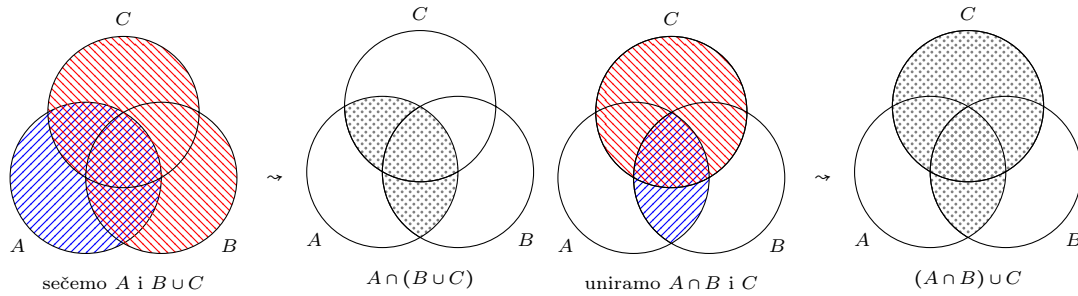
- $(\forall A, B) A \cap (A \cup B) = A$;
- $(\forall A, B) A \cup (A \cap B) = A$;
- $(\forall A, B, C) A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$;
- $(\forall A, B, C) A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Jednakosti u kojima učestvuju tri skupa možemo da vidimo i na Venovom dijagramu za tri skupa, koga skiciramo na sledeći način:



Svaki element možemo predstaviti na prethodnom dijagramu u jednoj od osam oblasti u zavisnosti da li pripada ili ne datim skupovima.

Primer 3.8. Za proizvoljne skupove A, B, C ispitaćemo u kom su odnosu skupovi $A \cap (B \cup C)$ i $(A \cap B) \cup C$. Najpre ćemo da skiciramo ove skupove na Venovom dijagramu:



Venov dijagram nam sugerše sledeću hipotezu:

$$(\forall A, B, C) A \cap (B \cup C) \subseteq (A \cap B) \cup C.$$

(Tj. levi skup je deo desnog skupa.) Dokažimo prethodnu inkluziju i formalno.

Neka su A, B, C proizvoljni skupovi, neka je x proizvoljan element i neka $x \in A \cap (B \cup C)$; cilj je da dokažemo $x \in (A \cap B) \cup C$. Iz $x \in A \cap (B \cup C)$, $x \in A$ i $x \in B \cup C$. Iz $x \in B \cup C$ imamo dva slučaja: $x \in B$ ili $x \in C$.

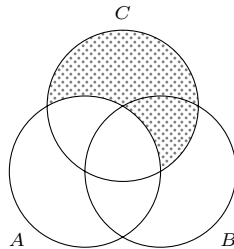
1° Ako $x \in B$, tada $x \in A \cap B$, pa $x \in (A \cap B) \cup C$.

2° Ako $x \in C$, tada $x \in (A \cap B) \cup C$.

U svakom slučaju $x \in (A \cap B) \cup C$, i završili smo dokaz.

Odrdedimo sada i neki jednostavan potreban i dovoljan uslov da važi jednakost $A \cap (B \cup C) = (A \cap B) \cup C$.

Ako se vratimo na sliku, jednakost će važiti ako je sledeći skup prazan:



To znači da su jedini elementi skupa C oni koji već pripadaju skupu A , tj. $C \subseteq A$. Dakle, možemo da postavimo sledeću hipotezu:

$$(\forall A, B, C)(A \cap (B \cup C) = (A \cap B) \cup C \leftrightarrow C \subseteq A).$$

Dajemo formalni dokaz. Neka su A, B, C proizvoljni skupovi.

($\Rightarrow$) Pretpostavimo $A \cap (B \cup C) = (A \cap B) \cup C$ i dokažimo $C \subseteq A$. Neka je $x \in C$ proizvoljan element, cilj je da dokažemo $x \in A$. Iz $x \in C$ sledi $x \in (A \cap B) \cup C$. Kako je $A \cap (B \cup C) = (A \cap B) \cup C$, imamo $x \in A \cap (B \cup C)$, pa specijalno $x \in A$. Time smo završili dokaz smeru ($\Rightarrow$).

($\Leftarrow$) Pretpostavimo da je $C \subseteq A$ i dokažimo $A \cap (B \cup C) = (A \cap B) \cup C$. Inkluzija ($\subseteq$) već smo dokazali u opštem slučaju, pa dokazujemo ($\supseteq$). Neka je $x \in (A \cap B) \cup C$ i cilj je da dokažemo $x \in A \cap (B \cup C)$. Iz $x \in (A \cap B) \cup C$ imamo dva slučaja $x \in A \cap B$ ili $x \in C$.

1° Ako $x \in A \cap B$, $x \in A$ i $x \in B$. Iz poslednjeg je $x \in B \cup C$, pa imamo $x \in A \cap (B \cup C)$.

2° Ako $x \in C$, onda $x \in B \cup C$, ali i $x \in A$ jer $C \subseteq A$. Dakle, opet je $x \in A \cap (B \cup C)$.

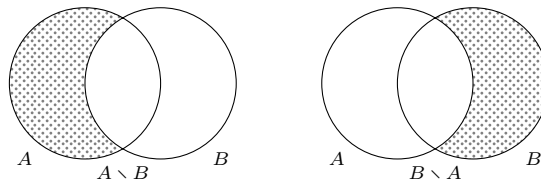
U svakom slučaju je $x \in A \cap (B \cup C)$, i završili smo dokaz.

Definicija 3.9. Razlika skupova A i B (tim redom) je skup elemenata iz A koji nisu u B :

$$A \setminus B = \{x: x \in A \wedge x \notin B\},$$

tj. $x \in A \setminus B$ akko $x \in A$ i $x \notin B$.

Na Venovom dijagramu razlike $A \setminus B$ i $B \setminus A$ skiciramo sa:



Prethodna skica već sugerise da komutativan zakon $A \setminus B = B \setminus A$ ne važi u opštem slučaju (zapravo nije teško videti da $A \setminus B = B \setminus A$ važi akko $A = B$).

Od osnovnih osobina izdvajamo:

- $(\forall A, B)(A \setminus B = \emptyset \leftrightarrow A \subseteq B)$;
- $(\forall A, B) A \setminus B = A \setminus (A \cap B) = (A \cup B) \setminus B$;
- $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$;
- $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$;
- $(A \cap B) \setminus C = (A \setminus C) \cap (B \setminus C)$;
- $(A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C)$.

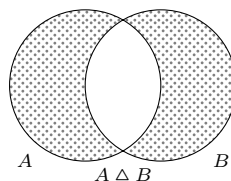
Zadatak 3.10. Ispitati u kom su odnosu skupovi $A \setminus (B \setminus C)$ i $(A \setminus B) \setminus C$ u opštem slučaju. Odrediti neki jednaostavan potreban i dovoljan uslov da važi jednakost.

Definicija 3.11. *Simetrična razlika* skupova A i B je skup onih elemenata koji su u tačnom jednom od ovih skupova:

$$A \triangle B = \{x: x \in A \vee x \in B\},$$

tj. $x \in A \triangle B$ akko ili $x \in A$ ili $x \in B$.

Venov dijagram simetrične razlike je:



Od osnovnih osobina izdvajamo:

- $(\forall A, B) A \triangle B = B \triangle A$;
- $(\forall A, B, C) A \triangle (B \triangle C) = (A \triangle B) \triangle C$;
- $(\forall A, B) A \triangle B = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$.

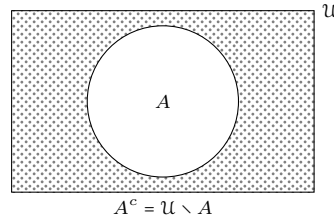
Prema drugoj osobini, asocijativnosti simetrične razlike, zapis $A \triangle B \triangle C$, kao i simetrična razlika više od tri skupova, ima smisla. Element pripada simetričnoj razlici nekog broja skupova akko je element neparno mnogo od njih.

Definicija 3.12. *Komplement* skupa A je skup svih elemenata koji nisu u A (ali jesu u unapred poznatom podrazumevanom univerzumu):

$$A^c = \{x: x \notin A\},$$

tj. $x \in A^c$ akko $x \notin A$, za bilo koji element x iz univerzuma. Dakle, A^c računamo relativno u odnosu na podrazumevani univerzum, i tada možemo da zapišemo $A^c = \mathcal{U} \setminus A$. U formalnom zasnivanju skupova, apsolutni komplement ne može da postoji.

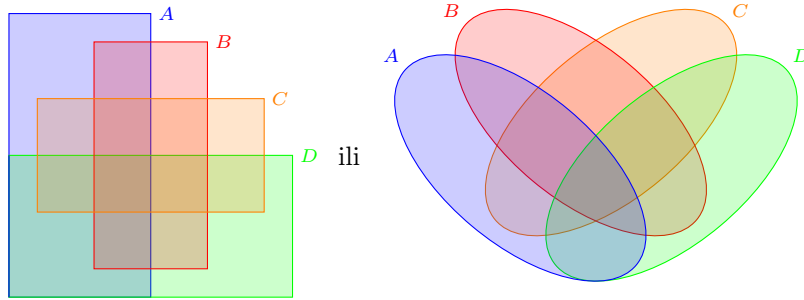
Simetričnu razliku skiciramo sa:



Od osobina izdvajamo:

- $(\forall A) (A^c)^c = A$;
- $(\forall A, B) A \setminus B = A \cap B^c$;
- $(\forall A, B) (A \cap B)^c = A^c \cup B^c$;
- $(\forall A, B) (A \cup B)^c = A^c \cap B^c$;
- $(\forall A, B) (A \triangle B)^c = A^c \triangle B^c$.

Skupovne izraze u kojima učestvuje više od tri skupa nije jednostavno skicirati. Venov dijagram za četiri skupa možemo nacrtati na sledeći način:



Postoje i Venovi dijagrami za pet i više skupova, ali su značajno komplikovaniji.

3.3 Veza za iskaznom logikom

Fiksirajmo simbole za skupove $A_1, A_2, \dots, A_k$. Skupovni izraz nad ovim simbolima rekurentno gradimo u konačno mnogo koraka na sledeći način:

- svaki simbol A_i je skupovni izraz;
- ako su σ_1 i σ_2 već izgrađeni skupovni izrazi, onda su i $\sigma_1 \cap \sigma_2$, $\sigma_1 \cup \sigma_2$, $\sigma_1 \setminus \sigma_2$, $\sigma_1 \triangle \sigma_2$ i σ_1^c skupovni izrazi.

Složenost skupovnog izraza σ , $sl(\sigma)$, je broj skupovnih operacija u izrazu σ , npr. $sl(A_1) = 0$, $sl(A_1 \setminus A_2) = 1$, $sl((A_1 \setminus A_2^c) \triangle A_1) = 3$, itd.

Svakom skupovnom izrazu σ nad simbolima $A_1, A_2, \dots, A_k$ pridružujemo iskaznu formulu $\hat{\sigma}$ nad slovima $p_1, p_2, \dots, p_k$ (iskazno slovo p_i odgovara skupovnom simbolu A_i) rekurentno na sledeći način:

- ako je $\sigma = A_i$, onda je $\hat{\sigma} = p_i$;
- ako je $\sigma = \sigma_1 \cap \sigma_2$, onda je $\hat{\sigma} = \hat{\sigma}_1 \wedge \hat{\sigma}_2$;
- ako je $\sigma = \sigma_1 \cup \sigma_2$, onda je $\hat{\sigma} = \hat{\sigma}_1 \vee \hat{\sigma}_2$;
- ako je $\sigma = \sigma_1 \setminus \sigma_2$, onda je $\hat{\sigma} = \hat{\sigma}_1 \wedge \neg \hat{\sigma}_2$;
- ako je $\sigma = \sigma_1 \triangle \sigma_2$, onda je $\hat{\sigma} = \hat{\sigma}_1 \underline{\vee} \hat{\sigma}_2$;

- ako je $\sigma = \sigma_1^c$, onda je $\hat{\sigma} = \neg \hat{\sigma}_1$

Npr. izrazu $(A_1 \setminus A_2^c) \triangle A_1$ pridružimo $(p_1 \wedge \neg \neg p_2) \vee p_1$, izrazu $(A_2 \cap A_3)^c \cup A_5$ pridružimo $\neg(p_2 \wedge p_3) \vee p_5$, itd.

Fiksirajmo sada konkretne skupove $A_1, A_2, \dots, A_k$. Elementom x određena je sledeća valuacija v_x :

$$v_x(p_i) = \begin{cases} T & \text{ako } x \in A_i \\ N & \text{ako } x \notin A_i \end{cases}.$$

Primetimo da valuacija v_x ne zavisi samo od x , već i od izbora $A_1, A_2, \dots, A_k$, ali kako smo njih fiksirali, nećemo ih naglašavati u zapisu. Uvek će biti jasno u odnosu na koje skupove smo definisali v_x .

Lema 3.13. Neka su $A_1, A_2, \dots, A_k$ proizvoljni skupovi, x proizvoljan element i σ proizvoljan izraz nad $A_1, A_2, \dots, A_k$. Tada:

$$x \in \sigma \iff \hat{v}_x(\hat{\sigma}) = T.$$

Dokaz. Fiksirajmo $A_1, A_2, \dots, A_k$ i x . Potpunom indukcijom po složenosti izraza σ izvodimo dokaz. Razmatramo sledeće slučajeve:

1° $\sigma = A_i$: Tada je $\hat{\sigma} = p_i$, pa je:

$$x \in \sigma \iff x \in A_i \iff v_x(p_i) = T \iff \hat{v}_x(\hat{\sigma}) = T,$$

i tvrđenje važi u ovom slučaju.

2° $\sigma = \sigma_1 \cap \sigma_2$: Tada je $\hat{\sigma} = \hat{\sigma}_1 \wedge \hat{\sigma}_2$. Po indukcijskoj hipotezi imamo $x \in \sigma_1 \iff \hat{v}_x(\hat{\sigma}_1) = T$ i $x \in \sigma_2 \iff \hat{v}_x(\hat{\sigma}_2) = T$, pa:

$$x \in \sigma \iff x \in \sigma_1 \text{ i } x \in \sigma_2 \iff \hat{v}_x(\hat{\sigma}_1) = T \text{ i } \hat{v}_x(\hat{\sigma}_2) = T \iff \hat{v}_x(\underbrace{\hat{\sigma}_1 \wedge \hat{\sigma}_2}_{=\hat{\sigma}}) = T,$$

i tvrđenje važi i u ovom slučaju.

Na sličan način dokazujemo da tvrđenje važi i u slučajevima 3° $\sigma = \sigma_1 \cup \sigma_2$, 4° $\sigma = \sigma_1 \setminus \sigma_2$, 5° $\sigma = \sigma_1 \triangle \sigma_2$ i 6° $\sigma = \sigma_1^c$, čime završavamo dokaz. $\square$

Zadatak 3.14. Završiti dokaz prethodne leme.

Teorema 3.15. Neka su σ_1 i σ_2 dva skupovna izraza nad $A_1, A_2, \dots, A_k$. Tada:

- (i) $(\forall A_1, A_2, \dots, A_k) \sigma_1 \subseteq \sigma_2$ akko $\models \hat{\sigma}_1 \rightarrow \hat{\sigma}_2$;
- (ii) $(\forall A_1, A_2, \dots, A_k) \sigma_1 = \sigma_2$ akko $\models \hat{\sigma}_1 \leftrightarrow \hat{\sigma}_2$.

Dokaz. (i) $(\Rightarrow)$ Pretpostavimo $(\forall A_1, \dots, A_k) \sigma_1 \subseteq \sigma_2$ i dokažimo $\models \hat{\sigma}_1 \rightarrow \hat{\sigma}_2$. Pretpostavimo suprotno, postoji valuacija v takva da $\hat{v}(\hat{\sigma}_1 \rightarrow \hat{\sigma}_2) = N$, tj. $\hat{v}(\hat{\sigma}_1) = T$ i $\hat{v}(\hat{\sigma}_2) = N$. Izaberimo proizvoljan element x i pridružimo valuaciji v sledeće skupove $A_1, \dots, A_k$:

$$A_i = \begin{cases} \{x\} & \text{ako } v(p_i) = T \\ \emptyset & \text{ako } v(p_i) = N \end{cases}.$$

Elementu x i skupovima $A_1, \dots, A_k$ sada možemo da pridružimo valuaciju v_x kako smo opisali ranije. Primetimo $v_x = v$. (Zaista, ako je $v(p_i) = T$, $A_i = \{x\}$, pa $x \in A_i$, pa je $v_x(p_i) = T$; ako je $v(p_i) = N$, $A_i = \emptyset$, pa $x \notin A_i$, pa je $v_x(p_i) = N$. Dakle, $v(p_i) = v_x(p_i)$.)

Dakle, $\hat{v}_x(\hat{\sigma}_1) = T$ i $\hat{v}_x(\hat{\sigma}_2) = N$, pa po lemi 3.13, $x \in \sigma_1$ i $x \notin \sigma_2$. To znači da $\sigma_1 \not\subseteq \sigma_2$, što nije moguće jer $\sigma_1 \subseteq \sigma_2$ po pretpostavci važi za proizvoljne skupove $A_1, \dots, A_k$. Ova kontradikcija završava dokaz prvog smera.

$(\Leftarrow)$ Pretpostavimo $\models \hat{\sigma}_1 \rightarrow \hat{\sigma}_2$ i dokažimo $(\forall A_1, \dots, A_k) \sigma_1 \subseteq \sigma_2$. Neka su $A_1, \dots, A_k$ proizvoljni skupovi, i neka je $x \in \sigma_1$ proizvoljno. Tada je $\hat{v}_x(\hat{\sigma}_1) = T$ po lemi 3.13, pa kako je $\models \hat{\sigma}_1 \rightarrow \hat{\sigma}_2$ to je i $\hat{v}_x(\hat{\sigma}_2) = T$, odakle je $x \in \sigma_2$, opet po lemi 3.13. Prema tome, $\sigma_1 \subseteq \sigma_2$.

(ii) sledi direktno prema (i) imajući u vidu da je $\sigma_1 = \sigma_2$ akko $\sigma_1 \subseteq \sigma_2$ i $\sigma_2 \subseteq \sigma_1$, i $\models \hat{\sigma}_1 \leftrightarrow \hat{\sigma}_2$ akko $\models \hat{\sigma}_1 \rightarrow \hat{\sigma}_2$ i $\models \hat{\sigma}_2 \rightarrow \hat{\sigma}_1$. $\square$

Primer 3.16. Da bismo dokazali da je $(A \setminus B) \setminus C \subseteq A \setminus (B \setminus C)$ za proizvoljne skupove A, B, C , prema teoremi 3.15 dovoljno je da dokažemo:

$$\models (p \wedge \neg q) \wedge \neg r \rightarrow p \wedge \neg(q \wedge \neg r),$$

gde skupovima A, B, C redom dodelimo slova p, q, r . Prethodno možemo da poverimo tablicom:

p	q	r	$(p \wedge \neg q) \wedge \neg r \rightarrow p \wedge \neg(q \wedge \neg r)$
T	T	T	N
T	T	N	N
T	N	T	T
T	N	N	T
N	T	T	N
N	T	N	N
N	N	T	N
N	N	N	N

Razmotrimo obratnu inkluziju $A \setminus (B \setminus C) \subseteq (A \setminus B) \setminus C$. Formula koja joj odgovara je:

$$p \wedge \neg(q \wedge \neg r) \rightarrow (p \wedge \neg q) \wedge \neg r.$$

Tablica ove formule je:

p	q	r	$p \wedge \neg(q \wedge \neg r) \rightarrow (p \wedge \neg q) \wedge \neg r$
T	T	T	N
T	T	N	N
T	N	T	T
T	N	N	T
N	T	T	N
N	T	N	N
N	N	T	N
N	N	N	N

Jasno je da prethodna formula nije tautologija, pa prema teoremi 3.15 gornja inkluzija ne važi za proizvoljne A, B, C . Međutim, tablica može da nam pomogne da odredimo neki jednostavan potreban i dovoljan uslov da inkluzija važi. Naime, pridružena formula je netačna u valuacijama (T, T, T) i (T, N, T) , pa prema lemi 3.13 ne smemo da imamo element x za koji je v_x jedna od ove dve valuacije. Dakle, ne smemo da imamo element koji je i u A i u B i u C , kao ni element koji je u A i C , ali nije u B . Dakle, ne smemo da imamo element koji je u A i C , tj. mora biti $A \cap C = \emptyset$. I zaista, sad možemo da dokažemo sledeće:

$$A \setminus (B \setminus C) \subseteq (A \setminus B) \setminus C \iff A \cap C = \emptyset.$$

Dokaz ostavljamo za vežbu.

Primer 3.17. Koristeći teoremu 3.15 možemo da dokažemo i identitet $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$ koji ćemo kooristiti u sledećem odeljku. Dovoljno je da proverimo:

$$\models p \wedge (q \triangle r) \leftrightarrow ((p \wedge q) \triangle (p \wedge r)).$$

I ovo vidimo iz tablice:

p	q	r	$p \wedge (q \vee r)$	$\leftrightarrow$	$((p \wedge q) \vee (p \wedge r))$
T	T	T	T	T	T
T	T	N	T	T	N
T	N	T	T	T	T
T	N	N	N	T	N
N	T	T	N	T	N
N	T	N	N	T	N
N	N	T	N	T	N
N	N	N	N	T	N

3.4 Algebarska normalna forma

Sada ćemo prikazati jedan aritmetički način za zapis i račun sa skupovnim izrazima. Najpre definišimo zbir i proizvod dva skupa:

$$\begin{aligned} A + B &:= A \triangle B \\ A \cdot B &:= A \cap B \end{aligned}$$

Takođe, definišimo $0 := \emptyset$ i $1 := \mathcal{U}$, gde $\mathcal{U}$ univerzum iz koga izdvajamo sve skupove o kojima govorimo.

Kao i obično, umesto $A \cdot B$ pišemo samo AB . Koristeći $+$ i $\cdot$ možemo da predstavimo i ostale skupovne operacije:

$$\begin{aligned} A^c &= 1 + A & \text{jer} & \quad A^c = \mathcal{U} \triangle A \\ A \setminus B &= A + AB & \text{jer} & \quad A \setminus B = A \triangle (A \cap B) \\ A \cup B &= A + B + AB & \text{jer} & \quad A \cup B = A \triangle B \triangle (A \cap B) \end{aligned}$$

Već znamo da su $+$ i $\cdot$ (tj. $\triangle$ i $\cap$) komutativne i asocijativne operacije (zbog asocijativnosti $+$ ne navodimo zagrade u gornjem zapisu), i takođe izbegavamo da pišemo zagrade podrazumevajući, kao što je i uobičajeno, da je $\cdot$ prioritetnija operacija u odnosu na $+$.

Ovako definisano množenje i sabiranje imaju sva očekivana svojstva. Pored već navedene komutativnosti i asocijativnosti naglasimo i:

$$\begin{aligned} A + 0 &= A & \text{jer} & \quad A \triangle \emptyset = A \\ A \cdot 0 &= 0 & \text{jer} & \quad A \cap \emptyset = \emptyset \\ A \cdot 1 &= A & \text{jer} & \quad A \cap \mathcal{U} = A \\ A(B + C) &= AB + AC & \text{jer} & \quad A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C) \end{aligned}$$

Što se tiče treće osobine, setimo se da je $\mathcal{U}$ univerzum, pa je $A \subseteq \mathcal{U}$, a što se tiče četvrte osobine, odgovarajući identitet dokazali smo na kraju prethodnog odeljka.

Pored navedenih svojstava, definisano sabiranje i množenje imaju i dodatne osobine:

$$\begin{aligned} 2A &= A + A = 0 & \text{jer} & \quad A \triangle A = \emptyset \\ A^2 &= A \cdot A = A & \text{jer} & \quad A \cap A = A \end{aligned}$$

Zadatak 3.18. Proveriti sve navedene osobine korišćene u prethodnim pasusima.

Definicija 3.19. *Skupovni monom* nad skupovima $A_1, A_2, \dots, A_k$ je ili 1 ili proizvod nekoliko od ovih skupova, npr. $A_4, A_1A_2, A_2A_3A_k$, itd. Skupovni izraz σ nad $A_1, A_2, \dots, A_k$ je u *algebarskoj normalnoj formi* ili *ANF* ako je zbir različitih skupovnih monoma, npr. $1 + A_1A_2, A_4 + A_2A_3A_k$, itd. Za skupovni izraz u ANF još kažemo da je u obliku *Žegalkinog polinoma*.

