DISKRETNA MATEMATIKA

KOMBINATORIKA, TEORIJA GRAFOVA I ALGORITMI

Dragan Stevanović
Prirodno-matematički fakultet, Univerzitet u Nišu

February 17, 2003

Sadržaj

Predgovor

Ova knjiga je namenjena studentima Odseka za matematiku Prirodno-matematičkog fakulteta u Nišu koji slušaju predmet "Diskretna matematika".

Pod diskretnom matematikom se podrazumevaju oblasti matematike, kao što su logika, algebra, kombinatorika, teorija grafova ili odredjeni delovi verovatnoće; u opštem slučaju, to su sve oblasti matematike čiji se predmet proučavanja ne može opisati pomoću neprekidnosti funkcija, odnosno pojmova izvoda i integrala. U ovom udžbeniku se koncentrišemo na kombinatoriku i teoriju grafova, s obzirom da na Prirodno-matematičkom fakultetu u Nišu postoje posebni predmeti u kojima se izučavaju preostale oblasti.

Kombinatorika razmatra tri vrste problema: probleme egzistencije, probleme prebrojavanja i probleme konstrukcija raznih objekata. U ovoj knjizi najviše se koncentrišemo na problem prebrojavanja.

Knjiga od čitaoca traži minimalno prethodno znanje iz logike i algebre, a na nekoliko mesta i iz linearne algebre. Za svaki slučaj, u uvodnom poglavlju su date neke osnovne matematičke definicije i tehnike.

U prvom delu knjige bavimo se kombinatorikom, odnosno, načinima prebrojavanja konačnih skupova.

U poglavlju "Teorija grafova" iznosimo neke od značajnih teorema iz teorije grafova, a pored toga prikazujemo i način za povezivanje teorije grafova sa linearnom algebrom, tzv. *spektralnu teoriju grafova.*

A kako se pomoću grafova mogu matematički modelirati brojni praktični problemi, u poglavlju "Algoritmi" predstavljamo osnovne algoritme koji rešavaju neke od tih praktičnih problema.

Dragan Stevanović — Niš, oktobar 2002.

Glava 1

Uvod

U ovoj glavi opisujemo osnovne matematičke pojmove koji će nam trebati u daljem radu. Polazimo od samih osnova, tako da ova glava sadrži četiri sekcije posvećene skupovima, funkcijama, relacijama i matematičkoj indukciji.

1.1 Skupovi

Osnovni matematički objekat je *skup*. Skup se zapisuje navodjenjem njegovih elemenata izmedju vitičastih zagrada { i }. Skup koji sadrži brojeve 1, 3 i 5 (i nijedan više) zapisuje se kao $\{1, 3, 5\}$. Ovaj skup se može zapisati i kao $\{3, 1, 5\}$, ali i kao $\{1, 3, 5, 3, 1\}$, jer se višestruko ponavljanje istog elementa ne uzima u obzir. Tri tačke $(\ldots)$ u $\{2, 4, 6, 8, \ldots\}$ znače "i tako dalje, po istom obrascu", tj. ovaj zapis označava skup svih parnih prirodnih brojeva. Odgovarajući obrazac treba da bude očigledan. Na primer, $\{2^1, 2^2, 2^3, \ldots\}$ je lako razumljivo kao skup svih stepena broja 2, dok je zapis $\{2, 4, 8, \ldots\}$ manje očigledan.

Skupovi se obično označavaju velikim slovom, s tim što je za najvažniji skup matematike i čovečanstva uopšte, skup prirodnih brojeva $\{1, 2, 3, \ldots\}$, rezervisano slovo N. Još jedan važan skup je skup bez elemenata. Postoji samo jedan takav skup, označava se sa $\emptyset$ i naziva *prazan skup*. Primetimo da prazan skup može da bude element drugog skupa. Na primer, $\{\emptyset\}$ je skup koji sadrži prazan skup kao svoj element, pa nije isto što i $\emptyset$!

Činjenica da skup X sadrži element x zapisuje se pomoću simbola $\in$. Zapis $x \in X$ se čita kao "x je element X", "x pripada X", "X sadrži x", itd. U slučaju da element x ne pripada skupu X pišemo $x \notin X$.

Složeniji i interesantniji skupovi obično se dobijaju od poznatih skupova pomoću nekih pravila ili osobina. Takvi skupovi se zapisuju u sledećem obliku

$$A = \{x \colon x \text{ ima osobinu } P\}.$$

Na primer, skup svih kvadrata prirodnih brojeva može da se zapiše kao

$$\{n \in N\colon \text{ postoji } k \in N \text{ tako da je } n = k^2\}.$$

ili kraće kao

$$\{k^2 : k \in N\}.$$

Napomena Pogrešno je misliti da svaka osobina P definiše skup. Do ovakvog zaključka je došao Bertrand Russell 1911. godine. Posmatrajmo sledeću situaciju: vojni frizer treba da šiša sve vojnike koji se ne šišaju sami—treba li on, kao jedan od vojnika, da šiša samog sebe? Do istog "paradoksa" se dolazi i ako definišemo sledeći skup:

$$A = \{X : X \text{ je skup koji ne sadrži samog sebe}\}.$$

Da li skup A sadrži samog sebe? Ako pretpostavimo da A sadrži samog sebe, tada po osobini elemenata skupa A važi da A ne sadrži samog sebe. S druge strane, ako pretpostavimo da A ne sadrži samog sebe, tada on zadovoljava osobinu elemenata skupa A, pa mora da pripada samom sebi. U svakom slučaju dolazimo do kontradikcije. Jedini izlaz je reći da A nije skup! Objekte kao što je skup A, matematičari obično zovu *familije* skupova.

Koristeći pojam pripadanja skupu, $\in$, možemo da definišemo mnoge relacije izmedju skupova i operacije na skupovima. Na primer, dva skupa X i Y su jednaka ako imaju iste elemente. U tom slučaju pišemo $X = Y$. Ako su X, Y skupovi, zapis $X \subseteq Y$ (rečima: "X je podskup Y") znači da svaki element X pripada skupu Y. Primetimo da je $X = Y$ ako i samo ako je $X \subseteq Y$ i $Y \subseteq X$.

Ako je $X \subseteq Y$, ali je $X \neq Y$, tada Y sadrži bar jedan element koji ne pripada X. U tom slučaju se kaže da je X *pravi podskup* Y i piše $X \subset Y$.

Ako $X \not\subseteq Y$ i $Y \not\subseteq X$, tada se kaže da su skupovi X i Y *neuporedivi.* Za skupove X i Y se kaže da su *disjunktni* ako nemaju zajedničkih elemenata. Skupovi $\{1,3,5\}$ i $\{2,4,6\}$ su disjunktni, dok skupovi $\{1,3,5\}$ i $\{2,3,4\}$ nisu disjunktni. Za niz skupova $X_1, X_2, X_3, \ldots$ se kaže da su uzajamno disjunktni, ako su svaka dva od njih disjunktna. Prema tome,

$$\begin{array}{ll} \{1,2\},\{3,4\},\{5,6\} & \text{su uzajamno disjunktni} \\ \{1,2\},\{3,4\},\{1,6\} & \text{nisu uzajamno disjunktni} \end{array}$$

Skup koji se sastoji od svih mogućih podskupova skupa X naziva se *partitivni skupa* skupa X i označava sa $P(X)$. Na primer, za $X = \{a, b, c\}$ imamo da je

$$P(X) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\}\}.$$

Primetimo da važi $\emptyset \in P(X)$ i $X \in P(X)$. (ali da nije $X \subseteq P(X)$!)

Operacije sa skupovima

Najvažnije i najčešće operacije sa skupovima su *unija*, *presek*, *razlika*, *simetrična razlika* i *komplement.* Za skupove X i Y ove operacije se definišu na sledeći način:

$$\begin{array}{rrl} \text{Unija:} & X \cup Y = & \{z : z \in X \text{ ili } z \in Y\} \\ \text{Presek:} & X \cap Y = & \{z : z \in X \text{ i } z \in Y\} \\ \text{Razlika:} & X \setminus Y = & \{z : z \in X \text{ i } z \notin Y\} \\ \text{Simetrična razlika:} & X \Delta Y = & (X \setminus Y) \cup (Y \setminus X) \end{array}$$

Komplement $\overline{X}$ skupa X sadrži sve elemente koji ne pripadaju skupu X. Da bi ova definicija imala smisla (i da $\overline{X}$ ne bi sadržao i suvišne elemente kao što su ljudi, životinje, biljke, ...) svi skupovi sa kojima radimo moraju da budu podskupovi nekog većeg skupa, tzv. *univerzuma* U. Tada je

$$\text{Komplement:} \quad \overline{X} = \quad \{z \in U : z \notin X\}.$$

Zgodno slikovno predstavljanje operacija sa skupovima je pomoću *Venovih dijagrama*. Pogledajte sliku 1.1. Ako zamislimo skupove X i Y kao unutrašnjosti odgovarajućih krugova, tada osenčene površine na slikama 1.1a,b,c,d,e redom predstavljaju skupove $X \cup Y$, $X \cap Y$, $X \setminus Y$, $X \Delta Y$ i $\overline{X}$.

Ovde idu Venovi dijagrami.

Slika 1.1: Operacije sa skupovima

Za ove operacije sa skupovima važe odredjeni zakoni. Najvažniji od njih su navedeni u sledećoj teoremi.

Teorema 1.1.1 *Neka su X, Y i Z skupovi. Tada važi:*

(a) Asocijativnost:

$$\begin{aligned} X \cup (Y \cup Z) &= (X \cup Y) \cup Z \\ X \cap (Y \cap Z) &= (X \cap Y) \cap Z \end{aligned}$$

(b) Komutativnost:

$$\begin{aligned} X \cup Y &= Y \cup X \\ X \cap Y &= Y \cap X \end{aligned}$$

(c) Apsorptivnost:

$$\begin{aligned} X \cap (X \cup Y) &= X \\ X \cup (X \cap Y) &= X \end{aligned}$$

(d) Distributivnost:

$$\begin{aligned} X \cap (Y \cup Z) &= (X \cap Y) \cup (X \cap Z) \\ X \cup (Y \cap Z) &= (X \cup Y) \cap (X \cup Z) \end{aligned}$$

(e) De Morganovi zakoni:

$$X \setminus (Y \cup Z) = (X \setminus Y) \cap (X \setminus Z)$$
$$X \setminus (Y \cap Z) = (X \setminus Y) \cup (X \setminus Z)$$

Dokaz Dokazaćemo samo prvi de Morganov zakon. Dokazivanje ostalih zakona može poslužiti čitaocu za vežbu.

Neka je $x \in X \setminus (Y \cup Z)$. To znači da $x \in X$, ali da $x \notin Y \cup Z$. Iz $x \notin Y \cup Z$ sledi da $x \notin Y$ i $x \notin Z$. Dalje, iz $x \in X$ i $x \notin Y$ sledi da $x \in X \setminus Y$ i slično iz $x \in X$ i $x \notin Z$ sledi da $x \in X \setminus Z$, pa važi da $x \in (X \setminus Y) \cap (X \setminus Z)$. Kako ovo važi za svaki element skupa $X \setminus (Y \cup Z)$, zaključujemo da je

$$X \setminus (Y \cup Z) \subseteq (X \setminus Y) \cap (X \setminus Z). \tag{1.1}$$

Neka je sada $x \in (X \setminus Y) \cap (X \setminus Z)$. Ovo znači da $x \in X \setminus Y$ i $x \in X \setminus Z$. Odavde dobijamo da je $x \in X$, $x \notin Y$ i $x \notin Z$. Iz $x \notin Y$ i $x \notin Z$ sledi da $x \notin Y \cup Z$, pa dobijamo da $x \in X \setminus (Y \cup Z)$. Ovo takodje važi za svaki element skupa $(X \setminus Y) \cap (X \setminus Z)$, pa zaključujemo da je

$$(X \setminus Y) \cap (X \setminus Z) \subseteq X \setminus (Y \cup Z). \tag{1.2}$$

Iz (1.1) i (1.2) sledi da je

$$X \setminus (Y \cup Z) = (X \setminus Y) \cap (X \setminus Z). \quad \blacksquare$$

Ako su $X_1, X_2, \ldots, X_n$ skupovi, njihova unija $X_1 \cup X_2 \cup \ldots \cup X_n$ može kraće da se zapiše kao

$$\bigcup_{i=1}^{n} X_i.$$

Slično se presek $X_1 \cap X_2 \cap \ldots \cap X_n$ kraće zapisuje kao

$$\bigcap_{i=1}^{n} X_i.$$

Zakoni iz teoreme 1.1.1 važe i u slučaju kada imamo više skupova, i koristeći skraćeni zapis, oni glase:

Distributivnost:

$$\begin{aligned} X \cap \left(\bigcup_{i=1}^{n} Y_i \right) &= \bigcup_{i=1}^{n} (X \cap Y_i) \\ X \cup \left(\bigcap_{i=1}^{n} Y_i \right) &= \bigcap_{i=1}^{n} (X \cup Y_i) \end{aligned}$$

De Morganovi zakoni:

$$\begin{aligned} X \setminus \left(\bigcup_{i=1}^{n} Y_i \right) &= \bigcap_{i=1}^{n} (X \setminus Y_i) \\ X \setminus \left(\bigcap_{i=1}^{n} Y_i \right) &= \bigcup_{i=1}^{n} (X \setminus Y_i) \end{aligned}$$

Proizvod skupova

Kao što već znamo, $\{x, y\}$ označava skup koji sadrži elemente x i y. Skup $\{x, y\}$ se ponekad naziva i *neuredjeni par* x i y. Primetimo da je $\{x, y\}$ isto što i $\{y, x\}$, kao i da $\{x, y\}$ ima samo jedan element ako je $x = y$.

U primenama se često nameće potreba za razlikovanjem elemenata u paru. Stoga uvedimo notaciju (x, y) za *uredjeni par* x i y. Pritom važi:

$$(x, y) = (z, t) \text{ ako i samo ako } x = z \text{ i } y = t.$$

Napomena Zanimljivo je da uredjeni par može da se definiše pomoću neuredjenog para na sledeći način:

$$(x, y) = \{\{x\}, \{x, y\}\}.$$

Slično se definiše i *uredjena n-torka* $(x_1, x_2, \ldots, x_n)$ koja se sastoji od elemenata $x_1, x_2, \ldots, x_n$. Pritom važi:

$$(x_1, x_2, \ldots, x_n) = (y_1, y_2, \ldots, y_n) \text{ ako i samo ako je } x_i = y_i \text{ za } i = 1, 2, \ldots, n.$$

Poslednja operacija koju spominjemo je *proizvod* $X \times Y$ skupova X i Y. Proizvod skupova X i Y je skup svih uredjenih parova (x, y), gde $x \in X$ i $y \in Y$, ili preciznije,

$$X \times Y = \{(x, y) \colon x \in X, y \in Y\}.$$

Na primer, za $X = \{1, 2, 3\}$ i $Y = \{a, b\}$ imamo da je

$$\begin{aligned} X \times Y &= \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}, \\ Y \times X &= \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3)\}. \end{aligned}$$

Primetimo da u opštem slučaju $X \times Y$ nije isto što i $Y \times X$, tj. proizvod skupova nije komutativan.

Slično proizvodu dva skupa, proizvod $X_1 \times X_2 \times \ldots \times X_n$ skupova X_1, X_2,...,X_n, ili kraće

$$\prod_{i=1}^{n} X_n,$$

definiše se kao skup svih uredjenih n-torki $(x_1, x_2, \ldots, x_n)$ tako da za $i = 1, 2, \ldots, n$ važi $x_i \in X_i$.

Proizvod skupa X sa samim sobom kraće se označava stepenom uz X, tj.

$$X \times X = X^2, \quad X \times X \times X = X^3, \quad X \times X \times X \times X = X^4, \quad \ldots$$

Zadaci

1.2 Funkcije

Sa funkcijama ili preslikavanjima, kako se drugačije zovu, sreli smo se već u srednjoškolskoj matematici. Tada smo naučili da se funkcija definiše pravilom preslikavanja koje elementima jednog skupa dodeljuje elemente drugog skupa. Na primer, jedna moguća funkcija je $f_1(n) = 2n - 1$, gde je $n \in N$. Isto tako se može zadati i funkcija $f_2(x) = 2x - 1$, gde je $x \in R$. Ovakvo predstavljanje funkcija naglašava samo pravilo preslikavanja. Pri tome se obično kaže kom skupu pripadaju argumenti funkcije (s tim što se ponekad koristimo logikom da n označava prirodan broj, dok x označava realan broj), medjutim skoro nikad se ne kaže kom skupu pripadaju vrednosti funkcija. Zbog toga je ovo *intuitivno predstavljanje* funkcija.

Matematička definicija funkcija

Definicija 1.2.1 *Pod funkcijom se podrazumeva uredjena trojka (A, B, f), gde je $f \subseteq A \times B$, pri čemu za svako $x \in A$ postoji tačno jedno $y \in B$ tako da $(x, y) \in f$. Skup A se naziva* domen*, skup B se naziva* kodomen*, a f je* pravilo preslikavanja*. Činjenica da funkcija preslikava elemente domena A u elemente kodomena B pomoću pravila preslikavanja f se zapisuje pomoću*

$$f : A \mapsto B,$$

a za $(x, y) \in f$ ravnopravno (i češće) pišemo $f(x) = y$. Samo pravilo preslikavanja f se zadaje formulom ili navodjenjem parova elemenata (x, y) koji pripadaju f.

Definicija 1.2.2 *Skup $f(A) = \{f(x) \,|\, x \in A\}$ se naziva* slika *funkcije f.*

Primer Funkcija $f_1(n) = 2n - 1$ se pravilno zapisuje na sledeći način:

$$f_1 : N \mapsto N, \quad f_1(n) = 2n - 1,$$

dok se funkcija $f_2(x) = 2x - 1$ zapisuje pomoću

$$f_2 : R \mapsto R, \quad f_2(x) = 2x - 1.$$

Primer Ako je $A = \{1, 2, 3\}$, a $B = \{1, 3, 5\}$, tada možemo definisati funkciju f_3 pomoću

$$f_3 : A \mapsto B, \quad f_3(a) = 2a - 1,$$

ili drugačije

$$f_3 : A \mapsto B, \quad f_3 = \{(1, 1), (2, 3), (3, 5)\}.$$

U poslednjem slučaju smo funkciju definisali pomoću navodjenja svih parova elemenata koji joj pripadaju.

Vrste funkcija

Važni i najčešće korišćeni tipovi funkcija u matematici su dati u sledećoj definiciji.

Definicija 1.2.3 *Funkcija $f : A \mapsto B$ naziva se* 1-1 *ukoliko važi*

$$(\forall x_1, x_2 \in A) \quad x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2).$$

Funkcija $f : A \mapsto B$ naziva se na *ukoliko važi*

$$(\forall y \in B)\,(\exists x \in A) \quad f(x) = y.$$

Funkcija $f : A \mapsto B$ naziva se bijekcija *ili* obostrano jednoznačno preslikavanje *ako je funkcija istovremeno i 1-1 i na.*

Primer Funkcija $a : \{1,2\} \mapsto \{1,3,5\}$ data pravilom preslikavanja $a(x) = 2x - 1$ je 1-1, ali nije na, jer se nijedan element domena ne preslikava u element 5 iz kodomena. Funkcija $b : \{1,2,3\} \mapsto \{1,3\}$ data pravilom preslikavanja $b = \{(1,1),(2,3),(3,1)\}$ jeste na, ali nije 1-1, jer se elementi 1 i 3 domena preslikavaju u isti element kodomena. Na kraju, funkcija $c : \{1,2,3\} \mapsto \{1,3,5\}$ data pravilom preslikavanja $c(x) = 2x - 1$ jeste i 1-1 i na, pa zaključujemo da je to bijekcija.

Funkcija $f : A \mapsto B$ se može slikovno predstaviti tako što najpre predstave domen A i kodomen B funkcije, a onda se usmerenim linijama svaki element $x \in A$ poveže sa vrednošću $f(x) \in B$. Na sl. 1.2 su predstavljene funkcije a, b i c iz gornjeg primera.

Slikovno predstavljanje funkcija a, b i c.

Slika 1.2: Slikovno predstavljanje funkcija

Operacije sa funkcijama

S obzirom da su funkcije u stvari skupovi parova elemenata, sa njima možemo da vršimo sve operacije kao i sa skupovima. Medjutim, pored njih, postoje i operacije koje su namenjene samo funkcijama.

Definicija 1.2.4 *Ako su date funkcije $f : A \mapsto B$ i $g : B \mapsto C$, tada se pod* slaganjem funkcija *f i g podrazumeva funkcija $g \circ f : A \mapsto C$ data pravilom preslikavanja*

$$g \circ f(x) = g(f(x)), \quad x \in A.$$

Definicija 1.2.5 *Ako su dati funkcija $f : A \mapsto B$ i podskup $A' \subseteq A$, tada se pod* redukcijom funkcije *f na poddomen A', u oznaci $f|_{A'}$, podrazumeva funkcija $f' : A' \mapsto B$ data pravilom preslikavanja*

$$f|_{A'}(x) = f(x), \quad x \in A'.$$

Definicija 1.2.6 *Za proizvoljan skup A, funkcija $i_A : A \mapsto A$ data pravilom preslikavanja*

$$i_A(x) = x, \quad x \in A$$

naziva se identička funkcija na skupu A.

