1. Uvod

Trenutačna znanstvena monografija, koja je prema našim spoznajama prva koja je posvećena teoriji dokaza na hrvatskom jeziku, rezultat je višegodišnjeg rada na temi dokaza u logici. Na početku se od autora očekuje dati osvrt o tome koja je centralna tema knjige, no kako je knjiga znatno proširivana i revidirana i ponovno pisana, tako je sve manje i manje jasno koja bi bila **ta**[1] srž knjige. S jedne strane, knjiga je nastala kao rezultat dodatnog znanstvenog istraživanja uz disertaciju, pa postoji manji dio sadržaja koji dijeli s disertacijom, ali je taj dio ovdje znatno proširen i objašnjen. S druge strane, skočiti odmah u napredne znanstvene teme je možda prikladno za disertaciju, ali svakako nije prikladno za znanstvenu monografiju koja, usprkos tome što je po svojoj samoj prirodi pristupačna tek upućenima, morala bi biti pristupačna što većem auditoriju kako bi odigrala i diseminacijsku ulogu. Ovo znači da se stvari često pojednostavljuju, a zbog želje za sažetošću se i preskaču – kada ne bi bilo preskakanja, monografija koja bi pokrivala isto što i trenutačna i raspisana do zadnjih detalja, obuhvaćala bi tisuće i tisuće stranica. Rasprava i prezentacija često bez posebne najave izlaze iz formalne logike i ulaze u filozofiju matematike i logike.

Ova je monografija doživjela razne modifikacije i znatno se mijenjala kroz godine u kojima je nastajala, kako su se mijenjale ideje i cilj što ona predstavlja. Trenutačno je najveća želja autora da ova monografija uspije prenijeti onu intuiciju koja je njemu bila relativno teško iščitljiva iz inače izvrsnih udžbenika i znanstvenih radova koje je prolazio. Ova želja je iznjedrila jedan pomalo drukčiji pristup od standardnog, i posebno, pristup koji zbog toga nije uniforman kroz cijelu knjigu: na početku je sve objašnjeno, a pred kraj su rezultati prezentirani kako bi bili prezentirani u znanstvenim radovima, no uvijek se trudimo ponuditi objašnjenje i komentare.

[1] Pokaznu zamjenicu taj, ta, to ćemo koristiti u značenju nalik engleskom određenom članu **the**.

Jedna kratica kojom ćemo se često koristiti je b.s.o. ili b.s.o.m.p., u značenju "bez smanjenja općenitosti (možemo pretpostaviti)" (engl. *without loss of generality*). Ovime se koristimo kada želimo pojednostavniti dokaz, ali znamo da je proširenje na izvornu tvrdnju trivijalno. Na primjer, ako se želi dokazati da vrijedi: "Ako su tri životinje psi ili mačke, tada su nužno barem dvije životinje iste vrste". Dokaz bi glasio "Bez smanjenja općenitosti možemo pretpostaviti da je prva životinja pas, tada nam preostaju dvije životinje. Ako je jedna od tih životinja pas, gotovi smo. Ako nijedna od tih dviju životinja nije pas, onda su obje preostale životinje mačke, što je trebalo i pokazati (lat. *Quod erat demonstrandum*)."

U prvom poglavlju se istražuje i prikazuje naivna teorija skupova i dodatni pojmovi kojima ćemo se koristiti. Ovo poglavlje služi razvijanju osnovnih intuicija oko toga što bi bila logika i koje su osnovne notacijske konvencije koje se koriste. Diskusija možda nije uvijek savršeno dosljedna, ali to nije bez razloga: (i) kao što smo ranije napomenuli, kada bismo bili dosljedni, ne bi bilo dovoljno 25 stranica ni za uvod u uvod i (ii) dosljednost bi zahtijevala formalnije izvode, a formalni izvodi nisu korisni za razvijanje intuicije za razumijevanje formalnih izvoda. Ta ideja je slična "pedagoškoj" ideji da se dijete baci u more pa će već proplivati, što možda jest stav nekih, no mi ga definitivno ne dijelimo, jer ga smatramo fundamentalno neprofesionalnim: mi kao edukatori moramo nekog naučiti nečemu, a ne samo provjeriti je li ta osoba može to sama naučiti. Shvaćajući neizvjesnost današnjeg vremena, kao i cvjetanje informacijskih tehnologija, dali smo poseban naglasak na ideju podatkovnih tipova, koja bi (kada bismo je konzistentno usvojili) odvela cijelu knjigu u bitno drukčijem smjeru – bila bi to druga knjiga. Mi smo htjeli ovime potakuti neke čitatelje, kojima je taj aspekt zanimljiv ili koristan, na gledanje cijele logike iz aspekta programiranja, ili, ljepše rečeno, iščitavanje komputacijskog sadržaja iz logike. Autor ima značajno programersko iskustvo u privredi i veze koje su ovdje implicirane će biti jasne svakome tko dijeli ovu pozadinu, posebno ako se radi o aplikacijama za neka područja umjetne inteligencije. Mnoge će takve aplikacije uskoro biti dostupne u obliku programskog koda, zajedno s opsežnim uvodima o programiranju u Pythonu[2] na `www.python.blue`, pa zainteresiranog čitatelja usmjeravamo na ovu web-adresu u izradi.