Svaki skupovni izraz može se svesti na ANF koristeći jednakosti navedene gore. Do na raspored sabiraka ANF je jedinstvena, pa možemo da dokažemo identitet $\sigma_1 = \sigma_2$ ako dokažemo da su ANF izraza σ_1 i σ_2 jednake. Takođe, možemo da dokažemo $\sigma_1 \subseteq \sigma_2$ ako dokažemo ekvivalentnu jednakost $\sigma_1\sigma_2 = \sigma_1$.

Primer 3.20. Zapišimo ANF izraza $\sigma_1 = (A \setminus B) \setminus C$:

$$\sigma_1 = (A + AB) \setminus C = A + AB + (A + AB)C = A + AB + AC + ABC.$$

Zapišimo i ANF izraza $\sigma_2 = A \setminus (B \setminus C)$:

$$\sigma_2 = A + A(B \setminus C) = A + A(B + BC) = A + AB + ABC.$$

Primetimo da dobijene ANF nisu jednake, pa $\sigma_1 = \sigma_2$ ne važi u opštem slučaju. Takođe primetimo da jednakost važi akko $AC = 0$ (višak monom u σ_1), tj. akko $A \cap C = \emptyset$.

Pomnožimo σ_1 i σ_2 :

$$\begin{aligned} \sigma_1 \sigma_2 &= (A + AB + AC + ABC)(A + AB + ABC) = \\ &= A^2 + A^2 B + A^2 BC + A^2 B + A^2 B^2 + A^2 B^2 C + \\ &\quad + A^2 C + A^2 BC + A^2 BC^2 + A^2 BC + A^2 B^2 C + A^2 B^2 C^2 = \\ &= A + AB + ABC + AB + AB + ABC + \\ &\quad + AC + ABC + ABC + ABC + ABC + ABC = \\ &= A + 3AB + AC + 7ABC = A + AB + AC + ABC = \sigma_1, \end{aligned}$$

gde smo iskoristili $A^2 = A$, $B^2 = B$, $C^2 = C$, $2AB = 0$ i $2ABC = 0$. Kako je $\sigma_1 \sigma_2 = \sigma_1$, to znači da uvek važi $\sigma_1 \subseteq \sigma_2$.

Primer 3.21. Dokažimo identitet $(A^c \cup (A^c \setminus B))^c = A$ koristeći ANF. Računamo:

$$\begin{aligned} (A^c \cup (A^c \setminus B))^c &= 1 + ((1+A) \cup ((1+A) \setminus B)) = 1 + ((1+A) \cup (1+A + (1+A)B)) = \\ &= 1 + ((1+A) \cup (1+A+B+AB)) = 1 + 1 + A + 1 + A + B + AB + (1+A)(1+A+B+AB) = \\ &= 3 + 2A + B + AB + 1 + A + B + AB + A + A + AB + AB = 4 + 5A + 2B + 4AB = A, \end{aligned}$$

gde smo implicitno koristili $A^2 = A$, i gde $4 = 0$, $4A = 0$, $2B = 0$ i $4AB = 0$.

3.5 Partitivni skup

Definicija 3.22. *Partitivni skup* skupa A , $\mathcal{P}(A)$, je skup svih podskupova od A :

$$\mathcal{P}(A) = \{X : X \subseteq A\},$$

tj. $X \in \mathcal{P}(A)$ akko $X \subseteq A$.

Npr. podskupovi skupa $\{1, 2, 3\}$ su: prazan skup, tri jednočlana podskupa $\{1\}$, $\{2\}$ i $\{3\}$, tri dvočlana podskupa $\{1, 2\}$, $\{1, 3\}$ i $\{2, 3\}$, i jedan tročlan podskup – ceo skup $\{1, 2, 3\}$. Dakle:

$$\mathcal{P}(\{1, 2, 3\}) = \{ \emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\} \}.$$

Jedini podskup praznog skupa je prazan skup: $\mathcal{P}(\emptyset) = \{\emptyset\}$. Primetite da poslednji skup nije prazan, on ima jedan element – prazan skup. Skup $\{\emptyset\}$ je jednočlan, pa ima dva podskupa: $\emptyset$ i $\{\emptyset\}$, tj. $\mathcal{P}(\{\emptyset\}) = \{ \emptyset, \{\emptyset\} \}$. Takođe, dvočlani skup $\{\emptyset, \{\emptyset\}\}$ ima podskupove: prazan skup, dva jednočlana podskupa $\{\emptyset\}$ i $\{\{\emptyset\}\}$ i jedan dvočlan podskup – ceo skup $\{\emptyset, \{\emptyset\}\}$:

$$\mathcal{P}(\{\emptyset, \{\emptyset\}\}) = \{ \emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\} \}.$$

Zadatak 3.23. Dokazati da je $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$.

Zadatak 3.24. Dokazati da je $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$, kao i da jednakost važi akko $A \subseteq B$ ili $B \subseteq A$.

Zadatak 3.25. Ako je A konačan skup sa n elemenata, dokazati da $\mathcal{P}(A)$ ima 2^n elemenata.

3.6 Dekartov proizvod

Definicija 3.26. Uređeni par elemenata a i b je matematički objekat, obično obeležen sa (a, b) , koji zadovoljava sledeću osobinu:

$$(a, b) = (a', b') \iff a = a' \wedge b = b'.$$

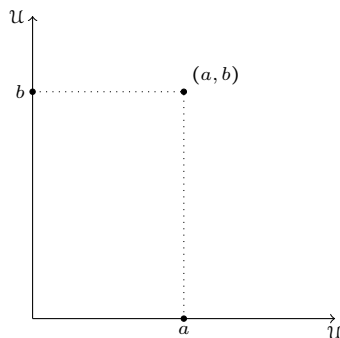
Formalno, uređeni par može da se definiše kao $(a, b) = \{\{a\}, \{a, b\}\}$, i nije teško proveriti da ovako definisani objekat zadovoljava prethodnu osobinu, ali zaista formalna definicija uređenog para nam nije od značaja, jedino bitno je navedena osobina.

Element a u paru (a, b) je *prva koordinata* ili *prva komponenta* para, a element b je *druga koordinata* ili *druga komponenta* para.

Na sličan način definišemo i *uređenu n -torku* ili *vektor* elemenata $a_1, a_2, \dots, a_n$. To je objekat $(a_1, a_2, \dots, a_n)$ koji zadovoljava osobinu:

$$(a_1, a_2, \dots, a_n) = (b_1, b_2, \dots, b_n) \iff a_1 = b_1 \wedge a_2 = b_2 \wedge \dots \wedge a_n = b_n.$$

Ako elementi u uređenim parovima žive u univerzumu $\mathcal{U}$, par (a, b) možemo predstaviti na uobičajen način u ravni:



Koordinatne ose su univerzum $\mathcal{U}$, a uređen par je tačka u ravni koja se projektuje u svoje koordinate na koordinatnim osama.

Definicija 3.27. Dekartov proizvod skupova A i B je skup:

$$A \times B = \{(a, b) : a \in A \wedge b \in B\}.$$

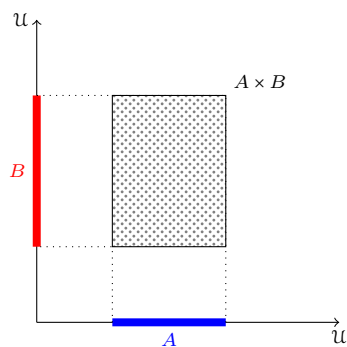
Slično, Dekartov proizvod skupova $A_1, A_2, \dots, A_n$ je skup:

$$A_1 \times A_2 \times \dots \times A_n = \{(a_1, a_2, \dots, a_n) : a_1 \in A_1 \wedge a_2 \in A_2 \wedge \dots \wedge a_n \in A_n\}.$$

Npr. Ako je $A = \{1, 2\}$ i $B = \{a, b, c\}$, $A \times B = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\}$, a $B \times A = \{(a, 1), (a, 2), (b, 1), (b, 2), (c, 1), (c, 2)\}$.

Zadatak 3.28. Ako skup A ima m , a skup B ima n elemenata, dokazati da $A \times B$ ima mn elemenata.

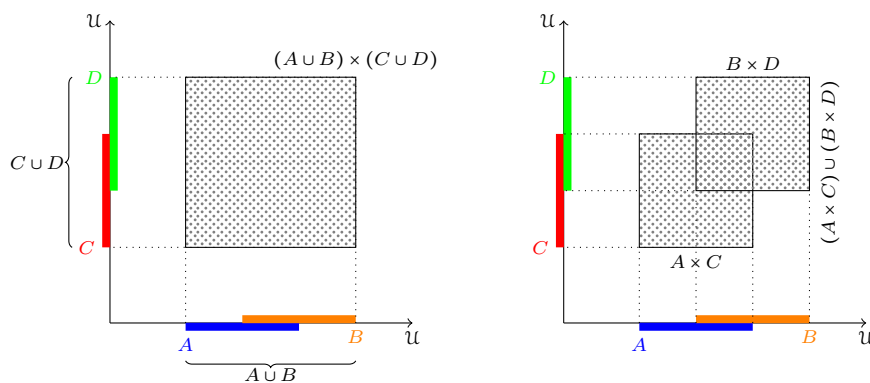
Dekartov proizvod predstavljamo na slici kao pravougaonik na sledeći način:



Zadatak 3.29. Dokazati:

- $A \times (B \cap C) = (A \times B) \cap (A \times C)$;
- $A \times (B \cup C) = (A \times B) \cup (A \times C)$;
- $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$;
- $A \times (B \Delta C) = (A \times B) \Delta (A \times C)$.

Primer 3.30. Ispitajmo u kom su odnosu skupovi $(A \cup B) \times (C \cup D)$ i $(A \times C) \cup (B \times D)$. Skicirajmo date skupove:



Slika nam sugeriše sledeću hipotezu: u opštem slučaju važi:

$$(A \times C) \cup (B \times D) \subseteq (A \cup B) \times (C \cup D).$$

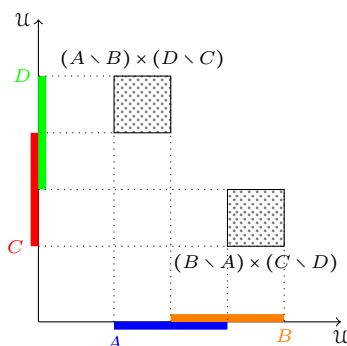
Dokažimo je i formalno. Neka je $(x, y) \in (A \times C) \cup (B \times D)$ proizvoljan uređen par. Tada imamo dva slučaja: $(x, y) \in A \times C$ ili $(x, y) \in B \times D$.

1° Ako $(x, y) \in A \times C$, tada $x \in A$ i $y \in C$, pa sigurno $x \in A \cup B$ i $y \in C \cup D$, odakle $(x, y) \in (A \cup B) \times (C \cup D)$.

2° Ako $(x, y) \in B \times D$, tada $x \in B$ i $y \in D$, pa ponovo $x \in A \cup B$ i $y \in C \cup D$, odakle $(x, y) \in (A \cup B) \times (C \cup D)$.

U svakom slučaju $(x, y) \in (A \cup B) \times (C \cup D)$, što znači da smo dokazali željenu inkluziju.

Razmotrimo i uslove pod kojima važi jednakost. Slika nam sugeriše da bi sledeće oblasti trebalo da su prazne:



Primetimo:

$$(A \setminus B) \times (D \setminus C) = \emptyset \text{ i } (B \setminus A) \times (C \setminus D) = \emptyset$$

akko $(A \setminus B = \emptyset \text{ ili } D \setminus C = \emptyset) \text{ i } (B \setminus A = \emptyset \text{ ili } C \setminus D = \emptyset)$

akko $(A \subseteq B \text{ ili } D \subseteq C) \text{ i } (B \subseteq A \text{ ili } C \subseteq D)$

akko $(A \subseteq B \text{ i } B \subseteq A) \text{ ili } (A \subseteq B \text{ i } C \subseteq D) \text{ ili } (D \subseteq C \text{ i } B \subseteq A) \text{ ili } (D \subseteq C \text{ i } C \subseteq D)$

akko $A = B \text{ ili } (A \subseteq B \text{ i } C \subseteq D) \text{ ili } (D \subseteq C \text{ i } B \subseteq A) \text{ ili } C = D.$

Dakle, hipoteza je: Jednakost $(A \times C) \cup (B \times D) = (A \cup B) \times (C \cup D)$ važi akko važi bar jedno od:

- $A = B$;
- $C = D$;
- $A \subseteq B \text{ i } C \subseteq D$;
- $B \subseteq A \text{ i } D \subseteq C$.

Dokažimo je i formalno.

Smer $(\Rightarrow)$ dokazaćemo kontrapozicijom. Pretpostavimo da ne važi nijedna od ponuđenih opcija. Dakle, $A \neq B$, $C \neq D$, $(A \not\subseteq B \text{ ili } C \not\subseteq D) \text{ i } (B \not\subseteq A \text{ ili } D \not\subseteq C)$. Iz $A \neq B$ pretpostavićemo da imamo element x takav da $x \in A$ i $x \notin B$; obratan slučaj je simetričan. Svakako $x \in A \cup B$. Iz $C \neq D$ imamo dva slučaja:

1° Imamo element y takav da $y \in C$ i $y \notin D$; svakako $y \in C \cup D$. Iz četvrtog uslova, $B \not\subseteq A$ ili $D \not\subseteq C$ razmotrićemo dva podslučaja:

1°1° Važi $B \not\subseteq A$. Tada postoji i element x' takav da $x' \in B$ i $x' \notin A$; svakako $x' \in A \cup B$. Svakako $(x', y) \in (A \cup B) \times (C \cup D)$. Međutim, $(x', y) \notin A \times C$ jer $x' \notin A$, ali i $(x', y) \notin B \times D$ jer $y \notin D$. Prema tome, $(x', y) \notin (A \times C) \cup (B \times D)$, pa $(A \cup B) \times (C \cup D) \neq (A \times C) \cup (B \times D)$.

1°2° Važi $D \not\subseteq C$. Tada postoji i element y' takav da $y' \in D$ i $y' \notin C$; svakako $y' \in C \cup D$. Svakako $(x, y') \in (A \cup B) \times (C \cup D)$. Međutim, $(x, y') \notin A \times C$ jer $y' \notin C$, ali i $(x, y') \notin B \times D$ jer $x \notin B$. Prema tome, $(x, y') \notin (A \times C) \cup (B \times D)$, pa $(A \cup B) \times (C \cup D) \neq (A \times C) \cup (B \times D)$.

2° Imamo element y takav da $y \notin C$ i $y \in D$; svakako $y \in C \cup D$. Tada $(x, y) \in (A \cup B) \times (C \cup D)$. Međutim, $(x, y) \notin A \times C$ jer $y \notin C$, ali i $(x, y) \notin B \times D$ jer $x \notin B$. Prema tome, $(x, y) \notin (A \times C) \cup (B \times D)$, pa $(A \cup B) \times (C \cup D) \neq (A \times C) \cup (B \times D)$.

U svakom slučaju $(A \cup B) \times (C \cup D) \neq (A \times C) \cup (B \times D)$, čime smo dokazali prvi smer.

$(\Leftarrow)$ Inkluziju $(A \times C) \cup (B \times D) \subseteq (A \cup B) \times (C \cup D)$ dokazali smo u opštem slučaju, pa treba da dokažemo samo obratnu inkluziju. Razmotrićemo sva četiri slučaja.

1° Pretpostavimo $A = B$. Neka je $(x, y) \in (A \cup B) \times (C \cup D)$ proizvoljan par. Kako je $A = B$, $x \in A \cup B$ povlači $x \in A$ i $x \in B$. Iz $y \in C \cup D$ imamo dva podslučaja:

1°1° Ako $y \in C$, tada $(x, y) \in A \times C$, pa i $(x, y) \in (A \times C) \cup (B \times D)$.

1°2° Ako $y \in D$, tada $(x, y) \in B \times D$, pa i $(x, y) \in (A \times C) \cup (B \times D)$.

U oba podslučaja, $(x, y) \in (A \times C) \cup (B \times D)$, što završava dokaz u slučaju 1°.

2° Slučaj $C = D$ razmatramo analogno kao 1°. Detalje ostavljamo za vežbu.

3° Pretpostavimo $A \subseteq B$ i $C \subseteq D$. Neka je $(x, y) \in (A \cup B) \times (C \cup D)$ proizvoljan par. Kako je $A \subseteq B$, $A \cup B = B$, pa $x \in B$. Kako je $C \subseteq D$, $C \cup D = D$, pa $y \in D$. Dakle, $(x, y) \in B \times D$, pa i $(x, y) \in (A \times C) \cup (B \times D)$, što završava slučaj 3°.

4° Slučaj $B \subseteq A$ i $D \subseteq C$ razmatramo analogno kao 3°. Detalje ostavljamo za vežbu.

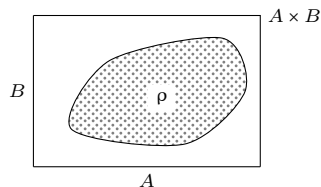
Završili smo dokaz i drugog smera.

Zadatak 3.31. Ispitati odnos između skupova:

- $(A \cap B) \times (C \cap D) \text{ i } (A \times C) \cap (B \times D)$;
- $(A \setminus B) \times (C \setminus D) \text{ i } (A \times C) \setminus (B \times D)$;
- $(A \triangle B) \times (C \triangle D) \text{ i } (A \times C) \triangle (B \times D)$.

4 Relacije

Definicija 4.1. Binarna relacija između skupova A i B je bilo koji podskup $\rho \subseteq A \times B$.



Ako par (a, b) pripada relaciji ρ , $(a, b) \in \rho$, običaj je da to zapisujemo sa $a \rho b$ i čitamo „ a je u relaciji ρ sa b “. Sa druge strane, ako $(a, b) \notin \rho$, običaj je da pišemo $a \not\rho b$ i čitamo „ a nije u relaciji ρ sa b “.

Ako je $A = B$, tj. ako je $\rho \subseteq A \times A$, kažemo da je ρ binarna relacija na skupu A .

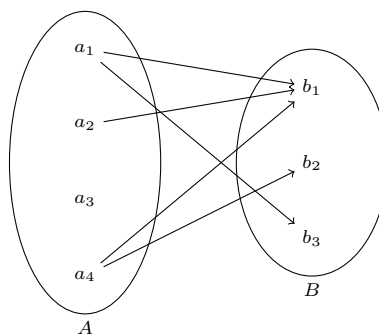
U slučaju da su skupovi A i B konačni, relaciju ρ između skupova A i B možemo da predstavimo *matricom relacije*, tj. tablicom čije su vrste označene elementima skupa A , a kolone elementima skupa B , i u polju indeksiranim sa $a \in A$ i $b \in B$ upišemo istinitosnu vrednost (T ili N) iskaza $a \rho b$. Takođe, ρ možemo da skiciramo *grafom relacije*. Naime, ako je element $a \in A$ u relaciji ρ sa elementom $b \in B$, $a \rho b$, crtamo to kao strelicu $a \rightarrow b$, dok u slučaju $a \not\rho b$, ne crtamo ništa.

Primer 4.2. Neka su $A = \{a_1, a_2, a_3, a_4\}$ i $B = \{b_1, b_2, b_3\}$. Primer relacije ρ između A i B je relacija:

$$\rho = \{(a_1, b_1), (a_1, b_3), (a_2, b_1), (a_4, b_1), (a_4, b_2)\}.$$

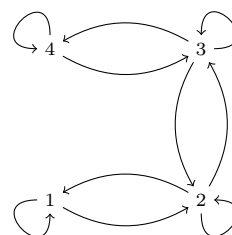
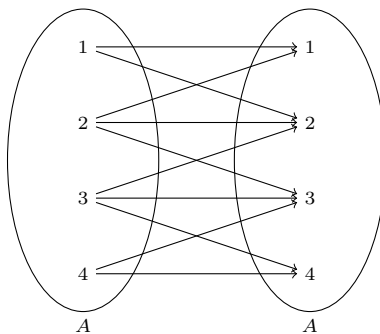
Činjenicu da npr. $(a_1, b_1) \in \rho$ zapisujemo sa $a_1 \rho b_1$, a da npr. $(a_1, b_2) \notin \rho$ zapisujemo sa $a_1 \not\rho b_2$. Matrica i graf prethodne relacije su:

	b_1	b_2	b_3
a_1	T	N	T
a_2	T	N	N
a_3	N	N	N
a_4	T	T	N



Primer 4.3. Neka je $A = \{1, 2, 3, 4\}$ i ρ relacija na A definisana sa $x \rho y$ akko $|x - y| \leq 1$. Lako vidimo $1 \rho 1$ (jer $|1 - 1| = 0 \leq 1$), $1 \rho 2$ (jer $|1 - 2| \leq 1$), $1 \not\rho 3$ (jer $|1 - 3| \not\leq 1$), $1 \not\rho 4$, $2 \rho 1$, $2 \rho 2$, $2 \rho 3$, $2 \not\rho 4$, $3 \not\rho 1$, $3 \rho 2$, $3 \rho 3$, $3 \rho 4$, $4 \not\rho 1$, $4 \not\rho 2$, $4 \rho 3$ i $4 \rho 4$. Matrica relacije je zapisana ispod levo. Relaciju možemo da skiciramo kao u prethodnom primeru (slika u sredini):

	1	2	3	4
1	T	T	N	N
2	T	T	T	N
3	N	T	T	T
4	N	N	T	T



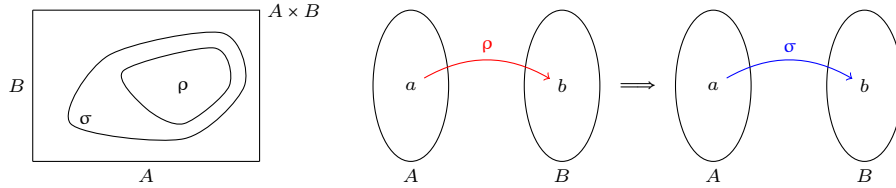
ali možemo da skiciramo kao i graf na slici desno.

4.1 Podrelacija i skupovne operacije sa relacijama

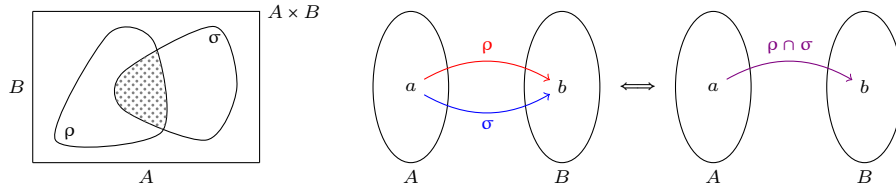
Neka su $\rho, \sigma \subseteq A \times B$ dve relacije između A i B . S obzirom da su ρ i σ pre svega skupovi, možemo govoriti o tome da li je $\rho \subseteq \sigma$, možemo govoriti o preseku $\rho \cap \sigma$, uniji $\rho \cup \sigma$, razlici $\rho \setminus \sigma$, simetričnoj razlici $\rho \Delta \sigma$ i komplementu ρ^c . Iako to nije obavezno, kada govorimo o prethodnim stvarima *uvek* ćemo podrazumevati da su ρ i σ obe između A i B (nećemo posmatrati ρ između A_1 i B_1 , a σ između nekog A_2 i B_2).

Do kraja ovog odeljka pretpostavljamo da su ρ i σ dve relacije između A i B .

Definicija 4.4. Ako je $\rho \subseteq \sigma$ kažemo da je ρ *grublja* od σ , odnosno da je σ *finija* od ρ . (Dakle, $\emptyset$ je najgrublja relacija između A i B , a $A \times B$ je najfinija relacija između A i B .) To znači da $a \rho b$ povlači $a \sigma b$, tj. ako postoji strelica $a \xrightarrow{\rho} b$, onda postoji i strelica $a \xrightarrow{\sigma} b$ (slika desno).