Definicija 1.2.7 *Ako je data funkciju $f : A \mapsto B$, tada se za funkciju $g : B \mapsto A$ kaže da je* inverzna funkcija *za funkciju f ako važi*

$$g(f(x)) = x, \qquad x \in A,$$
$$f(g(y)) = y, \qquad y \in B,$$

tj. ako važi

$$g \circ f = i_A \quad i \quad f \circ g = i_B.$$

Inverzna funkcija za funkciju f se obično obeležava sa f^{-1}.

Inverzna funkcija ne postoji za svaku funkciju. To možemo videti i iz sledeće teoreme.

Teorema 1.2.8 *Za funkciju $f : A \mapsto B$ postoji inverzna funkcija ako i samo ako je f bijekcija.*

Dokaz Pretpostavimo da funkcija $f : A \mapsto B$ ima inverznu funkciju $f^{-1} : B \mapsto A$ i dokažimo da je f bijekcija. Funkcija f je 1-1, jer ako je $f(x_1) = f(x_2) = y$ za $x_1 \neq x_2$, tada iz definicije inverzne funkcije sledi da je $f^{-1}(y) = f^{-1}(f(x_1)) = x_1$ i $f^{-1}(y) = f^{-1}(f(x_2)) = x_2$, što je kontradiktorno činjenici da je f^{-1} funkcija i da, prema tome, može da ima samo jednu vrednost za datu vrednostargumenta. S druge strane, funkcija f je na, jer za svako $y \in B$ važi $f(f^{-1}(y)) = y$.

Pretpostavimo sada da je f bijekcija i dokažimo da onda postoji funkcija h koja je njena inverzna funkcija. Funkciju h ćemo definisati na sledeći način:

$$h \subseteq B \times A, \quad (y, x) \in h \text{ ako i samo ako je } f(x) = y.$$

Primetimo da smo ovim, u stvari, samo definisali jedan podskup $h \subseteq B \times A$, pa stoga moramo tek da pokažemo da je h zaista funkcija, tj. da za svako $y \in B$ postoji tačno jedno $x \in A$ tako da je $h(y) = x$. Najpre, pošto je funkcija f na, to za $y \in B$ postoji $x \in A$ tako da je $f(x) = y$, pa po definiciji h važi i $(y, x) \in h$. Dalje, pošto je funkcija f i 1-1, ovakvo x je jedinstveno, pa smo se zaista uverili da je h funkcija i možemo slobodno da pišemo

$$h : B \mapsto A, \quad h(y) = x \text{ ako i samo ako je } f(x) = y.$$

Sada je jasno da važi $h(f(x)) = x$ i $f(h(y)) = y$, pa je h inverzna funkcija za f.
■

Permutacije

Pod *permutacijom* skupa A se podrazumeva svaka bijekcija $f : A \mapsto A$ skupa A na samog sebe. Skup svih permutacija skupa A obično se obeležava sa $\mathrm{Sym}\,(A)$. Za skup $\mathrm{Sym}\,(A)$ svih permutacija skupa A važi sledeća teorema, koju ćemo dokazati kasnije. Ona ilustruje algebarsku strukturu skupa $\mathrm{Sym}\,(A)$.

Teorema 1.2.9 *Ako je dat skup A, tada za skup* $\mathrm{Sym}\,(A)$ *važe sledeće osobine:*

(i) (zatvorenost)

$$(\forall f, g \in \mathrm{Sym}\,(A)) \quad f \circ g \in \mathrm{Sym}\,(A);$$

(ii) (asocijativnost)

$$(\forall f, g, h \in \mathrm{Sym}\,(A)) \quad f \circ (g \circ h) = (f \circ g) \circ h;$$

(iii) (postojanje neutralnog elementa)

$$(\exists i_A \in \mathrm{Sym}\,(A))\,(\forall x \in A) \quad i_A(x) = x;$$

(iv) (postojanje inverznog elementa)

$$(\forall f \in \mathrm{Sym}\,(A))\,(\exists f^{-1} \in \mathrm{Sym}\,(A)) \quad f \circ f^{-1} = f^{-1} \circ f = i_A. \quad \blacksquare$$

Zadaci

1.3 Relacije

Relacija, u najkraćem, predstavlja odnos izmedju elemenata nekih skupova. Stroga matematička definicija je sledeća.

Definicija 1.3.1 *Ako su dati skupovi A_1, A_2, $\ldots$, A_k, $k \in N$, tada se pod* relacijom *dužine k izmedju elemenata skupova A_1, A_2, $\ldots$, A_k podrazumeva podskup $\rho \subseteq A_1 \times A_2 \times \ldots \times A_k$. Ako $(x_1, x_2, \ldots, x_k) \in \rho$, tada kažemo da su elementi x_1, x_2, $\ldots$, x_k u relaciji ρ. S druge strane, ako je $A_1 = A_2 = \ldots = A_k = A$, tada kažemo da je ρ relacija dužine k na skupu A.*

Primer Razmotrimo sledeće skupove:

$$\begin{aligned} A &= \{\text{ Ćira, Dragan, Marko }\}, \\ B &= \{\text{ logika, algebra, diskretna matematika }\}, \\ C &= \{\text{ ponedeljak, utorak, sreda, četvrtak, petak }\}. \end{aligned}$$

Tada

$$\begin{aligned} \rho = \{ & (\text{Ćira, logika, utorak}), \\ & (\text{Dragan, algebra, utorak}), \\ & (\text{Dragan, diskretna matematika, četvrtak}), \\ & (\text{Marko, diskretna matematika, petak})\} \end{aligned}$$

predstavlja relaciju dužine 3, koja može da predstavlja obaveze profesora i asistenata u pogledu predmeta i datuma.

Definicija 1.3.2 *Relacija $\rho \subseteq A \times B$ dužine 2 se naziva* binarna relacija. *Uobičajeno je da se za elemente $x \in A$ i $y \in B$ koji su u relaciji ρ umesto $(x, y) \in \rho$ piše $x\,\rho\,y$. Skup $\{a \in A \mid a\,\rho\,b \text{ za neko } b \in B\}$ se naziva* domen *relacije ρ, a skup $\{b \in B \mid a\,\rho\,b \text{ za neko } a \in A\}$ se naziva* kodomen *relacije ρ.*

Napomena Primetimo da je svaka funkcija $f : A \mapsto B$, takodje binarna relacija, jer je $f \in A \times B$.

Primer Na skupu $\{1, 2, 3, 4, 6\}$ možemo da definišemo binarnu relaciju ρ tako što ćemo da je $x\,\rho\,y$ ako je x manje od y i x deli y. Relaciju ρ tada čine sledeći parovi elemenata

$$\rho = \{(1, 2), (1, 3), (1, 4), (1, 6), (2, 4), (2, 6), (3, 6)\}.$$

Ova relacija je slikovno predstavljena na sl. 1.3a slično načinu na koji se predstavljaju funkcije, tako što se usmerenim linijama povežu parovi elemenata koji su u relaciji.

Načini predstavljanja relacije ρ.

Slika 1.3: Načini predstavljanja relacija

Medjutim, binarna relacija ρ na konačnom skupu A može se predstaviti još na dva načina:

- tablično - tako što se nacrta tablica čije vrste i kolone predstavljaju elemente A, a zatim se u preseku vrste x i kolone y stavlja 1 ukoliko je $x\,\rho\,y$, a 0 ukoliko nije $x\,\rho\,y$.
- pomoću orijentisanih grafova - tako što se svaki element skupa A predstavi čvorom, a zatim se čvorovi x i y povežu usmerenom linijom od x ka y ako je $x\,\rho\,y$.

Ova dva načina predstavljanja su prikazana na sl. 1.3b i sl. 1.3c.

Kao i funkcije, i relacije se mogu slagati.

Definicija 1.3.3 *Neka su date relacije $\rho \subseteq A \times B$ i $\sigma \subseteq B \times C$. Tada se pod* slaganjem relacija *ρ i σ podrazumeva relacija $\rho \circ \sigma \subseteq A \times C$ odredjena sa*

$$\rho \circ \sigma = \{(a, c) \mid \textit{postoji } b \in B \textit{ tako da je } a\,\rho\,b \textit{ i } b\,\sigma\,c\}.$$

Napomena S obzirom da su funkcije poseban slučaj relacija, i slaganje funkcija je poseban slučaj slaganja relacija. Medjutim, primetimo veoma bitnu razliku: slaganje funkcija $f : A \mapsto B$ i $g : B \mapsto C$ označava se sa $g \circ f$, dok se slaganje relacija $\rho \subseteq A \times B$ i $\sigma \subseteq B \times C$ označava sa $\rho \circ \sigma$. Znači, kod slaganja funkcija prvu funkciju stavljamo iza $\circ$, dok kod slaganja relacija prvu relaciju stavljamo ispred $\circ$.

Nadalje ćemo posmatrati samo binarne relacije kod kojih se domen i kodomen poklapaju i pritom posvetiti pažnju važnim vrstama relacija—relacijama ekvivalencije i relacijama poretka.

Relacije ekvivalencija

Definicija 1.3.4 *Relacija ρ na skupu A je:*

(i) refleksivna*, ako*

$$(\forall x \in A) \quad x\,\rho\,x;$$

(ii) simetrična*, ako*

$$(\forall x, y \in A) \quad x\,\rho\,y \;\Rightarrow\; y\,\rho\,x;$$

(iii) tranzitivna*, ako*

$$(\forall x, y, z \in A) \quad x\,\rho\,y \;\wedge\; y\,\rho\,z \;\Rightarrow\; x\,\rho\,z.$$

Definicija 1.3.5 *Relacija ρ na skupu A je* relacija ekvivalencije *ako je refleksivna, simetrična i tranzitivna.*

Primer Definišimo relaciju na skupu prirodnih brojeva, tako da su dva prirodna broja u relaciji ako i samo ako su jednaki. Ova relacija je refleksivna, jer je svaki broj jednak samom sebi, simetrična, jer iz $x = y$ sigurno sledi da je $y = x$, i tranzitivna, jer iz $x = y$ i $y = z$ sledi da je $x = z$. Relacija jednakosti je svakako najjednostavniji primer relacije ekvivalencije i njena svojstva su služila kao inspiracija za definiciju relacije ekvivalencije.

Primer Relacija ρ na skupu prirodnih brojeva, tako da su dva prirodna broja u relaciji ρ ako je njihova razlika deljiva sa 4 (tj. ako daju isti ostatak pri deljenju sa 4) je takodje relacije ekvivalencije. Naime, ova relacija je refleksivna, jer $4|x - x = 0$, simetrična, jer iz $4|x - y$ sledi da $4|y - x$, i tranzitivna, jer iz $4|x - y$ i $4|y - z$ sledi da $4|(x - y) + (y - z) = x - z$.

Primer Neka su dati skup $A = \{1, 2, 3, 4, 5, 6, 7\}$ i njegovi uzajamno disjunktni podskupovi $B_1 = \{1, 2, 3\}$, $B_2 = \{4, 5\}$ i $B_3 = \{6, 7\}$. Na skupu A možemo da definišemo relaciju ρ na sledeći način:

$$x\,\rho\,y \quad \Leftrightarrow \quad x \text{ i } y \text{ pripadaju istom podskupu } B_i.$$

Ova relacija je očigledno refleksivna i simetrična, a tranzitivnost sledi iz činjenice da ako je $x\,\rho\,y$ i $y\,\rho\,z$ tada x i z pripadaju istom podskupu kome pripada i y, a kako y pripada tačno jednom podskupu B_i, jer su oni uzajamno disjunktni, to i x i z pripadaju ovom istom podskupu B_i, pa zaključujemo da je $x\,\rho\,z$. Predstavljanje ove relacije pomoću orijentisanih grafova dato je na sl. 1.4.

Poslednji primer ujedno ilustruje i sledeću definiciju.

Predstavljanje relacije ekvivalencije pomoću orijentisanih grafova

Slika 1.4: Primer relacije ekvivalencije

Definicija 1.3.6 *Neka je ρ relacija ekvivalencije na skupu A i neka je $x \in A$. Skup*

$$C_x = \{y \in A \mid x \rho y\}$$

naziva se klasa ekvivalencije *elementa x.*

Teorema 1.3.7 *Neka je ρ relacija ekvivalencije na skupu A. Tada važi:*

(i) $(\forall x, y \in A) \quad C_x = C_y \quad \vee \quad C_x \cap C_y = \emptyset$.

(ii) $A = \bigcup_{x \in A} C_x$.

Dokaz (i) Pretpostavimo da je $C_x \cap C_y \neq \emptyset$ i neka $z \in C_x \cap C_y$. Tada je $x \rho z$ i $y \rho z$, pa kako je relacija ρ simetrična i tranzitivna, dobijamo da je $x \rho y$. Sada iz $w \in C_x$ sledi da je $w \rho x$ i $x \rho y$, pa iz tranzitivnosti imamo $w \rho y$, tj. $w \in C_y$. Takodje važi i obrnuto, tj. iz $w \in C_y$ sledi da je $w \rho y$ i $y \rho x$, pa imamo i $w \rho x$, tj. $w \in C_x$. Ovo pokazuje da je sada $C_x = C_y$.

(ii) Kako za svako $x \in A$ važi da je $C_x \subseteq A$, to sledi i da je $\bigcup_{x \in A} C_x \subseteq A$. S druge strane, za svako $y \in A$ važi da je $y \in C_y \subseteq \bigcup_{x \in A} C_x$, pa zaključujemo da je $A = \bigcup_{x \in A} C_x$. ■

Iz prethodne teoreme vidimo da su različite klase ekvivalencije uzajamno disjunktne, a da unija svih klasa ekvivalencije daje ceo skup. Podela skupa na podskupove sa ovakvim svojstvima drugačije se naziva *particija* skupa, tačnije

Definicija 1.3.8 *Neka je A proizvoljan skup i $\mathcal{C} \subseteq P(A)$. Ukoliko važi*

$$(\forall X, Y \in \mathcal{C}) \quad X = Y \quad \vee \quad X \cap Y = \emptyset$$

i

$$A = \bigcup_{X \in \mathcal{C}} X,$$

tada se $\mathcal{C}$ naziva particija *skupa A.*

Iz teoreme 1.3.7 vidimo da klase ekvivalencije obrazuju particiju skupa. Medjutim, važi i obratno: svakoj particiji skupa odgovara relacija ekvivalencije na tom skupu čije su klase ekvivalencije upravo elementi particije.

Teorema 1.3.9 *Neka je $\mathcal{C}$ particija skupa A. Definišimo relaciju ρ na skupu A pomoću*

$$x \rho y \quad \Leftrightarrow \quad x \text{ i } y \text{ pripadaju istom elementu particije } \mathcal{C}.$$

Tada je ρ relacija ekvivalencije čije su klase ekvivalencije upravo elementi particije $\mathcal{C}$.

Dokaz Relacija ρ je refleksivna i simetrična po svojoj definiciji. Neka je sada $x\,\rho\,y$ i $y\,\rho\,z$. Pošto je $\mathcal{C}$ particija skupa A, postoji tačno jedan podskup $C \in \mathcal{C}$ tako da $y \in C$ (u suprotnom, ako bi postojala dva različita podskupa koji sadrže y onda bi oni imali neprazan presek, što je nemoguće). Sada iz $x\,\rho\,y$ sledi da $x \in C$ i iz $y\,\rho\,z$ sledi i da $z \in C$, tako da zaključujemo da važi $x\,\rho\,z$, jer pripadaju istom elementu C particije $\mathcal{C}$. Prema tome, ρ je relacija ekvivalencije.

S druge strane, kao što smo već videli, za svako $x \in A$ postoji tačno jedan podskup $C \in \mathcal{C}$ tako da $x \in C$. Klasu ekvivalencije C_x elementa x po definiciji čine svi oni elementi $y \in A$ koji takodje pripadaju C, odakle vidimo da je $C_x = C$, tj. klase ekvivalencije su upravo elementi particije $\mathcal{C}$. ∎

Relacije poretka

Definicija 1.3.10 *Relacija ρ na skupu A je* antisimetrična *ako važi*

$$(\forall x, y \in A) \quad x\,\rho\,y \ \wedge\ y\,\rho\,x \quad \Rightarrow \quad x = y.$$

Definicija 1.3.11 *Relacija ρ na skupu A je* relacija poretka *ako je refleksivna, antisimetrična i tranzitivna.*

Relacija poretka se takodje naziva i parcijalno uredjenje.

Definicija 1.3.12 *Uredjeni par (A, ρ), gde je ρ relacija poretka na skupu A, naziva se* parcijalno uredjen skup*.*

Primer Relacija "manje ili jednako" $\leq$ na skupu N je relacija poretka, jer je

$$\begin{gathered}(\forall x \in N) \quad x \leq x,\\ (\forall x, y \in N) \quad x \leq y \ \wedge\ y \leq x \quad \Rightarrow \quad x = y,\\ (\forall x, y, z \in N) \quad x \leq y \ \wedge\ y \leq z \quad \Rightarrow \quad x \leq z.\end{gathered}$$

Kao i kod jednakosti, i u ovom slučaju su svojstva relacije $\leq$ vodila ka definiciji relacije poretka.

Primer Relacija "deliti" $\mid$ na skupu N je relacija poretka, jer je

$$\begin{gathered}(\forall x \in N) \quad x \mid x,\\ (\forall x, y \in N) \quad x \mid y \ \wedge\ y \mid x \quad \Rightarrow \quad x = y,\\ (\forall x, y, z \in N) \quad x \mid y \ \wedge\ y \mid z \quad \Rightarrow \quad x \mid z.\end{gathered}$$

Primer Za proizvoljan skup A relacija $\subseteq$ na skupu $P(A)$ je relacija poretka, jer je

$$\begin{gathered}(\forall X \in P(A)) \quad X \subseteq X,\\ (\forall X, Y \in P(A)) \quad X \subseteq Y \ \wedge\ Y \subseteq X \quad \Rightarrow \quad X = Y,\\ (\forall X, Y, Z \in P(A)) \quad X \subseteq Y \ \wedge\ Y \subseteq Z \quad \Rightarrow \quad X \subseteq Z.\end{gathered}$$

S obzirom na gornje primere relacija $\leq$ i $\subseteq$ u matematici je postalo uobičajeno da se relacija poretka označava simbolom $\preceq$. Sada ćemo definisati nekoliko često sretanih pojmova kod parcijalnih uredjenja.

Definicija 1.3.13 *Neka je* $(A, \preceq)$ *parcijalno uredjenje i neka je* $B \subseteq A$. *Za element* $a \in A$ *se kaže da je* donja granica *za* B *ako je*

$$(\forall x \in B) \quad a \preceq x.$$

Element $a \in A$ *je* najmanji element *u* B *ako je* $a \in B$ *i* a *je donja granica za* B.

Za element $a \in A$ *se kaže da je* gornja granica *za* B *ako je*

$$(\forall x \in B) \quad x \preceq a.$$

Element $a \in A$ *je* najveći element *u* B *ako je* $a \in B$ *i* a *je gornja granica za* B.

Primetimo da kod parcijalnog uredjenja mogu da postoje elementi koji nisu uporedivi, pa stoga mogu da postoje i podskupovi koji nemaju najmanji element, odnosno najveći element. Na primer, ako posmatramo relaciju poretka $\subseteq$ na skupu $P(\{1,2,3\})$, tada skup $\{\{1\},\{2\},\{3\}\}$ nema niti najmanji, niti najveći element.

Svojstva relacije poretka $\leq$ na skupu N su poslužila kao inspiracija za još dve važne vrste uredjenja.

Definicija 1.3.14 *Relacija poretka* $\preceq$ *na skupu* A *je* linearno uredjenje *ako za svaka dva elementa* $x, y \in A$ *važi* $x \preceq y$ *ili* $y \preceq x$.

Definicija 1.3.15 *Linearno uredjenje* $\preceq$ *na skupu* A *je* dobro uredjenje *ako svaki konačan podskup od* A *ima najmanji element u odnosu na uredjenje* $\preceq$.

Za slikovno predstavljanje relacija poretka na konačnom skupu mogu se iskoristiti tzv. Haseovi dijagrami. Da bismo mogli da opišemo konstrukciju Haseovog dijagrama potrebna nam je sledeća pomoćna definicija.

Definicija 1.3.16 *Neka je* ρ *relacija poretka na konačnom skupu* A *i neka je* $x \in A$ *proizvoljni element skupa* A. *Za element* $y \in A$ *se kaže da je* neposredni prethodnik *elementa* x *ako je* $y \, \rho \, x$, $y \neq x$ *i važi*

$$(\forall z \in A) \quad y \, \rho \, z \ \wedge \ z \, \rho \, x \quad \Rightarrow \quad z = y \ \vee \ z = x.$$

Drugim rečima, y je neposredni prethodnik od x ako nijedan drugi element skupa A ne može da se "smesti" izmedju y i x.