Drugo poglavlje nudi uvod u propozicijsku logiku klasičnim školskim metodama, ali se trudimo dati informacije o tome kako će se te teme dalje razvijati. Ovo će posebno biti očito oko istinitosnih tablica, gdje također

[2]Python je glavni istraživački progamski jezik danas, posebno za područje umjetne inteligencije.

nagovještavamo neke računalne probleme. Treće poglavlje nudi proširenje ovih rezultata na logiku prvog reda kao i standardni dio metateorija. Ovim poglavljem završava školski dio logike i naprednije teme počinju. Vrlo blagi tretman jedne relativno nepristupačne teme dajemo u poglavlju 4. Koliko smo bili uspješni u tome, čitatelj će sam procijeniti – ako nam uspije dokazati da smo loše obradili temu, smatrat ćemo da smo dobro odradili svoj posao. Sljedeće poglavlje je posvećeno aritmetici i dokazu nepotpunosti. Početna želja nam je bila uključiti i teme iz ograničene aritmetike i drugih fragmenata aritmetike prvog reda, no to bi zauzelo previše prostora i dodatno debalansiralo knjigu. Šesto poglavlje je relativno elementarno i prezentira neke osnovne rezultate klasične teorije dokaza. Sedmo poglavlje posvećeno je logici drugog reda. Sva prethodna poglavlja mogu se smatrati opsežnim uvodom za dokaz eliminacije reza za logiku drugog reda koji je ovdje prezentiran na originalan način: kao konstruktivan dokaz što je znanstvena novost. Zadnje poglavlje temu logike drugog reda povezuje s onime što mnogi nazivaju logikom za računarstvo, odnosno teorijom konačnih modela. Ovdje će se čitatelj naći u žarištu jednog od najvećih otvorenih problema logike (pa time i matematike, računarstva i filozofije), problema **P =? NP**.

Autor duguje zahvalu mnogima što je ova knjiga ugledala svjetlo dana. Najviše bih htio zahvaliti svojim profesorima od kojih sam kroz godine učio, i čiju sam metodologiju upijao da bih formirao svoj pristup. Zbog ovoga mi je teško reći gdje njihov pristup završava a moj počinje, pa premda sam ih možda na nekim mjestima citirao, vjerujem da sam se na mnogim mjestima koristio njihovom metodologijom a da nisam spomenuo odgovarajuće reference. Zato im se želim ovdje zahvaliti na svom prenesenom znanju i ispričati za mnoge nenavedene reference na njihov rad. To su profesori Srećko Kovač, Davor Lauc, Zvonimir Šikić, Goran Švob i Mladen Vuković. Također bih htio zahvaliti profesoru Stipi Kutleši i profesoru Zvonimiru Šikiću što su prihvatili recenzirati ovu monografiju i time značajno podigli njenu kvalitetu. Za sve propuste i netočnosti koje su se potkrale, smatram se jedinim krivcem.

www.element.hr

2. Skupovi i funkcije

2.1. Naivna teorija skupova

Ovo je poglavlje posvećeno skupovima i funkcijama. Iz naše perspektive skupovi i funkcije tvore elementarne didaktičke blokove, pa smo zato odlučili započeti njima, a i velik dio kasnijeg teksta pretpostavlja odgovarajuće poznavanje skupova i funkcija.

Teorija skupova koju ćemo ovdje prikazati je takozvana naivna teorija skupova. Mi ćemo naivnu teoriju skupova predstaviti kao skupinu operatora koji se ponašaju na određene načine. Formalno govoreći, teorija skupova se predstavlja na bitno drukčiji način, preko aksioma, ali kako nam je ovdje cilj prvenstveno stvoriti preduvjete za razumijevanje daljnjeg teksta, predstavit ćemo je na jednostavan način. Kao elementaran i nedefiniran pojam uzimamo "A je član B", odnosno $A \in B$, gdje je B skup, a A je ili pojedinačan predmet ili skup. Poseban skup koji isto uzimamo je prazan skup, skup koji nema članova, koji označavamo s $\emptyset$.

Naivnu teoriju skupova NTS čine operatori nad skupovima:

- Podskup: neka su A u B skupovi. Kažemo da je B podskup od A i pišemo $B \subseteq A$ ako i samo ako je svaki član B također član A.
- Ekstenzionalnost (ili skupovna jednakost): ako skupovi A i B imaju iste članove, onda je to jedan te isti skup, $A = B$.
- Unija: ako su A i B skupovi, onda je $A \cup B$ unija A i B, a to je skup koji sadrži sve članove A i sve članove B.
- Presjek: ako su A i B skupovi, onda je $A \cap B$ presjek A i B, a to je skup koji sadrži samo zajedničke članove A i B.