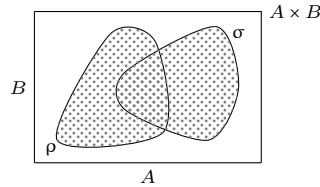


Što se tiče preseka, $\rho \cap \sigma$ su zajednički parovi, tj. strelice, relacija ρ i σ :

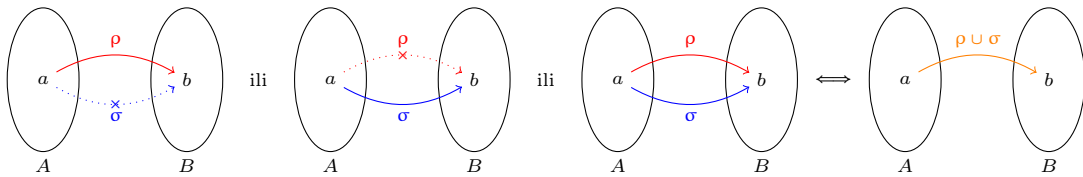


Na slici desno smo naznačili da strelica $a \xrightarrow{\rho \cap \sigma} b$ postoji ako i samo ako postoje obe strelice $a \xrightarrow{\rho} b$ i $a \xrightarrow{\sigma} b$.

Unija $\rho \cup \sigma$ su svi parovi, tj. strelice, relacije ρ i relacije σ :

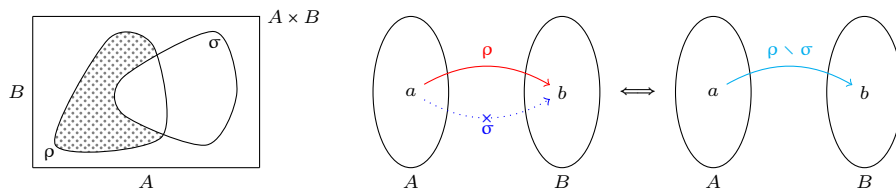


Na grafu to znači da strelica $a \xrightarrow{\rho \cup \sigma} b$ postoji ako i samo ako postoje bar jedna od strelica $a \xrightarrow{\rho} b$ i $a \xrightarrow{\sigma} b$:

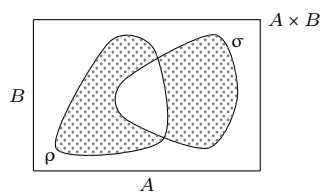


(Činjenicu sa neka strelica ne postoji naglasili smo prekrštenom tačkastom strelicom.)

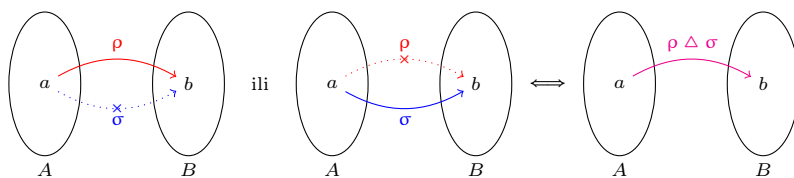
Razlika $\rho \setminus \sigma$ su svi parovi, tj. strelice, koje jesu ρ , ali nisu σ :



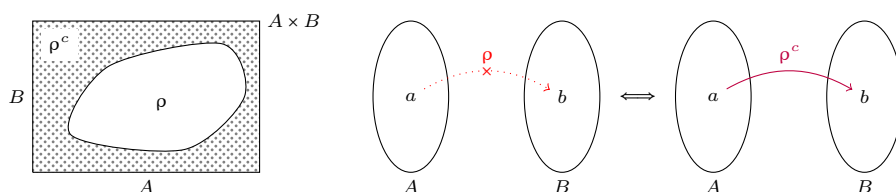
Simetrična razlika $\rho \Delta \sigma$ su svi parovi, tj. strelice, koji su u tačno jedno od relacija ρ i σ :



Na grafu to znači:



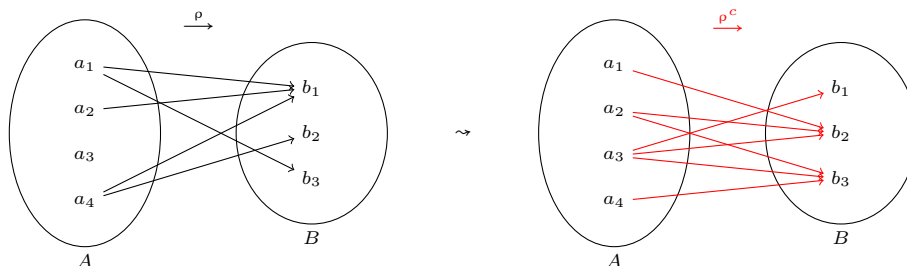
Konačno, komplement relacije ρ , ρ^c , su svi parovi, tj. strelice, skupa $A \times B$ koji nisu u relaciji ρ (dakle, komplement računamo relativno u odnosu na $A \times B$):



Primer 4.5. Komplement relacije ρ :

$$\rho = \{(a_1, b_1), (a_1, b_3), (a_2, b_1), (a_4, b_1), (a_4, b_2)\}$$

između $A = \{a_1, a_2, a_3, a_4\}$ i $B = \{b_1, b_2, b_3\}$ dobijamo uzimajući sve strelice koje nisu ρ , i samo njih:



Skupovno zapisano: $\rho^c = \{(a_1, b_2), (a_2, b_2), (a_2, b_3), (a_3, b_1), (a_3, b_2), (a_3, b_3), (a_4, b_3)\}$.

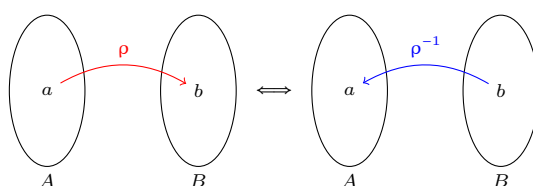
Sve osobine relacije $\subseteq$ i operacija $\cap, \cup, \setminus, \Delta$ i c koje važe generalno za skupove, važe i za relacije.

4.2 Inverzna relacija

Definicija 4.6. Neka je $\rho \subseteq A \times B$. Inverzna relacija relacije ρ ili inverz relacije ρ je relacija $\rho^{-1} \subseteq B \times A$ definisana sa:

$$\rho^{-1} = \{(b, a) \mid (a, b) \in \rho\},$$

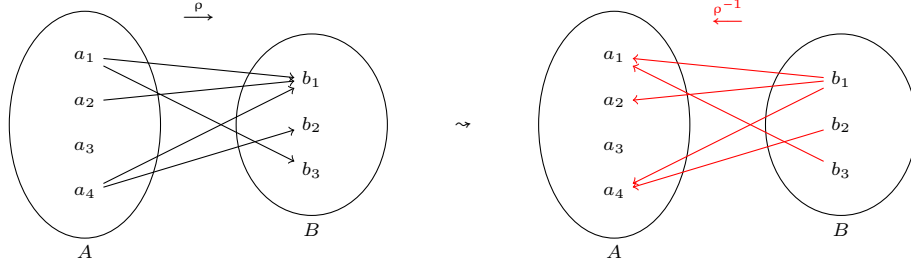
tj. data sa $b \rho^{-1} a$ akko $a \rho b$, odnosno dobijena obrtanjem svih strelica na grafu:



Primer 4.7. Inverz relacije ρ :

$$\rho = \{(a_1, b_1), (a_1, b_3), (a_2, b_1), (a_4, b_1), (a_4, b_2)\}$$

između $A = \{a_1, a_2, a_3, a_4\}$ i $B = \{b_1, b_2, b_3\}$ dobijamo obrtanjem svih strelica na grafu relacije ρ :

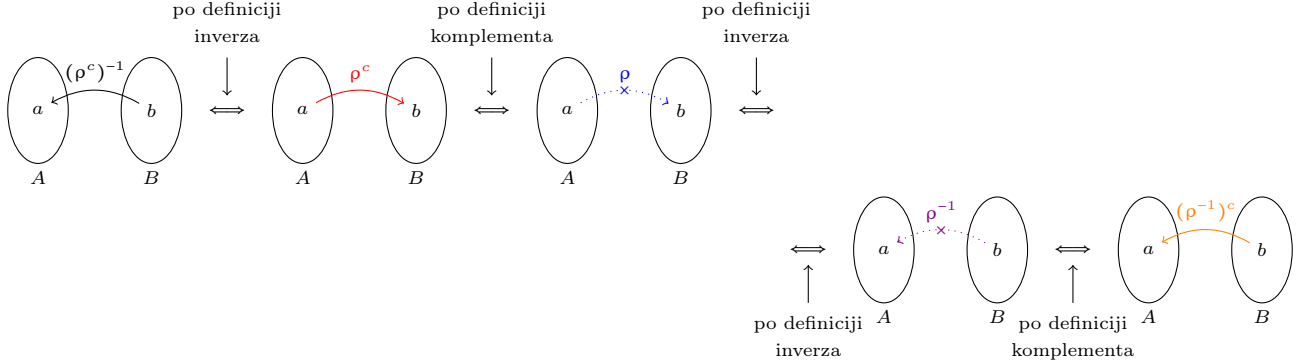


Skupovno zapisano: $\rho^{-1} = \{(b_1, a_1), (b_1, a_4), (b_2, a_4), (b_3, a_1)\}$.

Tvrđenje 4.8. Neka su $\rho, \sigma \subseteq A \times B$. Tada važi:

- | | |
|--|---|
| (i) $(\rho^{-1})^{-1} = \rho$; | (v) $(\rho \setminus \sigma)^{-1} = \rho^{-1} \setminus \sigma^{-1}$; |
| (ii) $\rho \subseteq \sigma$ povlači $\rho^{-1} \subseteq \sigma^{-1}$; | (vi) $(\rho \triangle \sigma)^{-1} = \rho^{-1} \triangle \sigma^{-1}$; |
| (iii) $(\rho \cap \sigma)^{-1} = \rho^{-1} \cap \sigma^{-1}$; | (vii) $(\rho^c)^{-1} = (\rho^{-1})^c$. |
| (iv) $(\rho \cup \sigma)^{-1} = \rho^{-1} \cup \sigma^{-1}$; | |

Dokaz. Dokazi svih delova su pravolinijski po definicijama. Npr. da bismo dokazali poslednji deo, $(\rho^c)^{-1} = (\rho^{-1})^c$, možemo da razmotrimo sledeću sliku:



Na slici smo različite relacije predstavili strelicama različitih boja. Prva ekvivalencija dobija se samo obrtanjem strelica po definiciji inverza. Druga ekvivalencija sledi po definiciji komplementa, tj. leva strelica postoji akko desna ne postoji. Treća ekvivalencija ponovo važi po definiciji inverza, a četvrta po definiciji komplementa. Dakle, između b i a postoji crna strelica akko postoji narandžasta strelica, pa su ove dve relacije $((\rho^c)^{-1})$ predstavljena crnom i $(\rho^{-1})^c$ predstavljena narandžastom strelicom) jednake.

Formalno dokaz možemo da zapišemo na sledeći način: Neka su $a \in A$ i $b \in B$. Imamo:

$$\begin{aligned}
 b (\rho^c)^{-1} a &\iff a \rho^c b && \text{po definiciji inverza} \\
 &\iff \neg a \rho b && \text{po definiciji komplementa} \\
 &\iff \neg b \rho^{-1} a && \text{po definiciji inverza} \\
 &\iff b (\rho^{-1})^c a && \text{po definiciji komplementa.}
 \end{aligned}$$

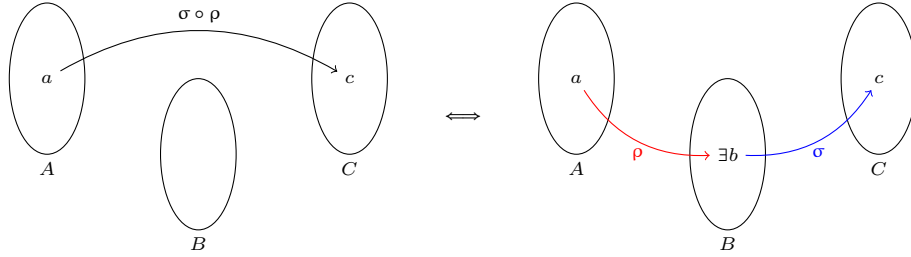
Prema tome, relacije $(\rho^c)^{-1}$ i $(\rho^{-1})^c$ sadrže iste parove, pa su jednake. $\square$

4.3 Kompozicija relacija

Definicija 4.9. Neka su $\rho \subseteq A \times B$ i $\sigma \subseteq B \times C$ relacije. *Kompozicija* relacija ρ i σ je relacija $\sigma \circ \rho \subseteq A \times C$ ⁷ definisana sa:

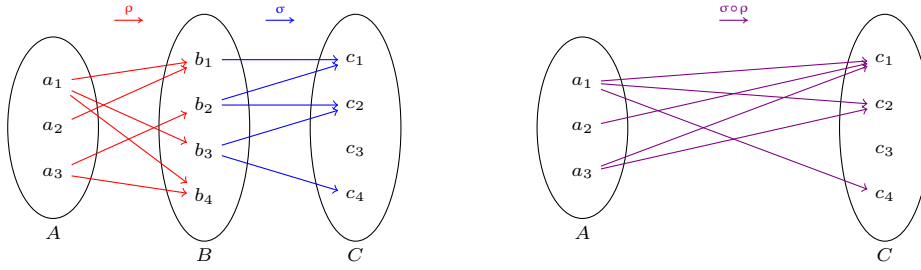
$$a \sigma \circ \rho c \iff (\exists b \in B) a \rho b \text{ i } b \sigma c,$$

za $a \in A$ i $c \in C$. Na grafu to možemo predstaviti na sledeći način:



Dakle, imamo strelicu $a \xrightarrow{\sigma \circ \rho} c$ akko imamo strelice $a \xrightarrow{\rho} b$ i $b \xrightarrow{\sigma} c$ za neki element $b \in B$.

Primer 4.10. Neka su $A = \{a_1, a_2, a_3\}$, $B = \{b_1, b_2, b_3, b_4\}$ i $C = \{c_1, c_2, c_3, c_4\}$, i relacije $\rho \subseteq A \times B$ i $\sigma \subseteq B \times C$ date grafovima na slici levo:



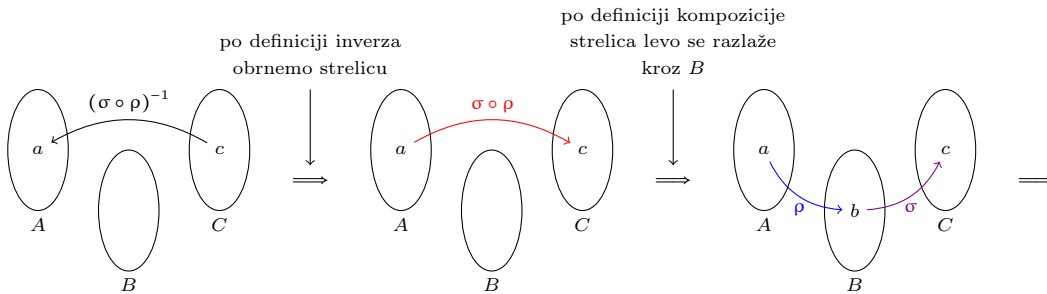
Kompoziciju $\sigma \circ \rho$ dobijamo nastavljajući strelice polazeći od elemenata iz A i završavajući u C . Npr. kako $a_1 \xrightarrow{\rho} b_1 \xrightarrow{\sigma} c_1$ imamo $a_1 \xrightarrow{\sigma \circ \rho} c_1$, kako $a_1 \xrightarrow{\rho} b_3 \xrightarrow{\sigma} c_2$ imamo $a_1 \xrightarrow{\sigma \circ \rho} c_2$, itd. Dobijamo graf na slici desno. Skupovno zapisano kompozicija relacija ρ i σ je $\sigma \circ \rho = \{(a_1, c_1), (a_1, c_2), (a_1, c_4), (a_2, c_1), (a_3, c_1), (a_3, c_2)\}$.

Tvrđenje 4.11. Neka su $\rho \subseteq A \times B$, $\sigma \subseteq B \times C$ i $\tau \subseteq C \times D$ relacije. Tada:

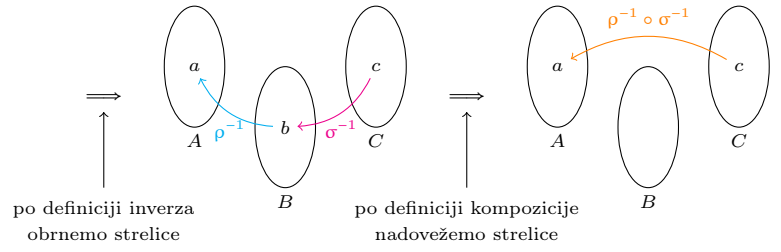
(i) $(\sigma \circ \rho)^{-1} = \rho^{-1} \circ \sigma^{-1}$;

(ii) $\tau \circ (\sigma \circ \rho) = (\tau \circ \sigma) \circ \rho$.

Dokaz. (i) Najpre primetimo da su obe strane jednakosti definisane relacije iz C u A . Razmotrimo najpre inkluziju $(\subseteq)$ na grafu:



⁷Obratite pažnju na redosled zapisa: zapisujemo relacije s desna na levo!



Dakle, ako imamo $(\sigma \circ \rho)^{-1}$ -strelicu $c \rightarrow a$, onda imamo i $\rho^{-1} \circ \sigma^{-1}$ -strelicu $c \rightarrow a$, pa možemo da zaključimo $(\sigma \circ \rho)^{-1} \subseteq \rho^{-1} \circ \sigma^{-1}$. Nije teško videti da prethodna slika čitana zdesna na levo dokazuje i obratnu inkluziju.

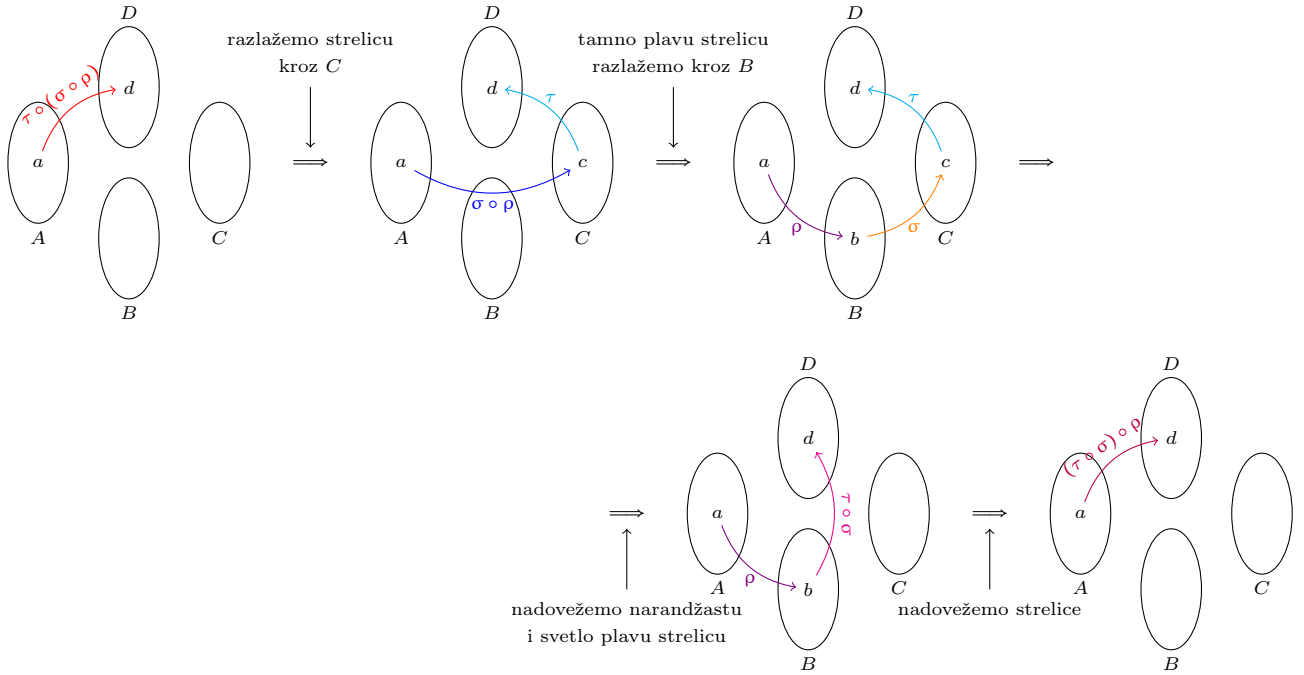
Sada možemo zapisati i formalan dokaz: Neka su $a \in A$ i $c \in C$ proizvoljni elementi. Tada:

$$\begin{aligned}
 c (\sigma \circ \rho)^{-1} a &\iff a \sigma \circ \rho c && \text{po definiciji inverza} \\
 &\iff a \rho b \text{ i } b \sigma c, \text{ za neko } b \in B && \text{po definiciji kompozicije} \\
 &\iff b \rho^{-1} a \text{ i } c \sigma^{-1} b, \text{ za neko } b \in B && \text{po definiciji inverza} \\
 &\iff c \rho^{-1} \circ \sigma^{-1} a && \text{po definiciji kompozicije}
 \end{aligned}$$

Prema tome, $(\sigma \circ \rho)^{-1} = \rho^{-1} \circ \sigma^{-1}$.

(ii) Opet najpre primetimo da su obe relacije $\tau \circ (\sigma \circ \rho)$ i $(\tau \circ \sigma) \circ \rho$ iz A u D , pa ima smisla da ih upoređujemo.

Razmotrimo inkluziju ($\subseteq$) na grafu:



Dakle, ako imamo $\tau \circ (\sigma \circ \rho)$ -strelicu $a \rightarrow d$, onda imamo i $(\tau \circ \sigma) \circ \rho$ -strelicu $a \rightarrow d$, pa $\tau \circ (\sigma \circ \rho) \subseteq (\tau \circ \sigma) \circ \rho$. Postupajući unazad, prethodno razmatranje nam daje i obratnu inkluziju. Zapišimo sada i formalno dokaz:

Neka su $a \in A$ i $d \in D$ proizvoljni. Imamo:

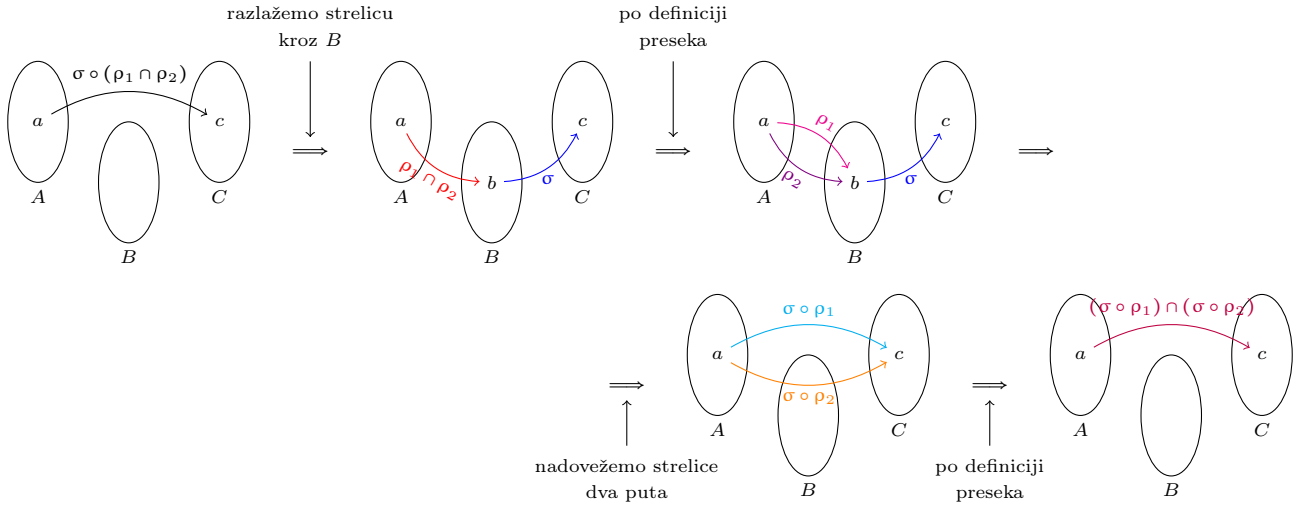
$$\begin{aligned}
 a \tau \circ (\sigma \circ \rho) d &\iff a \sigma \circ \rho c \text{ i } c \tau d, \text{ za neko } c \in C \\
 &\iff a \rho b \text{ i } b \sigma c \text{ i } c \tau d, \text{ za neke } b \in B, c \in C \\
 &\iff a \rho b \text{ i } b \tau \circ \sigma d, \text{ za neko } b \in B \\
 &\iff a (\tau \circ \sigma) \circ \rho d.
 \end{aligned}$$

Svi koraci u prethodnom nizu su po definiciji kompozicije. Prema tome, $\tau \circ (\sigma \circ \rho) = (\tau \circ \sigma) \circ \rho$. □

Komentar 4.12. Ako $\rho \subseteq A \times B$, $\sigma \subseteq B \times C$ i $\tau \subseteq C \times D$, prema prthodnom tvrđenju (asocijativnosti kompozicije) možemo da pišemo $\tau \circ \sigma \circ \rho$. Iz dokaza vidimo da $a \tau \circ \sigma \circ \rho d$ znači da postoje $b \in B$ i $c \in C$ tako da $a \rho b$, $b \sigma c$ i $c \tau d$, što kraće možemo da zapišemo i sa $a \rho b \sigma c \tau d$. Analogno važi i ako imamo definisanu kompoziciju više od tri relacije.