Kada je data relacija poretka ρ na konačnom skupu A, tada za svaki element skupa A možemo da odredimo *nivo* u odnosu na relaciju ρ. Naime, element $x \in A$ je na nivou 0 ako nema neposrednog prethodnika. U suprotnom, element x je na nivou k, $k > 0$, ako ima bar jednog neposrednog prethodnika na nivou $k-1$, dok se svi ostali neposredni prethodnici nalaze na nivoima najviše $k-1$.

Sada se Haseov dijagram relacije ρ dobija na sledeći način: elementi skupa A se poredjaju po nivoima počev od nivoa 0 na dnu, do najvećeg nivoa na vrhu i svaki element se spaja linijom sa svim svojim neposrednim prethodnicima. Na sl. 1.5 su prikazani Haseovi dijagrami za relacije $\subseteq$ na skupu $P(\{1,2,3\})$ i $|$ na skupu $\{1,2,3,4,5,6,7,8,9\}$.

Haseov dijagram za dve relacije poretka

Slika 1.5: Haseov dijagram relacije poretka

Iz načina konstrukcije Haseovog dijagrama možemo da vidimo da su elementi na istom nivou neuporedivi. Iz ovoga zaključujemo da kod linearnog uredjenja, kod koga su svaka dva elementa uporediva, na svakom nivou postoji tačno jedan element. Stoga je Haseov dijagram linearnog uredjenja veoma jednostavan: on predstavlja niz elemenata skupa poredjanih jedan iznad drugog.

1.4 Matematička indukcija

Matematička indukcija je jedan od najčešćih načina dokazivanja matematičkih tvrdjenja u diskretnoj matematici, ali se često sreće i u drugim granama matematike. S obzirom na njenu toliku rasprostranjenost, važno je da se sa njom što bolje upoznamo.

Neka je $S(n)$ neko tvrdjenje koje zavisi od prirodnog broja n; na primer, $S(n)$ može da bude tvrdjenje "zbir prvih n neparnih brojeva jednak je n^2". Računajući ove zbirove možemo da proverimo da tvrdjenje važi za neke male vrednosti n. Na primer,

$$1 = 1^2, \quad 1+3 = 2^2, \quad 1+3+5 = 3^2, \quad 1+3+5+7 = 4^2,$$
$$1+3+5+7+9 = 5^2.$$

Čak i ako tvrdjenje proverimo pomoću računara za prvih milion vrednosti n, to još uvek nije dokaz. Ko zna, milion i prvi broj i dalje može da bude kontraprimer. Ispravnost ovog tvrdjenja dokazujemo pomoću *principa matematičke indukcije*, koji se sastoji u sledećem:

(i) Dokazati da je $S(1)$ tačno;

(ii) Dokazati da važi "ako je $S(n)$ tačno, tada je i $S(n+1)$ tačno"; pritom, dokaz mora da važi za proizvoljan prirodan broj n.

Dokaz pod (i) se zove *baza indukcije*, dok se dokaz pod (ii) zove *induktivni korak*.

U našem primeru, tvrdjenje $S(n)$ je

$$1 + 3 + \ldots + (2n-1) = n^2.$$

Dokaz ovog tvrdjenja matematičkom indukcijom odvija se na sledeći način:

(i) $S(1)$ je tačno, jer je $1 = 1^2$;

(ii) Ako je za neki broj n tvrdjenje $S(n)$ tačno, tada važi

$$1 + 3 + \ldots + (2n-1) = n^2.$$

Dodajući sa obe strane $2n+1$ dobijamo da važi

$$1+3+\ldots+(2n-1)+(2n+1)=n^2+2n+1=(n+1)^2,$$

što pokazuje da je i $S(n+1)$ tačno.

Ovim je dokaz završen. Deluje jednostavno, zar ne? Da vidimo sada zbog čega je ovo zaista dokaz da tvrdjenje $S(n)$ važi za svaki prirodan broj n. U bazi indukcije najpre dokazujemo da je $S(1)$ tačno. Ako zatim stavimo vrednost $n=1$ u induktivni korak tada dobijamo da je $S(2)$ takodje tačno. Ako sada novu vrednost $n=2$ stavimo u induktivni korak, tada dobijamo da je $S(3)$ takodje tačno. Ponavljajući ovaj postupak, redom dobijamo da su tačna tvrdjenja $S(4)$, $S(5)$, $S(6)$, $\ldots$ i vidimo da na ovaj način možemo da dokažemo da je tvrdjenje $S(n)$ tačno za svaki prirodan broj n. Tačnije, induktivni korak nam daje sledeći beskonačan niz implikacija:

$$S(1)\Rightarrow S(2)\Rightarrow S(3)\Rightarrow S(4)\Rightarrow S(5)\Rightarrow S(6)\Rightarrow\ldots\Rightarrow S(n)\Rightarrow\ldots$$

dok baza indukcije služi da započnemo kretanje po ovom nizu tako što dokazuje tačnost prvog tvrdjenja u njemu.

Primer Dokazati da za svaki prirodan broj n važi $1+2+\ldots+n=\frac{n(n+1)}{2}$.

Dokaz Najpre dokazujemo bazu indukcije. Za $n=1$ tvrdjenje se svodi na $1=\frac{1(1+1)}{2}$, što je tačno. Zatim prelazimo na dokaz induktivnog koraka. Stoga pretpostavimo da je tvrdjenje

$$1+2+\ldots+n=\frac{n(n+1)}{2}$$

tačno za neki prirodan broj n. Dodajući $n+1$ na obe strane dobijamo da važi

$$1+2+\ldots+n+(n+1)=\frac{n(n+1)}{2}+(n+1)=(n+1)\left(\frac{n}{2}+1\right)=\frac{(n+1)(n+2)}{2},$$

što dokazuje da je tvrdjenje tačno i za broj $n+1$. Po principu matematičke indukcije, dokaz je završen. ∎

Primer Dokazati da je za svaki prirodan broj n vrednost izraza 5^n-4n-1 deljiva sa 16.

Dokaz Za $n=1$ imamo da je $5^1-4\cdot1-1=0$, pa je svakako deljivo sa 16. Ako sada pretpostavimo da je tvrdjenje tačno za neki prirodan broj n, tada je 5^n-4n-1 deljivo sa 16. Šta se dešava sa ovim izrazom za $n+1$? Imamo da je

$$\begin{aligned} & 5^{n+1}-4(n+1)-1=5(5^n)-4n-5= \\ = \; & 5(5^n-4n-1)+20n+5-4n-5=5(5^n-4n-1)+16n. \end{aligned}$$

Sada vidimo da je broj $5^{n+1}-4(n+1)-1$ zbir dva broja, od kojih je svaki deljiv sa 16, pa je i on sam deljiv sa 16. Znači, tvrdjenje je tačno i za broj $n+1$, pa je po principu matematičke indukcije dokaz završen. ∎

Pri radu sa matematičkom indukcijom treba paziti da baza indukcije obezbedi važnost prvog tvrdjenja u beskonačnom nizu implikacija koji se dobija ponavljanjem induktivnog koraka. Možete li naći grešku u sledećem primeru?

Primer Neka su l_1, l_2, ..., l_n, $n \geq 2$, različite prave u ravni, tako da nikoje dve nisu paralelne. Dokazati da se sve prave seku u istoj tački.

Lažni dokaz Za $n = 2$ tvrdjenje je tačno, jer se svake dve neparalelne prave seku. Pretpostavimo zato da tvrdjenje važi za neki prirodan broj n i posmatrajmo tvrdjenje za $n+1$. Ako su date prave l_1, l_2,..., l_n, l_{n+1}, tada po indukcijskoj pretpostavci sve prave osim poslednje (tj. prave l_1, l_2, ..., l_{n-1}, l_n) imaju zajedničku tačku; označimo je sa A. Takodje, sve prave osim pretposlednje (tj. prave l_1, l_2, ..., l_{n-1}, l_{n+1}) imaju zajedničku tačku; označimo je sa B. Prava l_1 se nalazi u obe grupe, pa sadrži obe tačke A i B. Slično se i prava l_{n-1} nalazi u obe grupe pa i ona sadrži obe tačke A i B. Kako se l_1 i l_{n-1} seku samo u jednoj tački, to mora da bude $A = B$. Prema tome, sve prave l_1, l_2, ..., l_n, l_{n+1} imaju zajedničku tačku A. ■

Rešenje Iako u prethodnom "dokazu" sve izgleda u redu, tvrdjenje je očigledno netačno. U čemu je onda problem? Označimo tvrdjenje sa $S(n)$. Očigledno je da je $S(2)$ tačno, pa je baza indukcije u redu. Induktivni korak na prvi pogled deluje tačno. Ali kada ga malo bolje pogledamo, vidimo da je moguće zaključiti da se tačke A i B poklapaju samo ako su prave l_1 i l_{n-1} različite, tj. ako je $n \neq 2$. To znači da induktivni korak generiše niz implikacija

$$S(3) \Rightarrow S(4) \Rightarrow S(5) \Rightarrow S(6) \Rightarrow \ldots \Rightarrow S(n) \Rightarrow \ldots$$

ali baza indukcije ne dokazuje prvo tvrdjenje iz ovog niza, tako da dokaz indukcijom nije korektan.

Kada bi mogli da dokažemo da je $S(3)$ tačno, tada bi tvrdjenje važilo za sve prirodne brojeve. Medjutim, jasno je da tri različite prave u ravni ne moraju da se seku u jednoj tački, pa ni $S(3)$ ne može da bude tačno. ■

U nekim slučajevima za dokaz tačnosti tvrdjenja $S(n+1)$ u induktivnom koraku jednostavnije je zameniti pretpostavku da je $S(n)$ tačno tvrdjenje pomoću jače pretpostavke da su sva prethodna tvrdjenja $S(1)$, $S(2)$, ..., $S(n)$ tačna. Ovakav modifikovani princip se naziva *jaka indukcija*, a koristi se na sledeći način:

(i) Dokazati da je $S(1)$ tačno tvrdjenje;

(ii) Dokazati da važi "ako su sva tvrdjenja $S(1)$, $S(2)$, ..., $S(n)$ tačna, tada je i $S(n+1)$ tačno tvrdjenje".

Lako je videti da i ovaj princip garantuje tačnost tvrdjenja $S(n)$ za svaki prirodan broj n. Štaviše, postoji još mnogo drugih varijanti indukcije koje se sve sastoje iz baze indukcije i induktivnog koraka. Njihova glavna odlika je da induktivni korak generiše beskonačan niz implikacija koje služe da se "dodje" do tvrdjenja $S(n)$ za proizvoljan prirodni broj n, a baza indukcije služi da pokaže tačnost uslova u prvoj implikaciji takvog beskonačnog niza.

Primer Definišimo *Fibonačijeve brojeve* F_1, F_2, F_3, ... tako da je $F_1 = 1$ i $F_2 = 1$, dok je svaki sledeći član niza jednak zbiru dva prethodna člana, tj.

$$F_n = F_{n-1} + F_{n-2}, \quad n \geq 3.$$

Prema tome, prvih nekoliko Fibonačijevih brojeva je $1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots$ Dokazati da važi nejednakost

$$F_n \leq \left(\frac{1+\sqrt{5}}{2}\right)^{n-1}.$$

Dokaz Označimo broj $(1+\sqrt{5})/2$ sa ϕ, a tvrdjenje "$F_n \leq \phi^{n-1}$" pomoću $S(n)$. U ovom slučaju, baza indukcije će se sastojati od dokaza dva posebna tvrdjenja $S(1)$ i $S(2)$, dok će induktivni korak imati oblik "ako su tvrdjenja $S(n-1)$ i $S(n)$ tačna, tada je tačno i tvrdjenje $S(n+1)$". Razlog za ovakvu varijantu matematičke indukcije je način definisanja Fibonačijevih brojeva i jedno interesantno svojstvo broja ϕ.

Ako je $n = 1$, tada je $F_1 = 1 = \phi^0 = \phi^{n-1}$, pa je tvrdjenje $S(1)$ tačno. Ako je $n = 2$, tada je $F_2 = 1 < 1,6 < \phi^1 = phi^{n-1}$, pa je i tvrdjenje $S(2)$ tačno.

Pretpostavimo sada da su za neki prirodan broj n tačna tvrdjenja $S(n-1)$ i $S(n)$. Tada je $F_{n-1} \leq \phi^{n-2}$ i $F_n \leq \phi^{n-1}$, pa je

$$F_{n+1} = F_n + F_{n-1} \leq \phi^{n-1} + \phi_{n-2} = \phi^{n-2}(\phi + 1).$$

Važno svojstvo broja ϕ, zbog koga smo i izabrali ovakvu varijantu indukcije, je da važi

$$\phi^2 = \phi + 1.$$

Sada je $F_{n+1} \leq \phi^{n-2}(\phi+1) = \phi^n$, pa je i tvrdjenje $S(n+1)$ tačno. Ovim smo završili dokaz induktivnog koraka i samim tim dokazali da tvrdjenje $S(n)$ važi za sve prirodne brojeve n. ■

Napomena Princip matematičke indukcije je ekvivalentan činjenici da je skup prirodnih brojeva dobro uredjen. Ova ekvivalencija se stoga može iskoristiti za nešto drugačije dokazivanje tvrdjenja koja važe za prirodne brojeve.

Pretpostavimo da imamo tvrdjenje $S(n)$ za koje važi da su tačna tvrdjenja $S(1)$ i tvrdjenje "ako je $S(n)$ tačno, tada je i $S(n+1)$ tačno". Drugačiji način da se dokaže da u tom slučaju $S(n)$ važi za sve prirodne brojeve n je sledeći:

> Pretpostavimo da postoji n tako da tvrdjenje $S(n)$ nije tačno i neka X označava skup svih prirodnih brojeva n za koje tvrdjenje $S(n)$ nije tačno. Kako je skup prirodnih brojeva dobro uredjen, to znači da ako je skup X neprazan, tada on ima najmanji element n_0. Kako je $S(1)$ tačno, imamo da je $n_0 > 1$. Pošto je n_0 najmanji element skupa X, to je $n_0 -$

$1 \notin X$ i tvrdjenje $S(n_0 - 1)$ je tačno. Sada iz induktivnog koraka za $n = n_0 - 1$ dobijamo da je tvrdjenje $S(n_0)$ tačno, tj. da je $n_0 \notin X$, što je kontradikcija. Ova kontradikcija pokazuje da je skup X prazan, tj. da je tvrdjenje $S(n)$ tačno za sve prirodne brojeve n.

Način dokazivanja gde počinjemo rečenicom "Neka je n_0 najmanji broj koji ne zadovoljava tvrdjenje koje želimo da dokažemo" i završavamo kontradikcijom ponekad zamenjuje matematičku indukciju. Oba načina u suštini rade isto, a stvar je okolnosti ili ličnog ukusa koji će se način koristiti.

Zadaci

Glava 2

Kombinatorika

Glavna tema u ovom poglavlju je razvijanje efikasnih metoda za prebrojavanje konačnog skupa X. Kada se X pojavi u složenom problemu, njegovi elementi obično imaju strukturu koju je lako opisati matematičkim jezikom, ali su za njihovo prebrojavanje potrebni mnogo delotvorniji metodi od pukog nabrajanja svih elemenata.

U ovom poglavlju počinjemo da razvijamo takve metode. Prvi odeljak se bavi definicijom i osnovnim principima prebrojavanja, na koje smo se svi toliko navikli da retko obraćamo pažnju na njih. Zbog toga će prvih par teorema iz ovog odeljka možda biti "dosadne", ali su neophodne za strogo zasnivanje kombinatorike. Posle prvog odeljka stvari postaju mnogo "zanimljivije". U drugom i trećem odeljku posmatramo uredjene i neuredjene izbore elemanata skupa. U četvrtom odeljku izučavamo identitete sa binomnim koeficijentima, a u poslednjem odeljku se bavimo još jednim principom prebrojavanja—principom uključenja i isključenja.

Priča o prebrojavanju se nastavlja u sledećem poglavlju, gde ćemo proučavati metod funkcije generatrise, koji će predstavljati naše najjače orudje medju metodima prebrojavanja.

2.1 Principi prebrojavanja

Matematička definicija prebrojavanja

Šta mislimo kada kažemo da skup ima n elemenata? Podsetimo se, najpre, kako prebrojavamo jednostavne skupove. To radimo tako što redom pokazujemo na elemente skupa i izgovaramo reči "jedan, dva, tri, …". Kada svaki element dobije svoj broj, stajemo i poslednji izgovoreni broj predstavlja broj elemenata u skupu.

Da bismo ovu *kaži-i-pokaži* tehniku preveli na jezik matematike, moramo da, za svaki prirodan broj n, definišemo skup

$$N_n = \{1, 2, 3, \ldots, n\}.$$

Kaži-i-pokaži tehnika svakom elementu skupa N_n pridružuje element skupa X koga prebrojavamo; drugim rečima, ona odredjuje funkciju f iz N_n u X (sl. 2.1). Jasno je da je funkcija f bijekcija, jer ukoliko nismo pogrešili pri brojanju, svaki element X dobija tačno jedan broj. Znači, ako je X skup i n prirodan broj i postoji bijekcija iz N_n u X, tada kažemo da X ima n elemenata.

Slika 2.1: Prebrojavanje studenata

Primetimo odmah da naša definicija prebrojavanja ne isključuje mogućnost da skup može istovremeno imati i m elemenata i n elemenata za $m \neq n$. U suštini, svi smo već iskusili situaciju kada smo brojali neki dosta veliki skup, recimo broj automobila na parkingu, i stalno dobijali različite odgovore. Sledeća teorema je glavni korak u dokazu da je ovo moguće samo zbog greške u brojanju, i da je broj elemenata skupa jedinstven.

Teorema 2.1.1 *Ako su m i n prirodni brojevi tako da je $m < n$, tada ne postoji injekcija iz N_n u N_m.*

Dokaz Neka S označava skup prirodnih brojeva n za koje postoji injekcija iz N_n u N_m za neko $m < n$. Ako S nije prazan skup, onda postoji njegov najmanji element k, a pošto je k u S, tada postoji injekcija i iz N_k u N_l za neko $l < k$. Ne može da bude $l = 1$, pošto svaka funkcija iz N_k u N_1 može da uzme jedino vrednost 1 i stoga ne može da bude injekcija definisana na N_k za $k > 1$. Prema tome $l - 1$ je prirodan broj i situacija može da se prikaže kao na sl. 2.2.

Slika 2.2: Pretpostavljena injekcija $i\colon N_k \mapsto N_l$.

Ako nijedna od vrednosti $i(1), i(2), \ldots, i(k-1)$ nije jednaka l, tada restrikcija i na skup N_{k-1} daje injekciju iz N_{k-1} u N_{l-1}. S druge strane, ako je $i(b) = l$ za neko b za koje je $1 \leq b \leq k-1$, tada mora biti $i(k) = c \leq l$, pošto je i injekcija. U ovom slučaju možemo da konstruišemo injekciju i^* iz N_{k-1} u N_{l-1} kao što je prikazano na sl. 2.3, tj.

$$i^*(b) = c, \quad i^*(r) = i(r) \quad (r \neq b).$$

U svakom slučaju, postojanje injekcije iz N_{k-1} u N_{l-1} je u kontradikciji sa izborom k kao najmanjeg elementa u S. Prema tome, S je prazan skup i tvrdjenje je dokazano. ∎

Slika 2.3: Konstrukcija injekcije i^* kada je $i(b) = l$.

Pretpostavimo da postoji skup X koji ima n elemenata, a takodje i m elemenata za neko $m < n$. Zaključujemo da postoje bijekcije

$$\beta: N_n \mapsto X, \quad \gamma: N_m \mapsto X,$$

pa su i γ^{-1} i $\gamma^{-1}\beta$ takodje bijekcije. Posebno, $\gamma^{-1}\beta$ je injekcija iz N_n u N_m, što je suprotno teoremi 2.1.1. Prema tome, tvrdjenje "X ima n elemenata" može da važi za najviše jedan prirodan broj n.

Princip jednakosti

Kada X ima n elemenata pišemo $|X| = n$ i kažemo da je *kardinalnost* (ili *veličina*) skupa X jednaka n. Za prazan skup posebno usvajamo da je

$$|\emptyset| = 0.$$

Kada je $|X| = n$, često je pogodno pisati

$$X = \{x_1, x_2, \ldots, x_n\},$$

što je samo drugi način da se kaže da postoji bijekcija β iz N_n u X tako da je $\beta(i) = x_i$ $(1 \leq i \leq n)$.

Skup X je *konačan* ako je prazan ili je $|X| = n$ za neki prirodan broj n. Skup je *beskonačan* ako nije konačan. Takav je, na primer, skup svih prirodnih brojeva N. Sada dolazimo do prvog principa prebrojavanja—principa jednakosti.