- Skupovna razlika: ako su A i B skupovi, onda je $A \setminus B$ skupovna razlika A i B, a taj skup sadrži samo članove A koji nisu članovi B.
- Komplement: za razliku od standardnih tekstova, komplement od A (u skupu B) smatramo pokratom za $B \setminus A$, ali u slučaju kada je B očit ili jasan; komplement od A pišemo $\bar{A}$.
- Partitivni skup: ako je A skup, onda je $\mathcal{P}(A)$ partitivni skup skupa A, a to je skup koji kao članove sadrži sve moguće njegove podskupove kao članove. Tako za svaki B, ako $B \subseteq A$, onda $B \in \mathcal{P}(A)$. Ako skup A ima n članova, tada njegov partitivni skup $\mathcal{P}(A)$ ima 2^n članova.
- Komprehenzija: ako je $SVOJS(x)$ neko svojstvo, tada svi predmeti koji zadovoljavaju to svojstvo tvore skup, koji zapisujemo kao $\{x|SVOJS(x)\}$.

Nekoliko napomena. Neka $A = \{0,1,2,3\}$ i $B = \{1,2\}$. Tada vrijedi $B \subseteq A$. Neka $A = \{1,2\}$ i $B = \{1,2\}$. Tada vrijedi $B \subseteq A$ i $A \subseteq B$ i prema ekstenzionalnosti slijedi $A = B$. Prema ekstenzionalnosti također vrijedi $\{0,1\} = \{1,0\} = \{1,1,0\} = \{0,0,1\} = \{0,1,0\} = \{0,0,0,0,0,0,0,0,0,0,1,0,0\}$. Zašto? Prema ekstenzionalnosti, ako dva skupa imaju *iste članove* (bez obzira na raspored, ili koliko puta se ponavljaju), tada su to isti skupovi. Prazan skup može biti član nekog drugog skupa, ali je po definiciji prazan skup *podskup* bilo kojeg skupa.

Neka su $A = \{0,1,2,3\}$ i $B = \{1,2\}$. Tada je $A \cup B = \{0,1,2,3\} = A$. Drugim riječima, B nije ništa novo donio u uniju (temeljem aksioma ekstenzionalnosti $A \cup B = \{0,1,2,3\} \cup \{1,2\} = \{0,1,2,3,1,2\} = \{0,1,2,3\} = A$), pa je cijela unija ista kao i A. Neka su A i B dva skupa koji nemaju zajednički element, dakle $A \cap B = \emptyset$. Takve skupove nazivamo *disjunktnim*. Skup B iz definicije komplementa ($\bar{A} = B \setminus A$) naziva se *univerzumom*.

Ako $B \subseteq A$ i $A \neq B$ (ovo pišemo $B \subsetneq A$), onda $A \setminus B \neq \emptyset$. Uzmimo da je $A = \{a,b,c\}$, tada $\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a,b\}, \{b,c\}, \{a,c\}, \{a,b,c\}\}$. Uočite da je broj članova 2^3.

Komprehenzija je onaj aksiom zbog kojeg se naivna teorija skupova ne može konzistentno aksiomatizirati. Da bismo shvatili problem, prvo napomenimo da bilo koji skup mora imati točno i jasno definirane članove. Naravno, skup može biti beskonačan (i puno veći od toga), ali u načelu bi za bilo koji x trebalo biti moguće reći je li u tom skupu ili nije[1]. Ako uzmemo da je $SVOJS(x) = x \notin x$, tada dobivamo iz komprehenzije skup

[1] Funkcija koja to radi zove se *karakteristična funkcija* skupa A i piše se $\chi_A(x)$, a dobiva vrijednost 1 ako $x \in A$, a 0 ako $x \notin A$.

$C = \{x | x \notin x\}$. Ako se pitamo je li ovaj skup svoj član[2], dolazimo do paradoksa: ako pretpostavimo da nije, onda po definiciji svojstva koje tvori skup ulazi u taj skup. Ako pretpostavimo da jest, onda ne zadovoljava svojstvo $x \notin x$, pa ne bi trebao biti unutra. U svakom slučaju, ne znamo koji su točno članovi C, i s obzirom na to, C nije skup, što znači da komprehenzija ne generira *samo* skupove, nego i paradoksalne kreacije poput C.

Ovaj se paradoks tradicionalno zove Russellov paradoks, i postoje dva, dosta slična rješenja. Prvo rješenje je maknuti komprehenziju i dodati nove aksiome koji nam govore što je skup. Tako aksiomi teorije skupova točno definiraju što je skup i ne hvataju kreacije poput C. Ovaj pristup je pristup standardnih teorija skupova, poput ZFC. Drugi pristup (zapravo je jako sličan prvom, ali ovo nije na prvi pogled vidljivo), ograničiti je što sve $SVOJS(x)$ može biti. Prednost ovog pristupa je zadržavanje jednostavnosti komprehenzije. Time se dobivaju razne ograničene komprehenzije, za određene vrste svojstava. Logika drugog reda je u mnogočemu povezana s raznim oblicima komprehenzije.

Ono što nam preostaje, prije nego što krenemo dalje, izložiti je kako se ponašaju novodefinirani operatori na skupovima. Postoje mnoge kombinacije, i ostavljamo čitatelju da istraži neke od njih. Mi dajemo neke od najčešćih pretvorbi:

- $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$
- $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$
- $(A \bar{\cap} B) = \bar{A} \cup \bar{B}$
- $(A \bar{\cup} B) = \bar{A} \cap \bar{B}$
- $\bar{\bar{A}} = A$
- $(A \setminus C) \cup (B \setminus C) = (A \cup B) \setminus C$
- $(A \setminus C) \cap (B \setminus C) = (A \cap B) \setminus C$
- $\mathcal{P}(A \cup B) \supseteq \mathcal{P}(A) \cup \mathcal{P}(B)$, ali drugi smjer ne vrijedi.
- $\mathcal{P}(A \cup B) \neq \mathcal{P}(A) \cup \mathcal{P}(B)$

[2]Skupovi mogu biti svoji članovi. Uzet ćemo klasičan primjer: skup svih ideja je ideja pa je time svoj član.