Primer 4.13. Neka $\rho_1, \rho_2 \subseteq A \times B$ i $\sigma \subseteq B \times C$. Ispitajmo u kom su odnosu relacije $\sigma \circ (\rho_1 \cap \rho_2)$ i $(\sigma \circ \rho_1) \cap (\sigma \circ \rho_2)$, koje su obe između A i C .

Pretpostavimo najpre da imamo $a \sigma \circ (\rho_1 \cap \rho_2) c$ i razmotrimo graf:



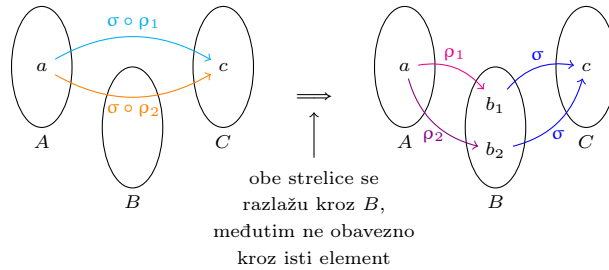
Prema tome, ako imamo $\sigma \circ (\rho_1 \cap \rho_2)$ -strelicu $a \rightarrow c$, onda imamo i $(\sigma \circ \rho_1) \cap (\sigma \circ \rho_2)$ -strelicu $a \rightarrow c$, pa važi $\sigma \circ (\rho_1 \cap \rho_2) \subseteq (\sigma \circ \rho_1) \cap (\sigma \circ \rho_2)$. Formalno, dokaz ove inkluzije zapisujemo sa: Neka su $a \in A$ i $c \in C$ proizvoljne.

Imamo:

$$\begin{aligned}
 a \sigma \circ (\rho_1 \cap \rho_2) c &\implies a \rho_1 \cap \rho_2 b \text{ i } b \sigma c, \text{ za neko } b \in B && \text{po def. kompozicije} \\
 &\implies a \rho_1 b \text{ i } a \rho_2 b \text{ i } b \sigma c, \text{ za neko } b \in B && \text{po def. preseka} \\
 &\implies a \sigma \circ \rho_1 c \text{ i } a \sigma \circ \rho_2 c && \text{po def. kompozicije} \\
 &\implies a (\sigma \circ \rho_1) \cap (\sigma \circ \rho_2) c && \text{po def. preseka.}
 \end{aligned}$$

Dakle, u opštem slučaju važi $\sigma \circ (\rho_1 \cap \rho_2) \subseteq (\sigma \circ \rho_1) \cap (\sigma \circ \rho_2)$.

Po definiciji kompozicije, prva implikacija se može obrnuti. Takođe, po definiciji preseka, druga i četvrta implikacija se mogu obrnuti. Međutim, treća implikacija ne može. Pogledajmo graf:



Sada vidimo da ne moramo obavezno da pređemo na presek $\rho_1 \cap \rho_2$.

Poslednja sličica nam sugerise i kontraprimer za obratnu inkluziju. Naime, uzmimo baš $A = \{a\}$, $B = \{b_1, b_2\}$, $C = \{c\}$, $\rho_1 = \{(a, b_1)\}$, $\rho_2 = \{(a, b_2)\}$ i $\sigma = \{(b_1, c), (b_2, c)\}$. Tada je $\rho_1 \cap \rho_2 = \emptyset$, pa je i $\sigma \circ (\rho_1 \cap \rho_2) = \emptyset$. Sa druge strane, $\sigma \circ \rho_1 = \{(a, c)\}$ i $\sigma \circ \rho_2 = \{(a, c)\}$, pa je $(\sigma \circ \rho_1) \cap (\sigma \circ \rho_2) = \{(a, c)\}$. Dakle, imamo primer u kome važi:

$$\sigma \circ (\rho_1 \cap \rho_2) \subsetneq (\sigma \circ \rho_1) \cap (\sigma \circ \rho_2).$$

Zadatak 4.14. Neka $\rho_1, \rho_2 \subseteq A \times B$ i $\sigma \subseteq B \times C$. Dokazati:

- (i) $\rho_1 \subseteq \rho_2$ povlači $\sigma \circ \rho_1 \subseteq \sigma \circ \rho_2$;
- (ii) $\sigma \circ (\rho_1 \cup \rho_2) = (\sigma \circ \rho_1) \cup (\sigma \circ \rho_2)$;
- (iii) $\sigma \circ (\rho_1 \setminus \rho_2) \supseteq (\sigma \circ \rho_1) \setminus (\sigma \circ \rho_2)$.
- (iv) Primerom pokazati da u (i) ne mora da važi obratna implikacija.
- (v) Primerom pokazati da u (iii) ne mora da važi obratna inkluzija.

4.4 Osobine binarnih relacija na skupu S

Definicija 4.15. Neka je ρ binarna relacija na skupu S . Ističemo nekoliko osobina koje relacija ρ može (i ne mora) da ima:

- (R) $(\forall x \in S) x \rho x$; (refleksivnost)
- (I) $(\forall x \in S) x \not\rho x$; (irefleksivnost)
- (S) $(\forall x, y \in S)(x \rho y \rightarrow y \rho x)$; (simetričnost)
- (a) $(\forall x, y \in S)(x \rho y \rightarrow y \not\rho x)$; (asimetričnost)
- (A) $(\forall x, y \in S)(x \rho y \wedge y \rho x \rightarrow x = y)$; (antisimetričnost)
- (T) $(\forall x, y, z \in S)(x \rho y \wedge y \rho z \rightarrow x \rho z)$. (tranzitivnost)

Na grafu relacije ρ uslov refleksivnosti kaže da oko svakog elementa postoji petlja, dok uslov irefleksivnosti ide u drugu krajnost: ni oko jednog elementa nema petlje. Uslov simetričnosti kaže da ako imamo strelicu $x \rightarrow y$, moramo da imamo i strelicu $y \rightarrow x$:

$$\text{ako } x \xrightarrow{\quad} y, \text{ onda mora biti i } x \xleftarrow{\quad} y.$$

Uslov simetričnosti odnosi se i na potencijalno jednake $x = y$, ali ne daje nikakvu informaciju (kaže samo da ako imamo petlju u x , onda imamo petlju u x , što je uvek tačna implikacija).

Uslov asimetričnosti kaže da ako imamo strelicu $x \rightarrow y$, onda nemamo strelicu $y \rightarrow x$:

$$\text{ako } x \xrightarrow{\quad} y, \text{ onda mora biti } x \not\xleftarrow{\quad} y.$$

I uslov asimetričnosti odnosi se na potencijalno jednake x i y . U tom slučaju uslov asimetričnosti kaže da je tačna implikacija: ako postoji petlja u x , onda ne postoji petlja u x , što je tačno akko ni u jednom x nemamo petlju. Dakle, asimetričnost specijlno podrazumeva irefleksivnost.

Uslov antisimetričnosti kaže da ako imamo obe strelice $x \rightarrow y$ i $y \rightarrow x$, onda x i y moraju da budu jednaki. Drugim rečima ako $x \neq y$, nemamo sledeću situaciju:

$$x \xleftrightarrow{\quad} y$$

Primitimo da asimetričnost povlači antisimetričnost. Oba uslova zabranjuju obe strelice između različitih elemenata. Jedina razlika je što asimetričnost zabranjuje petlje, dok antisimetričnost dozvoljava da oko nekih elemenata postoje petlje.

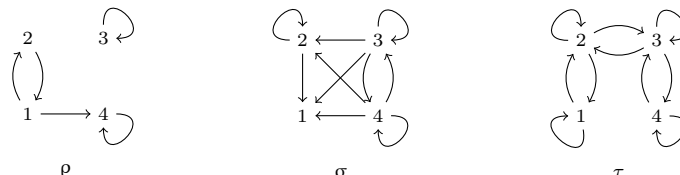
Uslov tranzitivnosti kaže da ako postoje strelice $x \rightarrow y$ i $y \rightarrow z$, mora da postoji i strelica $x \rightarrow z$:

$$\text{ako } x \xrightarrow{\quad} y \xrightarrow{\quad} z, \text{ onda mora biti i } x \xrightarrow{\quad} z.$$

I uslov tranzitivnosti odnosi se i na x, y, z od kojih su neki potencijalno jednaki. Ako je $x = y$ ili $y = z$, implikacija u uslovu tranzitivnosti očigledno je zadovoljena. Ističemo slučaj $x \neq y$ i $x = z$. U ovom slučaju tranzitivnost kaže da ako imamo obe strelice između dva različita elementa x i y , moramo da imamo i obe petlje u x i y :

$$\text{ako } x \xleftrightarrow{\quad} y, \text{ onda mora biti i } \bigcirc \xrightarrow{\quad} x \xleftrightarrow{\quad} y \xleftarrow{\quad} y \xleftarrow{\quad} \bigcirc.$$

Primer 4.16. Na skupu $\{1, 2, 3, 4\}$ uočimo relacije skicirane sa:



Ispitajmo koje osobine imaju ove relacije.

Relacija ρ nije refleksivna (jer nema petlje oko 1 i 2), a nije ni irefleksivna (jer ima petlje oko 3 i 4). Relacija nije simetrična jer imamo $1 \rightarrow 4$, ali nemamo $4 \rightarrow 1$. Relacija nije ni asimetrična ni antisimetrična jer imamo $1 \rightarrow 2$ i $2 \rightarrow 1$ i $1 \neq 2$; relacija nije asimetrična jer nije ni irefleksivna. Konačno ρ nije ni tranzitivna jer imamo $2 \rightarrow 1$ i $1 \rightarrow 4$, ali nemamo $2 \rightarrow 4$.

Relacija σ nije refleksivna (nema petlju oko 1) ni irefleksivna (ima sve ostale petlje). Relacija nije simetrična jer npr. $2 \rightarrow 1$ ali nije $1 \rightarrow 2$. Relacija nije asimetrična niti antisimetrična jer imamo $3 \rightarrow 4$ i $4 \rightarrow 3$. Konačno relacija jeste tranzitivna. Nije teško izračunati da je $\sigma \circ \sigma = \sigma$, što znači da σ jeste tranzitivna.

Relacija τ jeste refleksivna i simetrična, ali ne zadovoljava ostale osobine.

Definicija 4.17. *Dijagonala* skupa S je relacija na S data sa $\Delta_S = \{(x, x) \mid x \in S\}$.

Primetimo da je Δ_S samo druga oznaka za relaciju jednakosti na S .

Sada možemo da damo i sledeće, skupovne karakterizacije gore uvedenih osobina. Najpre, očigledno relacija ρ na S je refleksivna akko $\Delta_S \subseteq \rho$, a ρ je irefleksivna akko $\Delta_S \cap \rho = \emptyset$.

Kako je $y \rho x$ akko $x \rho^{-1} y$, uslov simetričnosti ekvivalentan je sa $\rho \subseteq \rho^{-1}$. Ovo je ekvivalentno i sa $\rho = \rho^{-1}$ jer $\rho \subseteq \rho^{-1}$ povlači i $\rho^{-1} \subseteq (\rho^{-1})^{-1} = \rho$.

Kako je $y \not\rho x$ akko $x \not\rho^{-1} y$ akko $x (\rho^{-1})^c y$, uslov asimetričnosti ekvivalentan je sa $\rho \subseteq (\rho^{-1})^c$, tj. sa $\rho \cap \rho^{-1} = \emptyset$.

Sad lako vidimo i da je uslov antisimetričnosti ekvivalentan sa $\rho \cap \rho^{-1} \subseteq \Delta_S$.

Konačno, razmotrimo i tranzitivnost. Iskaz $(\forall x, y, z \in S)(x \rho y \wedge y \rho z \rightarrow x \rho z)$ ekvivalentan je sa: $(\forall x, z \in S)((\exists y \in S)(x \rho y \wedge y \rho z) \rightarrow x \rho z)$. Kako je $(\exists y \in S)(x \rho y \wedge y \rho z)$ ekvivalentno sa $x \rho \circ \rho z$, uslov tranzitivnosti ekvivalentan je sa $\rho \circ \rho \subseteq \rho$.

4.5 Ekvivalencije

Zadatak 4.18. Na skupu $\{a, b, c\}$ konstruisati relaciju ρ koja je:

- (i) refleksivna i simetrična, ali nije tranzitivna;
- (ii) refleksivna i tranzitivna, ali nije simetrična;
- (iii) simetrična i tranzitivna, ali nije refleksivna.

Definicija 4.19. Relacija $\approx$ na skupu S je *ekvivalencija* ako je refleksivna, simetrična i tranzitivna.

Prvi primer ekvivalencije na bilo kom skupu je jednakost na tom skupu. Izborom simbola $\approx$ naglašavamo da ekvivalencije imaju iste osnovne osobine kao i jednakost.

Primer 4.20. Neka je $m \in \mathbb{N}$. Na skupu $\mathbb{Z}$ definišemo relaciju $\equiv_m$ sa $x \equiv_m y$ akko $m \mid x - y$, tj. akko $(\exists k \in \mathbb{Z}) x - y = mk$.

Relacija $\equiv_m$ je refleksivna jer za sve $x \in \mathbb{Z}$ važi $x - x = m \cdot 0$. Ako je $x \equiv_m y$, tj. $x - y = mk$ za neko celo k , tada je $y - x = m(-k)$ i $-k \in \mathbb{Z}$, pa $y \equiv_m x$, što znači da je $\equiv_m$ simetrična. Ako je $x \equiv_m y$ i $y \equiv_m z$, tj. $x - y = mk$ i $y - z = ml$ za neke cele k i l , sabiranjem je i $x - z = m(k + l)$ i $k + l \in \mathbb{Z}$, pa je $x \equiv_m z$, što dokazuje tranzitivnost.

Za $m = 0$, $x \equiv_0 y$ akko $x - y = 0 \cdot k$ za neko $k \in \mathbb{Z}$, akko $x = y$, pa je relacija $\equiv_0$ relacija jednakosti na skupu $\mathbb{Z}$. Za $m = 1$, $x \equiv_1 y$ akko $x - y = 1 \cdot k$ za neko $k \in \mathbb{Z}$, što je tačno za proizvoljne brojeve x i y . Dakle, $\equiv_1$ je relacija $\mathbb{Z} \times \mathbb{Z}$.

Zanimljivi slučajevi su kada je $m \geq 2$.

Definicija 4.21. Neka je $\approx$ ekvivalencija na skupu S i $a \in S$. *Klasa* elementa a je skup u oznaci $[a]_\approx$, ili samo $[a]$ ako je ekvivalencija $\approx$ jasna iz konteksta, definisan sa:

$$[a] = \{x \in S \mid x \approx a\}.$$

Zbog simetričnosti direktno imamo i $[a] = \{x \in S \mid a \approx x\}$.

Tvrđenje 4.22 (Osnovne osobine klasa). Neka je $\approx$ ekvivalencija na S i $a, b \in S$. Tada:

- (i) $a \in [a]$; specijalno, $[a] \neq \emptyset$;
- (ii) $a \approx b$ akko $[a] = [b]$;
- (iii) $a \not\approx b$ akko $[a] \cap [b] = \emptyset$.

Dokaz. (i) Uslov $a \in [a]$ ekvivalentan je sa $a \approx a$, što jeste tačno jer je $\approx$ refleksivna.

(ii) $(\Rightarrow)$ Pretpostavimo $a \approx b$. Dokažimo najpre $[a] \subseteq [b]$. Ako $x \in [a]$, tada $x \approx a$, pa kako $a \approx b$, po tranzitivnosti $x \approx b$, tj. $x \in [b]$; dakle, $[a] \subseteq [b]$. Ovime smo dokazali da $a \approx b$ povlači $[a] \subseteq [b]$. Kako $a \approx b$ zbog simetričnosti povlači i $b \approx a$, prema prethodnom imamo i $[b] \subseteq [a]$. Dakle, važi $[a] = [b]$.

$(\Leftarrow)$ Pretpostavimo $[a] = [b]$. Kako $a \in [a]$ prema (i), važi i $a \in [b]$, što znači $a \approx b$.

(iii) $(\Rightarrow)$ Dokažimo kontrapoziciju. Pretpostavimo $[a] \cap [b] \neq \emptyset$ i neka je $x \in [a] \cap [b]$. Tada $a \approx x$ i $x \approx b$, pa i $a \approx b$ zbog tranzitivnosti, što znači da ne važi $a \not\approx b$.

$(\Leftarrow)$ Pretpostavimo $[a] \cap [b] = \emptyset$. Kako $[a], [b] \neq \emptyset$ prema (i), to povlači $[a] \neq [b]$, odakle $a \not\approx b$ prema (ii). $\square$

Prema (i) i (ii), $x \in [a]$ akko $x \approx a$ akko $[x] = [a]$, i $x \notin [a]$ akko $x \not\approx a$ akko $[x] \cap [a] = \emptyset$. Dakle, svi elementi u klasi su u relaciji samo sa elementima te klase i ni sa jednim više, i imaju tu istu klasu. Klase ekvivalencije dele skup S na međusobno disjunktne (presek je prazan) neprazne delove. Ovakva podela skupa S naziva se *particija* skupa S .

Primer 4.23. Vratimo se na primer 4.20 i neka je $m \geq 2$. Izračunajmo klase relacije $\equiv_m$. Za $a \in \mathbb{Z}$ imamo:

$$\begin{aligned} x \in [a] &\iff x \equiv_m a \\ &\iff x - a = mk \text{ za neko } k \in \mathbb{Z} \\ &\iff x = a + mk \text{ za neko } k \in \mathbb{Z} \end{aligned}$$

pa je $[a] = \{a + mk \mid k \in \mathbb{Z}\}$. Nije teško videti da imamo m različitih klasa. Naime, klasa $[a]$ određena je ostatkom pro deljenju broja a sa m . Zaista, ako je $a = mq + r$, $0 \leq r < m$, tada $a \in [r]$, pa je $[a] = [r]$. Sa druge strane, za $0 \leq r_1 < r_2 < m$, jasno je da $m \nmid r_1 - r_2$, pa $r_1 \not\equiv_m r_2$, što znači da $[r_1] \neq [r_2]$. Dakle, imamo m različitih klasa i one su određene ostacima pri deljenju sa m : $[0], [1], \dots, [m-1]$.

Definicija 4.24. Skup svih klasa ekvivalencije $\approx$ na skupu S zove se *količnčki skup* i označava se sa $S/\approx$:

$$S/\approx = \{[a] \mid a \in S\}.$$

U prethodnom primeru $\mathbb{Z}/\equiv_m = \{[0], [1], \dots, [m-1]\}$.

Definicija 4.25. *Transverzala* ili *skup predstavnika* ekvivalencije $\approx$ na skupu S je bilo koji podskup $T \subseteq S$ koji sadrži po tačno jedan element iz svake klase.

Npr. u gornjem primeru skup $\{0, 1, \dots, m-1\}$ je jedna prirodna transverzala ekvivalencije $\equiv_m$.

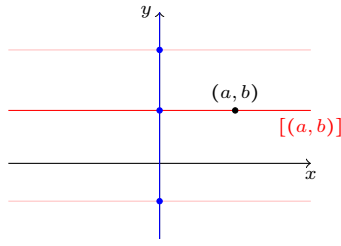
Primer 4.26. Na skupu $\mathbb{R} \times \mathbb{R}$ definišemo relaciju $\approx$ sa:

$$(x_1, y_1) \approx (x_2, y_2) \iff y_1 = y_2.$$

Nije teško videti da je $\approx$ ekvivalencija. Izračunajmo klasu tačke (a, b) :

$$\begin{aligned} (x, y) \in [(a, b)] &\iff (x, y) \approx (a, b) \\ &\iff y = b \end{aligned} \quad \text{tj. } [(a, b)] = \{(x, b) \mid x \in \mathbb{R}\}.$$

Prethodni skup je prava kroz (a, b) paralelna sa x -osom:



Prema tome količinski skup, $(\mathbb{R} \times \mathbb{R})/\approx$, je skup svih pravih paralelnih sa x -osom. Da bismo uočili neku transversalu treba sa svake od tih pravih da izaberemo po jednu tačku. Npr. y -osa je jedna transversala. Ili bilo koja prava koja nije paralelna sa x -osom. Ili graf funkcije $y = x^3$. Svi ovi skupovi seku prave paralelne sa x -osom u po jednoj tački.

Primer 4.27. Na skupu $\mathbb{R} \times \mathbb{R}$ definišemo relaciju $\approx$ sa:

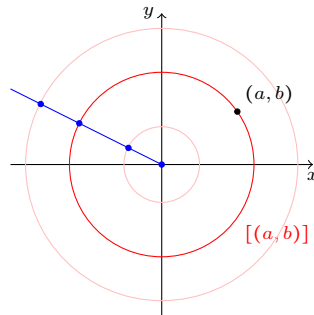
$$(x_1, y_1) \approx (x_2, y_2) \iff x_1^2 + y_1^2 = x_2^2 + y_2^2.$$

Ponovo lako vidimo da je $\approx$ ekvivalencija, i računamo klasu tačke (a, b) :

$$\begin{aligned} (x, y) \in [(a, b)] &\iff (x, y) \approx (a, b) \\ &\iff x^2 + y^2 = a^2 + b^2 \quad \text{tj. } [(a, b)] = \{(x, y) \mid x^2 + y^2 = a^2 + b^2 \in \mathbb{R}\}. \end{aligned}$$

Ako sa r označimo

rastojanje (a, b) od koordinatnog početka, po Pitagorinoj teoremi je $a^2 + b^2 = r^2$, pa je prethodni skup zapravo skup tačaka (x, y) za koje je $x^2 + y^2 = r^2$, i prepoznavamo da je u pitanju kružnica sa centrom u koordinatnom početku poluprečnika r , tj. koja prolazi kroz (a, b) :



Prema tome količinski skup je skup svih kružnica sa centrom u koordinatnom početku (uključujući i jedan degenerisan slučaj, $[(0, 0)] = \{(0, 0)\}$, što možemo da razumemo kao kružnicu sa centrom u koordinatnom početku poluprečnika 0). Sa svake takve kružnice treba da odaberemo po jednu tačku da bismo odredili jednu transversalu, i jedan prirodan način je da uzmemo bilo koju polupravu sa temenom u koordinatnom početku.

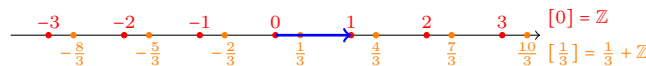
Primer 4.28. Na skupu $\mathbb{R}$ data je relacija $\approx$ sa:

$$x \approx y \iff x - y \in \mathbb{Z}.$$

Ova relacija takođe jeste ekvivalencija, a klasa broja a je:

$$\begin{aligned} x \in [a] &\iff x \approx a \\ &\iff x - a \in \mathbb{Z} \\ &\iff x = a + k \text{ za neko } k \in \mathbb{Z} \end{aligned}$$

tj. $[a] = \{a + k \mid k \in \mathbb{Z}\} = a + \mathbb{Z}$. Dakle, klasa elementa a je skup $\mathbb{Z}$ transliran za a :



Primitimo da svaka klasa ima jedinstvenog predstavnika u intervalu $[0, 1)$. Zaista, za klasu $[a]$ to je $a - [a] \in [0, 1)$. Prema tome jedna prirodna transversala je interval $[0, 1)$.

Primer 4.29. Na skupu $\mathbb{R}$ data je relacija $\approx$ sa:

$$x \approx y \iff x - y \in \mathbb{Q}.$$

I ova relacija jeste ekvivalencija, a klasa broja a je, slično kao u prethodnom primeru, skup $\mathbb{Q}$ transliran za a : $[a] = a + \mathbb{Q}$. Do sada smo imali prirodne načine da odaberemo transversale, međutim u ovom slučaju, ako se malo udubimo, videćemo da to nije tako. I zaista, može se pokazati da ne postoji prirodan način da konstruišemo transversalu.