Teorema 2.1.2 *(Princip jednakosti) Ako izmedju dva konačna skupa A i B postoji bijekcija, tada je $|A| = |B|$.*

Dokaz Zbog postojanja bijekcije izmedju A i B, iz $A = \emptyset$ sledi da je $B = \emptyset$, a takodje iz $B = \emptyset$ sledi da je $A = \emptyset$, pa u svakom slučaju važi $|A| = |B| = 0$.

U suprotnom, neka je $|A| = n$, $|B| = m$ za neke prirodne brojeve n i m i neka su $\alpha: N_n \mapsto A$, $\beta: N_m \mapsto B$ i $\gamma: A \mapsto B$ bijekcije. Tada je $\beta^{-1}\gamma\alpha$ bijekcija iz N_n u N_m. Ako je $m < n$, tada je $\beta^{-1}\gamma\alpha$ ujedno i injekcija iz N_n u N_m, što je u kontradikciji sa teoremom 2.1.1. Ako je $m > n$, tada je $\alpha^{-1}\gamma^{-1}\beta$ injekcija iz N_m u N_n, što je opet u kontradikciji sa teoremom 2.1.1. Prema tome, mora da važi $m = n$. ■

Princip zbira

Sledeći princip je takodje veoma jednostavan i korišćen je pri prebrojavanju još od pradavnih vremena.

Teorema 2.1.3 *(Princip zbira) Ako su A i B neprazni i disjunktni konačni skupovi (tj. $A \cap B = \emptyset$), tada je*

$$|A \cup B| = |A| + |B|.$$

Dokaz Pošto su A i B neprazni i konačni skupovi, možemo da ih zapišemo u standardnom obliku:

$$A = \{a_1, a_2, \ldots, a_r\}, \qquad B = \{b_1, b_2, \ldots, b_s\}.$$

Pošto su A i B disjunktni, unija $A \cup B$ može da se zapiše u sličnom obliku:

$$A \cup B = \{c_1, c_2, \ldots, c_r, c_{r+1}, c_{r+2}, \ldots, c_{r+s}\},$$

gde je

$$c_i = a_i \ (1 \leq i \leq r) \quad \text{i} \quad c_{r+i} = b_i \ (1 \leq i \leq s).$$

Prema tome, $|A \cup B| = r + s = |A| + |B|$. ■

Jasno je da princip zbira i dalje važi ako je jedan od skupova A i B prazan (ili čak i oba). Ovaj princip se na očigledan način može proširiti na uniju proizvoljnog broja disjunktnih konačnih skupova A_1, A_2, $\ldots$, A_n:

$$|A_1 \cup A_2 \cup \ldots \cup A_n| = |A_1| + |A_2| + \ldots + |A_n|.$$

Dokaz ove činjenice je laka vežba za korišćenje matematičke indukcije.

Princip proizvoda

Često smo u situaciji da brojimo stvari koje se lakše predstavljaju kao parovi objekata, nego kao pojedinačni objekti. Pretpostavimo, na primer, da je studentska služba na Odseku za matematiku sredjivala prijave studenata za oktobarski ispitni rok. Pritom su došli do situacije kao u tabeli 2.1.

	Algebra	Diskretna mat.	$\cdots$	Mat. analiza
Ana	✓	✓		
Branko		✓		✓
Ceca	✓			✓
$\ldots$				
Zlatko	✓	✓		✓

Tabela 2.1: Ispiti prijavljeni u oktobarskom roku.

U tabeli, svaka vrsta odgovara jednom studentu, svaka kolona jednom predmetu, a ako je student x prijavio ispit y tada je na odgovarajućoj poziciji (x, y) u tabeli postavljen znak ✓. Ukupan broj ovih znakova je ujedno i broj ispitnih prijava. Drugim rečima, problem je prebrojati skup S parova (x, y) tako da je student x prijavio ispit y. U opštem obliku, ako su X i Y dati skupovi, problem je prebrojati podskup S skupa $X \times Y$.

Jasno je da postoje dva načina prebrojavanja ispitnih prijava iz tabele 2.1. S jedne strane, možemo da prebrojavamo predmete koje je prijavio svaki student ponaosob i saberemo rezultate, dok s druge strane, možemo da prebrojavamo studente koji su prijavili svaki predmet ponaosob i saberemo rezultate. Naravno, za očekivati je da će oba načina dati isti broj.

Ova razmatranja možemo da preciziramo na sledeći način. Pretpostavimo da je podskup S skupa $X \times Y$ (gde su X i Y konačni skupovi) dat pomoću znakova $\checkmark$u opštem obliku tabele 2.2 iz studentske službe.

	$\cdot$	$\cdot$	y	$\cdots$	Zbir u vrsti
$\cdot$	$\checkmark$		$\checkmark$		$\cdot$
$\cdot$		$\checkmark$		$\checkmark$	$\cdot$
x	$\checkmark$	$\checkmark$		$\checkmark$	$r_x(S)$
$\cdot$		$\checkmark$	$\checkmark$		$\cdot$
$\cdot$	$\checkmark$			$\checkmark$	$\cdot$
Zbir u koloni	$\cdot$	$\cdot$	$c_y(S)$	$\cdots$	$\|S\|$

Tabela 2.2: Ispiti prijavljeni u oktobarskom roku.

Prvi način prebrojavanja je da izbrojimo koliko se puta znak $\checkmark$pojavljuje u vrsti x i dobijemo vrednost $r_x(S)$, za svako x u X (tj. $r_x(S) = |S \cap \{(x,y)\colon y \in Y\}|$). Ukupan zbir se dobija sabiranjem svih zbirova po vrstama:

$$|S| = \sum_{x \in X} r_x(S).$$

Drugi način je da izbrojimo koliko se puta znak $\checkmark$pojavljuje u koloni y i dobijemo vrednost $c_y(S)$, za svako y u Y (tj. $c_y(S) = |S \cap \{(x,y)\colon x \in X\}|$). U ovom slučaju ukupan zbir se dobija sabiranjem svih zbirova po kolonama:

$$|S| = \sum_{y \in Y} c_y(S).$$

Činjenica da imamo dva različita izraza za $|S|$ često se koristi u praksi za proveru rezultata računanja. Ona takodje ima veliku važnost i u teoriji, zato što ponekad možemo da dobijemo veoma neočekivane rezultate izjednačavanjem dva izraza od kojih svaki prebrojava isti skup samo na drugačiji način. Ovim dolazimo i do sledećeg principa prebrojavanja.

Teorema 2.1.4 *Neka su X i Y konačni neprazni skupovi, i neka je S podskup $X \times Y$. Tada važi:*

(i) Broj elemenata skupa S je dat sa

$$|S| = \sum_{x \in X} r_x(S) = \sum_{y \in Y} c_y(S),$$

gde su $r_x(S)$ i $c_y(S)$ zbirovi po vrstama i kolonama kako su ranije navedeni.

(ii) Ako je $r_x(S) = r$ za svako x i $c_y(S) = c$ za svako y, tada je

$$r|X| = c|Y|.$$

(iii) (Princip proizvoda) Broj elemenata skupa $X \times Y$ jednak je

$$|X \times Y| = |X| \cdot |Y|.$$

Dokaz (i) "Skup znakova ✓u vrsti x" može se formalno definisati kao skup parova iz S čija je prva koordinata jednaka x, tako da je $r_x(S)$ kardinalnost ovog skupa. Pošto su ovi skupovi disjunktni, iz principa sabiranja sledi da je $|S|$ jednako zbiru brojeva $r_x(S)$. Slično se dokazuje i rezultat za $c_y(S)$.

(ii) Ako je $r_x(S) = r$ za sve $x \in S$, tada u prvom izrazu za $|S|$ ima $|X|$ sabiraka jednakih r, pa je

$$|S| = r|X|.$$

Slično je $|S| = c|Y|$ i rezultat sledi.

(iii) U ovom slučaju je $S = X \times Y$, pa je $r_x(S) = |Y|$ za svako x iz X. Iz dela (ii) sada sledi da je $|X \times Y| = |X| \cdot |Y|$. ■

Primer Pretpostavimo da je Odsek za matematiku odlučio da svaki student mora da prijavi tri ispita u oktobarskom roku. Pošto su ispiti održani, asistenti su prijavili da su brojevi studenata koji su izašli na ispite jednaki 32, 28, 14, 10, 9, 5. Šta zaključujemo iz ovoga?

Rešenje Neka je n ukupan broj studenata. Pošto se pretpostavlja da je svaki student izašao na tri ispita, po metodu "zbira po vrstama" ukupan broj studenata koji su izašli na ispite je $3n$. S druge strane, asistenti su prijavili "zbirove po kolonama", pa treba da važi

$$3n = 32 + 28 + 14 + 10 + 9 + 5 = 98.$$

Medjutim, ovo je nemoguće, jer 98 nije deljivo sa 3. Kako odbacujemo mogućnost da su asistenti dali pogrešne brojeve, jedini zaključak je da neki studenti nisu izašli na prijavljene ispite. Ali to ionako više nikoga ne začudjuje! ■

Dirihleov princip

Teorema 2.1.1, koju smo dokazali da bi opravdali definiciju kardinalnosti, može da se upotrebi na još nekoliko načina. Pretpostavimo da imamo skup X, čije ćemo elemente zvati "loptice", i skup Y, čije ćemo elemente zvati "kutije". *Distribucija* loptica u kutije je jednostavno funkcija f iz X u Y: ako loptica x ide u kutiju y, tada je $f(x) = y$. Za primer, distribucija na sl. 2.4 odgovara funkciji prikazanoj na desnoj strani.

U ovom modelu, funkcija je surjekcija ako se u svakoj kutiji nalazi bar jedna loptica, a injekcija je ako se u svakoj kutiji nalazi najviše jedna loptica. Sada

Slika 2.4: Distribucija i odgovarajuća funkcija.

je jasno da ako ima više loptica nego kutija tada se u nekoj kutiji moraju naći bar dve loptice; drugim rečima funkcija ne može da bude injekcija. Formalno, ovo je posledica teoreme 2.1.1. Pretpostavimo da je $|X| = m$ i $|Y| = n$, gde je $m > n$; tada injekcija iz X u Y daje injekciju iz N_m u N_n, što je u suprotnosti sa teoremom. Ovo zapažanje je poznato kao *Dirihleov princip*:

> *ako je m loptica smešteno u n kutija i $m > n$,*
> *tada se bar u jednoj kutiji nalaze bar dve loptice.*

Ima mnogo očiglednih primena Dirihleovog principa, kao što su:

(i) U svakom skupu od 13 ili više osoba, postoje bar dve koje su rodjene istog meseca.

(ii) U svakom skupu od 367 ili više osoba, postoje bar dve koje su rodjene istog dana.

(iii) U svakom skupu od milion osoba, postoje bar dve koje imaju isti broj dlaka na glavi.

Naravno, postoje i nešto umesnije primene.

Primer Dokazati da ako je X skup osoba, tada postoje dve osobe u X koje imaju isti broj prijatelja u X. (Pretpostavlja se da ako je x prijatelj y, tada je i y prijatelj x.)

Rešenje Posmatrajmo funkciju f definisanu na X tako da je za svaku osobu x iz X,

$$f(x) = \text{broj prijatelja } x \text{ u } X.$$

Ako je $|X| = m$, moguće vrednosti $f(x)$ su $0, 1, \ldots, m-1$, pošto prijatelj x može da bude svaka osoba iz X izuzev x. Prema tome, f je funkcija iz X u $Y = \{0, 1, \ldots, m-1\}$.

U ovom trenutku ne možemo odmah da primenimo Dirihleov princip, pošto skupovi X i Y imaju isti broj elemenata. Medjutim, ako postoji osoba x^* koja ima $m-1$ prijatelja, onda je svaka osoba prijatelj x^*, pa prema tome ne postoji osoba koja nema prijatelja. Drugim rečima, brojevi $m-1$ i 0 ne mogu istovremeno biti vrednosti funkcije f. To znači da je f funkcija iz skupa veličine m na skup veličine $m-1$ (ili manje), pa nam Dirihleov princip kaže da postoje dve osobe x_1 i x_2, za koje je $f(x_1) = f(x_2)$, kao što se i tvrdilo. ■

Primenom principa zbira dobija se nešto opštiji oblik Dirihleovog principa. Pretpostavimo da je odredjeni broj loptica smešten u n kutija i neka A_i označava skup loptica u kutiji i ($1 \leq i \leq n$). Pošto su skupovi A_i disjunktni, ukupan broj loptica je $|A_1| + |A_2| + \ldots + |A_n|$, i ako se u svakoj kutiji nalazi najviše r loptica, ukupan broj loptica je najviše

$$r + r + \ldots + r = nr.$$

Drugim rečima:

> *ako je m loptica smešteno u n kutija i $m > nr$,*
> *tada se bar u jednoj kutiji nalazi bar $r + 1$ loptica.*

Primer Dokazati da u svakom skupu od šest osoba postoje tri osobe tako da se one uzajamno poznaju ili se uzajamno ne poznaju.

Rešenje Neka je a proizvoljna osoba iz ovog skupa i smestimo preostalih pet osoba u dve kutije: kutija 1 sadrži osobe koje poznaju a, a kutija 2 sadrži osobe koje ne poznaju a. Pošto je $5 > 2 \cdot 2$, jedna od ovih kutija sadrži bar tri osobe.

Pretpostavimo da kutija 1 sadrži osobe b, c i d (a možda i još neke). Ako se bilo koje dve od osoba b, c i d poznaju, recimo b i c, tada je $\{a, b, c\}$ skup od tri osobe koje se uzajamno poznaju. U suprotnom, nikoje dve osobe iz skupa $\{b, c, d\}$ se ne poznaju, pa taj skup takodje zadovoljava uslove tvrdjenja.

U slučaju da kutija 2 sadrži tri ili više osoba, sličnim razmatranjem se dolazi do istog zaključka. ■

Primer Ovde treba staviti neki žešći primer upotrebe Dirihleovog principa. Tako nešto bi trebalo da se nadje u knjizi "Proofs from THE BOOK". ■

Zadaci

1. Predavanju iz Diskretne matematike prisustvuje 26 studenata. Svaki mladić poznaje tačno 8 devojaka na predavanju, a svaka devojka poznaje tačno 5 mladića. Koliko devojaka ima na predavanju?
2. Dato je nekoliko različitih podskupova skupa $\{1, 2, \ldots, 8\}$, tako da svaki od njih ima četiri elementa i da se svaki element skupa $\{1, 2, \ldots, 8\}$ nalazi u tačno tri od datih podskupova. Koliko ima podskupova? Nadjite bar jednu familiju podskupova sa takvim osobinama.
3. Da li je moguće naći familiju podskupova skupa $\{1, 2, \ldots, 8\}$ tako da svaki od njih ima tačno tri elementa i da se svaki element skupa $\{1, 2, \ldots, 8\}$ nalazi u tačno pet podskupova?
4. Slepi čovek ima hrpu od 10 sivih i 10 crnih čarapa. Koliko čarapa treba da izabere da bi bio siguran da ima par iste boje? Koliko njih treba da izabere da bi bio siguran da ima par sive boje?
5. U kvadratu stranice 2 dato je 5 tačaka.
   a) Dokazati da postoje dve tačke tako da je njihovo rastojanje najviše $\sqrt{2}$.
   b) Koliko tačaka mora da bude izabrano tako da postoji bar jedan par tačaka na rastojanju najviše $\frac{\sqrt{2}}{n}$ za $n \in N$?

6. U kvadratu stranice 1 data je 101 tačka, pri čemu nikoje tri nisu kolinearne. Dokazati da postoji trougao sa temenima u datim tačkama, čija površina nije veća od $0,01$.
7. Dokazati da postoji $n \in N$, tako da se decimalni zapis broja 3^n završava sa 0001.
8. Dat je skup $X = \{1, 2, \ldots, 2n\}$.
   a) dokazati da ako iz skupa X izaberemo $n+1$ broj tada medju njima postoje brojevi a i b tako da $a|b$;
   b) dokazati da postoji podskup sa n elemenata tako da nijedan od njegovih elemenata ne deli neki drugi od njegovih elemenata.

   Uputstvo Pod a) neka je X' podskup koji čini $n+1$ izabrani broj, a Y skup svih neparnih brojeva $\{1, 3, \ldots, 2n-1\}$. Definišimo funkciju $f' : X \mapsto Y$ pomoću

   $$f(x) = \text{najveći neparan prirodan broj koji deli } x.$$

   Sada još treba pokazati da f nije injektivno preslikavanje ...
9. Dokazati da u proizvoljnom skupu od $n+1$ prirodnih brojeva postoje dva čija je razlika deljiva sa n. Da li tvrdjenje ostaje u važnosti ako se reč "razlika" zameni sa "zbir"?
10. Dokazati da u nizu brojeva $a_1, a_2, \ldots, a_n$ postoji podniz brojeva čiji je zbir elemenata deljiv sa n.
11. Dokazati da se medju $n+1$ različitih prirodnih brojeva manjih od $2n$ mogu naći tri broja tako da jedan od njih bude jednak zbiru ostala dva.
12. Neka je $x_1, x_2, \ldots, x_r$ niz različitih celih brojeva. Za svako i $(1 \leq i \leq r)$ neka m_i označava dužinu najdužeg rastućeg podniza koji počinje sa x_i i neka n_i označava dužinu najdužeg opadajućeg podniza koji počinje sa x_i. Dokazati da je funkcija f, koja broju i $(1 \leq i \leq r)$ dodeljuje par (m_i, n_i), injektivna funkcija.

    Na osnovu ovoga pokazati da niz od $mn+1$ različitih celih brojeva mora da sadrži ili rastući podniz sa m elemenata ili opadajući podniz sa n elemenata.
13. Pokazati da u skupu od 10 osoba postoje ili četiri osobe koje se sve medjusobno poznaju ili tri osobe od kojih se nikoje dve ne poznaju.

2.2 Uredjeni izbori elemenata

Ponekad je poredak u kojem se elementi nalaze bitan, dok ponekad nije. Na primer, reč *STOP* je različita od reči *POTS*, bez obzira što su obe reči formirane od slova iz skupa $\{O, P, S, T\}$. S druge strane, zbir brojeva $1 + 2 + 3$ je isti kao zbir $2 + 3 + 1$, bez obzira što je redosled ovih brojeva promenjen. U ovom odeljku ćemo naučiti kako da prebrojimo odredjene izbore elemenata kod kojih je poredak bitan, a kasnije ćemo proučavati izbore elemenata kod kojih poredak nije bitan. Takodje ćemo naučiti da je važno da li je ili nije dozvoljeno ponavljanje elemenata.

Primer Posmatrajmo skup $\{A, B, C, D\}$. Na koliko načina možemo da izaberemo dva slova?

Rešenje Postoje *četiri* moguća odgovora na ovo pitanje, u zavisnosti od toga da li je bitan poredak slova, kao i da li je dozvoljeno ponavljanje slova.

(a) Ako je poredak bitan i dozvoljeno je ponavljanje slova, tada postoji 16 mogućih izbora:

$$\begin{array}{cccc} AA & BA & CA & DA \\ AB & BB & CB & DB \\ AC & BC & CC & DC \\ AD & BD & CD & DD \end{array}$$

(b) Ako je poredak bitan, a ponavljanje nije dozvoljeno, tada postoji 12 mogućih izbora:

$$\begin{array}{cccc} AB & BA & CA & DA \\ AC & BC & CB & DB \\ AD & BD & CD & DC \end{array}$$

(c) Ako poredak nije bitan, a dozvoljeno je ponavljanje, tada postoji 10 mogućnosti:

$$\begin{array}{cccc} AA & BB & CC & DD \\ AB & BC & CD & \\ AC & BD & & \\ AD & & & \end{array}$$

(d) Ako poredak nije bitan, a nije dozvoljeno ni ponavljanje, tada postoji samo 6 mogućnosti:

$$\begin{array}{ccc} AB & BC & CD \\ AC & BD & \\ AD & & \end{array}$$

■

Ovaj primer pokazuje četiri najvažnija tipa kombinatornih problema. U ovom i sledećem odeljku naučićemo da rešavamo sve ove tipove problema u *opštem slučaju*, tj. kada je problem izabrati n elemenata iz skupa sa m elemenata. U ovom odeljku uopštićemo slučajeve (a) i (b), dok ćemo kasnije proučiti slučajeve (c) i (d).

Uredjeni izbori sa ponavljanjem

U prethodnom primeru smo videli da je u slučaju (a) broj izbora jednak $16 = 4^2$. Evo još jednog sličnog primera:

Primer Koliko postoji različitih reči sa 5 slova (koristeći naše pismo sa 30 slova i uključujući i besmislene reči kao *kćndv*)?