Kardinalnost skupa je broj članova skupa i označavamo ga s $||A||$. Operacije unije i Kartezijeva produkta (naravno, ni operacije presjeka ni razlike) ne povećavaju kardinalnost skupa. Operacija komplementa $\bar{A}$ može povećati kardinalnost s obzirom na početnu kardinalnost skupa A, ali je limitirana veličinom skupa B, što je u skladu s definicijom komplementa kao razlike. Kada komplement ne bismo definirali kao razliku, komplementiranjem bismo mogli napraviti jako velike skupove, puno veće od onih dobivenih partitivnim skupom, ali bismo tada podvaljivali neke stvari kao legitimne (poput skupa svih skupova). Općenito, ako je $\star \in \{\cup, \cap, \setminus\}$ bilo koja skupovna operacija (unija, presjek, razlika), $||A \star B|| \leq \max(||A||, ||B||)$.

Operacija partitivnog skupa s druge strane uvijek povećava kardinalnost:

Teorem 1. *Za svaki skup A, ako $||A|| = n$, onda $||\mathcal{P}(A)|| = 2^n$.*

Dokaz. Dokaz će se kasnije prezentirati. □

2.2. Relacije

Prva stvar koju možemo definirati skupovnim operacijama je proširivanje skupa. Primjerice, ako želimo stvoriti skup $\{a, b\}$ iz skupova $\{a\}$ i $\{b\}$, tada se koristimo aksiomom unije. Ako želimo taj skup stvoriti iz a i b, tada se koristimo komprehenzijom i $\{a, b\}$ definiramo kao $\{x | x = a \text{ ili } x = b\}$. Ovo "definiramo kao" pišemo kao $:=$, odnosno $\{a, b\} := \{x | x = a \text{ ili } x = b\}$. Skup $\{a, b\}$ zovemo *neuređenim* parom a i b, jer je redoslijed članova nebitan. Uređeni par je par gdje je bitno koji član je na prvom mjestu, a koji na drugom. Moguće je definirati uređene parove uz pomoć skupova, a ideja potječe od K. Kuratowskija:

Definicija 1. *Skup $\{x, \{x, y\}\}$ nazivamo uređenim parom x i y; ekstenzionalnost jamči jedinstvenost, pa zapisujemo $\langle x, y \rangle$. Da bismo pokazali da su time uređeni parovi dobro definirani, neka su $\langle x, y \rangle$ i $\langle z, w \rangle$ uređeni parovi: tada $\langle x, y \rangle = \langle z, w \rangle$ ako i samo ako $x = z$ i $y = w$. Znači, $\{x, \{x, y\}\} = \{z, \{z, w\}\}$ ako i samo ako $x = \{z, w\}$ ili ako $x = z$. Neka $x = \{z, w\}$, tada, prema ekstenzionalnsti, $x = z = w$, pa onda $x = y$, odnosno $x = y = z = w$. Neka $x = z$, onda $\{x, y\} = \{z, w\}$, odnosno, jer $x = z$, $y = w$ po ekstenzionalnosti.*

Uz pomoć uređenog para dalje se definira Kartezijev produkt skupova koji omogućava stvaranje skupova n-torki.

Definicija 2 (Kartezijev produkt skupova)**.** *Neka su A i B skupovi, tada $C := \{(x, y)|x \in A \wedge y \in B\}$ nazivamo Kartezijevim produktom skupova A i B. Iz ekstenzionalnosti slijedi jedinstvenost, pa za skup C uvodimo oznaku $A \times B$. Poseban je slučaj ako $B = A$, kada Kartezijev produkt nazivamo još i Kartezijevim kvadratom i pišemo A^2.*

Proširenje na produkt više od dvaju skupova je trivijalno. Posebno se često koristi A^n da bi se uhvatile uređene n-torke iz A. Uz pomoć n-torki iz A^n definiraju se i relacije:

Definicija 3 (Relacije nad skupom)**.** *Neka je R^n podskup skupa A^n definiran kao skup $R^n \subseteq \{(x, \ldots, x_n)|x, \ldots, x_n \in A\}$. Tada R^n zovemo n-mjesnom relacijom nad skupom A.*

Neformalno govoreći, relacija nad skupom je odnos među članovima skupa. Primjerice, $<$ je relacija nad prirodnim brojevima. Napomenimo da *relacije* nisu istinite ili neistinite, već one postoje između *određenih* članova skupa, ili ne postoje. Primjerice, između brojeva 1 i 3 postoji relacija $<$, odnosno taj par brojeva jest u toj relaciji. Za razliku od tog para brojeva koji je u toj relaciji, par brojeva 5 i 3, ili par brojeva 3 i 1, nije u toj relaciji. Ovo je različito od pitanja je li *relacijski simbol* $<$ koji predstavlja relaciju $<$ u određenoj teoriji, zajedno s dvjema konstantama 1 i 3, koje predstavljaju brojeve 1 i 3, tvori rečenicu te određene teorije $1 < 3$. Rečenica je onda istinita ili neistinita, što ovisi o tome je li par brojeva 1 i 3 iz skupa prirodnih brojeva u relaciji $<$.