S obzirom da ne postoji način da konstruišemo prethodnu transversalu, prirodno je pitanje da li ona postoji. Odgovor daje *aksioma izbora*.

Aksioma 4.30 (Aksioma izbora). Svaka ekvivalencija ima transversalu.

Specijalne transversale relacije iz primera 4.29 nazivaju se Vitalijevi skupovi, i već kod njih vidimo prve čudne posledice aksiome izbora. Pogledajte odeljak 4.7*.

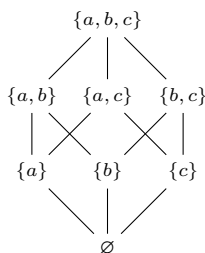
4.6 Uređenja

Definicija 4.31. Relacija $\preceq$ na skupu S je (*parcijalno*) *uređenje* (*poredak*) ako je refleksivna, antisimetrična i tranzitivna.

Osnovni primeri uređenja su $\leq$ na $\mathbb{R}$ ili $\subseteq$ na familijama skupova. Primetimo da za uređenja koristimo oznaku $\preceq$ koja bi trebalo da nas podseća na osnovne primere. Ako $a \preceq b$, element a doživljavamo kao manji (ili jednak) od b , a b veći (ili jednak) od a . Treba da naglasimo jednu bitnu razliku između proizvoljnog uređenja i primera $\leq$ na $\mathbb{R}$. Naime, $\leq$ na $\mathbb{R}$ ima i dodatnu osobinu *linearnosti*:

$$(L) \quad (\forall x, y \in S)(x \preceq y \vee y \preceq x) \quad (\text{linearnost})$$

koja kaže da za svaka dva elementa možemo da uporedimo koji je manji, a koji veći. Ovo u opštem slučaju ne važi, i npr. $\subseteq$ u opštem slučaju nema ovu osobinu. Npr. na skupu $\mathcal{P}(\{a, b, c\})$, skupove $\{a\}$ i $\{b\}$, ili $\{a\}$ i $\{b, c\}$, ili $\{a, b\}$ i $\{a, c\}$ ne možemo da uporedimo sa $\subseteq$. Kad smo kod ovog primera, naglasimo i da uređenja možemo da skiciramo na sledeći način:



Na prethodnom dijagramu crtamo manje skupove ispod većih i crticom naglašavamo koji skup je neposredno iznad nekog drugog. Kad god je moguće, ovako ćemo skicirati i druga uređenja. Na prethodnom dijagramu lako uočavamo i odgovarajuće parove neuporedivih elemenata.

Ako uređenje $\preceq$ zadovoljava i uslov linearnosti, kažemo da je $\preceq$ *linearno uređenje*.

Definicija 4.32. Relacija $\triangleleft$ na skupu S je *strogo* (*parcijalno*) *uređenje* (*poredak*) ako je irefleksivna, asimetrična i tranzitivna (ekvalentno samo irefleksivna i tranzitivna, ekvalentno samo asimetrična i tranzitivna).

Osnovni primeri strogog uređenja su $<$ na $\mathbb{R}$ ili $\subsetneq$ na familijama skupova. Strogo uređenje je *linearno* ako zadovoljava odgovarajući uslov linearnosti:

$$(L) \quad (\forall x, y \in S)(x \triangleleft y \vee x = y \vee y \triangleleft x) \quad (\text{linearnost})$$

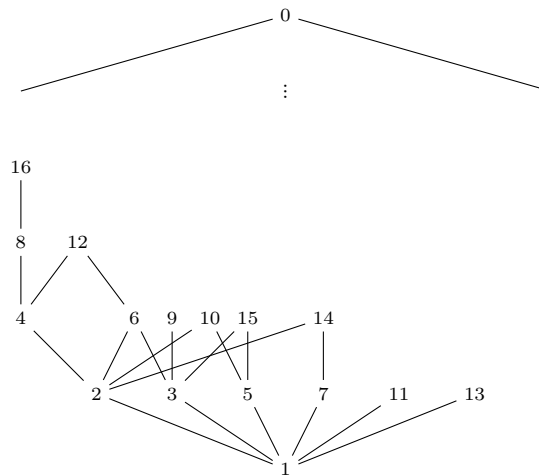
Svako uređenje ima prirodno pridruženo strogo uređenje, i obratno. Pridruživanje je dato na sledeći način:

uređenje	$\longleftrightarrow$	strogo uređenje
dato $\trianglelefteq$	$\longrightarrow$	$x \triangleleft y : \iff x \trianglelefteq y \wedge x \neq y$
$x \trianglelefteq y : \iff x \triangleleft y \vee x = y$	$\longleftarrow$	dato $\triangleleft$

Pridruženo (strogo) uređenje ima očekivane osobine. Npr. ako imamo uređenje $\trianglelefteq$ i pridruženo strogo uređenje $\triangleleft$, ako $a \trianglelefteq b$ i $b \triangleleft c$, onda $a \triangleleft c$, itd.

Primer 4.33. Relacija deljivosti $|$ na $\mathbb{N}$ definisana sa $a | b$ akko $b = ak$ za neko $k \in \mathbb{N}$ je uređenje. Refleksivnost, $a | a$, važi jer $a = a \cdot 1$. Tranzitivnost važi jer $a | b$ i $b | c$ povlači $b = ak$ i $c = bl$ za neke $k, l \in \mathbb{N}$, pa $c = a(kl)$ i $kl \in \mathbb{N}$ povlače $a | c$. Konačno, za antisimetričnost pretpostavimo $a | b$ i $b | a$, tj. $b = ak$ i $a = bl$ za neke $k, l \in \mathbb{N}$. Tada je $b = b(kl)$, tj. $b(1 - kl) = 0$. Ako je $b = 0$, onda je i $a = bl = 0$, i važi $a = b$, a ako je $1 - kl = 0$, tada je $kl = 1$, pa je $k = l = 1$ jer $k, l \in \mathbb{N}$; opet $a = bl = b$.

Primetimo da u smislu relacije deljivosti $a | b$ znači da je a manji a b veći element. Primetimo dve osobine. Za svako a važi $1 | a$ jer $a = 1 \cdot a$, kao i $a | 0$ jer $0 = a \cdot 0$. Dijagram ovog uređenja predstavljamo na sledeći način:



Naglasimo da je 0 na vrhu, veća od svih drugih elemenata.

Definicija 4.34. Neka je $\trianglelefteq$ uređenje na S , $A \subseteq S$ i $a \in S$.

Element a je *najmanji* element skupa A ako $a \in A$ i $(\forall x \in A) a \trianglelefteq x$.⁸

Element a je *minimalni* element skupa A ako $a \in A$ i $(\forall x \in A) x \not\triangleleft a$.⁹

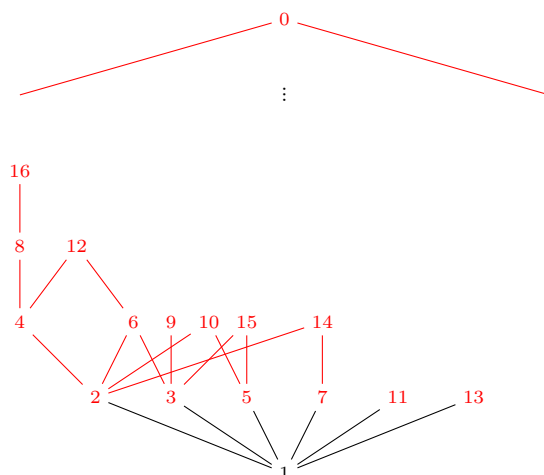
Dualno definujemo pojmove *najvećeg* i *maksimalnog* elementa.

Primer 4.35. Vratimo se na primer 4.33. Skup $A = \mathbb{N}$ ima najmanji element 1 jer $1 | a$ za sve $a \in \mathbb{N}$, kao i najveći element 0 jer $a | 0$ za sve $a \in \mathbb{N}$. Nijedan drugi element $a \neq 1$ nije najmanji jer ne deli 1, i nijedan drugi element $a \neq 0$ nije najveći jer ga ne deli 0. Takođe, jedino „ispod“ 1 ne postoje drugi elementi, što znači da je 1 i jedini minimalni element, kao i jedino „iznad“ 0 ne postoje drugi elementi, što znači da je 0 jedini maksimalni element.

Neka je sada $B = \mathbb{N} \setminus \{1\}$:

⁸Najmanji element u skupu je onaj koji je manji (ili jednak) od svih u tom skupu.

⁹Minimalni element u skupu je onaj od kojeg nijedan element iz tog skupa nije strogo manji.



Skup B nema više najmanji element jer bilo koji $a \neq 1$ ne deli sve preostale elemente u B , npr. $a \nmid a+1$. Međutim skup B ima beskonačno mnogo minimalnih elemenata: to su prosti brojevi. Jedino ispod njih nema drugih „crvenih“ elemenata.

Skup $C = \mathbb{N} \setminus \{0\}$ nema najveći element, ali nema ni maksimalne elemente. Zaista, za $a \neq 0$ važi $a \mid 2a$ i $a \neq 2a$, pa a nije veći od $2a$, što znači da a nije najveći, i od a je strogo veći $2a$, što znači da a nije maksimalan.

Tvrđenje 4.36. Neka je $\preceq$ uređenje na S i $A \subseteq S$.

- (i) Najmanji element skupa A , ako postoji, jedinstven je.
- (ii) Najmanji element skupa A , ako postoji, je jedini minimalni element skupa A .
- (iii) Ako je A lanac¹⁰, minimalni element skupa A , ako postoji, je i najmanji element skupa A .

Analogno važi i ako termine najmanji/minimalni zamenimo sa najveći/maksimalni.

Dokaz. (i) Pretpostavimo da su $a, b \in A$ najmanji elementi. Tada je $a \preceq b$ jer je a najmanji, pa je manji i od b , i $b \preceq a$ jer je b najmanji, pa je manji i od a . Zbog asimetričnosti $a = b$. Dakle, ako postoji, najmanji element je jedinstven.

(ii) Pretpostavimo da je $a \in A$ najmanji element. Za svako $x \in A$ tada važi $a \preceq x$, pa nije $x \prec a$, što znači da a jeste minimalan. Da bismo videli da je jedini minimalan pretpostavimo da je $b \in A$ minimalan element. Tada je $a \preceq b$ jer je a najmanji, pa je manji i od b , ali $a \not\prec b$ jer je b minimalni pa ništa, ni a , nije strogo manje od njega. Prema tome $a = b$ i zaključujemo da je a jedini minimalni u A .

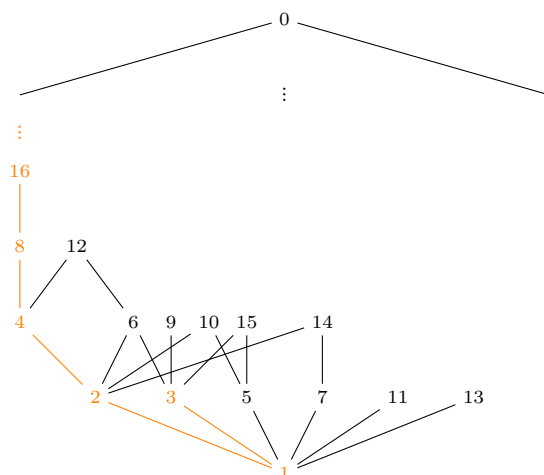
(iii) Pretpostavimo da je A lanac i da je $a \in A$ minimalni element. Tada za sve $x \in A$ važi $x \not\prec a$, ali kako je A lanac, x je uporediv sa a , pa mora biti $a \preceq x$. Dakle, a je najmanji u A . $\square$

Definicija 4.37. Ako postoji, najmanji element skupa A obeležavamo sa $\min(A)$, a najveći element sa $\max(A)$.¹¹

Primer 4.38. Prethodno tvrđenje povlači da ako skup A nema minimalne (maksimalne) elemente, ili ima bar dva minimalna (maksimalna) elementa, onda A ne može da ima najmanji (najveći) element. Ostaje otvoreno pitanje da li je moguće da A ima jedinstveni minimalni (maksimalni) element, a da ipak nema najmanji (najveći). Odgovor je pozitivan. Npr. uočimo u primeru 4.33 skup $A = \{2^n \mid n \geq 0\} \cup \{3\}$:

¹⁰Skup A je lanac ako su svaka dva njegova elementa uporediva.

¹¹Oznake $\min$ i $\max$ su skraćenice za *minimum* i *maksimum*, što su sinonimi za najmanji i najveći element, i ne treba mešati ove termine sa minimalan i maksimalan.



Skup A ima jedinstveni maksimalni element 3, ali on nije najveći.

Tvrđenje 4.39. Neka je $\leq$ uređenje na S i $A \subseteq S$ je neprazan konačan podskup. Tada A ima minimalan element (i slično, ima i maksimalan element).

Dokaz. Dokaz možemo izvesti indukcijom po broju elemenata n u skupu A . Ako je $n = 1$, tj. $A = \{a\}$, a je očigledno minimalan element u A . Pretpostavimo da A ima $n + 1$ element i izaberimo proizvoljni element $a \in A$. Ako je a slučajno minimalan, završili smo posao. Pretpostavimo da a nije minimalan, pa postoji $a' \in A$ takav da $a' \triangleleft a$. Po indukcijskoj hipotezi skup $A \setminus \{a\}$ ima minimalan element b , što znači da nijedan element u A različit od a nije strogo manji od b . Prema tome $a' \not\triangleleft b$, pa kako $a' \triangleleft a$, mora biti i $a \not\triangleleft b$. To znači da nijedan element u A nije strogo manji od b (za elemente različite od a to važi po izboru b , a sad smo videli da važi i za a), pa je b minimalan u A . $\square$

Definicija 4.40. Neka je $\leq$ uređenje na S i $A \subseteq S$.

Element $a \in S$ je *donje ograničenje* za A ako $(\forall x \in A) a \leq x$. Skup svih donjih ograničenja skupa A obeležavamo sa A^- .

Element $a \in S$ je *infimum* skupa A ako je najveće donje ograničenje, tj. $a = \max(A^-)$.

Dualno definišemo pojam *gornjeg ograničenja*, skup A^+ i pojam *supremuma*.

Komentar 4.41. Po definiciji ako neko donje ograničenje od A pripada A , ono je najmanji element skupa A . Takođe, ako infimum skupa A postoji, mora biti jedinstven (jer je $\max(A^-)$ jedinstven). Infimum skupa A obeležavamo sa $\inf(A)$; supremum skupa A obeležavamo sa $\sup(A)$.

Dakle, po definiciji, $\inf(A) = \max(A^-)$ i $\sup(A) = \min(A^+)$.

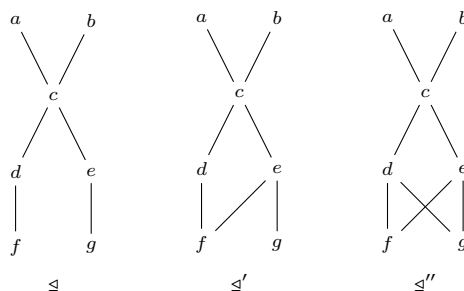
Zadatak 4.42. Neka je $\leq$ uređenje na S i $A \subseteq S$.

- (i) Ako postoji $\min(A)$, onda je $\inf(A) = \min(A)$.
- (ii) Ako postoji $\inf(A)$ i $\inf(A) \in A$, onda je $\min(A) = \inf(A)$.

Analogno važi i ako $\min/\inf$ zamenimo sa $\max/\sup$.

Primer 4.43. Vratimo se na primer 4.33. Uočimo $A = \{4, 6\}$. Tada je A^- skup zajedničkih delioca brojeva 4 i 6, $A^- = \{1, 2\}$, pa je $\inf(A) = \max(A^-) = 2$. Naglasimo da je infimum od A najveći među donjim ograničenjima, tj. zajedničkim deliocima, od A , pa je $\inf(A)$ zapravo NZD brojeva 4 i 6. Slično, gornja ograničenja skupa A su zajednički sadržaoци brojeva 4 i 6, tj. $A^+ = \{12n \mid n \in \mathbb{N}\}$, pa je $\sup(A) = \min(A^+) = 12$, što je NZS brojeva 4 i 6.

Primer 4.44. Na skupu $\{a, b, c, d, e, f, g\}$ imamo tri uređenja data dijagramima:



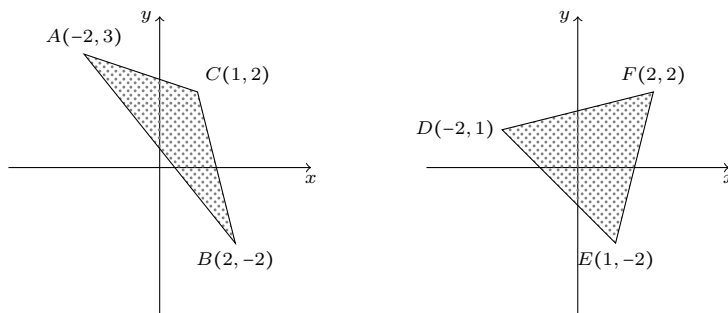
U sva tri slučaja, skup $A = \{c, d, e\}$ ima najveći element $\max(A) = c$ i dva minimalna elementa d i e . Skup $A^+ = \{a, b, c\}$ i on ima najmanji element c , pa je $\sup(A) = \min(A^+) = c = \max(A)$.

Što se tiče donjih ograničenja $A_{\preceq}^- = \emptyset$, $A_{\preceq'}^- = \{f\}$ i $A_{\preceq''}^- = \{f, g\}$. Prema tome $\inf_{\preceq}(A)$ ne postoji jer je $A_{\preceq}^-$ prazan, $\inf_{\preceq'}(A) = \max(A_{\preceq'}^-) = f$, a $\inf_{\preceq''}(A)$ ponovo ne postoji jer $A_{\preceq''}^-$, iako neprazan, nema najveći element (ima dva maksimalna elementa).

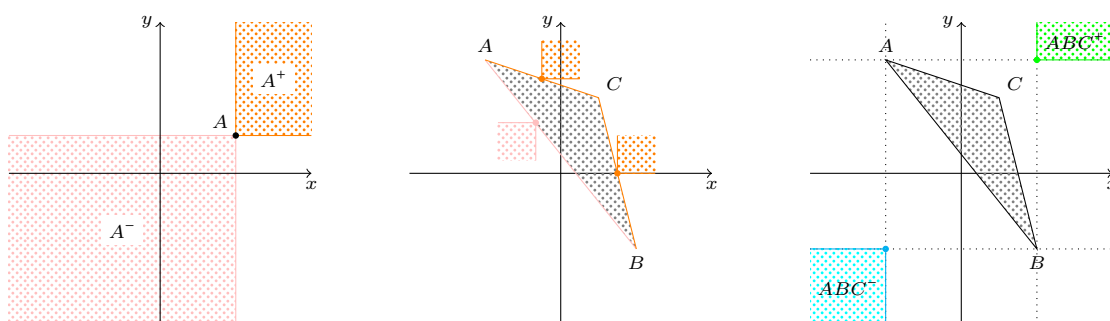
Primer 4.45. U realnoj ravni definišemo uređenje $\preceq$ sa:

$$(x_1, y_1) \preceq (x_2, y_2) \quad :\Longleftrightarrow \quad x_1 \leq x_2 \wedge y_1 \leq y_2.$$

(Nije teško videti da je $\preceq$ zaista uređenje na $\mathbb{R} \times \mathbb{R}$.) Odredimo značajne tačke trouglova:



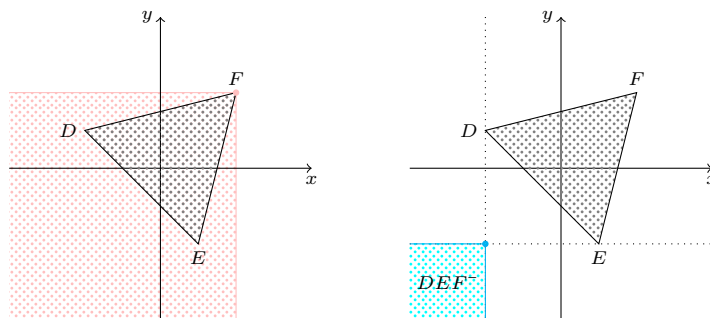
Šta na slici znači da je tačka A manja od tačke B ? To znači da je A „levo-dole“ u odnosu na B jer su joj obe koordinate manje od koordinata tačke B . Dakle, skup manjih tačaka od A , A^- , i skup većih tačaka od A , A^+ su (slika levo):



Pogledajmo sliku u sredini. Primetimo da od tačaka na stranici AB , i samo od njih, nijedna tačka trougla nije storgo manja, kao i da od tačaka na stranicama AC i BC , i samo od njih, nijedna tačka trougla nije strogo veća. To znači da su tačke duži AB minimalni elementi trougla ABC u našem uređenju, a da su tačke duži AC i BC maksimalni elementi trougla ABC . Prema tome trougao ABC nema ni najmanji ni najveći element jer ima beskonačno mnogo minimalnih i maksimalnih elemenata. Primetimo i da su tačke A i B dve tačke trougla koje su ujedno i minimalne i maksimalne.

Da bismo sračunali infimum i supremum trougla ABC treba da sračunamo ABC^- i ABC^+ . Pogledjamo sliku desno. Donje ograničenje trougla ABC mora da bude levlje od njegove najlevlje tačke i ispod od njegove najniže tačke, pa vidimo da je $ABC^- = \{(x, y) \mid x \leq -2, y \leq -2\}$. Ovaj skup ima najveći element i to je baš tačka $(-2, -2)$, pa je $\inf(ABC) = (-2, -2)$. Na sličan način vidimo da je $\sup(ABC) = (2, 3)$.

Što se tiče trougla DEF , slično kao malopre vidimo da su njegovi minimalni elementi tačke stranice DE , pa najmanji element ne postoji. Sa druge strane, teme F jeste najveći element trougla DEF , pa i jedini makismalni i supremum trougla (slika levo):



Infimum računamo slično kao kod trougla ABC i vidimo $\inf(DEF) = (-2, -2)$.

4.7* Vitalijev skup

Vratimo se na primer 4.29. Na $\mathbb{R}$ imamo definisanu ekvivalenciju $\approx$ sa $x \approx y$ akko $x - y \in \mathbb{Q}$. Po aksiomi izbora ova relacija ima bar jednu transversalu T . Možemo da pretpostavimo da je $T \subseteq [0, 1]$. Zaista, izabranog predstavnika svoje klase $t \in T$ možemo zameniti sa predstavnikom iste klase $t - [t] \in [0, 1]$ (primetimo $t \approx t - [t]$ jer $t - (t - [t]) = [t] \in \mathbb{Z} \subseteq \mathbb{Q}$), pa zamenom T sa $\{t - [t] \mid t \in T\}$ možemo pretpostaviti $T \subseteq [0, 1]$.

Želimo da odgovorimo na sledeće pitanje: Da li je moguće izračunati dužinu skupa T ?

Nećemo ulaziti u zasnivanje pojma mere (konkretno dužine), navešćemo samo nekoliko prirodnih osobina koje bi dužina trebalo da ima, a biće nam dovoljni da završimo ovaj primer. Označimo sa $\lambda(S)$ dužinu skupa $S \subseteq \mathbb{R}$; jasno je da $\lambda(S) \in [0, +\infty]$. Razne podskupove od $\mathbb{R}$ merimo na prirodan način. Uzimamo da je svaka tačka dužine nula. Dužina intervala (a, b) je $\lambda((a, b)) = b - a$. Prirodno uzimamo da je dužina konačno mnogo disjunktних skupova jednaka zbiru njihovih dužina: $\lambda(\bigcup_{i=1}^n S_i) = \sum_{i=1}^n \lambda(S_i)$ ako su S_i međusobno disjunktne. Takođe, prirodno uzimamo da je dužina translatorno invarijantna, što znači da je dužina skupa $a + S$, koji je dobijen translacijom skupa S za a , jednaka dužini skupa S : $\lambda(a + S) = \lambda(S)$. Konačno, podskupovi nekog skupa bi prirodno trebalo da su manje dužine: ako $S \subseteq S'$ onda $\lambda(S) \leq \lambda(S')$.