Rešenje Pošto se svako od 5 slova može nezavisno izabrati na 30 načina, nije teško videti da je odgovor 30^5. I, zaista, reč sa 5 slova se može posmatrati kao preslikavanje skupa $\{1, 2, \ldots, 5\}$ u skup slova {a,b,c,...,ž}: za svako od 5 mesta u reči, sa rednim brojevima $1, 2, \ldots, 5$, mi odredjujemo slovo na tom mestu. ■

Nalaženje ovakvih jednostavnih prevodjenja svakodnevnih problema na jezik matematike je jedna od osnovnih veština matematičkog zanata. Sada nije teško videti da uredjeni izbor n elemenata sa ponavljanjem iz skupa M sa m elemenata u stvari odgovara preslikavanju skupa $\{1, 2, \ldots, n\}$ u skup M.

Teorema 2.2.1 *Neka je N skup sa n elemenata (koji može da bude i prazan, tj. $n = 0, 1, 2, \ldots$) i neka je M skup sa m elemenata, $m \geq 1$. Broj svih mogućih preslikavanja $f\colon N \mapsto M$ jednak je m^n.*

Dokaz Do rezultata se može doći imitiranjem ideje iz prethodnog primera, ali ćemo iskoristiti priliku da se naviknemo na stroge matematičke dokaze.

Zato za dokaz koristimo metod matematičke indukcije po n. Šta teorema tvrdi za $n = 0$? U ovom slučaju, posmatramo sva preslikavanja f skupa $N = \emptyset$ u neki skup M. Definicija preslikavanja nam kaže da takvo f mora da bude skup uredjenih parova (x, y) tako da $x \in N = \emptyset$ i $y \in M$. Pošto prazan skup nema elemenata, f ne može da sadrži nijedan takav uredjeni par, pa je jedina mogućnost da je $f = \emptyset$ (nema uredjenih parova). S druge strane, $f = \emptyset$ zadovoljava definiciju preslikavanja: definicija kaže da za svako $x \in N$ nešto mora da važi, ali nema nijednog $x \in N$. Prema tome, postoji tačno jedno preslikavanje $f\colon \emptyset \mapsto M$. Ovo se slaže sa formulom, jer je $m^0 = 1$ za $m \geq 1$, pa zaključujemo da smo proverili slučaj $n = 0$ kao bazu indukcije.

Dalje, pretpostavimo da je teorema dokazana za sve $n \leq n_0$ i sve $m \geq 1$. Neka je $n = n_0 + 1$ i posmatrajmo skup N sa n elemenata i skup M sa m elemenata. Izaberimo proizvoljan element $a \in N$. Za opis preslikavanja $f\colon N \mapsto M$ potrebno je znati vrednost $f(a) \in M$ i preslikavanje $f'\colon N \backslash \{a\} \mapsto M$. Vrednost $f(a)$ može da se izabere na m načina, a za izbor f' imamo m^{n-1} mogućnosti po induktivnoj hipotezi. Svaki izbor $f(a)$ može da se poveže sa svakim izborom f', tako da je ukupan broj mogućnosti za f jednak $m \cdot m^{n-1} = m^n$.

Ovde ide slika sa strane 49 iz Nešetrilove knjige!!!

■

Napomena Uredjeni izbori elemenata se u mnogim knjigama nazivaju *varijacije*, tako da prethodna teorema tvrdi da je broj varijacija n elemenata od m elemenata sa ponavljanjem jednak m^n.

Teorema 2.2.2 *Svaki skup X sa n elemenata ima tačno 2^n podskupova $(n \geq 0)$.*

Dokaz Posmatrajmo proizvoljan podskup A skupa X i definišimo preslikavanje $f_A\colon X \mapsto \{0,1\}$. Za $x \in X$ odredjujemo

$$f_A(x) = \begin{cases} 1 & \text{ako } x \in A \\ 0 & \text{ako } x \notin A. \end{cases}$$

Ovo preslikavanje se često sreće u matematici i naziva se *karakteristična funkcija* skupa A. Vizuelno,

Ovde ide slika sa strane 50 iz Nešetrilove knjige!!!

Različiti skupovi A imaju različite funkcije f_A, i obrnuto, svako preslikavanje $f\colon X \mapsto \{0,1\}$ odredjuje skup $A = \{x \in X | f(x) = 1\}$ tako da je $f = f_A$. Prema tome, broj podskupova X je isti kao broj svih preslikavanja $X \mapsto \{0,1\}$, a to je 2^n po teoremi 2.2.1. ∎

Uredjeni izbori bez ponavljanja

Neka je f funkcija iz $\{1,2,\ldots,n\}$ u skup M koja odgovara uredjenom izboru elemenata. Kada je ponavljanje elemenata dozvoljeno, moguće je izabrati isti element dva puta, tako da važi $f(r) = f(s)$ za različite r i s iz $\{1,2,\ldots,n\}$. Ako ponavljanje nije dozvoljeno, tada je $f(r) \neq f(s)$ za svako $r \neq s$, pa vidimo da uredjenim izborima elemenata bez ponavljanja odgovaraju *injektivne* funkcije.

Teorema 2.2.3 *Neka je N skup sa n elemenata i neka je M skup sa m elemenata, $n, m \geq 0$. Broj svih injektivnih preslikavanja $f\colon N \mapsto M$ jednak je*

$$m(m-1)\cdots(m-n+1) = \prod_{i=0}^{n-1}(m-i).$$

Dokaz Dokaz izvodimo indukcijom po n. Kada je $n = 0$, prazno preslikavanje je injektivno, pa postoji tačno jedno injektivno preslikavanje, i ovo se slaže sa dogovorom da se vrednost praznog proizvoda definiše kao 1. Znači, formula važi za $n = 0$.

Primetimo (teorema 2.1.1) da ne postoji injektivno preslikavanje za $n > m$ i da se ovo takodje slaže sa formulom (jer se tada u njoj pojavljuje činilac 0).

Posmatrajmo skup N sa n elemenata, $n \geq 1$, i skup M sa m elemenata, $m \geq n$. Uzmimo element $a \in N$ i izaberimo vrednost $f(a) \in M$ proizvoljno, na jedan od m mogućih načina. Preostaje nam da izaberemo injektivno preslikavanje iz $N \setminus \{a\}$ u $M \setminus \{f(a)\}$. Po induktivnoj hipotezi, postoji $(m-1)(m-2)\cdots(m-n+1)$ mogućnosti za ovaj izbor. Sve u svemu, dobijamo $m(m-1)(m-2)\cdots(m-n+1)$ injektivnih preslikavanja $f\colon N \mapsto M$. ∎

Napomena Ovaj rezultat bi u drugim knjigama glasio: *broj varijacija sa n elemenata od m elemenata bez ponavljanja jednak je $m(m-1)\cdots(m-n+1)$.*

Zadaci

2.3 Permutacije

Napomena Smanjiti uvodnu priču koliko se može, ostaviti primer sa mešanjem karata, za primene reći samo ukratko da je algoritmu za sortiranje koji koristi samo medjusobno poredjenje dva elementa niza u opštem slučaju potrebno bar $cn \log n$ koraka za neku konstantu c (ili $\Theta(n \log n)$ koraka).

Generisanje permutacija treba da bude glavna stvar! Definicija leksikografskog poretka, rednog broja permutacije, nerekurzivni algoritmi iz Dragoša, odnosno Ruskey-a, kao i slučajne permutacije.

Bijektivno preslikavanje konačnog skupa X na samog sebe naziva se *permutacija* skupa X. Najčešće se za skup X uzima skup $\{1, 2, \ldots, n\}$. Primer permutacije skupa $\{1, 2, \ldots, 5\}$ je funkcija α definisana pomoću

$$\alpha(1) = 2, \quad \alpha(2) = 4, \quad \alpha(3) = 5, \quad \alpha(4) = 1, \quad \alpha(5) = 3.$$

Bijektivno preslikavanje konačnog skupa na samog sebe je ujedno i injekcija, i obrnuto svako injektivno preslikavanje konačnog skupa na samog sebe je bijekcija. Ovo znači da permutacije predstavljaju poseban slučaj uredjenog izbora elemenata kod koga se bira svih n od n elemenata. Prema teoremi 2.2.3, broj permutacija skupa sa n elemenata jednak je $n(n-1) \cdot \ldots \cdot 2 \cdot 1$. Ovaj broj se, posmatran kao funkcija od n, označava sa $n!$ i čita n *faktorijel*. Znači,

$$n! = n(n-1) \cdot \ldots \cdot 2 \cdot 1 = \prod_{j=0}^{n-1} (n-j) = \prod_{i=1}^{n} i.$$

Posebno za $n = 0$ važi $0! = 1$ (jer se $0!$ definiše kao prazan proizvod).

Napomena Funkcija $n!$ jako brzo raste, brže od svake eksponencijalne funkcije. Za procenu njene vrednosti koristi se *Stirling-ova formula* koja tvrdi da za veliko n važi

$$n! \approx \sqrt{2\pi n} \left(\frac{n}{e}\right)^n.$$

Ova procena je dosta dobra: čak i za $n = 8$ greška je samo $1,04\%$.

Ako se elementi skupa X nalaze u nekom poretku, permutaciju možemo da zamislimo i kao preuredjivanje elemenata u novi poredak. Gornja permutacija α, definisana na skupu $X = \{1, 2, \ldots, 5\}$, može da se zapiše i na sledeći način:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}.$$

U prvoj vrsti smo naveli elemente X i ispod svakog $x \in X$ u prvoj vrsti, napisali smo element $\alpha(x)$ u drugoj vrsti.

Iako se permutacije mogu posmatrati kao preuredjivanje elemenata uredjenog skupa, njihova definicija kao bijektivnih preslikavanja ima tu prednost što se permutacije, kao vrsta funkcija, mogu slagati na uobičajeni način. Neka je β permutacija skupa $\{1, 2, \ldots, 5\}$ data sa

$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 4 & 2 \end{pmatrix}.$$

Kako je slaganje dve bijekcije ponovo bijekcija, preslikavanje $\beta\alpha$, definisano sa $\beta\alpha(i) = \beta(\alpha(i))$, predstavlja novu permutacija skupa $\{1, 2, \dots, 5\}$ datu sa

$$\beta\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 2 & 3 & 1 \end{pmatrix}, \text{ što se vidi iz dijagrama } \begin{array}{cccccc} & 1 & 2 & 3 & 4 & 5 \\ \alpha & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 2 & 4 & 5 & 1 & 3 \\ \beta & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 5 & 4 & 2 & 3 & 1 \end{array}.$$

Drugi i pogodniji način zapisa permutacija je pomoću ciklusa. Primetimo da za permutaciju α važi

$$\alpha(1) = 2, \quad \alpha(2) = 4, \quad \alpha(4) = 1.$$

Prema tome, α prevodi 1 u 2, 2 u 4 i 4 nazad u 1, i iz ovog razloga kažemo da elementi 1, 2 i 4 čine *ciklus* (dužine 3). Slično, elementi 3 i 5 čine ciklus dužine 2, pa pišemo

$$\alpha = (1\ 2\ 4)(3\ 5).$$

Ovo je tzv. *ciklusna notacija* za α. Svaka permutacija α može da se zapiše u ciklusnoj notaciji na sledeći način:

1. počinjemo sa proizvoljnim elementom (npr. a) i zapisujemo elemente $\alpha(a)$, $\alpha(\alpha(a))$, $\alpha(\alpha(\alpha(a)))$, ... dok ponovo ne dodjemo do a, tako da dobijemo ciklus;

2. biramo element koji se ne pojavljuje u nekom od prethodnih ciklusa i zapisujemo ciklus koji on proizvodi;

3. prethodni postupak ponavljamo dok god svi elementi ne budu rasporedjeni u cikluse.

Permutacije β i $\beta\alpha$ se u ciklusnoj notaciji zapisuju kao

$$\beta = (1\ 3)(2\ 5)(4), \quad \beta\alpha = (1\ 5)(2\ 4\ 3).$$

Iako je predstavljanje permutacije u ciklusnoj notaciji u suštini jedinstveno, postoje dva očigledna načina da promenimo zapisivanje bez uticaja na samu permutaciju. Najpre, svaki ciklus može da počne bilo kojim od svojih elemenata—na primer, ciklusi (7 8 2 1 3) i (1 3 7 8 2) predstavljaju isti ciklus. Drugo, poredak ciklusa nije važan—na primer, (1 2 4)(3 5) i (3 5)(1 2 4) predstavljaju istu permutaciju. Važne stvari su broj i dužina ciklusa, kao i poredak elemenata unutar ciklusa, i oni su jedinstveno odredjeni. Prema tome, ciklusna notacija nam daje mnogo korisnih informacija o permutaciji.

Gde se primenjuju permutacije? One se koriste kod projektovanja i proučavanja različitih algoritama za sortiranje. U teoriji grupa, grupe permutacija (sa slaganjem funkcija kao operacijom u grupi) predstavljaju jedan od osnovnih predmeta proučavanja. Osnovni razlog za nemogućnost opšteg algebarskog rešenja jednačine petog stepena leži u osobinama grupe svih permutacija skupa sa pet elemenata. Rubikova kocka, koja je bila izuzetno popularna početkom 1980-ih, predstavlja lep primer složene grupe permutacija. Veoma zamršena svojstva permutacija se primenjuju kod matematičkog proučavanja mešanja karata. Ovo je samo mali uzorak oblasti gde permutacije igraju važnu ulogu.

Primer Karte označene brojevima 1 do 12 poredjane su kao što je prikazano dole levo. Karte se skupljaju po vrstama i zatim se ponovo dele, ali po kolonama umesto po vrstama, tako da se dobija raspored kao dole desno.

1	2	3		1	5	9
4	5	6		2	6	10
7	8	9		3	7	11
10	11	12		4	8	12

Koliko puta mora da se izvrši ovaj postupak pre nego što se karte ponovo nadju u početnom rasporedu?

Rešenje Neka je π permutacija koja predstavlja postupak premeštanja karata, tako da je $\pi(i) = j$ ako se karta j pojavljuje na mestu koje je pre premeštanja zauzimala karta i. Ako π predstavimo pomoću ciklusa dobijamo

$$\pi = (1)(2\ 5\ 6\ 10\ 4)(3\ 9\ 11\ 8\ 7)(12).$$

Ciklusi (1) i (12) znače da karte 1 i 12 sve vreme ostaju na svojim mestima. Preostala dva ciklusa imaju dužinu 5, tako da će se posle pet ponavljanja postupka sve karte naći na svojim početnim mestima. (Probajte.) Drugim rečima $\pi^5 = id$, gde π^5 predstavlja petostruko ponavljanje permutacije π, a id označava identičnu permutaciju, definisanu sa $id(j) = j$. ■

Primer Napiši priču o korišćenju poretka permutacija za tkanje različitim koncima i tu prikazi sliku Steinhaus-Johnson-Trotter tkanja, koja se nalazi u fajlu StJoTrWe.gif. Takodje napravi i odgovarajuću sliku za leksikografsko uredjenje permutacija. ■

Generisanje permutacija

Ovde će biti prikazano nekoliko načina za generisanje svih permutacija, za generisanje slučajne permutacije, i naravno, za generisanje permutacije sa datim rednim brojem (što je takodje prosto k'o pasulj—deliš broj sa najvećim mogućim faktorijelom i uzimaš onaj broj koji nije već potrošen blablabla...).

Slučajne permutacije mogu najjednostavnije na sledeći način:

for $k := n, n-1, \ldots, 2, 1$ **do** $swap(\pi(k), \pi(rand(k)))$

gde je $rand(k)$ slučajan broj izmedju 1 i $k-1$ (a možda može i izmedju 1 i k). Reference za ovo su sledeće:

R. Durstenfeld, *Algorithm 235: Random permutations*, CACM (1964), 420.

G. de Balbine, *Note on random permutations*, Mathematics of Computation 21 (1967), 710–712.

Obavezno stavi link na Frank Rusky-jev ”Combinatorial Object Server”, koji se nalazi na adresi http://www.theory.cs.uvic.ca/ cos/cos.html . Tamo stvarno ima puno vrednog da se nadje i za studente i za ostale, kao i za ovu knjigu, jer se tu nalaze i generisanje particija brojeva, a mozda nekog od njih to i zainteresuje, pa se odluci na prava istrazivanja!

Na kraju krajeva, ne zaboravi da u susednom direktorijumu “Resursi” imaš za ovo važnu četvrtu glavu iz knjige Frank-a Ruskey-a o generisanju kombinatornih objekata.

Varijacije nećemo generisati—samo ću reći da se odgovarajući algoritam za generisanje permutacija može lako prepraviti tako da radi za varijacije.

Zadaci

1. Komitet od devet osoba treba da izabere predsednika, sekretara i blagajnika. Na koliko načina je moguće obaviti ovaj izbor?
2. Na koliko načina se mogu izabrati jedno crno i jedno belo polje na šahovskoj tabli tako da se oni ne nalaze u istoj vrsti ili istoj koloni?
3. Na koliko načina možemo da rasporedimo osam topova na šahovskoj tabli tako da se nikoja dva ne nalaze u istoj vrsti ili istoj koloni?
4. Neka se u odeljenju nalazi m devojčica i n dečaka. Na koliko načina se oni mogu rasporediti u vrstu tako da su sve devojčice u vrsti jedna za drugom?
5. Koliko ima ukupno permutacija σ skupa $\{1, 2, \ldots, 6\}$ tako da je $\sigma^2 = id$, $\sigma \neq id$?
6. Napišite ciklusnu notaciju za permutaciju
$$\begin{array}{ccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 5 & 7 & 8 & 4 & 6 & 1 & 2 & 9. \end{array}$$
7. Neka su σ i τ permutacije skupa $\{1, 2, \ldots, 8\}$ date u ciklusnoj reprezentaciji pomoću
$$\sigma = (1\ 2\ 3)(4\ 5\ 6)(7\ 8), \quad \tau = (1\ 3\ 5\ 7)(2\ 6)(4)(8).$$
Zapišite u ciklusnoj notaciji permutacije $\sigma\tau$, $\tau\sigma$, σ^2, σ^{-1}, τ^{-1}.
8. Neka su α i β permutacije skupa $\{1, 2, \ldots, 9\}$ čije su ciklusne reprezentacije
$$\alpha = (1\ 2\ 3\ 7)(4\ 9)(5\ 8)(6), \quad \beta = (1\ 3\ 5)(2\ 4\ 6)(7\ 8\ 9).$$
Predstaviti u ciklusnoj reprezentaciji permutacije $\alpha\beta$, $\beta\alpha$, α^2, β^2, α^{-1}, β^{-1}.
9. Dokazati da je najveći stepen prostog broja p koji deli $n!$ jednak
$$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots + \left[\frac{n}{p^k}\right] + \ldots.$$
10. Dato je 10 studenata S_1, S_2, $\ldots$, S_{10}.
    (a) Na koliko načina se ovi studenti mogu poredjati u vrstu?
    (b) Koliko ima poredaka ako studenti S_2, S_6 i S_9 žele da stoje jedno pored drugog (u bilo kom poretku)?

(c) Koliko ima poredaka tako da S_2, S_6 i S_9 ne stoje svi jedno pored drugog?

11. Da li medju brojevima $1, 2, \dots, 10^{10}$ ima više onih koji sadrže cifru 9 u decimalnom zapisu ili onih koji je ne sadrže?

12. Koliko ima prirodnih brojeva sa najviše n cifara u kojima se pojavljuje cifra 9?

13. Koliko se binarnih relacija može definisati na skupu X sa n elemenata? Koliko postoji:

    a) refleksivnih relacija;

    b) simetričnih relacija;

    c) refleksivnih i simetričnih relacija?

14. (a) Koliko ima $n \times n$ matrica sa elementima iz skupa $\{0, 1, \dots, q-1\}$?

    (b) Neka je q prost broj. Koliko ima matrica kao u (a) čija determinanta nije deljiva sa q? (Drugim rečima, koliko ima nesingularnih matrica nad poljem sa q elemenata?)

    Uputstvo Izaberi prvu kolonu kao proizvoljan nenula vektor nad poljem sa q elemenata (takvih vektora ima $q^n - 1 = q^n - q^0$). Druga kolona ne sme da bude linearna kombinacija prve kolone, što isključuje q vektora. Treća kolona ne sme da bude linearna kombinacija prve dve kolone, što isključuje q^2 vektora (ovde treba pokazati da je svih q^2 linearnih kombinacija prve dve kolone zaista različito!). Uopšte, za i-tu kolonu imamo $q^n - q^{i-1}$ mogućnosti, pa je ukupan broj traženih matrica jednak

    $$(q^n - 1)(q^n - q)(q^n - q^2)\cdots(q^n - q^{n-1}) = \prod_{i=0}^{n-1}(q^n - q^i).$$

15. U koliko se permutacija skupa $\{1, 2, \dots, n\}$ izmedju brojeva 1 i n nalazi tačno r drugih brojeva?

16. Na koliko načina šest osoba može da sedne za okrugli sto oko kojeg se nalazi šest stolica (pri čemu se rasporedi koji se dobijaju rotiranjem oko centra stola smatraju istim)?