Mjesnost (ili aritet) relacije je broj predmeta koji jesu u toj relaciji. Jednomjesne relacije su svojstva. Sjetimo se $SVOJS(x)$: ova relacija je dopuštala da samo x varira. To nije značilo da se x pojavljuje samo jednom, a čak je moguće da se pojavljuju neki fiksni članovi, dakle da se od npr. dvomjesne relacije $x \neq y$ stvori jednomjesna relacija $x \neq 2$, čije je tada svojstvo x da nije parni prim-broj. Odnosno, ako $x \neq 2$ vrijedi, tada znamo da ako je x prim-broj, onda je neparan, ili alternativno, ako je x paran, onda sigurno nije prim-broj. Postoji mnogo svojstava koja djeluju dosta razrađeno, a koja se i dalje mogu vrlo jednostavno opisati aritmetičkim relacijama.

Dvomjesne relacije su (uz svojstva) glavna vrsta relacije, jer se u praksi tromjesne ili višemjesne relacije rijetko javljaju, ali svojstva i dvomjesne relacije su iznimno česte. Vidjeli smo gore kako se od dvomjesne relacije fiksiranjem jednog parametra dobiva svojstvo. Dvomjesne relacije same mogu biti različitih tipova. Neka je R dvomjesna relacija, a a, b, c predmeti, tada su tipovi relacija:

- R je *refleksivna* relacija ako za svaki a vrijedi Raa, odnosno ako Rxx vrijedi općenito. Primjer refleksivne relacije je $=$, jer za bilo koji a vrijedi $a = a$.

- R je *simetrična* relacija ako za sve a i b vrijedi Rab, onda vrijedi Rba. Primjer simetrične relacije je opet $=$, jer ako $a = b$ vrijedi, onda i $b = a$ vrijedi.

- R je *asimetrična* relacija ako za sve a i b vrijedi Rab, onda ne vrijedi Rba. Primjer asimetrične relacije je $<$, jer ako $a < b$ vrijedi, onda $b < a$ ne vrijedi.

- R je *antisimetrična* relacija ako za sve a i b vrijedi Rab i Rba, onda vrijedi $a = b$. Primjer antisimetrične relacije je $\leq$, jer ako $a \leq b$ i $b \leq a$ vrijedi, onda $a = b$ vrijedi.

- R je *tranzitivna* relacija ako za sve a, b i c vrijedi Rab i Rbc, onda vrijedi Rac. Primjer tranzitivne relacije je $<$, jer ako $a < b$ i $b < c$, onda $a < c$.

- R je *linearna* relacija ako za sve a i b vrijedi ili Rab ili Rba ili $a = b$. Primjer linearne relacije je $<$ na prirodnim brojevima: za bilo koje m, n, ili vrijedi $m < n$ ili vrijedi $n < m$ ili su m i n isti broj.

Naravno, ovdje smo ilustrirali svojstva relacija s elementarnim aritmetičkim operacijama $<$, $\leq$ i $=$, ali bilo koja relacija koja se tako ponaša naziva se simetrična: to može biti relacija "x je paralelan sa y", ili primjerice relacija "x ide u razred sa y". Lako je vidjeti da su ove dvije relacije simetrične.

Svaka dvomjesna relacija Rxy koja je (1) refleksivna, (2) tranzitivna i (3) simetrična naziva se relacijom ekvivalencije. Bilo koja relacija ekvivalencije (ovo ne znači da su ti predmeti doslovno ekvivalentni) uređuje skup nad kojim živi na poseban način: relacija ekvivalencija dijeli skup na takozvane *klase ekvivalencije*, od kojih svaka sadrži predmete koji su ekvivalenti po toj relaciji. Ako je primjerice ta relacija ekvivalencije "x je paralelan sa y", tada će ta relacija početni skup podijeliti na klase ekvivalencije od kojih će svaka klasa sadržavati međusobno paralelne elemente. Skup koji je tako uređen relacijom ekvivalencije R naziva se *kvocijentni skup prema* R.

Radi zornosti, relacije se često prikazuju simbolom $\prec$ umjesto R. Gore smo već napomenuli kako relacija ekvivalencije uređuje skup i stvara kvocijentni skup. Općenito, razni tipovi relacija uređuju skupove, a u sljedećoj definiciji preciziramo što to znači.