Skrećemo pažnju na još jednu činjenicu. Pretpostavimo da imamo međusobno disjunktne skupove $S_1, S_2, S_3, \dots$. Kako smo već naglasili dužina skupa $\bigcup_{i=1}^n S_i$ jednaka je $\sum_{i=1}^n \lambda(S_i)$, pa je prirodno da je dužina skupa $S = \bigcup_{i=1}^{\infty} S_i$ jednaka

$$\lambda(S) = \lim_{n \rightarrow \infty} \lambda\left(\bigcup_{i=1}^n S_i\right) = \lim_{n \rightarrow \infty} \sum_{i=1}^n \lambda(S_i).$$

Sve prethodno važi pod pretpostavkom da su odgovarajuće dužine definisane.

Vratimo se na transversalu $T \subseteq [0, 1]$ ekvivalencije $\approx$. Dokazaćemo da ne možemo da izmerimo dužinu skupa T . Pretpostavimo suprotno, $\lambda(T) = \epsilon$; jasno $\epsilon \geq 0$, kao i $\epsilon \leq 1$ jer $T \subseteq [0, 1]$.

Neka je $\mathbb{Q} \cap (-1, 1) = \{q_1, q_2, q_3, \dots\}$.¹² Neka je $T_i = q_i + T$ - skup T transliran za q_i ; za sve i je $\lambda(T_i) = \lambda(q_i + T) = \lambda(T) = \epsilon$. Primetimo da za različite i, j imamo $T_i \cap T_j = \emptyset$. Zaista, ako $x \in T_i \cap T_j$, tada je $x = q_i + t' = q_j + t''$ za neke $t', t'' \in T$, pa je $t' - t'' = q_j - q_i \in \mathbb{Q}$, odakle $t' \approx t''$, pa kako je T transversala mora biti $t' = t''$, odakle je i $q_i = q_j$, pa i $i = j$. Prema tome, $\lambda(\bigcup_{i=1}^n T_i) = n\epsilon$. Uočimo skup $S = \bigcup_{i=1}^{\infty} T_i$. Njegova dužina je

$$\lambda(S) = \lim_{n \rightarrow \infty} \lambda\left(\bigcup_{i=1}^n T_i\right) = \lim_{n \rightarrow \infty} n\epsilon, \text{ što je } 0 \text{ ako je } \epsilon = 0 \text{ i } \infty \text{ ako je } \epsilon > 0.$$

Primetimo da je $(0, 1) \subseteq S$. Zaista, ako $x \in (0, 1)$, izaberimo $t \in T$ tako da $x \approx t$. Tada je $x - t \in \mathbb{Q}$. Kako je jasno i $x - t \in (-1, 1)$, $x - t$ jednak je nekom q_i , pa je $x = q_i + t \in T_i$, odakle, $x \in S$. Ovo znači da je $\lambda(S) \geq 1$, što eliminiše slučaj $\epsilon = 0$.

¹²Videćemo da je skup $\mathbb{Q} \cap (-1, 1)$ prebrojiv, što znači da možemo nabrojati njegove elemente.

Sa druge strane, kako je $T \subseteq [0, 1)$ i svaki $q_i \in (-1, 1)$, translat $T_i = q_i + T$ sadržan je u $(-1, 2)$. Prema tome i cela unija S sadržana je u ovom intervalu, a to znači da $\lambda(S) \leq 3$. Ovo eliminiše slučaj $\epsilon > 0$.

Dakle, ako pretpostavimo da možemo da izmerimo dužinu od T , dolazimo do kontradikcije, pa zaključujemo da skup T ne može da ima definisanu dužinu.

Skup T zove se *Vitalijev skup*.

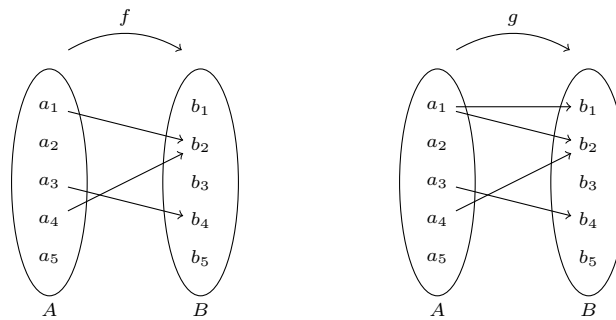
5 Funkcije

5.1 Funkcionalne relacije

Definicija 5.1. Relacija $f \subseteq A \times B$ je *funkcionalna* ili *parcijalna funkcija* ako:

$$(\forall a \in A)(\forall b_1, b_2 \in B)(a f b_1 \wedge a f b_2 \rightarrow b_1 = b_2).$$

Na grafu to znači da iz svakog elementa skupa A izlazi najviše jedna f -strelica ka B . Pogledajmo sliku:



Relacija f jeste funkcionalna; iz elemenata a_1, a_3, a_4 izlazi po jedna strelica dok iz elemenata a_2, a_5 ne izlazi nijedna. Sa druge strane, relacija g nije funkcionalna jer iz elementa a_1 izlaze dve strelice.

Definicija 5.2. Neka je $f \subseteq A \times B$ funkcionalna relacija.

- Ako iz $a \in A$ izlazi strelica ka (jedinstvenom) elementu $b \in B$, pišemo $b = f(a)$ i kažemo da je b *slika* elementa a . U tom slučaju, ako iz a izlazi strelica, pišemo i $f(a) \downarrow$ i čitamo $f(a)$ je *definisan*.
- Ako iz $a \in A$ ne izlazi strelica pišemo $f(a) \uparrow$ i čitamo $f(a)$ je *nedefinisan*.
- *Domen* funkcionalne relacije f je skup $\text{Dom}(f) = \{a \in A \mid f(a) \downarrow\}$ – skup svih elemenata iz kojih izlazi strelica.
- *Slika* funkcionalne relacije f je skup $\text{Im}(f) = \{f(a) \mid a \in \text{Dom}(f)\}$ – skup svih slika elemenata iz domena.

U gornjem primeru je $f(a_1) = b_2$, $f(a_2) \uparrow$, $f(a_3) = b_4$, $f(a_4) = b_2$, $f(a_5) \uparrow$, $\text{Dom}(f) = \{a_1, a_3, a_4\}$ i $\text{Im}(f) = \{b_2, b_4\}$.

Primer 5.3. Uočimo sledeće relacije na skupu $\mathbb{R}$:

- $f = \{(x, x^2) \mid x \in \mathbb{R}\};$
- $h = \{(x^2, x) \mid x \geq 0\};$
- $g = \{(x^2, x) \mid x \in \mathbb{R}\};$
- $k = \{(x^2, x) \mid x < -2\}.$

Relacija f jeste funkcionalna. Naime, ako $a f b_1$ i $a f b_2$, onda za neko $x \in \mathbb{R}$ važi $a = x$, $b_1 = x^2$ i $b_2 = x^2$, pa je $b_1 = b_2$. Time smo proverili definiciju funkcionalnosti. Očigledno je za svako $x \in \mathbb{R}$, $f(x) = x^2$, pa je $\text{Dom}(f) = \mathbb{R}$. Sa druge strane, $\text{Im}(f) = \{x^2 \mid x \in \mathbb{R}\} = [0, +\infty)$.

Ako $a g b_1$ i $a g b_2$, onda za neke $x_1, x_2 \in \mathbb{R}$ imamo $a = x_1^2$, $b = x_1$, $a = x_2^2$ i $b = x_2$. Odatle je $x_1^2 = x_2^2$, što ne povlači obavezno $x_1 = x_2$, tj. $b_1 = b_2$. Npr. važi $4 g 2$ i $4 g -2$, ali $2 \neq -2$, pa relacija g nije funkcionalna.

Ako $a h b_1$ i $a h b_2$, onda za neke $x_1, x_2 \geq 0$ imamo $a = x_1^2$, $b = x_1$, $a = x_2^2$ i $b = x_2$. Ponovo je $x_1^2 = x_2^2$, ali kako su $x_1, x_2 \geq 0$, sada važi $x_1 = x_2$, tj. $b_1 = b_2$. Prema tome h jeste funkcionalna. Broj a pripada domenu akko je kvadrat nenegativnog broja, pa je $\text{Dom}(h) = [0, +\infty)$. Za $a \in \text{Dom}(h)$, lako vidimo da je $h(a) = \sqrt{a}$ (jer je a kvadrat broja $h(a)$ koji je nenegativan). Prema tome i $\text{Im}(h) = [0, +\infty)$.

Slično kao u prethodnom pasusu, ako $a k b_1$ i $a k b_2$, onda za neke $x_1, x_2 < -2$ imamo $a = x_1^2$, $b = x_1$, $a = x_2^2$ i $b = x_2$. Odatle je $x_1^2 = x_2^2$, ali kako su $x_1, x_2 < -2$, opet važi $x_1 = x_2$, tj. $b_1 = b_2$. Prema tome i k jeste funkcionalna. Broj a pripada domenu akko je kvadrat broja manjeg od -2 , pa je $\text{Dom}(k) = (-\infty, -2)$. Za $a \in \text{Dom}(k)$, lako vidimo da je $k(a) = -\sqrt{a}$ (jer je a kvadrat broja $k(a)$ koji je manji od -2). Prema tome, $\text{Im}(k) = (-\infty, -2)$.

Tvrđenje 5.4. Neka su $f \subseteq A \times B$ i $g \subseteq B \times C$ funkcionalne relacije. Znamo $g \circ f \subseteq A \times C$.

- (i) Relacija $g \circ f$ je funkcionalna.
- (ii) $g \circ f(a) \downarrow$ akko $f(a) \downarrow$ i $g(f(a)) \downarrow$, i tada $g \circ f(a) = g(f(a))$.

Dokaz. (i) Neka $a g \circ f c_1$ i $a g \circ f c_2$. Tada za neke $b_1, b_2 \in B$ imamo $a f b_1 g c_1$ i $a f b_2 g c_2$. Iz $a f b_1$ i $a f b_2$ zaključujemo $b_1 = b_2 =: b$ jer je f funkcionalna. Sada imamo $b g c_1$ i $b g c_2$, odakle zaključujemo i $c_1 = c_2$ jer je g funkcionalna. Dakle, $g \circ f$ je funkcionalna.

(ii) Očigledno. □

Zadatak 5.5. Dati primere relacija $f \subseteq A \times B$ i $g \subseteq B \times C$ takve da:

- $g \circ f$ jeste, ali f i g nisu funkcionalne;
- f i $g \circ f$ jesu, ali g nije funkcionalna;
- g i $g \circ f$ jesu, ali f nije funkcionalna.

Komentar 5.6. Neka je $f \subseteq A \times B$. Relacija $f^{-1} \subseteq B \times A$ je funkcionalna po definiciji akko $(\forall b)(\forall a_1, a_2 \in A)(b f^{-1} a_1 \wedge b f^{-1} a_2 \rightarrow a_1 = a_2)$, što je ekvivalentno sa:

$$(\forall a_1, a_2 \in A)(\forall b \in B)(a_1 f b \wedge a_2 f b \rightarrow a_1 = a_2).$$

Čak i ako je f funkcionalna, f^{-1} ne mora biti. Npr. funkcionalna relacija f skicirana na početku odeljka nema funkcionalni inverz jer je $f^{-1} = \{(b_2, a_1), (b_2, a_4), (b_4, a_3)\}$, pa iz b_2 izlaze dve f^{-1} -strelice.

5.2 Funkcije

Definicija 5.7. Relacija $f \subseteq A \times B$ je *funkcija*, u oznaci $f : A \rightarrow B$, ako je f funkcionalna i $\text{Dom}(f) = A$. Drugim rečima, ako iz svakog elementa $a \in A$ izlazi tačno jedna strelica ka B , tj. za svako $a \in A$, $f(a) \downarrow$.

Kada govorimo o funkciji $f : A \rightarrow B$, skup B zovemo *kodomen* funkcije f .

Komentar 5.8. Kada govorimo o jednakosti dve funkcije uvek ćemo podrazumevati da govorimo o funkcijama sa istim domenom i kodomenom. Preciznije, funkcije $f : A \rightarrow B$ i $g : A' \rightarrow B'$ su jednake ako $A = A'$, $B = B'$, i f i g su jednake kao relacije.

Tvrđenje 5.9. Ako je $f : A \rightarrow B$ i $g : B \rightarrow C$, onda je $g \circ f : A \rightarrow C$.

Dokaz. Prema tvrđenju 5.4 kompozicija $g \circ f$ jeste funkcionalna relacija. Takođe, za $a \in A$, $g \circ f(a) \downarrow$ akko $f(a) \downarrow$ i $g(f(a)) \downarrow$. Kako je $\text{Dom}(f) = A$ to $f(a) \downarrow$, a kako je $\text{Dom}(g) = B$ to i $g(f(a)) \downarrow$, pa prema tome i $g \circ f(a) \downarrow$. Dakle, $\text{Dom}(g \circ f) = A$ i zaključujemo $g \circ f : A \rightarrow C$. □

Definicija 5.10. *Identiteta* na skupu A je funkcija $\text{id}_A : A \rightarrow A$ definisana sa $\text{id}_A(a) = a$ za sve $a \in A$. Ako je $A \subseteq B$, *inkluzija* iz A u B je funkcija $i_{A,B} : A \rightarrow B$ definisana sa $i_{A,B}(a) = a$ za sve $a \in A$.

Ako je $f : A \rightarrow B$ primetimo da su definisane kompozicije $\text{id}_B \circ f : A \rightarrow B$ i $f \circ \text{id}_A : A \rightarrow B$, i obe su jednake sa f . Ako je dodatno $C \subseteq A$, definisana je kompozicija $f \circ i_{C,A} : C \rightarrow B$ i za svako $c \in C$ važi $f \circ i_{C,A}(c) = f(c)$; funkcija $f \circ i_{C,A}$ zove se *restrikcija* funkcije f na C i češće se obeležava sa $f|_C$.

Ponekad će biti zgodno i da smanjimo kodomen funkcije $f : A \rightarrow B$. Preciznije, ako je skup D takav da $\text{Im}(f) \subseteq D \subseteq B$, imamo korektno definisanu funkciju $f' : A \rightarrow D$ sa $f'(a) = f(a)$ za sve $a \in A$. Ovako definisana funkcija ponekad se zove *korestrikcija na D* . Najčešće, kada posmatramo neku korestrikciju, u pitanju je korestrikcija na sliku (tj. $D = \text{Im}(f)$).

Komentar 5.11. Formalno, prazna relacija jeste funkcija $\emptyset : \emptyset \rightarrow B$ za bilo koje B . Međutim, kada govorimo o funkciji $f : A \rightarrow B$ uvek ćemo implicitno pretpostavljati da je $A \neq \emptyset$ (što povlači i da je f neprazna relacija jer $\text{Dom}(f) = A$, kao i $B \neq \emptyset$ jer za svako $a \in A$, a bar jedno takvo postoji, $f(a) \in B$).

5.3 1-1 i na funkcije, bijekcije

Definicija 5.12. Neka je $f : A \rightarrow B$. Funkcija f je:

- *1-1* ili *injekcija* ako:

$$(\forall a_1, a_2 \in A)(a_1 \neq a_2 \rightarrow f(a_1) \neq f(a_2)),$$

ili, po kontrapoziciji evivalentno:

$$(\forall a_1, a_2 \in A)(f(a_1) = f(a_2) \rightarrow a_1 = a_2);$$

- *na* ili *surjekcija* ako $\text{Im}(f) = B$, tj. ako:

$$(\forall b \in B)(\exists a \in A) f(a) = b;$$

- *bijekcija* ako je 1-1 i na.

Komentar 5.13. Primetimo da je $\text{id}_A : A \rightarrow A$ uvek bijekcija, dok je, za $A \subseteq B$, funkcija $i_{A,B} : A \rightarrow B$ uvek 1-1.

Neka je $f : A \rightarrow B$ funkcija. Primetimo da je korestrikcija funkcije f na $\text{Im}(f)$, tj. funkcija $f' : A \rightarrow \text{Im}(f)$ data sa $f'(a) = f(a)$ za sve $a \in A$, uvek na. Takođe, ako je dodatno f 1-1, korestrikcija f' je bijekcija.

Tvrđenje 5.14. Neka $f : A \rightarrow B$ i $g : B \rightarrow C$; znamo $g \circ f : A \rightarrow C$. Tada:

- (i) ako su f i g 1-1, onda je i $g \circ f$ 1-1;
- (ii) ako su f i g na, onda je i $g \circ f$ na;
- (iii) ako su f i g bijekcije, onda je i $g \circ f$ bijekcija;
- (iv) ako je $g \circ f$ 1-1, onda je i f 1-1;
- (v) ako je $g \circ f$ na, onda je i g na.

Dokaz. (i) Neka su $a_1, a_2 \in A$ različiti: $a_1 \neq a_2$. Tada je i $f(a_1) \neq f(a_2)$ jer je f 1-1. Odatle je i $g(f(a_1)) \neq g(f(a_2))$ jer je g 1-1. Dakle, $g \circ f(a_1) \neq g \circ f(a_2)$. Prema tome, $g \circ f$ je 1-1.

(ii) Neka je $c \in C$ proizvoljan element. Kako je g na, $c = g(b)$ za neko $b \in B$. Kako je f na, $b = f(a)$ za neko $a \in A$. Prema tome je $c = g(b) = g(f(a)) = g \circ f(a)$. Dakle, $g \circ f$ je na.

(iii) Ovo sada sledi direktno iz (i) i (ii).

(iv) Neka su $a_1, a_2 \in A$ različiti: $a_1 \neq a_2$. Tada je i $g \circ f(a_1) \neq g \circ f(a_2)$ jer je $g \circ f$ 1-1, tj. $g(f(a_1)) \neq g(f(a_2))$. Kako je g funkcija, odatle je $f(a_1) \neq f(a_2)$. Dakle, f je 1-1.

(v) Neka je $c \in C$ proizvoljno. Tada je $c = g \circ f(a)$ za neko $a \in A$, tj. $c = g(f(a))$. Dakle, g je na. □

Primer 5.15. U (iv) i (v) iz prethodnog primera ne možemo ništa više reći. Npr. funkcija $f : \mathbb{N} \rightarrow \mathbb{N}$ data sa $f(n) = n + 1$ jeste 1-1, ali nije na (jer $0 \notin \text{Im}(f)$), funkcija $g : \mathbb{N} \rightarrow \mathbb{N}$ data sa $g(n) = \begin{cases} n-1 & \text{ako } n > 0 \\ 0 & \text{ako } n = 0 \end{cases}$ jeste na, ali nije 1-1 (jer $g(0) = g(1)$). Ipak, kako je $g \circ f(n) = g(f(n)) = g(n+1) = n$, funkcija $g \circ f$ jednaka je sa $\text{id}_{\mathbb{N}}$, pa je bijekcija.

Tvrđenje 5.16. Neka je $f : A \rightarrow B$. Svakako, f^{-1} je relacija između B i A .

- (i) f^{-1} je funkcionalna relacija akko f je 1-1;
- (ii) $f^{-1} : B \rightarrow A$ akko f je bijekcija.

Dokaz. (i) Ovo sledi jer f^{-1} je funkcionalna relacija akko $(\forall b \in B, a_1, a_2 \in A)(b f^{-1} a_1 \wedge b f^{-1} a_2 \rightarrow a_1 = a_2)$, akko $(\forall b \in B, a_1, a_2 \in A)(a_1 f b \wedge a_2 f b \rightarrow a_1 = a_2)$, akko $(\forall a_1, a_2 \in A)(f(a_1) = f(a_2) \rightarrow a_1 = a_2)$, akko f je 1-1.

(ii) Ako $f^{-1} : B \rightarrow A$, prema (i) f je 1-1, ali i $\text{Im}(f) = \text{Dom}(f^{-1}) = B$, tj. f je na. Ako je f bijekcija, f^{-1} je funkcionalna prema (i), a takođe je $\text{Dom}(f^{-1}) = \text{Im}(f) = A$ jer je f na. $\square$

Komentar 5.17. Pretpostavimo $f : A \rightarrow B$ je bijekcija, tj. $f^{-1} : B \rightarrow A$. Primetimo $f(a) = b$ akko $f^{-1}(b) = a$. Oдавde lako vidimo $f^{-1} \circ f = \text{id}_A$ i $f \circ f^{-1} = \text{id}_B$. Primetimo i da je tada f^{-1} takođe i bijekcija (jer je $(f^{-1})^{-1} = f : A \rightarrow B$).

5.4 Egzistencija inverzne funkcije

Definicija 5.18. Neka je $f : A \rightarrow B$. Funkcija $g : B \rightarrow A$ je:

- *levi inverz* od f ako je $g \circ f = \text{id}_A$;
- *desni inverz* od f ako je $f \circ g = \text{id}_B$;
- *inverz* od f ako je $g \circ f = \text{id}_A$ i $f \circ g = \text{id}_B$.

Komentar 5.19. Jasno je da ako je g levi (odn. desni) inverz funkcije f , onda je f desni (odn. levi) inverz funkcije g , kao i da ako je g inverz od f onda je f inverz od g .

Ako je g levi inverz od f , tj. ako je $g \circ f = \text{id}_A$, prema tvrđenju 5.14 f mora biti 1-1 (a g mora biti na). Slično ako je g desni inverz od f , f mora biti na (a g mora biti 1-1). Ako je g inverz od f , obe moraju biti bijekcije. Pokazaćemo da ovi potrebni uslovi zaista jesu i dovoljni za egzistenciju odgovarajućeg inverza.

Teorema 5.20. Neka je $f : A \rightarrow B$. Tada:

- (i) f ima levi inverz akko f je 1-1;
- (ii) f ima desni inverz akko f je na;
- (iii) f ima inverz akko f je bijekcija. U tom slučaju, inverz je jedinstven i jednak je f^{-1} .

Dokaz. (i) U prethodnom komentaru videli smo da je uslov 1-1 potreban za egzistenciju levog inverza, pa dokažimo da je i dovoljan. Neka je $f : A \xrightarrow{1-1} B$. Tada je relacija f^{-1} funkcionalna. Izaberimo proizvoljno $a_0 \in A$. (Setimo se da implicitno pretpostavljamo, kada govorimo o funkcijama, da je domen neprazan, pa a_0 možemo da izaberemo.) Definišimo $g : B \rightarrow A$ na sledeći način:

$$g(b) := \begin{cases} f^{-1}(b) & \text{ako } b \in \text{Im}(f) \\ a_0 & \text{ako } b \notin \text{Im}(f) \end{cases}, \text{ za } b \in B.$$

(Naglasimo da oznaku $f^{-1}(b)$ smemo da koristimo jer je f^{-1} funkcionalna relacija.) Primetimo da je funkcija g definisana za svako $b \in B$, jer ako $b \in \text{Im}(f)$, onda $f^{-1}(b) \downarrow$. Za proizvoljno $a \in A$ imamo $g \circ f(a) = g(f(a)) = f^{-1}(f(a)) = a$, gde druga jednakost važi jer očigledno $f(a) \in \text{Im}(f)$. Dakle, $g \circ f = \text{id}_A$, pa f ima levi inverz.

(ii) Videli smo da je uslov na potreban da f ima desni inverz, pa dokazujemo da je dovoljan. Neka je $f : A \xrightarrow{na} B$. Za $b \in B$ uočimo skup $S_b := \{a \in A \mid f(a) = b\}$. Kako je f na, svaki od skupova S_b je neprazan. Definišimo $g : B \rightarrow A$ na sledeći način:

$$g(b) := \text{neki element skupa } S_b, \text{ za } b \in B.$$

Kako je $g(b) \in S_b$, to je $f(g(b)) = b$, tj. $f \circ g(b) = b$. Dakle, $f \circ g = \text{id}_B$, pa f ima desni inverz.

(iii) U prethodnom komentaru smo videli da je biti bijekcija potreban uslov da f ima inverz, pa dokazujemo da je i dovoljan. Neka je $f : A \xrightarrow{bij.} B$. Prema tvrđenju 5.16, $f^{-1} : B \rightarrow A$, a prema komentaru 5.17, f^{-1} zadovoljava uslove da bude inverz od f . Dakle, f ima inverz. Ostaje da dokažemo da je on jedinstven. Neka je $g : B \rightarrow A$ inverz od f : $g \circ f = \text{id}_A$ i $f \circ g = \text{id}_B$. Tada je:

$$g = g \circ \text{id}_B = g \circ (f \circ f^{-1}) = (g \circ f) \circ f^{-1} = \text{id}_A \circ f^{-1} = f^{-1},$$

što dokazuje jedinstvenost inverza. □

Komentar 5.21. U dokazu jedinstvenosti u (iii), u argumentu nismo koristili jednakost $f \circ g = \text{id}_B$, pa smo zapravo dokazali više: ako je f bijekcija, ona ima jedinstveni levi inverz. Slično možemo da dokažemo i: ako je f bijekcija, ona ima jedinstveni desni inverz.