17. Koliko postoji permutacija špila od 32 karte (od 7 do A) pri kojima se sva četiri asa nalaze medju prvih 10 karata?

18. Tri bele kuglice označene sa a, b i c i četiri crne kuglice označene sa 1, 2, 3 i 4 treba poredjati tako da istobojne kuglice nisu susedne. Na koliko načina se to može učiniti?

19. Ključevi se dobijaju pravljenjem useka različitih dubina na unapred odredjenim mestima. Ako postoji osam mogućih dubina, koliko mesta treba da postoji da bi napravili milion različitih ključeva?

20. Koliko reči sa četiri slova postoji u azbuci od 30 slova ako sva slova u reči moraju da budu različita?

21. Svaku sobu u kući, čiji je plan dat na sl. 2.5, treba okrečiti u jednu od n boja tako da sobe spojene vratima imaju različite boje. Na koliko načina se može izvršiti ovakvo krečenje?

Slika 2.5: Krečenje soba

22. Neka je u_n broj reči dužine n u azbuci $\{0,1\}$ kod kojih nikoje dve nule nisu uzastopne. Dokazati da je
$$u_1 = 2, \quad u_2 = 3, \quad u_n = u_{n-1} + u_{n-2} \quad (n \geq 3).$$
23. Špil od 52 karte je podeljen na dva jednaka dela i "promešan" tako da ako je početni poredak karata bio $1, 2, 3, 4, \ldots$ tada je novi poredak $1, 27, 2, 28, \ldots$. Koliko puta mora da se ponovi ovakvo mešanje pre nego što se špil ponovo nadje u početnom poretku?
24. Dokazati da u svakom skupu od 20 osoba ili postoje četiri osobe koje se sve medjusobno poznaju ili postoje četiri osobe tako da se nikoje dve ne poznaju.
25. Ako su s i t celi brojevi tako da je $s \geq 2$, $t \geq 2$, tada postoji najmanji ceo broj $r(s,t)$ tako da za svako $n \geq r(s,t)$ važi da u svakom skupu od n osoba ili postoji s osoba koje se sve medjusobno poznaju ili postoji t osoba tako da se nikoje dve ne poznaju. Dokazati da je
$$r(s,2) = s, \quad r(2,t) = t, \quad r(s,t) \leq r(s-1,t) + r(s,t-1).$$

2.4 Neuredjeni izbori elemenata

Neuredjeni izbori elemenata bez ponavljanja

U prethodnom odeljku smo za matematičko definisanje pojma uredjenog izbora k elemenata konačnog skupa X koristili preslikavanje f iz uredjenog skupa $\{1, 2, \ldots, k\}$ u skup X. Na ovaj način, bili smo u mogućnosti da kažemo da je element $f(1)$ izabran prvi, element $f(2)$ drugi, a element $f(k)$ poslednji.

S druge strane, kod neuredjenog izbora elemenata skupa X nije važno koji je element izabran prvi, a koji poslednji, tako da nema potrebe uvoditi preslikavanja. S obzirom da sada razmatramo neuredjene izbore elemenata bez ponavljanja vidimo da oni predstavljaju k-točlane podskupove skupa X.

Definicija 2.4.1 *Neka je X skup, a k nenegativan ceo broj. Simbol*
$$\binom{X}{k}$$
označava skup svih k-točlanih podskupova skupa X.

Na primer, $\binom{\{a,b,c\}}{2} = \{\{a,b\},\{a,c\},\{b,c\}\}$.

Definicija 2.4.2 *Neka su $n \geq k$ nenegativni celi brojevi. Binomni koeficijent $\binom{n}{k}$ je funkcija promenljivih n i k data pomoću*
$$\binom{n}{k} = \frac{n(n-1)(n-2)\cdots(n-k+1)}{k(k-1)\cdots 2\cdot 1} = \frac{\prod_{i=0}^{k-1}(n-i)}{k!}.$$

Primetimo da simbol $\binom{x}{k}$ sada ima dva značenja, u zavisnosti od toga da li je x skup ili broj. Opravdanje za ovo preklapanje simbola nalazi se u sledećoj teoremi.

Teorema 2.4.3 *Broj k-točlanih podskupova konačnog skupa X jednak je $\binom{|X|}{k}$, tj. važi*

$$\left|\binom{X}{k}\right| = \binom{|X|}{k}.$$

Proof Neka je $n = |X|$. Prebrojaćemo *uredjene* izbore k elemenata skupa X bez ponavljanja na dva načina. S jedne strane, iz teoreme 2.2.3 znamo da je ovaj broj jednak $n(n-1)\cdots(n-k+1)$. S druge strane, od svakog k-točlanog podskupa $M \in \binom{X}{k}$ uredjivanjem njegovih elemenata možemo da dobijemo $k!$ različitih uredjenih izbora k elemenata i svaki uredjeni izbor k elemenata može da se dobije samo iz jednog k-točlanog podskupa M na ovaj način. Prema tome,

$$n(n-1)\cdots(n-k+1) = k!\left|\binom{X}{k}\right|. \quad \blacksquare$$

Napomena Posebne vrednosti binomnih koeficijenata su $\binom{n}{0} = 1$, $\binom{n}{1} = n$ i $\binom{n}{n} = 1$. Primetimo inače da se definicija 2.4.2 može proširiti na sve realne vrednosti n, tako da možemo da pišemo

$$\binom{-2,5}{3} = \frac{-2,5\cdot(-3,5)\cdot(-4,5)}{3\cdot 2\cdot 1} = -6,5625.$$

Ovu definiciju možemo da proširimo i na negativne vrednosti k dogovorom da je

$$\binom{n}{k} = 0 \quad \text{za } k < 0.$$

Generisanje kombinacija

Ovde će biti dati odgovarajući algoritmi za generisanje kombinacija, što je moguće više analogno slučaju permutacija. Za generisanje kombinacija sa ponavljanjem nema potrebe, jer je iz dokaza teoreme u sledećem pododeljku jasno da se one mogu svesti na kombinacije bez ponavljanja.

Za ovo generisanje treba konsultovati web sajt Frank-a Ruskey-a sa univerziteta u Viktoriji, Kanada, koji piše knjigu o generisanju kombinatornih objekata. Tamo bi cela ova priča već trebalo da se nalazi.

S druge strane, najbolji algoritam za generisanje svih kombinacija se nalazi u sledećem radu:

P. Eades, B. McKay, *An algorithm for generating subsets of fixed size with a strong minimal change property*, Inf. Process. Lett. 19 (1984), 131–133.

Na kraju krajeva, ne zaboravi da u susednom direktorijumu "Resursi" imaš za ovo važnu četvrtu glavu iz knjige Frank-a Ruskey-a o generisanju kombinatornih objekata.

Neuredjeni izbori elemenata sa ponavljanjem

Ako dozvolimo ponavljanje u neuredjenom izboru elemenata, onda on više ne predstavlja običan podskup. Pretpostavimo da smo napravili jedan neuredjeni izbor k elemenata sa ponavljanjem iz konačnog skupa $X = \{a_1, a_2, \ldots, a_n\}$. Za $i = 1, 2, \ldots, n$ neka s_i označava koliko je puta element a_i izabran. Kako je ukupno izabrano k elemenata, to važi

$$s_1 + s_2 + \ldots + s_n = k, \quad s_i \geq 0,\ i = 1, 2, \ldots, k. \tag{2.1}$$

S druge strane, ukoliko imamo uredjenu n-torku nenegativnih celih brojeva $(s_1, s_2, \ldots, s_n)$ koja zadovoljava prethodnu jednačinu, tada ona jednoznačno opisuje jedan neuredjeni izbor elemenata sa ponavljanjem, jer s_i predstavlja broj pojavljivanja elementa a_i u izboru.

Prema tome, broj neuredjenih izbora k elemenata sa ponavljanjem skupa X jednak je broju uredjenih n-torki nenegativnih celih brojeva $(s_1, s_2, \ldots, s_n)$ koje zadovoljavaju (2.1).

Da bismo našli broj ovakvih uredjenih n-torki, pretpostavimo da svaka od n promenljivih s_1, s_2, ..., s_n odgovara jednoj od n kutija u nizu. Neka je dato k jednakih lopti koje treba rasporediti u kutije na neki način (uz pretpostavku da svaka kutija može da primi svih k lopti ako je potrebno). Tada svaki mogući raspored lopti odgovara jednom rešenju jednačine (2.1). Na primer, za $k = 7$ i $n = 6$ rešenje $0 + 1 + 0 + 3 + 1 + 2 = 7$ odgovara rasporedu lopti

$$\underline{|\;\;|\bullet|\;\;|\bullet\bullet\bullet|\bullet|\bullet|}$$

Sada smo dakle zainteresovani da nadjemo broj rasporeda lopti u kutijama. Ako obrišemo dna kutija, kao i krajnji levi i desni zid kutija, tada ostaje samo k lopti i $n - 1$ unutrašnji zid koji ih razdvaja:

$$|\bullet|\;\;|\bullet\bullet\bullet|\bullet|\bullet$$

Vidimo da raspored lopti u kutijama odgovara nizu od $n + k - 1$ objekata, od čega je k lopti i $n - 1$ unutrašnjih zidova. Svaki raspored lopti je odredjen k-točlanim podskupom skupa $\{1, 2, \ldots, n + k - 1\}$ koji predstavlja pozicije lopti u ovom nizu, pa je ukupan broj takvih rasporeda jednak $\binom{n+k-1}{k-1}$. Ovim smo dokazali

Teorema 2.4.4 *Broj neuredjenih izbora k elemenata sa ponavljanjem skupa X jednak je*

$$\binom{|X| + k - 1}{k - 1}. \quad \blacksquare$$

Zadaci

2.5 Binomni koeficijenti

Binomni koeficijenti $\binom{n}{k}$ imaju neobično veliki broj primena i sasvim sigurno su najvažniji kombinatorni pojam. Izmedju ostalog, oni se mnogo koriste i u analizi algoritama.

Faktorijelna reprezentacija

Binomni koeficijenti se najjednostavnije predstavljaju pomoću faktorijela.

Lema 2.5.1 *Za cele brojeve n i k za koje je $n \geq k \geq 0$ važi*

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}. \tag{2.2}$$

Dokaz Ova jednakost se dobija proširenjem razlomka u definiciji 2.4.2 binomnog koeficijenta sa $(n-k)!$. Naime,

$$\begin{aligned}\binom{n}{k} &= \frac{n(n-1)(n-2)\cdots(n-k+1)}{k(k-1)\cdots 2\cdot 1} \\ &= \frac{n(n-1)(n-2)\cdots(n-k+1)\cdot(n-k)!}{k(k-1)\cdots 2\cdot 1\cdot(n-k)!} = \frac{n!}{k!(n-k)!}. \quad \blacksquare\end{aligned}$$

Osim što se pomoću prethodne leme binomni koeficijenti mogu predstaviti pomoću faktorijela, ona takodje dopušta i obratnu mogućnost da kombinacije faktorijela predstavimo pomoću binomnih koeficijenata.

Uslov simetričnosti

Pomoću (2.2) lako se dokazuje i sledeća

Lema 2.5.2 *Za svaki ceo broj $n \geq 0$ i svaki ceo broj k važi*

$$\binom{n}{k} = \binom{n}{n-k}. \tag{2.3}$$

Dokaz Iz jednakosti (2.2) dobijamo

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n!}{(n-k)!k!} = \frac{n!}{(n-k)!(n-(n-k))!} = \binom{n}{n-k}. \quad \blacksquare$$

Kombinatorno, jednakost (2.3) znači da je broj k-točlanih podskupova skupa X sa n elemenata jednak broju podskupova sa $n-k$ elemenata. Ovo se može proveriti i direktno—dovoljno je svakom k-točlanom podskupu dodeliti njegov komplement u X.

Adiciona formula

Pomoću (2.2) je takodje moguće dokazati i

Lema 2.5.3 *Za cele brojeve n i k važi*

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}. \tag{2.4}$$

Dokaz U ovom slučaju elegantniji dokaz se dobija kombinatornim tumačenjem obe strane jednakosti (2.4). Leva strana (2.4) predstavlja broj k-točlanih podskupova nekog n-točlanog skupa X. Izaberimo proizvoljni element $a \in X$. Sada k-točlane podskupove skupa X možemo da podelimo u dve grupe u zavisnosti od toga da li sadrže a ili ne. Podskupovi koji ne sadrže a su upravo svi k-točlani podskupovi skupa $X \setminus \{a\}$, pa je njihov broj $\binom{n-1}{k}$. Ako je A neki k-točlani podskup skupa X koji sadrži a, tada podskupu A možemo da mu pridružimo podskup $A' = A \setminus \{a\}$ koji sadrži $k-1$ elemenata. Lako je proveriti da je ovo pridruživanje bijekcija izmedju svih k-točlanih podskupova skupa X koji sadrže a i svih podskupova sa $k-1$ elemenata skupa $X \setminus \{a\}$. Broj takvih podskupova je stoga jednak $\binom{n-1}{k-1}$. Sve u svemu, broj k-točlanih podskupova skupa X je jednak $\binom{n-1}{k} + \binom{n-1}{k-1}$. ■

Prethodna lema važi i u slučajevima kada je $k < 0$ ili $k > n$, jer su tada svi binomni koeficijenti jednaki 0. Ona takodje važi i kada n nije ceo broj ili kada je $n < 0$, s tim što u ovim slučajevima ona više nema kombinatorno tumačenje.

Jednakost (2.4) je blisko povezana sa tzv. *Paskalovim trouglom*:

$$\begin{array}{ccccccccccccc}
 & & & & & & 1 & & & & & & \\
 & & & & & 1 & & 1 & & & & & \\
 & & & & 1 & & 2 & & 1 & & & & \\
 & & & 1 & & 3 & & 3 & & 1 & & & \\
 & & 1 & & 4 & & 6 & & 4 & & 1 & & \\
 & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & \\
1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1 \\
 & & & \vdots & & & & & & \vdots & & &
\end{array}$$

Paskalov trougao se dobija tako što se počne sa redom koji sadrži samo broj 1, a zatim se svaki sledeći red dobija tako što se ispod svakog para uzastopnih brojeva u prethodnom redu napiše njihov zbir, i na kraju se na oba kraja novog reda stavi broj 1. Indukcijom uz pomoć jednakosti (2.4) može da se dokaže da $(n+1)$-vi red sadrži binomne koeficijente $\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{n}$. Paskalov trougao omogućava i da se proizvoljan binomni koeficijent izračuna koristeći samo sabiranje: dovoljno je naći samo one brojeve koji se u Paskalovom trouglu nalaze gore levo i gore desno od traženog binomnog koeficijenta.

Binomna teorema

Najvažnije svojstvo binomnih koeficijenata iskazano je u sledećoj

Teorema 2.5.4 *Za svaki nenegativni ceo broj n važi*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} \tag{2.5}$$

(ovo je jednakost dva polinoma sa promenljivama x i y, pa važi za proizvoljne vrednosti x i y).

Dokaz Binomnu teoremu dokazujemo indukcijom po n. Za $n = 0$ obe strane jednakosti (2.5) su jednake 1. Pretpostavimo stoga da (2.5) važi za neko $n = n_0 \geq 0$ i dokažimo da tada (2.5) važi i za $n = n_0 + 1$. Dakle,

$$\begin{aligned}
& (x+y)^{n_0+1} = (x+y)(x+y)^{n_0} \\
& \qquad \text{(induktivna pretpostavka za } (x+y)^{n_0}) \\
= \; & (x+y)\sum_{k=0}^{n_0}\binom{n_0}{k}x^k y^{n_0-k} \\
= \; & x\sum_{k=0}^{n_0}\binom{n_0}{k}x^k y^{n_0-k} + y\sum_{k=0}^{n_0}\binom{n_0}{k}x^k y^{n_0-k} \\
= \; & \sum_{k=0}^{n_0}\binom{n_0}{k}x^{k+1} y^{n_0-k} + \sum_{k=0}^{n_0}\binom{n_0}{k}x^k y^{n_0-k+1} \\
& \qquad \text{(promena granica promenljive } k \text{ u prvoj sumi)} \\
= \; & \sum_{k=1}^{n_0+1}\binom{n_0}{k-1}x^k y^{n_0-k+1} + \sum_{k=0}^{n_0}\binom{n_0}{k}x^k y^{n_0-k+1} \\
& \qquad \text{(izdvajanje dva posebna slučaja)} \\
= \; & \binom{n_0}{n_0}x^{n_0+1}y^0 + \sum_{k=1}^{n_0}\binom{n_0}{k-1}x^k y^{n_0-k+1} \\
+ \; & \binom{n_0}{0}x^0 y^{n_0+1} + \sum_{k=1}^{n_0}\binom{n_0}{k}x^k y^{n_0-k+1} \\
& \qquad \text{(koristimo } \tbinom{n_0}{n_0} = 1 = \tbinom{n_0+1}{n_0+1} \text{ i } \tbinom{n_0}{0} = 1 = \tbinom{n_0+1}{0}) \\
= \; & \binom{n_0+1}{n_0+1}x^{n_0+1}y^0 + \binom{n_0+1}{0}x^0 y^{n_0+1} \\
+ \; & \sum_{k=1}^{n_0}\left(\binom{n_0}{k-1} + \binom{n_0}{k}\right)x^k y^{n_0+1-k} \\
& \qquad \text{(koristimo } \tbinom{n_0}{k-1} + \tbinom{n_0}{k} = \tbinom{n_0+1}{k}) \\
= \; & \binom{n_0+1}{n_0+1}x^{n_0+1}y^0 + \binom{n_0+1}{0}x^0 y^{n_0+1} + \sum_{k=1}^{n_0}\binom{n_0+1}{k}x^k y^{n_0+1-k} \\
& \qquad \text{(vraćanje dva posebna slučaja)}
\end{aligned}$$

$$= \sum_{k=0}^{n_0+1} \binom{n_0+1}{k} x^k y^{n_0+1-k}. \quad \blacksquare$$

Ako u binomnoj teoremi stavimo $y = 1$ tada dobijamo važan specijalni slučaj

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k. \tag{2.6}$$

Iz binomne teoreme možemo da dobijemo razne identitete koji uključuju binomne koeficijente. Par najjednostavnijih se dobijaju ako u (2.6) redom stavimo $x = 1$ i $x = -1$:

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{n} = 2^n, \tag{2.7}$$

$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \ldots + (-1)^n \binom{n}{n} = 0. \tag{2.8}$$

Sabiranjem, odnosno oduzimanjem, identiteta (2.7) i (2.8) dobijamo takodje

$$\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \ldots = 2^{n-1},$$

$$\binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \ldots = 2^{n-1}.$$

Zadaci

2.6 Binomni identiteti

Binomni koeficijenti zadovoljavaju na hiljade identiteta, i već vekovima se istražuju njihova neverovatna svojstva. Cele knjige su posvećene samo njima, pa čak postoje i automatizovani metodi za dokazivanje identiteta sa binomnim koeficijentima. Jedan od jednostavnijih takvih metoda ćemo naći u sledećoj glavi.

U klasičnoj kombinatorici postoje dva opšte prihvaćena načina za dokazivanje binomnih identiteta—analitički i kombinatorni. Pod analitičkim dokazivanjem se podrazumeva korišćenje poznatih binomnih identiteta za transformaciju izraza sa binomnim koeficijentima, dok se pod kombinatornim dokazivanjem podrazumeva tumačenje obe strane identiteta kao izraza koji prebrojavaju neki skup objekata na dva različita načina.

Analitičko dokazivanje binomnih identiteta

Pored najjednostavnijih svojstava (2.2), (2.3), (2.4), kao i veoma važne binomne teoreme, za rad sa binomnim koeficijentima se često koriste i sledeće leme.

Izvlačenje iz zagrada

Lema 2.6.1 *Za ceo broj $k \neq 0$ i proizvoljan broj n važi*

$$\binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1} = \frac{n}{n-k}\binom{n-1}{k}. \tag{2.9}$$

Dokaz Ove jednakosti se lako dokazuju faktorijelnom reprezentacijom (2.2) binomnih koeficijenata:

$$\begin{aligned}\binom{n}{k} &= \frac{n!}{k!(n-k)!} = \frac{n(n-1)!}{k(k-1)!(n-k)!} = \frac{n}{k}\binom{n-1}{k-1},\\ \binom{n}{k} &= \frac{n!}{k!(n-k)!} = \frac{n(n-1)!}{k!(n-k)(n-k-1)!} = \frac{n}{n-k}\binom{n-1}{k}. \quad \blacksquare\end{aligned}$$

Sumaciona formula

Lema 2.6.2 *Za cele brojeve n i m, $n, m \geq 0$ važi*

$$\sum_{k=0}^{n}\binom{r+k}{k} = \binom{r}{0} + \binom{r+1}{1} + \ldots + \binom{r+n}{n} = \binom{r+n+1}{n}, \tag{2.10}$$

$$\sum_{k=0}^{n}\binom{k}{m} = \binom{0}{m} + \binom{1}{m} + \ldots + \binom{n}{m} = \binom{n+1}{m+1}. \tag{2.11}$$

Dokaz Obe formule dokazujemo matematičkom indukcijom po n uz pomoć adicione formule (2.4).