Definicija 4 (Uređaji)**.** *Skup A je dobro uređen s obzirom na relaciju $\prec$ (pišemo kratko $(A, \prec)dus$) ako i samo ako* (*a*) *A je skup, $\prec$ je tranzitivna i ne-refleksivna (što naziva se* irefleksivna*) relacija nad A,* (*b*) *po kojoj su svi elementi A usporedivi i* (*c*) *svaki neprazni podskup od A sadrži najmanji element s obzirom na $\prec$ $(\forall B \subseteq A)(\exists x)(x = min_{\prec}(B))$. Ako vrijedi samo* (*a*) *i* (*b*)*, uređaj nazivamo totalnim ili linearnim, pišemo $(A, \prec)lus$, a ako vrijedi samo* (*a*) *uređaj nazivamo parcijalnim pa pišemo $(A, \prec)pus$.*

Ideja iza ove definicije je da se parcijalno uređeni skup ponaša kao primjerice skupina predmeta i relacija "x stane u y". Na primjer, kuglica stane u čašu koja stane u kantu, koja pak stane u kadu. U svakom slučaju čaša stane direktno u kadu (tranzitivnost), ali čaša ne stane u čašu (sebe samu), pa refleksivnost ne vrijedi. Također, bitna odrednica parcijalnih uređaja je da se mogu granati po relaciji i ponovno spojiti: čaša stane u kantu, ali stane i u kutiju (a kutija ne stane u kantu, ni kanta u kutiju), a bilo kanta bilo kutija stanu u kadu. Razlog zašto parcijalne uređaje ne objašnjavamo matematičkim strukturama je zato što je parcijalni uređaj "najneuređeniji" uređaj, a većina matematičkih entiteta koji su prikladni za uvodno poglavlje ponašaju se uređenije od toga – najčešće su dobri uređaji.

Ako dodamo uvjet da svaki neprazni podskup mora imati najmanji element, dobivamo dobro uređeni skup. Dobro uređen skup je primjerice skup prirodnih brojeva. Većina skupova elementarne aritmetike su dobro uređeni skupovi, a temeljem aksioma izbora, sve je skupove moguće dobro urediti.

Definicija 5 (Supremum i infinum)**.** *Neka je $S \subseteq (A, \prec)pus$. Tada ako postoji jedinstveni $x \in A$ takav da $(\forall y \in S)(y \prec x \vee x = y)$, taj x nazivamo najmanjom gornjom međom od S ili supremumom od S. Jedinstvenost slijedi iz ekstenzionalnosti pa ga označavamo sa $sup(S)$. Razlika između supremuma skupa i najvećeg elementa (maksimuma) je ta da supremum nekog skupa S ne mora biti član skupa S. Analogno definiramo i infinum, odnosno najveću donju među nekog skupa S. Za skup S kažemo da je omeđen odozgo ako ima supremum, a da je omeđen odozdo ako ima infinum.*

Supremum i infinum su najmanja gornja i najveća donja granica. Primjerice, ako imamo niz $\{1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \ldots\}$ i gledamo sumu svih članova niza, tada je supremum te operacije 2, jer je on najmanji broj koji je sigurno veći od sume svih članova tog niza.

Definicija 6 (Maksimum i minimum)**.** *Neka je A skup omeđen odozgo i neka je $\prec$ neka relacija na njemu; ako su prema njoj članovi skupa usporedivi*[3]*,*

[3]Članovi nekog skupa zajedno s nekom relacijom $\prec$ su usporedivi ako $(\forall x, y \in A)(x = y \vee x \prec y \vee y \prec x)$.

onda $(\exists x \in A)(\forall y \in A)(x \neq y \rightarrow y \prec x)$. *Jedinstvenost je očita: neka postoji neki* $z \neq x$, *takav da* $(\forall y \in A)(z \neq y \rightarrow y \prec z)$, *ali tada* $x \prec z$ *što proturječi pretpostavci. Takav* x *nazivamo najvećim elementom skupa* A *ili, preciznije, maksimumom u* A *prema relaciji* $\prec$ *te ga označavamo s pomoću* $\max_{\prec}(A)$. *Potpuno analogno definiramo i minimum.*

Maksimum i minimum su najveći i najmanji element prema $\prec$. Oni su jedinstveni, jer ako nisu tada nisu maksimum i minimum nego maksimalni i minimalni elementi. Maksimum je *najveći element*, a maksimalan element je *element od kojeg nema većeg* po relaciji $\prec$. Definicija slijedi:

Definicija 7 (Maksimalan i minimalan element)**.** *Neka je* A *skup omeđen odozgo i neka je* $\prec$ *neka relacija na njemu; ako su prema njoj članovi skupa usporedivi, vrijedi* $(\exists x \in A)(\forall y \in A)(x \neq y \rightarrow \neg x \prec y)$. *Takav element nije (nužno) jedinstven, a nazivamo ga maksimalnim elementom skupa* A *prema relaciji* $\prec$ *te ga, zloupotrebom notacije (zbog nejedinstvenosti), označavamo* $ME_{\prec}(A)$. *Potpuno analogno definiramo i minimalni element.*

2.3. Funkcije

Kako smo uz pomoć skupova definirali relacije, tako ćemo uz pomoć relacija definirati funkcije:

Definicija 8 (Funkcija)**.** *Neka je* R^2 *dvomjesna relacija i neka su* A *i* B *skupovi. Ako za sve* $x \in A$ *postoji jedinstveni* $y \in B$ *takav da* (R^2xy), *tada* R^2 *nazivamo funkcijom od* x, *pri čemu joj je* x *argument, a* y *vrijednost, a označavamo je s pomoću* $f(x) = y$; *funkcije ćemo još označavati* $f(x)$, $g(x)$, $h(x)$, *ali i na druge načine kada bude potrebno. Dvomjesne funkcije označavamo* $f(x, y) = z$, *tromjesne* $f(x, y, z) = w$, *itd. Također, ako* $f(x) = y$, *tada* $f^{-1}(y) = x$, *koju nazivamo praslikom od* y *s obzirom na* $f(x)$. *Skup* A *nazivamo domenom funkcije, a skup* B *kodomenom. Skup svih* $f(x)$ *nazivamo slikom skupa* A *u* B *i označavamo sa* $f[A]$.