Primer 5.22. Funkcija $f : \mathbb{N} \rightarrow \mathbb{N}$ data sa $f(n) = n + 1$ jeste 1-1 (ali nije na). Primetimo da su sve funkcije $g_a : \mathbb{N} \rightarrow \mathbb{N}$, $a \in \mathbb{N}$, date sa:

$$g_a(n) := \begin{cases} n - 1 & \text{ako } n > 0 \\ a & \text{ako } n = 0 \end{cases}, \text{ za } n \in \mathbb{N},$$

njeni levi inverzi. (Štaviše, nije teško videti da su to svi njeni levi inverzi).

Funkcija $g_0 : \mathbb{N} \rightarrow \mathbb{N}$ jeste na (ali nije 1-1). Funkcija f jeste jedan njen desni inverz, ali i funkcija $f' : \mathbb{N} \rightarrow \mathbb{N}$ data sa $f'(n) := \begin{cases} n + 1 & \text{ako } n > 0 \\ 0 & \text{ako } n = 0 \end{cases}$, za $n \in \mathbb{N}$ je još jedan njen desni inverz. (Štaviše, lako vidimo da su joj to jedina dva desna inverza.)

Komentar 5.23. Naglasimo još i da smo u dokazu (ii) u gornjoj teoremi, kada smo definisali:

$$g(b) := \text{neki element skupa } S_b, \text{ za } b \in B,$$

morali odgovarajući element skupa S_b da izaberemo. Ovakav izbor ne možemo da uradimo bez aksiome izbora. Štaviše, tvrđenje da svaka na funkcija ima desni inverz ekvivalentno je aksiomi izbora.

5.5 Direktna i inverzna slika skupa

Definicija 5.24. Neka je $f : A \rightarrow B$, $X \subseteq A$ i $Y \subseteq B$.

- *Direktna slika* skupa X je skup:

$$f[X] := \{f(a) \mid a \in X\},$$

dakle skup svih slika elemenata iz X . Primetimo $f[X] \subseteq B$.

- *Inverzna slika* skupa Y je skup:

$$f^{-1}[Y] := \{a \in A \mid f(a) \in Y\},$$

dakle skup svih elemenata domena koji se slikaju unutar Y . Primetimo $f^{-1}[Y] \subseteq A$.

Komentar 5.25. (i) Prema definiciji inverzna slike direktno važi $a \in f^{-1}[Y] \Leftrightarrow f(a) \in Y$.

(ii) Prema definiciji direktne slike direktno važi $a \in X \Rightarrow f(a) \in f[X]$. Obratna implikacija ne mora da važi. Naime, može se desiti da imamo $a \notin X$, $a' \in X$ i $f(a) = f(a')$.

(iii) Prema prethodnoj rečenici, ako je f 1-1 onda važi $a \in X \Leftrightarrow f(a) \in f[X]$.

Prethodne hapomene možemo slobodno koristiti.

Zadatak 5.26. Neka je $f : A \rightarrow B$, $X, X_1, X_2 \subseteq A$, $Y, Y_1, Y_2 \subseteq B$. Dokazati:

- (i) $X_1 \subseteq X_2 \Rightarrow f[X_1] \subseteq f[X_2]$;
- (ii) $Y_1 \subseteq Y_2 \Rightarrow f^{-1}[Y_1] \subseteq f^{-1}[Y_2]$;
- (iii) $f^{-1}[f[X]] \supseteq X$; ako je f 1-1, važi jednakost;
- (iv) $f[f^{-1}[Y]] \subseteq Y$; ako je f na, važi jednakost;
- (v) $f[X_1 \cup X_2] = f[X_1] \cup f[X_2]$;
- (vi) $f[X_1 \cap X_2] \subseteq f[X_1] \cap f[X_2]$; ako je f 1-1, važi jednakost;
- (vii) $f[X_1 \setminus X_2] \supseteq f[X_1] \setminus f[X_2]$; ako je f 1-1, važi jednakost;
- (viii) $f^{-1}[Y_1 \cup Y_2] = f^{-1}[Y_1] \cup f^{-1}[Y_2]$;
- (ix) $f^{-1}[Y_1 \cap Y_2] = f^{-1}[Y_1] \cap f^{-1}[Y_2]$;
- (x) $f^{-1}[Y_1 \setminus Y_2] = f^{-1}[Y_1] \setminus f^{-1}[Y_2]$.

6 Kardinalnost

6.1 Definicija i osnovne osobine

Zadatak 6.1. Neka su A i B konačni skupovi. Označimo sa $|A|$ i $|B|$ broj elemenata skupa A , odnosno B . Dokazati:

- (i) $|A| \leq |B|$ akko postoji $A \xrightarrow{1-1} B$;
- (ii) $|A| = |B|$ akko postoji $A \xrightarrow{bij.} B$.

Inspirisani prethodnim zadatkom definišemo:

Definicija 6.2. Neka su A i B proizvoljni skupovi.

- (a) Skup A je manje ili jednake kardinalnosti od B , u oznaci $|A| \leq |B|$, ako postoji $A \xrightarrow{1-1} B$.
- (b) Skup A je jednake kardinalnosti kao i B , u oznaci $|A| = |B|$, ako postoji $A \xrightarrow{bij.} B$.
- (c) Skup A je manje kardinalnosti od B , u oznaci $|A| < |B|$, ako je $|A| \leq |B|$ i $|A| \neq |B|$, tj. ako postoji 1-1 funkcija, ali ne postoji bijekcija $A \rightarrow B$.

Kao i u konačnom slučaju, o $|A|$ mislimo kao o broju elemenata skupa A .

Uvedene oznake zadovoljavaju očekivane osobine:

Tvrđenje 6.3. Neka su A, B, C skupovi. Tada:

- (i) ako $|A| = |B|$, onda $|A| \leq |B|$;
- (ii) $|A| \leq |A|$ i $|A| = |A|$;
- (iii) ako $A \subseteq B$, onda $|A| \leq |B|$;
- (iv) ako $|A| \leq |B|$, onda postoji $B' \subseteq B$ takav da $|A| = |B'|$;
- (v) ako $|A| = |B|$, onda $|B| = |A|$;

(vi) ako $|A| = |B|$ i $|B| = |C|$, onda $|A| = |C|$;

(vii) ako $|A| \leq |B|$ i $|B| \leq |C|$, onda $|A| \leq |C|$.

Dokaz. (i) važi jer je svaka bijekcija specijalno 1-1. (ii) važi jer je $\text{id}_A : A \rightarrow A$ bijekcija (pa i 1-1). (iii) važi jer je inkluziono preslikavanje $i_{A,B} : A \rightarrow B$ dato sa $i_{A,B}(a) := a$ očigledno 1-1. (iv) Ako je $f : A \xrightarrow{1-1} B$, onda je $f' : A \rightarrow \text{Im}(f)$ dato sa $f'(a) := f(a)$ očigledno bijekcija, pa možemo da uzmemo $B := \text{Im}(f)$. (v) važi jer je inverz bijekcija takođe bijekcija. (vi) i (vii) važe jer je kompozicija bijekcija, odnosno 1-1 funkcija, takođe bijekcija, odnosno 1-1 funkcija. $\square$

Pored navedenih osobina, definisana oznaka $\leq$ zadovoljava i (očekivane) osobine antisimetričnosti i linearnosti, međutim ti rezultati nisu trivijalni.

Teorema 6.4 (Kantor, Šreder, Bernštajn (KŠB)). Ako $|A| \leq |B|$ i $|B| \leq |A|$, onda $|A| = |B|$.

Dokaz KŠB teoreme dajemo u odeljku 6.7.

Posledica 6.5. Neka su A, B, C skupovi. Tada:

(i) ako $|A| < |B|$ i $|B| \leq |C|$, onda $|A| < |C|$;

(ii) ako $|A| \leq |B|$ i $|B| < |C|$, onda $|A| < |C|$.

Dokaz. Dokazaćemo (i), deo (ii) dokazuje se na sličan način.

Neka je $|A| < |B|$, tj. $|A| \leq |B|$ i $|A| \neq |B|$, i neka je $|B| \leq |C|$. Prema tvrđenju 6.3(viii) važi $|A| \leq |C|$, pa treba da dokažemo $|A| \neq |C|$. Pretpostavimo suprotno, $|A| = |C|$; tada je i $|C| = |A|$, pa uočimo neku bijekciju $h : C \rightarrow A$. Uočimo i neku 1-1 funkciju $g : B \rightarrow C$ (ona postoji jer $|B| \leq |C|$). Tada je $h \circ g : B \rightarrow A$ 1-1 funkcija kao kompozicija 1-1 funkcija, pa je $|B| \leq |A|$. Kako je i $|A| \leq |B|$, prema KŠB teoremi zaključujemo $|A| = |B|$. Kontradikcija. $\square$

Teorema 6.6 (Bernštajn). Neka su A i B skupovi. Tada važi tačno jedno od $|A| < |B|$, $|A| = |B|$ i $|B| < |A|$.

Dokaz Bernštajnovе teoreme dajemo u odeljku 6.8*.

Naglasimo još jednu karakterizaciju relacije $|A| \leq |B|$:

Tvrđenje 6.7. Neka su A i B skupovi. Tada $|A| \leq |B|$ akko postoji $B \xrightarrow{na} A$.

Dokaz. ($\Rightarrow$) Ako je $|A| \leq |B|$, tada postoji $f : A \xrightarrow{1-1} B$, pa postoji i njen levi inverz $g : B \rightarrow A$; $g \circ f = \text{id}_A$. Funkcija g je na.

($\Leftarrow$) Pretpostavimo da imamo $f : B \xrightarrow{na} A$. Tada f ima desni inverz $g : A \rightarrow B$; $f \circ g = \text{id}_B$. Funkcija g je 1-1, pa je $|A| \leq |B|$. $\square$

Setimo se da egzistencija desnog inverza u opštem slučaju zavisi od aksiome izbora (štaviše, tvrđenje da svaka na funkcija ima desni inverz ekvivalentno je aksiomi izbora). Prema tome, gornji dokaz u smeru ($\Leftarrow$) implicitno koristi aksiomu izbora.

6.2 Neke opšte (ne)jednakosti

Tvrđenje 6.8. Pretpostavimo $|A| = |A'|$ i $|B| = |B'|$. Tada:

(i) ako $A \cap B = A' \cap B' = \emptyset$, onda je $|A \cup B| = |A' \cup B'|$;

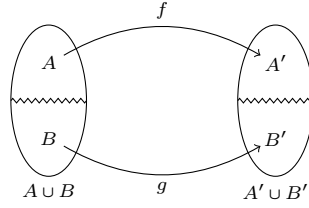
(ii) $|A \times B| = |A' \times B'|$;

(iii) $|^A B| = |^{A'} B'|$;

(iv) $|\mathcal{P}(A)| = |\mathcal{P}(A')|$.

Dokaz. Fiksirajmo funkcije $f : A \xrightarrow{\text{bij.}} A'$ i $g : B \xrightarrow{\text{bij.}} B'$.

(i) Skup $A \cup B$ disjunktno je podeljen na skupove A i B , i slično, skup $A' \cup B'$ disjunktno je podeljen na skupove A' i B' :



Funkcija f bijektivno preslikava skup A na A' , a funkcija g skup B na B' . Prema tome jasno je da ćemo bijekciju $h : A \cup B \rightarrow A' \cup B'$ dobiti „lepljenjem“ bijekcija f i g . Preciznije, definišimo:

$$h(x) := \begin{cases} f(x) & \text{ako } x \in A \\ g(x) & \text{ako } x \in B \end{cases}, \text{ za } x \in A \cup B.$$

Najpre primetimo da je h dobro definisana funkcija $h : A \cup B \rightarrow A' \cup B'$, tj. $h(x)$ jednoznačno je određeno jer $A \cap B = \emptyset$, i takođe je očigledno $h(x) \in A' \cup B'$.

Funkcija h je na. Neka je $y \in A' \cup B'$. Ako $y \in A'$, kako je f na, $y = f(x)$ za neko $x \in A$, pa je po definiciji i $h(x) = y$. Ako $y \in B'$, kako je g na, $y = g(x)$ za neko $x \in B$, pa je po definiciji i $h(x) = y$. Dakle, h jeste na.

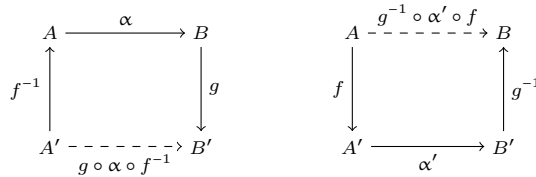
Funkcija h je 1-1. Neka su $x_1, x_2 \in A \cup B$ različiti elementi. Ako $x_1, x_2 \in A$, onda je $h(x_1) = f(x_1) \neq f(x_2) = h(x_2)$, gde nejednakost važi jer je f 1-1. Slično, ako $x_1, x_2 \in B$, $h(x_1) \neq h(x_2)$ jer je g 1-1. Poslednji slučaj je kada je $x_1 \in A$ i $x_2 \in B$ (ili obratno, što je simetrično). Tada je $h(x_1) = f(x_1) \neq g(x_2) = h(x_2)$, ali sada nejednakost važi jer $f(x_1) \in A'$, $g(x_2) \in B'$ i $A' \cap B' = \emptyset$. Dakle, h jeste 1-1.

(ii) Definišimo $h : A \times B \rightarrow A' \times B'$ sa $h(a, b) := (f(a), g(b))$. Da bismo pokazali da je h bijekcija, možemo lako da proverimo da jeste 1-1 i na, ali možemo da postupimo i na sledeći način. Definišimo i funkciju $k : A' \times B' \rightarrow A \times B$ sa $k(a', b') := (f^{-1}(a'), g^{-1}(b'))$. Dokazaćemo da je k inverz funkcije h , tj. proverićemo $k \circ h = \text{id}_{A \times B}$ i $h \circ k = \text{id}_{A' \times B'}$, što znači da je h bijekcija (i da je $h^{-1} = k$). Imamo:

$$k \circ h(a, b) = k(f(a), g(b)) = (f^{-1}(f(a)), g^{-1}(g(b))) = (a, b),$$

pa je zaista $k \circ h = \text{id}_{A \times B}$. Slično proveravamo i drugu jednakost.

(iii) Definišimo funkciju $h : {}^A B \rightarrow {}^{A'} B'$ sa $h(\alpha) = g \circ \alpha \circ f^{-1}$ za $\alpha \in {}^A B$, i funkciju $k : {}^{A'} B' \rightarrow {}^A B$ sa $h(\alpha') = g^{-1} \circ \alpha' \circ f$ za $\alpha' \in {}^{A'} B'$; pogledajte dijagrame:



(Sa dijagrama je jasno da $h(\alpha) \in {}^{A'} B'$ i $k(\alpha') \in {}^A B$.)

Primetimo da je:

$$k \circ h(\alpha) = k(g \circ \alpha \circ f^{-1}) = g^{-1} \circ g \circ \alpha \circ f^{-1} \circ f = \alpha,$$

jer se $g^{-1} \circ g$ i $f^{-1} \circ f$ ponište. Dakle, $k \circ h = \text{id}_{{}^A B}$. Slično vidimo i da je $h \circ k = \text{id}_{{}^{A'} B'}$, pa su h i k međusobno inverzne bijekcije.

(iv) Definišimo $h : \mathcal{P}(A) \rightarrow \mathcal{P}(A')$ sa $h(X) = f[X]$ za $X \subseteq A$, i definišimo $k : \mathcal{P}(A') \rightarrow \mathcal{P}(A)$ sa $k(Y) = f^{-1}[Y]$. Imamo da je:

$$k \circ h(X) = f^{-1}[f[X]] = X,$$

gde poslednja jednakost važi zato što je f 1-1, a:

$$h \circ k(Y) = f[f^{-1}[Y]] = Y,$$

gde poslednja jednakost važi zato što je f na. Dakle, $k \circ h = \text{id}_{\mathcal{P}(A)}$ i $h \circ k = \text{id}_{\mathcal{P}(A')}$, pa su h i k međusobno inverzne bijekcije. $\square$

Zadatak 6.9. Pretpostavimo $|A| \leq |A'|$ i $|B| \leq |B'|$. Dokazati:

- (i) $|A \cup B| \leq |A' \cup B'|$;
- (ii) $|A \times B| \leq |A' \times B'|$;
- (iii) $|^A B| \leq |^{A'} B'|$;
- (iv) $|\mathcal{P}(A)| \leq |\mathcal{P}(A')|$.

Tvrđenje 6.10. Za svaki skup A važi $|\mathcal{P}(A)| = |^A \{0, 1\}|$.

Dokaz. Za $X \subseteq A$ definišimo $\chi_X : A \rightarrow \{0, 1\}$ sa:

$$\chi_X(a) := \begin{cases} 1 & \text{ako } a \in X \\ 0 & \text{ako } a \notin X \end{cases}, \text{ za } a \in A.$$

Funkcija χ_X naziva se *karakteristična funkcija* skupa X (u odnosu na A). Definišimo sada funkciju $\chi : \mathcal{P}(A) \rightarrow ^A \{0, 1\}$ sa $\chi(X) := \chi_X$ za $X \subseteq A$. Dokazaćemo da je χ bijekcija.

χ je 1-1. Pretpostavimo da su $X, Y \subseteq A$ različiti. Tada postoji element $a \in A$ takav da $a \in X$ i $a \notin Y$ (ili obratno, što je simetričan slučaj). Tada je $\chi_X(a) = 1$ i $\chi_Y(a) = 0$, pa je $\chi_X \neq \chi_Y$, tj. $\chi(X) \neq \chi(Y)$, pa je χ 1-1.

χ je na. Neka je $f \in ^A \{0, 1\}$. Dokazaćemo $f = \chi_{f^{-1}[\{1\}]}$, tj. $f = \chi(f^{-1}[\{1\}])$ odakle zaključujemo da je χ na. Željena jednakost sledi jer je:

$$f(a) = 1 \Leftrightarrow a \in f^{-1}[\{1\}] \Leftrightarrow \chi_{f^{-1}[\{1\}]}(a) = 1$$

za svako $a \in A$, gde prva ekvivalencija važi po definiciji inverzne slike, a druga po definiciji karakteristične funkcije. $\square$

Teorema 6.11 (Kantor). Za svaki skup A je $|A| < |\mathcal{P}(A)|$.

Dokaz. Kako je funkcija $f : A \rightarrow \mathcal{P}(A)$ data sa $f(a) = \{a\}$ očigledno 1-1, važi $|A| \leq |\mathcal{P}(A)|$. Dokažimo i $|A| \neq |\mathcal{P}(A)|$.

Dovoljno je da dokažemo da ne postoji $A \xrightarrow{na} \mathcal{P}(A)$. Pretpostavimo suprotno, neka je $g : A \xrightarrow{na} \mathcal{P}(A)$. Uočimo skup $S := \{a \in A \mid a \notin g(a)\}$. Jasno je $S \in \mathcal{P}(A)$, pa kako je g na, $S = g(s)$ za neko $s \in A$. Prisetimo sada da imamo:

$$s \in S \Leftrightarrow s \notin g(s) \Leftrightarrow s \notin S,$$

gde prva ekvivalencija važi po definiciji skupa S , a druga jer je $g(s) = S$. Kontradikcija. $\square$

6.3 Prebrojivi skupovi

Definicija 6.12. (a) $\aleph_0 := |\mathbb{N}|$ – čita se *alef nula*.

(b) Skup A je *prebrojiv* ako je $|A| = \aleph_0$, tj. ako postoji $\mathbb{N} \xrightarrow{bij.} A$.

(c) Skup A je *neprebrojiv* ako nije konačan i nije prebrojiv.

Primer 6.13. Skupovi $\mathbb{N}^+$, $2\mathbb{N}$ i $\mathbb{Z}$ su prebrojivi. Zaista funkcija $f : \mathbb{N} \rightarrow \mathbb{N}^+$ data sa $f(n) = n + 1$ je jedna očigledna bijekcija. Takođe, $g : \mathbb{N} \rightarrow 2\mathbb{N}$ data sa $g(n) = 2n$ je očigledna bijekcija.

Da bismo dokazali da je $\mathbb{Z}$ prebrojiv iskoristićemo ideju tvrđenja 6.8(i). Podelimo $\mathbb{N}$ na parne ($2\mathbb{N}$) i neparne brojeve ($2\mathbb{N} + 1$) i $\mathbb{Z}$ na nenegativne ($\mathbb{N}$) i negativne brojeve ($\mathbb{Z}^-$). Imamo očigledne bijekcije $h : 2\mathbb{N} \rightarrow \mathbb{N}$ datu sa $h(n) = \frac{n}{2}$ i $k : 2\mathbb{N} + 1 \rightarrow \mathbb{Z}^-$ datu sa $k(n) = -\frac{n+1}{2}$. „Lepljenjem“ ove dve bijekcije dobijamo bijekciju $l : \mathbb{N} \rightarrow \mathbb{Z}$ datu sa:

$$l(n) := \begin{cases} \frac{n}{2} & \text{ako je } n \text{ paran} \\ -\frac{n+1}{2} & \text{ako je } n \text{ neparan} \end{cases}, \text{ za } n \in \mathbb{N}.$$

Istaknimo da prethodni primer kaže da kada izbacimo jedan element (nulu) iz skupa $\mathbb{N}$, dobijeni skup $\mathbb{N}^+$ i dalje ima isti broj elemenata kao skup $\mathbb{N}$. Situacija je zanimljivija, ako izbacimo iz $\mathbb{N}$ beskonačan skup neparnih brojeva, preostali deo $2\mathbb{N}$ ima isti broj elemenata kao ceo skup $\mathbb{N}$. Slično, i $\mathbb{Z}$ ima isti broj elemenata kao i $\mathbb{N}$. Ove napomene nam pokazuju da beskonačnosti imaju kontraintuitivna svojstva.

Komentar 6.14. Neka je A prebrojiv i $f : \mathbb{N} \rightarrow A$ neka bijekcija. Ako označimo sa $a_n := f(n)$, tada je $a_0, a_1, a_2, \dots$ jedno ređanje elemenata skupa A u niz indeksiran sa $\mathbb{N}$ (za ovakav niz reći ćemo da je *niz tipa* $\mathbb{N}$). Zaista, s obzirom da je f na, svaki element skupa A je izlistan u datom nizu, a kako je f 1-1, isti element ne pojavljuje se dva puta.

Sa druge strane, ako možemo da nađemo način da poređamo elemente skupa A u niz $a_0, a_1, a_2, \dots$ tipa $\mathbb{N}$, imamo bijekciju $f : \mathbb{N} \rightarrow A$ definisanu sa $f(n) := a_n$, pa je skup A prebrojiv.

Dakle, da bismo dokazali da je skup A prebrojiv, možemo da damo postupak koji pokazuje da se elementi tog skupa mogu poređati u niz tipa $\mathbb{N}$. Skup $\mathbb{N}^+$ iz gornjeg primera lako se ređa u takav niz, tj. već je poređan: $1, 2, 3, 4, \dots$, kao i skup $2\mathbb{N}$: $0, 2, 4, 6, \dots$. Skup $\mathbb{Z}$ možemo poređati u niz tipa $\mathbb{N}$ na sledeći način: $0, -1, 1, -2, 2, -3, 3, \dots$. Jasno je da će navedeni postupak izlistati svaki ceo broj.

Primer 6.15. Skup $\mathbb{N} \times \mathbb{N}$ je prebrojiv.

1. način. Pozitivni prirodni brojevi imaju zanimljivu osobinu. Svaki $a \geq 1$ može se zapisati na jedinstven način u obliku $2^n(2m+1)$ za neke $n, m \in \mathbb{N}$. (Zaista, najpre delimo a sa dvojkom onoliko puta koliko je to moguće, to je broj n ; preostali količnik je neparan pa se može zapisati u obliku $2m+1$.) Prema tome imamo bijekciju $f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}^+$ datu sa $f(n, m) := 2^n(2m+1)$, što znači da je $\mathbb{N} \times \mathbb{N}$ prebrojiv jer je $\mathbb{N}^+$ prebrojiv.