Za $n = 0$ obe strane jednakosti (2.10) su jednake 1. Pretpostavimo sada da jednakost (2.10) važi za neko $n = n_0$. Sada za $n = n_0 + 1$ imamo

$$\begin{aligned}\sum_{k=0}^{n_0+1}\binom{r+k}{k} &= \sum_{k=0}^{n_0}\binom{r+k}{k} + \binom{r+n_0+1}{n_0+1} && \text{(induktivna pretpostavka)}\\ &= \binom{r+n_0+1}{n_0} + \binom{r+n_0+1}{n_0+1} && \text{(adiciona formula)}\\ &= \binom{r+(n_0+1)+1}{n_0+1}.\end{aligned}$$

Što se tiče jednakosti (2.11) za $n = 0$ njena leva strana je jednaka $\binom{0}{m}$, dok je desna strana jednaka $\binom{1}{m+1}$. Tada su za $m = 0$ obe strane jednake 1, dok su za $m \neq 0$ obe strane jednake 0. U svakom slučaju, jednakost (2.11) važi za $n = 0$.

Pretpostavimo sada da ona važi za neko $n = n_0$. Tada za $n = n_0 + 1$ imamo

$$\begin{aligned}\sum_{k=0}^{n_0+1}\binom{k}{m} &= \sum_{k=0}^{n_0}\binom{k}{m} + \binom{n_0+1}{m} && \text{(induktivna pretpostavka)}\\ &= \binom{n_0+1}{m+1} + \binom{n_0+1}{m} && \text{(adiciona formula)}\\ &= \binom{(n_0+1)+1}{m+1}. \quad \blacksquare\end{aligned}$$

Jednakost (2.11) se često pojavljuje u primenama. Na primer, za $m = 1$ imamo zbir aritmetičke progresije

$$\binom{0}{1} + \binom{1}{1} + \ldots + \binom{n}{1} = 0 + 1 + \ldots + n = \binom{n+1}{2} = \frac{(n+1)n}{2}.$$

Pretpostavimo da želimo da nadjemo zbir $1^2 + 2^2 + \ldots + n^2$. Ako primetimo da je $k^2 = 2\binom{k}{2} + \binom{k}{1}$, tada se lako dobija da je

$$\sum_{k=0}^{n} k^2 = \sum_{k=0}^{n} \left(2\binom{k}{2} + \binom{k}{1}\right) = 2\binom{n+1}{3} + \binom{n+1}{2}.$$

Rešenje, koje smo dobili u binomnim koeficijentima, možemo da vratimo u uobičajenu notaciju:

$$\begin{aligned} 1^2 + 2^2 + \ldots + n^2 &= 2\frac{(n+1)n(n-1)}{6} + \frac{(n+1)n}{2} \\ &= \frac{1}{3}n(n+\frac{1}{2})(n+1). \end{aligned}$$

Zbir $1^3 + 2^3 + \ldots + n^3$ može da se dobije na sličan način; u suštini, *svaki* polinom $a_0 + a_1k + a_2k^2 + \ldots + a_mk^m$ može da se izrazi u obliku $b_0\binom{k}{0} + b_1\binom{k}{1} + \ldots + b_m\binom{k}{m}$ za pogodno izabrane koeficijente $b_0, b_1, \ldots, b_m$.

Negacija gornjeg indeksa

Lema 2.6.3 *Za svaki ceo broj k i proizvoljan broj n važi*

$$\binom{-n}{k} = (-1)^k\binom{n+k-1}{k}. \tag{2.12}$$

Dokaz Ova se jednakost dobija jednostavno iz same definicije binomnog koeficijenta:

$$\begin{aligned} \binom{-n}{k} &= \frac{-n(-n-1)(-n-2)\cdots(-n-k+1)}{k(k-1)\cdots 2\cdot 1} \\ &= \frac{(-1)^k n(n+1)(n+2)\cdots(n+k-1)}{k(k-1)\cdots 2\cdot 1} = (-1)^k\binom{n+k-1}{k}. \quad \blacksquare \end{aligned}$$

Negacija gornjeg indeksa je često korisna transformacija gornjeg indeksa u binomnom koeficijentu.

Primer Dokazati sumacionu formulu

$$\sum_{k=0}^{n}(-1)^k\binom{r}{k} = \binom{r}{0} - \binom{r}{1} + \cdots + (-1)^n\binom{r}{n} = (-1)^n\binom{r-1}{n}. \tag{2.13}$$

Dokaz Koristeći redom negaciju gornjeg indeksa (2.12) i prvu sumacionu formulu (2.10) dobijamo

$$\sum_{k=0}^{n}(-1)^k\binom{r}{k} = \sum_{k=0}^{n}\binom{-r+k-1}{k} = \binom{-r+n}{n} = (-1)^n\binom{r-1}{n}. \quad \blacksquare$$

Pojednostavljivanje proizvoda

Lema 2.6.4 *Za sve cele brojeve m i k i proizvoljan broj n važi*

$$\binom{n}{m}\binom{m}{k} = \binom{n}{k}\binom{n-k}{m-k} \tag{2.14}$$

Dokaz Ovu jednakost je dovoljno dokazati u slučaju kada je n ceo broj $\geq m$. Pritom možemo da pretpostavimo da je $0 \leq k \leq m$, jer su u suprotnom obe strane jednakosti jednake 0. Sada imamo

$$\begin{aligned}\binom{n}{m}\binom{m}{k} &= \frac{n!m!}{m!(n-m)!k!(m-k)!} \\ &= \frac{n!(n-k)!}{k!(n-k)!(m-k)!(n-m)!} = \binom{n}{k}\binom{n-k}{m-k}. \quad \blacksquare\end{aligned}$$

Prethodnu jednakost smo dokazali samo za cele vrednosti n koje su $\geq m$. Medjutim ona važi za sve realne vrednosti n. Naime, već smo dokazali da jednakost

$$\binom{n}{m}\binom{m}{k} = \binom{n}{k}\binom{n-k}{m-k}$$

važi za *beskonačno mnogo vrednosti* n. Obe strane ove jednakosti su *polinomi* po promenljivoj n. Nenula polinom stepena r može da ima najviše r različitih korena, tako da ako (oduzimanjem) *dva polinoma stepena $\leq r$ imaju istu vrednost u $r+1$ ili više različitih tačaka, onda su ti polinomi identički jednaki.* Ovaj princip se može koristiti za proširenje važnosti mnogih identiteta sa celih brojeva na realne brojeve.

Sume proizvoda

Jednakosti u sledećoj lemi se koriste kada treba sumirati proizvod dva binomna koeficijenta u kojima se sumacioni indeks k nalazi na donjem mestu.

Lema 2.6.5 *Za svaki ceo broj n i svaki ceo broj $r \geq 0$ važi*

$$\sum_k \binom{r}{k}\binom{s}{n-k} = \binom{r+s}{n}, \tag{2.15}$$

$$\sum_k \binom{r}{k}\binom{s}{n+k} = \binom{r+s}{r+n}. \tag{2.16}$$

Ovu lemu ćemo dokazati malo kasnije. Najpre ćemo da vidimo par primera kako se prethodne jednakosti mogu koristiti za rad sa binomnim identitetima.

Primer Ako je r nenegativni ceo broj, koja je vrednost izraza $\sum_k \binom{r}{k}\binom{s}{k}k$?

Dokaz Izvlačenjem iz zagrada (2.9) možemo da se oslobodimo spoljasnjeg k:

$$\sum_k \binom{r}{k}\binom{s}{k}k = \sum_k \binom{r}{k}\binom{s-1}{k-1}\frac{s}{k}k = s\sum_k \binom{r}{k}\binom{s-1}{k-1}.$$

Sada može da se primeni jednakost (2.16) sa $n = -1$. Krajnje rešenje je

$$\sum_k \binom{r}{k}\binom{s}{k}k = s\binom{r+s-1}{r-1}. \quad \blacksquare$$

Kombinatorno dokazivanje binomnih identiteta

Kao što smo već rekli, pod kombinatornim dokazivanjem se podrazumeva tumačenje obe strane identiteta kao izraza koji prebrojavaju neki skup objekata na dva različita načina. Ovaj način dokazivanja primenjujemo u dokazu leme 2.6.5.

Dokaz leme 2.6.5 Najpre ćemo dokazati jednakost (2.15)

$$\sum_k \binom{r}{k}\binom{s}{n-k} = \binom{r+s}{n}.$$

Neka je dat skup X sa $r+s$ elemenata. Desna strana gornje jednakosti predstavlja broj n-točlanih podskupova skupa X.

Obojimo sada r elemenata skupa X u crvenu, a preostalih s elemenata u plavu boju. Drugi način da se izabere n-točlani podskup skupa X jeste da se izabere k crvenih elemenata i $n-k$ plavih elemenata. Za svako k postoji $\binom{r}{k}$ načina da se izaberu crveni elementi, i nezavisno od toga, $\binom{s}{n-k}$ načina da se izaberu plavi elementi. Sveukupno, n-točlani podskup skupa X može da se izabere na $\sum_k \binom{r}{k}\binom{s}{n-k}$ načina, što je upravo leva strana gornje jednakosti.

Jednakost (2.16) se dokazuje pomoću prethodne jednakosti i dvostruke primene uslova simetričnosti. Naime, važi

$$\sum_k \binom{r}{k}\binom{s}{n+k} = \sum_k \binom{r}{k}\binom{s}{s-n-k} = \binom{r+s}{s-n} = \binom{r+s}{r+n}. \quad \blacksquare$$

Primer Dokazati da važi

$$\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}.$$

Dokaz Za dokaz koristimo uslov simetričnosti i jednakost (2.15) sa $r = n$, $s = n$:

$$\sum_{k=0}^{n} \binom{n}{k}^2 = \sum_{k=0}^{n} \binom{n}{k} \binom{n}{n-k} = \binom{2n}{n}. \quad \blacksquare$$

Primer Dokazati da važi

$$\sum_{k=0}^{n} \binom{2n}{2k} \binom{2k}{k} 2^{2n-2k} = \binom{4n}{2n}.$$

Dokaz Nalaženje odgovarajućeg kombinatornog tumačenja ovog binomnog identiteta je malo teže.

Neka je dat skup $X = \{x_1, x_2, \ldots, x_{4n}\}$. Desna strana gornje jednakosti predstavlja broj podskupova skupa X sa $2n$ elemenata.

Sada treba ove podskupove prebrojati na drugačiji način. Neka je $A_i = \{x_{2i-1}, x_{2i}\}$ za $i = 1, 2, \ldots, 2n$. Skupovi A_i, $i = 1, 2, \ldots, 2n$ predstavljaju particiju skupa X. Neka je $M \subset X$ proizvoljan podskup sa $2n$ elemenata. Za svako $i = 1, 2, \ldots, 2n$ presek $M \cap A_i$ ima 0, 1 ili 2 elementa, medjutim važi da je

$$2n = |M| = \sum_{i=1}^{2n} |M \cap A_i|.$$

Neka je k broj skupova A_i tako da je $|M \cap A_i| = 2$. Iz prethodne jednakosti tada sledi da je broj skupova A_i tako da je $|M \cap A_i| = 1$ jednak $2n - 2k$, dok je broj skupova A_i tako da je $M \cap A_i = \emptyset$ jednak takodje k.

Posle ovog razmatranja konačno vidimo kako se drugačije mogu prebrojati podskupovi skupa X sa $2n$ elemenata. Naime, od ukupno $2n$ skupova A_1, A_2, $\ldots$, A_{2n} izabraćemo $2n - 2k$ skupova iz kojih ćemo izabrati po jedan element u podskup. Izbor ovih skupova možemo da napravimo na $\binom{2n}{2n-2k} = \binom{2n}{2k}$ načina. Kako svaki skup A_i ima po dva elementa, to za svaki od izabranih skupova postoje dva načina da izaberemo jedan element u podskup, pa je ukupan broj načina za to jednak 2^{2n-2k}. Konačno, od preostalih $2k$ skupova A_i treba izabrati još k skupova čija ćemo oba elementa izabrati u podskup, što se može uraditi na $\binom{2k}{k}$ načina, tako da je ukupan broj načina da se izabere podskup skupa X sa $2n$ elemenata jednak

$$\sum_{k=0}^{n} \binom{2n}{2k} \binom{2k}{k} 2^{2n-2k}. \quad \blacksquare$$

Zadaci

2.7 Multinomijalni koeficijenti

Postoji nekoliko uopštenja pojma binomnog koeficijenta, od kojih su najvažniji multinomijalni koeficijenti. Razmotrimo sledeći problem: koliko različitih reči, uključujući besmislene, može da se sastavi od slova reči ABRAKADABRA? Drugim rečima, na koliko različitih načina se mogu preurediti ova slova? Zamislimo najpre da se sva slova u reči razlikuju, tako da imamo 5 različitih slova A itd. Na primer, možemo da ih učinimo različitim dodajući im indekse: $\mathrm{A_1B_1R_1A_2K_1A_3D_1A_4B_2R_2A_5}$. Sada imamo 11 različitih slova koja mogu da se preurede na 11! različitih načina. Posmatrajmo proizvoljnu reč sačinjenu od "neindeksirane" reči ABRAKADABRA, na primer BAKARADABAR. Od koliko različitih "indeksiranih" reči možemo da dobijemo ovu reč brisanjem indeksa? Indeksi 5 slova A mogu da se rasporede na 5! načina, indeksi 2 slova B mogu da se rasporede (nezavisno) na 2! načina, za 2 slova R takodje imamo 2! mogućnosti i konačno za po jedno slovo K i D imamo po 1! mogućnost. Prema tome, reč BAKARADABAR, kao i bilo koju drugu reč dobijenu od reči ABRAKADABRA, možemo da indeksiramo na 5!2!2!1!1! načina. Broj neindeksiranih reči, što je i rešenje problema, jednak je 11!/(5!2!2!1!1!).

Isti argument vodi i do sledećeg opšteg rezultata: ako imamo $k_1+k_2+\ldots+k_m$ objekata od m različitih vrsta, od čega k_i jednakih objekata i-te vrste, tada je broj različitih rasporeda ovih objekata u nizu dat izrazom

$$\frac{(k_1+k_2+\ldots+k_m)!}{k_1!k_2!\cdots k_m!}.$$

Ovaj izraz se obično zapisuje kao

$$\binom{k_1+k_2+\ldots+k_m}{k_1,k_2,\ldots,k_m}$$

i naziva *multinomijalni koeficijent*. U suštini, za $m=2$ dobijamo binomni koeficijent, tj. $\binom{n}{k,n-k}$ označava isto što i $\binom{n}{k}$. Štaviše, svaki multinomijalni koeficijent se može predstaviti pomoću binomnih koeficijenata:

$$\binom{k_1+k_2+\ldots+k_m}{k_1,k_2,\ldots,k_m} = \binom{k_1+k_2}{k_1}\binom{k_1+k_2+k_3}{k_1+k_2}\cdots\binom{k_1+k_2+\ldots+k_m}{k_1+\ldots+k_{m-1}}.$$

Najvažnije svojstvo multinomijalnih koeficijenata predstavlja sledeće uopštenje binomne teoreme.

Teorema 2.7.1 (Multinomijalna teorema) *Za proizvoljne realne brojeve x_1, x_2, …, x_m i za svaki prirodan broj $n \geq 1$ važi*

$$(x_1+x_2+\ldots+x_m)^n = \sum_{\substack{k_1+\ldots+k_m=n\\ k_1,\ldots,k_m\geq 0}} \binom{n}{k_1,k_2,\ldots,k_m} x_1^{k_1}x_2^{k_2}\cdots x_m^{k_m}.$$

Desna strana multinomijalne formule obično ima prilično mnogo sabiraka, pošto se sabira po svim kompozicijama broja n u m sabiraka, ali se ova teorema ionako najčešće koristi kako bismo odredili koeficijent uz neki odredjeni član. Na primer, multinomijalna teorema nam kaže da je koeficijent uz član $x^2y^3z^5$ u razvoju izraza $(x + y + z)^1 0$ jednak $\binom{10}{2,3,5} = 2520$.

Multinomijalna teorema se može dokazati indukcijom po n, ali se elegantniji dokaz može dobiti tehnikama koje ćemo obraditi u sledećoj glavi.

Zadaci

2.8 Princip uključenja-isključenja

Jedan od osnovnih principa prebrojavanja—princip zbira (teorema 2.1.3) tvrdi da je $|A \cup B|$ zbir $|A|$ i $|B|$ kada su A i B disjunktni skupovi. Ako A i B nisu disjunktni, sabiranjem $|A|$ i $|B|$ elemente preseka $|A \cap B|$ brojimo dva puta (sl. 2.6a). Stoga, da bi dobili pravu vrednost $|A \cup B|$ moramo oduzeti $|A \cap B|$:

$$|A \cup B| = |A| + |B| - |A \cap B|. \tag{2.17}$$

Slično rasudjivanje primenjujemo i u slučaju tri skupa (sl. 2.6b). Kada saberemo $|A|$, $|B|$ i $|C|$ elemente preseka $|A \cap B|$, $|B \cap C|$ i $|C \cap A|$ brojimo dva puta (ukoliko nisu u preseku sva tri skupa). Da ovo ispravimo, oduzimamo $|A \cap B|$, $|B \cap C|$ i $|C \cap A|$. Ali sada smo elemente $A \cap B \cap C$, koje smo u $|A| + |B| + |C|$ brojali tri puta, oduzeli takodje tri puta. Stoga, da bi dobili pravu vrednost $|A \cup B \cup C|$, moramo da dodamo $|A \cap B \cap C|$:

$$\begin{aligned} |A \cup B \cup C| = (|A| + |B| + |C|) - (|A \cap B| + |B \cap C| + |C \cap A|) \\ +|A \cap B \cap C|. \end{aligned} \tag{2.18}$$

Slika 2.6: Preseci dva i tri skupa

Primer Na drugoj godini Odseka za matematiku ima 50 studenata. Od njih će u oktobarskom ispitnom roku 24 izaći na matematičku analizu, 20 na algebru i 13 na diskretnu matematiku. Matematičku analizu i algebru će polagati 6 studenata, algebru i diskretnu matematiku 5 studenata, a analizu i diskretnu matematiku 4 studenta. Ako jedino Zlatko polaže sva tri ispita, koliko studenata neće izaći ni na jedan ispit?

Rešenje Neka M, A i D označaju skupove studenata koji izlaze na matematičku analizu, algebru i diskretnu matematiku, redom. Iz gornjih uslova imamo da je

$$\begin{aligned} &|M| + |A| + |D| = 24 + 20 + 13 = 57, \\ &|M \cap A| + |A \cap D| + |D \cap M| = 6 + 5 + 4 = 15, \\ &|M \cap A \cap D| = 1. \end{aligned}$$

Iz jednakosti (2.18) imamo

$$|M \cup A \cup D| = 57 - 15 + 1 = 43,$$

pa je broj studenata koji neće izaći ni na jedan ispit jednak $50 - 43 = 7$. ■

Prethodno rasudjivanje možemo da proširimo i na slučaj n konačnih skupova $A_1, A_2, \dots, A_n$. Broj elemenata $|A_1 \cup A_2 \cup \dots \cup A_n|$ dobija se na sledeći način: saberemo veličine svih skupova, zatim oduzmemo veličine svih preseka dva skupa, dodamo veličine svih preseka tri skupa, oduzmemo veličine svih preseka četiri skupa, ... U poslednjem koraku, ili dodajemo (za neparno n) ili oduzimamo (za parno n) veličinu preseka svih n skupova.