Uočimo jedan iznimno važan detalj: funkcija $f(x) = y$ ima uvijek točno određenu vrijednost y s obzirom na dobiveni x, dakle funkcija dobiva jedan jedini broj. Relacija Rxy s druge strane (ako nije funkcija, a to možemo pretpostaviti) nema točno određenu vrijednost, odnosno ako se odabere određeni x, ne znamo što može doći za y, ili, u najboljem slučaju, imamo skup vrijednosti koje bi mogle biti ili, preciznije rečeno, koje *jesu* y. To znači da

je vrijednost funkcije kada se odabere x konkretan broj, a za relaciju kada odaberemo x trebamo još odabrati neki y i tada provjeravamo je li stvarno vrijedi Rxy, odnosno je li Rxy tada istinito ili nije.

Zanimljivo je vidjeti kako se ponašaju slika i praslika s obzirom na presjek:

- $f[A \cup B] = f[A] \cup f[B]$
- $f[A \cap B] \subseteq f[A] \cap f[B]$
- $f^{-1}[A \cup B] = f^{-1}[A] \cup f^{-1}[B]$
- $f^{-1}[A \cap B] = f^{-1}[A] \cap f^{-1}[B]$

Razlog zašto drugi smjer s presjekom ne vrijedi može se vidjeti ako se uzme $A = \{a\}$, $B = \{b\}$, a $f(a) = c$ i $f(b) = c$. Tada $f[A \cap B] = \emptyset$, jer je $A \cap B = \emptyset$ (slika praznog skupa $f[\emptyset]$ je uvijek prazan skup[4]), ali $f[A] \cap f[B] = \{c\}$.

Kada želimo stvoriti niz, to se radi tako da se niz definira kao funkcija iz prirodnih brojeva u neki skup A, odnosno $f : \mathbb{N} \to A$. Razlog zašto se skup prirodnih brojeva uzima za domenu, a ne za kodomenu je zato što se ovako može dogoditi da isti a iz kodomene dobije broj m i n, pa postane a_m i a_n i tada $a_m = a_n$, ali da je obrnuto bi se moglo dogoditi da su $a, b \in A$, za koje $a \neq b$, dobiju isti broj n, odnosno isto mjesto u nizu, što uništava cijelu ideju niza odnosno nizanja, jer tada više neće biti linearno uređeno temeljem brojeva s pomoću kojih se niže.

Općenito, moguće je ideju niza poopćiti s prirodnih brojeva kao indeksa na bilo koji skup. Dodatna mogućnost je da želimo tako pobrojiti srodne skupove, koji imaju slične članove. To se najbolje može napraviti tako da se definira (indeksirana) familija skupova. Neka su A i I skupovi, tada $A_i : I \to \mathcal{P}(A)$ nazivamo familijom skupova. Po tipu, funkcija može biti injekcija, surjekcija ili bijekcija:

Definicija 9 (Injekcija, surjekcija, bijekcija)**.** *Neka je f funkcija s domenom A. Tada, ako $(\forall x \in A)(\forall y \in A)(x \neq y \to f(x) \neq f(y))$, kažemo da je f injekcija. Neka je f funkcija s domenom A i kodomenom B. Tada, ako $f[A] = B$, kažemo da je f surjekcija. Neka je $f(x)$ funkcija koja je injekcija i surjekcija. Takvu funkciju nazivamo bijekcijom.*

[4]Ovo je različito od slučaja gdje je prazan skup član nekog skupa pa se gleda slika praznog skupa u smislu $f(\emptyset)$.

Bit će nam potreban još i pojam restrikcije funkcije:

Definicija 10 (Restrikcija)**.** *Neka je $f(x) = y$ funkcija s domenom A, kodomenom B i neka je $C \subseteq A$. Tada funkciju $g(x) = y$, takvu da $g : C \to B$ nazivamo restrikcijom funkcije $f(x)$ i zapisujemo kao $f|_C(x)$. Sliku $f[C]$ takve restringirane funkcije označavamo $f''(A)$.*

Ponekad je teško dokazati surjektivnost funkcije $f : A \to B$, jer je za to potrebno proučiti cijelu kodomenu i vidjeti da ne ostaje nijedan član koji nije slika nečega. Puno je lakše dokazati injektivnost: sve što treba je pažljivo definirati funkciju da se dva člana domene ne "zalijepe" i dobiju isti član kodomene. Zato je vrlo koristan sljedeći rezultat koji nam omogućava da ako imamo injekciju iz A u B i injekciju iz B u A.