2. način. Možemo da iskoristimo KŠB teoremu. Naime, imamo očiglednu 1-1 funkciju $f : \mathbb{N} \rightarrow \mathbb{N} \times \mathbb{N}$ datu sa $f(n) := (n, 0)$, pa je $\aleph_0 \leq |\mathbb{N} \times \mathbb{N}|$. Sa druge strane, funkcija $g : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ data sa $g(m, n) = 2^m 3^n$ takođe je 1-1 (po osnovnoj teoremi aritmetike), pa je $|\mathbb{N} \times \mathbb{N}| \leq \aleph_0$. Prema tome, $|\mathbb{N} \times \mathbb{N}| = \aleph_0$.

3. način. Opisaćemo i jedan postupak kojim se $\mathbb{N} \times \mathbb{N}$ ređa u niz tipa $\mathbb{N}$. Zapišimo skup $\mathbb{N} \times \mathbb{N}$:

$$\begin{array}{ccccccc} (0,0) & \rightarrow & (0,1) & (0,2) & (0,3) & (0,4) & \cdots \\ & \swarrow & \nearrow & \swarrow & \nearrow & \swarrow & \nearrow \\ (1,0) & & (1,1) & (1,2) & (1,3) & (1,4) & \cdots \\ & \swarrow & \nearrow & \swarrow & \nearrow & \swarrow & \nearrow \\ (2,0) & & (2,1) & (2,2) & (2,3) & (2,4) & \cdots \\ & \swarrow & \nearrow & \swarrow & \nearrow & \swarrow & \nearrow \\ (3,0) & & (3,1) & (3,2) & (3,3) & (3,4) & \cdots \\ \vdots & & \vdots & \vdots & \vdots & \vdots & \ddots \end{array}$$

Jedan postupak ređanja prethodne tablice u niz tipa $\mathbb{N}$ predstavljen je strelicama. Naime, polazeći od gornjeg levog ugla, idemo redom i ređamo u niz elemente jedne po jedne dijagonale (pod k -tom dijagonalom, $k \geq 0$, podrazumevamo skup parova (m, n) takvih da je $m+n=k$). Proizvoljan par (m, n) nalazi se u $(m+n)$ -toj dijagonali. Kako su sve dijagonale konačne, prethodne dijagonale smo poređali u konačno mnogo koraka, pa ćemo i do para (m, n) stići u konačno mnogo koraka. Dakle svaki par će u nekom konačnom trenutku biti poređan. Prema tome, $\mathbb{N} \times \mathbb{N}$ je prebrojiv. Napomenimo da nije preterano teško doći do formule ovakvog ređanja, i ona je:

$$f(m, n) := \frac{(m+n)(m+n+1)}{2}.$$

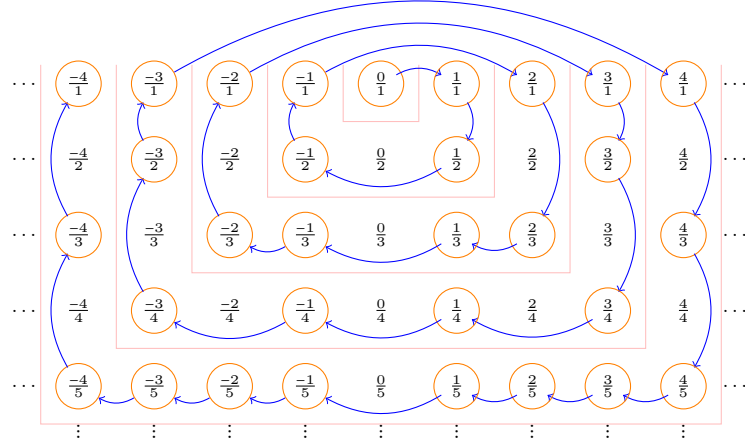
Sada kao posledicu prethodog primera imamo da su svi skupovi $\underbrace{\mathbb{N} \times \cdots \times \mathbb{N}}_n$, $n \geq 1$, prebrojivi. Zaista, ovo sad

lako vidimo indukcijom po n koristeći prethodni primer i tvrđenje 6.8(ii). I generalnije, proizvod $A_1 \times \cdots \times A_n$ konačno mnogo prebrojivih skupova je prebrojiv.

Primer 6.16. Skup $\mathbb{Q}$ je prebrojiv.

1. način. Primetimo da se svaki racionalan broj može zapisati u obliku $\frac{m}{n}$, gde $m \in \mathbb{Z}$ i $n \in \mathbb{N}^+$. To znači da je funkcija $f: \mathbb{Z} \times \mathbb{N}^+ \rightarrow \mathbb{Q}$ data sa $f(m, n) = \frac{m}{n}$ na, pa je prema tvrđenju 6.7, $|\mathbb{Q}| \leq |\mathbb{Z} \times \mathbb{N}^+| = |\mathbb{N} \times \mathbb{N}| = \aleph_0$. Sa druge strane je $\aleph_0 \leq |\mathbb{Q}|$ jer je $\mathbb{N} \subseteq \mathbb{Q}$. Po KŠB teoremi je $|\mathbb{Q}| = \aleph_0$.

2. način. Zapišimo sve razlomke $\frac{m}{n}$, gde $m \in \mathbb{Z}$ i $n \in \mathbb{N}^+$:



Najpre podelimo gornju tabelu na konačne trake kao što je označeno na slici, a onda ređamo elemente jedne po jedne trake na sledeći način. Počinjemo od gornjeg desnog ugla trake i idemo u smeru sata. Posmatrajmo proizvoljan razlomak $\frac{m}{n}$. Jasn je da smo pre njega poređali samo konačno mnogo elemenata. Najpre proverimo da li smo razlomak $\frac{m}{n}$ već poređali u našem nizu (što radimo u konačno mnogo koraka). Ako jesmo, preskočimo dati razlomak, a ako nismo stavimo ga u niz. (Na slici je strelicama naglašen postupak. Počnemo sa $\frac{0}{1}$. Nastavimo niz sa $\frac{1}{1}$ i $\frac{1}{2}$. Dolazimo do $\frac{0}{2}$; proverimo i vidimo da je ovaj broj već pobrojan, pa ga preskačemo. Nastavljamo sa $\frac{-1}{2}$ i $\frac{-1}{1}$, i prelazimo na sledeću traku.) Jasn je da ovim postupkom ređamo $\mathbb{Q}$ u niz tipa $\mathbb{N}$.

6.4 Skupovi moći kontinuumu

Definicija 6.17. (a) $\mathfrak{c} := |\mathbb{R}|$ – čita se *kontinuum*.

(b) Skup A je *moći kontinuumu* ako je $|A| = \mathfrak{c}$, tj. ako postoji $\mathbb{R} \xrightarrow{\text{bij.}} A$.

Primer 6.18. Poznato je da je funkcija $f: (-\frac{\pi}{2}, \frac{\pi}{2}) \rightarrow \mathbb{R}$ data sa $f(x) = \text{tg}(x)$ bijekcija, što znači da je $|(-\frac{\pi}{2}, \frac{\pi}{2})| = \mathfrak{c}$.

Linearna funkcija $g: (0, 1) \rightarrow (a, b)$, gde $a < b$, data sa $g(x) = (b-a)x + a$ je bijekcija, pa svi otvoreni intervali (a, b) su iste kardinalnosti kao $(0, 1)$, a kako smo gore videli da je $(-\frac{\pi}{2}, \frac{\pi}{2})$ moći kontinuumu, zaključujemo da su svi otvoreni intervali moći kontinuumu.

Za $a < b$ imamo $(a, b) \subseteq (a, b] \subseteq (a, +\infty) \subseteq \mathbb{R}$, pa sada po KŠB teoremi zaključujemo da su i poluzatvoreni interval $(a, b]$ i interval $(a, +\infty)$ takođe moći kontinuumu. Na sličan način vidimo i da su svi ostali intervali moći kontinuumu.

Zadatak 6.19. Konstruisati eksplicitnu bijekciju $(0, 1] \rightarrow (0, 1)$.

6.5 Kardinalnost skupa $\mathcal{P}(\mathbb{N})$

Sada ćemo dokazati da je skup $\mathcal{P}(\mathbb{N})$ moći kontinuumu. Zajedno sa teoremom 6.11 to povlači da je $\aleph_0 = |\mathbb{N}| < |\mathcal{P}(\mathbb{N})| = \mathfrak{c}$, tj. kontinuum je strogo veći kardinal od $\aleph_0$. Specijalno, skup $\mathbb{R}$ je neprebrojiv.

Dokaz ćemo izvesti koristeći KŠB teoremu na sledeći niz nejednakosti:

$$|\mathbb{R}| \stackrel{(1)}{\leq} |\mathcal{P}(\mathbb{Q})| \stackrel{(2)}{=} |\mathcal{P}(\mathbb{N})| \stackrel{(3)}{=} |\mathbb{N}\{0, 1\}| \stackrel{(4)}{\leq} |\mathbb{R}|.$$

Jednakost (2) sledi prema tvrđenju 6.8(iv) jer je $\mathbb{Q}$ prebrojiv. Jednakost (3) sledi prema tvrđenju 6.10. Dakle, ostaje da dokažemo nejednakosti (1) i (4).

(1). Konstruišemo 1-1 funkciju $f : \mathbb{R} \rightarrow \mathcal{P}(\mathbb{Q})$. Za $x \in \mathbb{R}$ stavimo $f(x) := (-\infty, x) \cap \mathbb{Q}$. Zašto je f 1-1 funkcija? Pretpostavimo da su $x, y \in \mathbb{R}$ različiti, npr. $x < y$. Poznata je osobina da se između svaka dva realna broja može naći neki racionalni (kažemo da je skup $\mathbb{Q}$ *gust* u $\mathbb{R}$), pa izaberimo $q \in \mathbb{Q}$ takav da $x < q < y$. Tada $q \notin (-\infty, x) \cap \mathbb{Q} = f(x)$, ali $q \in (-\infty, y) \cap \mathbb{Q} = f(y)$, pa su $f(x)$ i $f(y)$ različiti skupovi, što pokazuje da je f 1-1.

(4). Element $a \in \mathbb{N}\{0, 1\}$ je funkcija $a : \mathbb{N} \rightarrow \{0, 1\}$, koja je identifikovana sa nizom nula i jedinica $a = (a(0), a(1), a(2), \dots)$. Definišimo funkciju $g : \mathbb{N}\{0, 1\} \rightarrow \mathbb{R}$ na sledeći način:

$$g(a) := 0, a(0)a(1)a(2)a(3)\dots, \text{ za niz } a \in \mathbb{N}\{0, 1\}.$$

Dakle, stavimo da su elementi niza decimale broja $g(a)$. I ovo dodeljivanje je 1-1, jer za dva različita niza a i b postoji neko n tako da je $a(n) \neq b(n)$, što znači da se decimale na n -tom mestu u brojevima $g(a)$ i $g(b)$ razlikuju, pa je $g(a) \neq g(b)$.

Sada po KŠB teoremi dobijamo $|\mathcal{P}(\mathbb{N})| = |\mathbb{N}\{0, 1\}| = \mathfrak{c}$.

Primer 6.20. Sada možemo da dokažemo da je $|\mathbb{N}\{0, 1\} \times \mathbb{N}\{0, 1\}| = \mathfrak{c}$. Uočimo sledeću funkciju $f : \mathbb{N}\{0, 1\} \times \mathbb{N}\{0, 1\} \rightarrow \mathbb{N}\{0, 1\}$ datu sa:

$$f(a, b) = (a(0), b(0), a(1), b(1), a(2), b(2), \dots), \text{ za nizove } a, b \in \mathbb{N}\{0, 1\}.$$

Nije teško videti da je ovakvo dodeljivanje bijektivno, odakle sledi $|\mathbb{N}\{0, 1\} \times \mathbb{N}\{0, 1\}| = \mathfrak{c}$.

Sada je i $|\mathbb{R} \times \mathbb{R}| = |\mathbb{N}\{0, 1\} \times \mathbb{N}\{0, 1\}| = \mathfrak{c}$ i $|\mathbb{C}| = |\mathbb{R} \times \mathbb{R}| = \mathfrak{c}$, jer je funkcija $g : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{C}$ data sa $g(x, y) = x + iy$ očigledna bijekcija.

Zadatak 6.21. Neka je $A \subseteq \mathbb{R}$ prebrojiv skup. Dokazati da postoji $b \in \mathbb{R}$ takav da $A \cap (b + A) = \emptyset$. Koliko ima takvih brojeva b ?

Zadatak 6.22. Neka je $\mathcal{F}$ neka familija otvorenih intervala u $\mathbb{R}$ takva da se nikoja dva intervala iz familije $\mathcal{F}$ ne seku. Dokazati da je $\mathcal{F}$ najviše prebrojiva (konačna je ili prebrojiva).

6.6 Kantorov dijagonalni argument

Sada ćemo na još jedan način dokazati da skup $\mathbb{R}$ nije prebrojiv, kako bismo ilustrovali postupak poznat kao *Kantorov dijagonalni argument*. Dovoljno je da pokažemo da interval $(0, 1)$ nije prebrojiv, jer smo već videla da je on moći kontinuumu.

Pretpostavimo suprotno, interval $(0, 1)$ je prebrojiv. To znači da ga možemo poredati u niz tipa $\mathbb{N}$, i neka je to $x_1, x_2, x_3, \dots$. U decimalnom zapisu svaki od x_i je oblika:

$$x_i = 0, x_i^1 x_i^2 x_i^3 \dots,$$

gde sa x_i^j označavamo j -tu decimalu broja x_i (ako je broj x_i racionalan sa konačnim decimalnim zapisom produžimo zapis sa nulama). Poređajmo ove brojeve u sledeću tablicu:

$$\begin{array}{rcl}
x_1 & = & 0, \quad \textcircled{x_1^1} \quad x_1^2 \quad x_1^3 \quad \cdots \quad x_1^n \quad \cdots \\
x_2 & = & 0, \quad x_2^1 \quad \textcircled{x_2^2} \quad x_2^3 \quad \cdots \quad x_2^n \quad \cdots \\
x_3 & = & 0, \quad x_3^1 \quad x_3^2 \quad \textcircled{x_3^3} \quad \cdots \quad x_3^n \quad \cdots \\
& \vdots & \\
x_n & = & 0, \quad x_n^1 \quad x_n^2 \quad x_n^3 \quad \cdots \quad \textcircled{x_n^n} \quad \cdots \\
& \vdots &
\end{array}$$

Pogledajmo decimale na dijagonali, tj. uočimo i -tu decimalu x_i^i broja x_i . Definišimo niz cifara $c_1, c_2, c_3, \dots$ na sledeći način:

$$c_i := \begin{cases} 1 & \text{ako } x_i^i \neq 1 \\ 2 & \text{ako } x_i^i = 1 \end{cases}, \text{ za sve } i \geq 1.$$

Primetimo da za svako i važi $c_i \neq x_i^i$. Posmatrajmo sada broj $c := 0, c_1 c_2 c_3 \dots$. Jasno je $c \in (0, 1)$. Kako smo elemente ovog intervala pobrojali, $c = x_n$ za neko $n \in \mathbb{N}$. Međutim, ovo povlači i da je n -ta decimala u zapisu broja c , c_n , jednaka sa n -tom decimalom u zapisu broja x_n , x_n^n : $c_n = x_n^n$. Ali ovo je kontradikcija.

6.7 Dokaz KŠB teoreme

Teorema 6.23 (Knaster, Tarski). Neka je $\alpha : \mathcal{P}(A) \rightarrow \mathcal{P}(A)$ neopadajuća funkcija, tj. važi:

$$(\forall X, Y \subseteq A) (X \subseteq Y \rightarrow \alpha(X) \subseteq \alpha(Y)).$$

Tada α ima fiksnu tačku, tj. postoji $S \subseteq A$ takav da $\alpha(S) = S$.

Dokaz. Uočimo familiju $\mathcal{F} := \{X \subseteq A \mid X \subseteq \alpha(X)\}$. Primetimo da je $\mathcal{F}$ neprazna familija jer $\emptyset \in \mathcal{F}$. Ako je $X \in \mathcal{F}$, tada $X \subseteq \alpha(X)$, pa je i $\alpha(X) \subseteq \alpha(\alpha(X))$ jer je α neopadajuća, što znači da $\alpha(X) \in \mathcal{F}$. Dakle:

$$X \in \mathcal{F} \rightarrow \alpha(X) \in \mathcal{F}. \quad (1)$$

Uočimo skup $S := \bigcup \mathcal{F}$; dokazaćemo da je S željeni skup.

Ako je $X \in \mathcal{F}$, sa jedne strane je $X \subseteq \alpha(X)$, a sa druge strane je $X \subseteq S$, pa je $\alpha(X) \subseteq \alpha(S)$ jer je α neopadajuća funkcija; prema tome, $X \subseteq \alpha(S)$. Kako ovo važi za sve $X \in \mathcal{F}$ zaključujemo i $\bigcup \mathcal{F} \subseteq \alpha(S)$, tj. $S \subseteq \alpha(S)$.

Prethodna inkluzija specijalno povlači i $S \in \mathcal{F}$, pa prema (1) i $\alpha(S) \in \mathcal{F}$, što znači da $\alpha(S)$ učestvuje u uniji $S = \bigcup \mathcal{F}$, tj. $\alpha(S) \subseteq S$.

Kako smo zaključili i $S \subseteq \alpha(S)$ i $\alpha(S) \subseteq S$, dobijamo $\alpha(S) = S$. □

Zadatak 6.24. Pod pretpostavkama teoreme Knastera i Tarskog, dokazati da je:

$$S' := \bigcap \{X \subseteq A \mid \alpha(X) \subseteq X\}$$

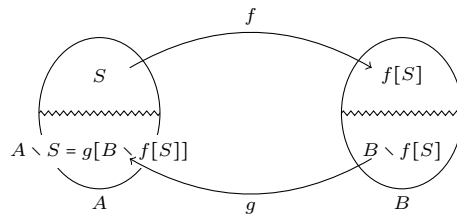
takođe fiksna tačka funkcije α .

Dokaz teoreme 6.4. Pretpostavimo $|A| \leq |B|$ i $|B| \leq |A|$, i uočimo neke 1-1 funkcije $f : A \rightarrow B$ i $g : B \rightarrow A$. Uočimo funkciju $\alpha : \mathcal{P}(A) \rightarrow \mathcal{P}(A)$ datu sa:

$$\alpha(X) = A \setminus g[B \setminus f[X]], \text{ za } X \subseteq A.$$

Primetimo da je funkcija α neopadajuća. Zaista, ako je $X \subseteq Y$, onda je i $f[X] \subseteq f[Y]$ zbog monotonosti direktne slike. Odatle je $B \setminus f[X] \supseteq B \setminus f[Y]$, pa je $g[B \setminus f[X]] \supseteq g[B \setminus f[Y]]$ ponovo zbog monotonosti direktne slike. Konačno, odatle dobijamo $A \setminus g[B \setminus f[X]] \subseteq A \setminus g[B \setminus f[Y]]$, tj. $\alpha(X) \subseteq \alpha(Y)$.

Prema teoremi Knastera i Tarskog postoji $S \subseteq A$ takav da $\alpha(S) = S$, tj. $A \setminus g[B \setminus f[S]] = S$. Odatle je $g[B \setminus f[S]] = A \setminus S$. Dakle, imamo situaciju da je skup A podeljen na disjunktne podskupove S i $A \setminus S = g[B \setminus f[S]]$, dok je skup B podeljen na disjunktne podskupove $f[S]$ i $B \setminus f[S]$:



Kako je f 1-1, f očigledno bijektivno preslikava S na $f[S]$, a kako je g 1-1, g očigledno bijektivno preslikava $B \setminus f[S]$ na $g[B \setminus f[S]] = A \setminus S$. Prema tome, bijekciju $h : A \rightarrow B$ dobijamo lepljenjem ovih bijekcija. Preciznije, definišemo:

$$h(a) := \begin{cases} f(a) & \text{ako } a \in S \\ g^{-1}(a) & \text{ako } a \in A \setminus S \end{cases}, \text{ za } a \in A.$$

(Primitite da g^{-1} jeste funkcionalna relacija jer je g 1-1, kao i da $g^{-1}(a) \downarrow$ za $a \in A \setminus S$ jer je $A \setminus S = g[B \setminus f[S]]$.)

Sada nije teško formalno zapisati da je h bijekcija. $\square$

6.8* Dokaz Bernštajnovih teorema

Za dokaz Bernštajnovih teorema potrebna nam je aksioma izbora. (Zapravo Bernštajnova teorema ekvivalentna je aksiomi izbora.) U dokazu ćemo koristiti Cornovu lemu 2.69.

Dokaz teorema 6.6. Neka su A i B dva skupa. Pretpostavimo $|A| \not\leq |B|$, tj. ne postoji 1-1 funkcija $A \rightarrow B$. Dovoljno je da nađemo 1-1 funkciju $B \rightarrow A$.

Uočimo familiju $\mathcal{F} := \{f \subseteq B \times A \mid f \text{ i } f^{-1} \text{ su funkcionalne relacije}\}$. Familija $\mathcal{F}$ je neprazna jer formalno prazna relacija joj pripada (prazna relacija zadovoljava uslove funkcionalnosti), ali i relacije $\{(b, a)\}$ joj pripadaju za svako $a \in A$ i $b \in B$.

Tvrdimo da $\mathcal{F}$ zadovoljava uslov Cornove leme: za svaki lanac $\mathcal{L} \subseteq \mathcal{F}$ važi $\bigcup \mathcal{L} \in \mathcal{F}$. Neka je $\mathcal{L} \subseteq \mathcal{F}$ lanac i neka je $\ell = \bigcup \mathcal{L}$. Treba da dokažemo da su ℓ i ℓ^{-1} funkcionalne relacije. Dokazaćemo da je ℓ funkcionalna relacija, drugi deo je potpuno simetričan. Pretpostavimo da je $b \ell a_1$ i $b \ell a_2$. Po definiciji ℓ , postoje $f_1, f_2 \in \mathcal{L}$ takve da $b f_1 a_1$ i $b f_2 a_2$. Međutim kako je $\mathcal{L}$ lanac, f_1 i f_2 su $\subseteq$ -uporedive, npr. $f_1 \subseteq f_2$. Ali tada je i $b f_2 a_1$ i $b f_2 a_2$, pa kako f_2 jeste funkcionalna (jer $f_2 \in \mathcal{L}$, pa i $f_2 \in \mathcal{F}$) zaključujemo $a_1 = a_2$. Dakle, ℓ jeste funkcionalna.

Prema Cornovoj lemi, $\mathcal{F}$ ima maksimalni element $\mathbf{m}$. Dokažimo da je $\mathbf{m} : B \xrightarrow{1-1} A$ željena funkcija. Znamo da $\mathbf{m}$ jeste funkcionalna relacija, kao i da je $\mathbf{m}^{-1}$ funkcionalna relacija (pa je $\mathbf{m}$ i 1-1, ako je funkcija), pa je dovoljno dokazati samo $\text{Dom}(\mathbf{m}) = B$. Pretpostavimo suprotno, $\text{Dom}(\mathbf{m}) \subsetneq B$; izaberimo $b \in B \setminus \text{Dom}(\mathbf{m})$. Primitimo da važi $\text{Im}(\mathbf{m}) \subsetneq A$. Zaista, ako je $\text{Im}(\mathbf{m}) = A$, onda je $\mathbf{m}^{-1} : A \xrightarrow{1-1} B$ (jer $\mathbf{m}^{-1}$ jeste funkcionalna, i inverz $(\mathbf{m}^{-1})^{-1} = \mathbf{m}$ je funkcionalan, pa je $\mathbf{m}^{-1}$ 1-1), što ne može biti jer smo pretpostavili da ne postoji 1-1 funkcija $A \rightarrow B$. Dakle, $\text{Im}(\mathbf{m}) \subsetneq A$, pa izaberimo i $a \in A \setminus \text{Im}(\mathbf{m})$. Proširimo relaciju $\mathbf{m}$ do relacije $\mathbf{m}'$ dodajući joj novu strelicu $b \rightarrow a$. Po izboru a i b , relacije $\mathbf{m}'$ i $\mathbf{m}'^{-1}$ su funkcionalne, pa $\mathbf{m}' \in \mathcal{F}$. Ovo protivreči činjenici da je $\mathbf{m}$ maksimalan element u $\mathcal{F}$. Dakle, $\text{Dom}(\mathbf{m}) = B$ i završili smo dokaz. $\square$