Teorem 2 (Cantor-Schröder-Bernsteinov teorem)**.** *Ako je $f : A \to B$ injekcija i $g : B \to A$ injekcija, tada postoji $h : A \to B$ koja je surjekcija i injekcija (bijekcija).*

Dokaz. Neka $A_0 := A$ i $B_0 := B$. Neka $A_{n+1} := g''(B_n)$ i $B_{n+1} := f''(A_n)$. Neka $A_\infty := \bigcup_{n\in\mathbb{N}} A_n$, a $B_\infty := \bigcup_{n\in\mathbb{N}} B_n$. Tada definiramo funkciju $h : A \to B$:

$$h(x) = \begin{cases} f(x), x \in A_\infty \cup \bigcup_{n\in\mathbb{N}}(A_{2n} \setminus A_{2n+1}) \\ g^{-1}, \text{inače} \end{cases}$$

Očito je da je h surjekcija, a injektivnost je naslijeđena iz f i činjenice da je g funkcija. □

Definicija 11. *Funkciju f nazivamo monotonom ako zadovoljava jedan od sljedeća dva uvjeta:*

- *Ako $x \leq y$ onda $f(x) \leq f(y)$.*
- *Ako $x \geq y$ onda $f(x) \geq f(y)$.*

Sljedeći pojam koji nam je potreban je pojam operacije. n-mjesna operacija je naziv za svaku funkciju $f : A^n \to A$. Poznate su aritmetičke operacije zbrajanja, množenja i eksponenciranja. Zanimljiva su svojstva inverznih operacija. Primjerice, zbrajanje na prirodnim brojevima je dobro definirano pa je zbroj svaka dva prirodna broja opet prirodan broj. Kažemo da je skup prirodnih brojeva $\mathbb{N}$ *zatvoren* pod zbrajanjem (i množenjem i eksponenciranjem). Skup prirodnih brojeva nije zatvoren pod operacijom oduzimanja, koja je *inverzna operacija* zbrajanju, ali uočimo da oduzimanje

nije *inverzna funkcija* zbrajanju. Inverzna funkcija zbrajanju ne postoji jer zbrajanje nije injekcija: ako uzmemo 8, je li to došlo od $5+3$ ili $7+1$? Da bismo dobili zatvorenost na oduzimanje, potrebno je uvesti cijele brojeve $\mathbb{Z}$. Oni su zatvoreni na zbrajanje i oduzimanje, ali i množenje. Da bismo dobili zatvorenost na dijeljenje, potrebno je uvesti racionalne brojeve $\mathbb{Q}$. Oni su zatvoreni pod zbrajanjem, oduzimanjem, množenjem, dijeljenjem i eksponenciranjem, ali nisu pod korjenovanjem – za to je potreban skup realnih brojeva $\mathbb{R}$.

Jednadžbe poput $2x^2 - 7x + 3 = 0$ nazivaju se polinomi, i mogu se shvatiti kao funkcije od x, pa je npr. $p(x)$ pokrata za $2x^2 - 7x + 3 = 0$, a to je funkcija čija je vrijednost 3, odnosno $p(x) = 3$. x naziva se korijen polinoma. U skupu $\mathbb{R}$, polinom $x^2 + 1 = 0$ (ali i mnogi drugi) nemaju korijen. Da bi svi polinomi imali korijene (ili, ekvivalentno, sve jednadžbe rješenja) potrebno je uvesti skup kompleksnih brojeva, koji je zatvoren pod korjenovanjem polinoma.

Zadnji pojam vezan uz funkcije koji nam zasad treba je pojam homomorfizma. Općenito, uređeni par nekog skupa A i relacije $\prec$ naziva se *struktura* (ponekad se naglasi kao "relacijska struktura")[5]. Ako je ta relacija zapravo operacija $\circ$ (operacije su posebne vrste funkcija koje su posebne vrste relacija), tada se struktura $\langle A, \circ \rangle$ naziva *algebarskom strukturom.*

Definicija 12 (Homomorfizam, monomorfizam, epimorfizam i izomorfizam)**.** *Neka su $\langle A, \circ \rangle$ i $\langle B, * \rangle$ algebarske strukture i $f : A \to B$ funkcija. Ako za sve $a, b \in A$ vrijedi $f(a \circ b) = f(a) * f(b)$, tada funkciju f nazivamo* homomorfizmom*. Sasvim analogno se definira za relacijske strukture (strukture općenito): $\mathcal{A} = \langle A, \prec \rangle$ i $\mathcal{B} = \langle B, < \rangle$ su strukture i $f : A \to B$ funkcija. Ako za sve $a, b \in A$ vrijedi $f(a \prec b) = f(a) < f(b)$, onda je f homomorfizam struktura $\mathcal{A}$ i $\mathcal{B}$, i pišemo $\mathcal{A} \cong \mathcal{B}$. Ako je funkcija f homomorfizam i injekcija, tada naziva se monomorfizam. Ako je f homomorfizam i surjekcija, tada naziva se epimorfizam, a ako je bijekcija onda naziva se izomorfizam.*

[5] Pojmovi "struktura" i "uređeni skup", odnosno "uređaj" su donekle sinonimni, ali u slučaju kada su sinonimi razlikuju se u naglasku: kada se govori o strukturama naglasak je na tome kako se članovi skupa ponašaju (uz prisustvo relacije), a kada govorimo o uređaju, naglasak je kako se relacija ponaša (na tom skupu).