Kako ovo zapisujemo u obliku formule? Prvi pokušaj bi mogao da bude

$$\begin{gathered}
|A_1 \cup A_2 \cup \dots \cup A_n| = |A_1| + |A_2| + \dots + |A_n| \\
-|A_1 \cap A_2| - |A_1 \cap A_3| - \dots - |A_1 \cap A_n| - |A_2 \cap A_3| - \dots - |A_{n-1} \cap A_n| \\
+|A_1 \cap A_2 \cap A_3| + |A_1 \cap A_2 \cap A_4| + \dots \\
+(-1)^{n-1}|A_1 \cap A_2 \cap \dots \cap A_n|.
\end{gathered}$$

Ovo je nezgrapan i ne preterano čitljiv način da se izrazi tako jednostavno pravilo. Nešto je bolji zapis koristeći sume:

$$\begin{aligned}
|A_1 \cup A_2 \cup \dots \cup A_n| &= \sum_{i=1}^{n} |A_i| - \sum_{1 \le i_1 < i_2 \le n} |A_{i_1} \cap A_{i_2}| \\
&\quad + \sum_{1 \le i_1 < i_2 < i_3 \le n} |A_{i_1} \cap A_{i_2} \cap A_{i_3}| \\
&\quad - \dots + (-1)^{n-1} |A_1 \cap A_2 \cap \dots \cap A_n|.
\end{aligned}$$

Ako se prisetimo oznake $\binom{X}{k}$ za skup svih k-elementnih podskupova skupa X, i ako upotrebimo oznaku sličnu $\sum$ za višestruke preseke i unije, istu formulu možemo zapisati i znatno elegantnije:

Teorema 2.8.1 *(Princip uključenja–isključenja) Za konačne skupove $A_1, A_2, \dots, A_n$ važi*

$$\left| \bigcup_{i=1}^{n} A_i \right| = \sum_{k=1}^{n} (-1)^{k-1} \sum_{I \in \binom{\{1,2,\dots,n\}}{k}} \left| \bigcap_{i \in I} A_i \right|. \tag{2.19}$$

Da biste bolje shvatili ovu formulu, mogli biste da je proradite detaljno za slučaj $n = 3$. Obratite pažnju pri tome da ne mešate brojeve sa skupovima! Ako vam je formula (2.19) i dalje suviše duga, postoji još jedan način zapisivanja principa uključenja–isključenja:

$$\left| \bigcup_{i=1}^{n} A_i \right| = \sum_{\emptyset \ne I \subseteq \{1,2,\dots,n\}} (-1)^{|I|-1} \left| \bigcap_{i \in I} A_i \right|. \tag{2.20}$$

Dokaz indukcijom Indukcija je po broju skupova n, s tim što za bazu indukcije koristimo $n = 2$. Kao što znamo, jednačina (2.19) važi za dva skupa. Pretpostavimo da ona važi za proizvoljnih $n-1$ konačnih skupova. Tada je

$$\left|\bigcup_{i=1}^{n} A_i\right| = \left|\left(\bigcup_{i=1}^{n-1} A_i\right) \cup A_n\right| = \left|\bigcup_{i=1}^{n-1} A_i\right| + |A_n| - \left|\left(\bigcup_{i=1}^{n-1} A_i\right) \cap A_n\right|$$

(ovde smo koristili princip uključenja-isključenja za dva skupa, tj. $|A \cup B| = |A| + |B| - |A \cap B|$ sa $A = A_1 \cup A_2 \cup \ldots \cup A_{n-1}$, $B = A_n$)

$$= \left|\bigcup_{i=1}^{n-1} A_i\right| + |A_n| - \left|\bigcup_{i=1}^{n-1} (A_i \cap A_n)\right|$$

(distributivnost preseka: $(X \cup Y) \cap Z = (X \cap Z) \cup (Y \cap Z)$; sada koristimo induktivnu pretpostavku dva puta, jednom za $|A_1 \cup A_2 \cup \ldots \cup A_{n-1}|$ i jednom za $|(A_1 \cap A_n) \cup (A_2 \cap A_n) \cup \ldots \cup (A_{n-1} \cap A_n)|$)

$$= \left(\sum_{k=1}^{n-1} (-1)^{k-1} \sum_{I \in \binom{\{1,2,\ldots,n-1\}}{k}} \left|\bigcap_{i \in I} A_i\right|\right) + |A_n|$$

$$- \left(\sum_{k=1}^{n-1} (-1)^{k-1} \sum_{I \in \binom{\{1,2,\ldots,n-1\}}{k}} \left|\bigcap_{i \in I \cup \{n\}} A_i\right|\right).$$

Dokaz je skoro gotov. U prvoj sumi sabiramo, sa odgovarajućim znacima, veličine svih preseka koji ne uključuju skup A_n. U drugoj sumi se pojavljuju veličine svih preseka koji uključuju skup A_n i presek $k+1$ skupova (tj. k skupova od A_1, A_2,$\ldots$,A_{n-1} i još A_n) sa znakom $-(-1)^{k-1} = (-1)^k$. Druga suma ne uključuje $|A_n|$, ali se taj sabirak pojavljuje izmedju dve sume. Sve u svemu, veličina preseka bilo kojih k skupova od A_1, A_2, $\ldots$, A_n pojavljuje se tačno jednom u izrazu sa znakom $(-1)^{k-1}$, što se slaže sa jednačinom (2.19), pa je dokaz indukcijom završen. Sada se vidi važnost razumljivog zapisa ovog principa, jer bi se bez toga lako izgubili u dokazu. ■

Dokaz prebrojavanjem Posmatrajmo proizvoljni element $x \in A_1 \cup A_2 \cup \ldots \cup A_n$. On doprinosi tačno 1 veličini unije na levoj strani jednačine (2.19). Razmotrimo sada koliko x doprinosi veličinama raznih preseka na desnoj strani ove jednačine. Neka je j broj skupova A_i koji sadrže x. Preimenujmo skupove tako da se x sadrži u skupovima A_1, A_2, $\ldots$, A_j.

Sada se element x pojavljuje u preseku svake k-torke skupova od A_1, A_2, $\ldots$, A_j i ni u jednom drugom preseku. Pošto postoji $\binom{j}{k}$ k-elementnih podskupova skupa sa j elemenata, x se pojavljuje u $\binom{j}{k}$ preseka k-torki skupova. Veličine preseka k-torki skupova se množe sa $(-1)^{k-1}$, tako da na desnoj strani jednačine (2.19) x doprinosi vrednošću

$$j - \binom{j}{2} + \binom{j}{3} - \ldots + (-1)^{j-1}\binom{j}{j}.$$

Po jednačini (2.8) za zbir binomnih koeficijenata sa naizmeničnim znacima, gornji izraz je jednak 1. Doprinos x obema stranama jednačine (2.19) je jednak 1, pa jednačina važi. ■

Primer Jednog zimskog dana poslanici, njih n na broju, dolaze na zasedanje Skupštine i ostavljaju svoje kapute u garderobi. Po završetku zasedanja, starija gospodja iz garderobe, možda potpuno rasejana, možda skoro slepa posle mnogo godina rada u slabo osvetljenoj garderobi, izdaje jedan kaput svakom poslaniku. Na koliko načina ona može da izda kapute tako da nijedan poslanik ne dobije svoj kaput?

Rešenje Preformulišimo ovaj problem koristeći permutacije. Ako označimo poslanike brojevima $1, 2, \ldots, n$, kao i njihove kapute, tada izdavanje kaputa iz garderobe odgovara permutaciji π skupa $\{1, 2, \ldots, n\}$, gde je $\pi(i)$ broj kaputa koji je vraćen i-tom poslaniku. Naše pitanje sada glasi: koliko ima permutacija π tako da je $\pi(i) \neq i$ za svako $i = 1, 2, \ldots, n$?

Neka je S_n skup svih permutacija skupa $\{1, 2, \ldots, n\}$ i za $i = 1, 2, \ldots, n$ neka je $A_i = \{\pi \in S_n : \pi(i) = i\}$. Kažemo da elementi skupa A_i (kojeg čine permutacije!) *fiksiraju* i. Koristeći princip uključenja-isključenja prebrojaćemo "loše" permutacije, tj. one koje fiksiraju bar jedan broj. Loše permutacije su upravo one koje se nalaze u uniji $A_1 \cup A_2 \cup \ldots \cup A_n$.

Da bi primenili princip uključenja-isključenja moramo da nadjemo veličinu preseka k-torke skupova A_i. Lako se vidi da je $|A_i| = (n-1)!$, jer je $\pi(i) = i$ fiksirano, a preostali brojevi se mogu proizvoljno poredjati. Koje permutacije leže u $A_i \cap A_j$? Upravo one koje fiksiraju brojeve i i j (dok se preostalih $n-2$ brojeva može poredjati proizvoljno), tako da je $|A_i \cap A_j| = (n-2)!$. Opštije, za proizvoljne $i_1 < i_2 < \ldots < i_k$ imamo da je $|A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_k}| = (n-k)!$, pa princip uključenja-isključenja daje

$$|A_1 \cup A_2 \cup \ldots \cup A_n| = \sum_{k=1}^{n} (-1)^{k-1} \binom{n}{k} (n-k)! = \sum_{k=1}^{n} (-1)^{k-1} \frac{n!}{k!}.$$

Ovim smo izračunali broj loših permutacija (koje fiksiraju bar jedan broj), pa je broj permutacija koje ne fiksiraju nijedan broj jednak

$$D(n) = n! - |A_1 \cup A_2 \cup \ldots \cup A_n| = n! - \frac{n!}{1!} + \frac{n!}{2!} - \cdots + (-1)^n \frac{n!}{n!}. \quad ■$$

Napomena Primetimo da je

$$D(n) = n! \left(1 - \frac{1}{1!} + \frac{1}{2!} - \cdots + (-1)^n \frac{1}{n!}\right).$$

Kao što smo naučili u analizi, red u zagradi konvergira ka e^{-1} kada $n \to \infty$ (gde je e Ojlerov broj) i to veoma brzo. Prema tome, važi približna ocena $D(n) \approx n!/e$.

Primer Neka su X i Y konačni skupovi sa $|X| = n$ i $|Y| = m$. Već nam je poznato da postoji m^n funkcija koje preslikavaju X u Y. Koliko od ovih funkcija je *na*?

Rešenje Kao i u prethodnom primeru, iskoristićemo princip uključenja-isključenja da najpre prebrojimo objekte (funkcije) koje ne zadovoljavaju traženi uslov (nisu *na*). Tada je broj funkcija *na* jednak razlici izmedju ukupnog broja funkcija m^n i broja "loših" funkcija.

Bez gubitka opštosti, pretpostavimo da je $Y = \{1, 2, \ldots, m\}$. Neka A_i označava skup funkcija koje preslikavaju X u Y i pritom ne uzimaju vrednost i. Ako funkcija $f\colon X \mapsto Y$ nije *na*, tada postoji $i \in Y$ tako da za svako $x \in X$ važi $f(x) \neq i$. Samim tim, funkcija f pripada skupu A_i, pa zaključujemo da funkcija nije *na* ako i samo ako pripada skupu $A_1 \cup A_2 \cup \ldots \cup A_m$.

Koliko ima funkcija u skupu A_i? Skup A_i sadrži sve funkcije koje preslikavaju X u $Y \setminus \{i\}$, pa je stoga $|A_i| = (m-1)^n$. Skup $A_i \cap A_j$ sadrži funkcije koje ne uzimaju vrednosti i i j, tj. sve funkcije koje preslikavaju X u $Y \setminus \{i, j\}$, pa je $|A_i \cap A_j| = (m-2)^n$. U opštem slučaju, $A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_k}$ sadrži sve funkcije koje ne uzimaju nijednu od vrednosti i_1, i_2, $\ldots$, i_k, tako da je $|A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_k}| = (m-k)^n$. Sada po principu uključenja-isključenja imamo da je

$$|A_1 \cup A_2 \cup \ldots \cup A_m| = \sum_{k=1}^{m} (-1)^{k-1} \binom{m}{k} (m-k)^n.$$

Prema tome, ukupan broj funkcija *na* je jednak

$$m^n - \sum_{k=1}^{m} (-1)^{k-1} \binom{m}{k} (m-k)^n = \sum_{k=0}^{m} (-1)^{k} \binom{m}{k} (m-k)^n. \quad \blacksquare$$

Napomena Ako vrednost $\sum_{k=1}^{m} (-1)^{k-1} \binom{m}{k} (m-k)^n$ podelimo sa $m!$, dobijamo ceo broj koji se naziva **Stirlingov broj druge vrste** i označava sa $\left\{ {n \atop m} \right\}$. Ovi brojevi se pojavljuju prilikom prebrojavanja podela n-elementnog skupa na m medjusobno disjunktnih podskupova. Nekoliko svojstava ovih brojeva naći ćete u zadacima.

Zadaci

Glava 3

Funkcije generatrise

3.1 Funkcije generatrise

U prethodnim odeljcima smo se upoznali sa osnovnim tehnikama prebrojavanja konačnih skupova. Sada ćemo predstaviti još jednu važnu tehniku prebrojavanja. Osnovna ideja, sasvim iznenadjujuća, je da beskonačnom nizu realnih brojeva dodelimo odredjenu neprekidnu funkciju, tzv. funkciju generatrisu niza. Problemi nad nizom se tada mogu prevesti na jezik neprekidnih funkcija i poznate analitičke metode.

U ovakvom uvodnom tekstu, mi ćemo obraditi samo jednostavnije primere, koji se u većini slučajeva, koristeći raznorazne trikove, mogu rešiti i bez primene funkcija generatrisa. Medjutim, ovo ne znači da funkcije generatrise ne treba učiti. One predstavljaju veoma moćnu tehniku prebrojavanja: postoji mnogo složenih problema za čije se rešavanje ostale tehnike ne mogu primeniti ili postaju suviše komplikovane.

Kako množimo polinome $p(x) = x + x^2 + x^3 + x^4$ i $q(x) = x + x^3 + x^4$? Jednostavno pravilo kaže da treba da pomnožimo svaki član iz $p(x)$ sa svakim članom iz $q(x)$ i da zatim saberemo sve dobijene proizvode. Njihovo sabiranje je u ovom slučaju jednostavno, jer su svi koeficijenti jednaki 1. Tako odmah dobijamo da je $p(x)q(x) = x^8 + 2x^7 + 2x^6 + 3x^5 + 2x^4 + x^3 + x^2$.

Hajde sada da razmotrimo drugačije pitanje. Izaberimo neki stepen x, na primer x^5, i želimo da saznamo koliki je koeficijent uz x^5 u proizvodu $p(x)q(x)$, ali bez računanja celog proizvoda. U ovom slučaju, x^5 se dobija množenjem člana x iz $p(x)$ sa članom x^4 iz $q(x)$, takodje i množenjem člana x^2 iz $p(x)$ sa članom x^3 iz $q(x)$ i konačno, množenjem člana x^4 iz $p(x)$ sa članom x iz $q(x)$. Svaki od ovih proizvoda dodaje 1 na odgovarajući koeficijent, pa možemo da zaključimo da je koeficijent uz x^5 jednak 3.

Ovo je, u suštini, isto kao kada bismo imali četiri zlatna novčića sa vrednostima od 1, 2, 3 i 4 dinara (ovo su stepeni promenljive x u $p(x)$) i tri srebrna novčića sa vrednostima od 1, 3 i 4 dinara (koji odgovaraju stepenima promenljive x u $q(x)$) i kada bismo pitali na koliko načina se može platiti 5 dinara pomoću jednog zlatnog i jednog srebrnog novčića. Matematički rečeno, koeficijent uz x^5 je jednak broju uredjenih parova (i, j), gde je $i+j = 5$, $i \in \{1, 2, 3, 4\}$ i $j \in \{1, 3, 4\}$.

Sada ćemo razmatranja koja smo izložili za dva odredjena polinoma da izrazimo nešto uopštenije. Neka su I i J konačni skupovi prirodnih brojeva. Formirajmo polinome $p(x) = \sum_{i\in I} x^i$ i $q(x) = \sum_{j\in J} x^j$ (primetimo da su koeficijenti u ovim polinomima nule i jedinice). Tada je, za svaki prirodan broj r, broj rešenja (i, j) jednačine

$$i + j = r$$

gde je $i \in I$ i $j \in J$, jednak koeficijentu uz x^r u proizvodu $p(x)q(x)$.

Sledeće, još interesantnije uopštenje ovog razmatranja bavi se proizvodom 3 i više polinoma.

Primer Na koliko načina se može platiti iznos od 21 dinara ako imamo šest novčića od 1 dinara, pet novčića od 2 dinara i četiri novčića od 5 dinara?

Rešenje Traženi broj jednak je broju rešenja jednačine

$$i_1 + i_2 + i_3 = 21$$

gde je

$$i_1 \in \{0, 1, 2, 3, 4, 5, 6\}, i_2 \in \{0, 2, 4, 6, 8, 10\} \quad \text{i} \quad i_3 \in \{0, 5, 10, 15, 20\}.$$

Ovde i_1 označava deo iznosa plaćen novčićima od 1 dinara, i_2 deo iznosa plaćen novčićima od 2 dinara, a i_3 deo iznosa plaćen novčićima od 5 dinara.

Ovog puta tvrdimo da je broj rešenja ove jednačine jednak koeficijentu uz x^{21} u proizvodu

$$\left(1 + x + x^2 + \ldots + x^6\right)\left(1 + x^2 + x^4 + x^6 + x^8 + x^{10}\right)$$
$$\left(1 + x^5 + x^{10} + x^{15} + x^{20}\right)$$

(naravno, posle sredjivanja ovog izraza). Zaista, član sa x^{21} se dobija tako što se pomnože neki član x^{i_1} iz prvog para zagrada, neki član x^{i_2} iz drugog para zagrada i neki član x^{i_3} iz trećeg para zagrada, ali tako da je $i_1 + i_2 + i_3 = 21$. Svaki takav izbor brojeva i_1, i_2 i i_3 dodaje 1 na odgovarajući koeficijent u proizvodu. ■

Kombinatorno značenje binomne teoreme

Jedan od oblika binomne teoreme tvrdi da je

$$(1 + x)^n = \binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \ldots + \binom{n}{n}x^n. \tag{3.1}$$

Na levoj strani imamo proizvod n polinoma—svaki je jednak $1 + x$. Analogno prethodnim razmatranjima sa novčićima, koeficijent uz x^r posle množenja i sredjivanja predstavlja broj rešenja jednačine

$$i_1 + i_2 + \ldots + i_n = r,$$

gde je $i_1, i_2, \ldots, i_n \in \{0, 1\}$. Svako rešenje ove jednačine označava izbor r promenljivih od i_1, i_2, ..., i_r koje su jednake 1—preostalih $n - r$ promenljivih mora da bude jednako 0. Broj ovakvih izbora je isti kao i broj r-točlanih podskupova skupa sa n elemenata, tj. $\binom{n}{r}$. Ovo znači da je koeficijent uz x^r u proizvodu $(1+x)^n$ jednak $\binom{n}{r}$. Upravo smo dokazali binomnu teoremu na kombinatorni način!

Veštim igranjem sa polinomom $(1+x)^n$ i njemu sličnim, možemo da dobijemo razne binomne identitete. U odeljku 2.5 već smo videli neke od njih: formule $\sum_{k=0}^{n} \binom{n}{k} = 2^n$ i $\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0$ dobijene su, redom, zamenom $x = 1$ i $x = -1$ u (3.1).

Primer Za svako $n \geq 1$ važi

$$\sum_{k=0}^{n} k \binom{n}{k} = n2^{n-1}.$$

Rešenje Ova jednakost se dobija diferenciranjem (3.1) po promenljivoj x. Na obe strane kao rezultat mora da se dobije isti polinom. Diferenciranjem leve strane dobija se $n(1 + x)^{n-1}$, a diferenciranjem desne strane dobija se $\sum_{k=0}^{n} k\binom{n}{k} x^{k-1}$. Zamenom $x = 1$ dobijamo traženi identitet. ■

Stepeni redovi

Definicija 3.1.1 Stepeni red *je beskonačna suma oblika*

$$a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n + \ldots,$$

gde su a_0, a_1, a_2, ..., a_n, ... *realni brojevi, a* x *je realna promenljiva*[1].

Jednostavan primer stepenog reda je

$$1 + x + x^2 + \ldots + x^n + \ldots$$

(svi a_i su jednaki 1). Ovo je već poznata geometrijska progresija koja, u slučaju da je $x \in (-1, 1)$, ima vrednost $\frac{1}{1-x}$. U ovom smislu, stepeni red (3.1) odredjuje funkciju $\frac{1}{1-x}$. S druge strane, ova funkcija već sadrži sve podatke o stepenom redu (3.1). Zaista, ako diferenciramo funkciju k puta i stavimo $x = 0$ u rezultat, dobićemo tačno $k!$ puta koeficijent uz x^k u stepenom redu. Drugim

[1]Ponekad je od velike koristi posmatrati x kao kompleksnu promenljivu i primeniti metode iz kompleksne analize. Ali mi se time ovde nećemo baviti.

rečima, stepeni red (3.1) je Taylorov red funkcije $\frac{1}{1-x}$ u tački $x = 0$. Prema tome, funkciju $\frac{1}{1-x}$ možemo da zamislimo kao inkarnaciju beskonačnog niza $(1, 1, 1, \ldots)$ i obrnuto. Ovakvo pretvaranje beskonačnih nizova u funkcije i nazad je temelj tehnike funkcija generatrisa.

Neka je $(a_0, a_1, a_2, \ldots, a_n, \ldots)$ niz realnih brojeva. Iz matematičke analize je poznato da ako postoji realni broj K tako da je $|a_n| \leq K^n$ za svako $n \geq 1$, tada red $a(x) = \sum_{i=0}^{\infty} a_i x^i$ konvergira za svako $x \in (-\frac{1}{K}, \frac{1}{K})$. Štaviše, funkcija $a(x)$ ima izvode svih redova u tački 0 i pritom važi da je

$$a_i = \frac{a^{(i)}(0)}{i!}.$$

Mi se ovde nećemo zamarati proverom da li dobijeni stepeni redovi konvergiraju u nekoj okolini tačke 0. Obično je to lako. Sem toga, u mnogo slučajeva ta se provera može izbeći na sledeći način: kada pronadjemo tačno rešenje problema koristeći funkcije generatrise, čak i na sumnjiv način, to rešenje se može proveriti nekim drugim metodom, na primer pomoću indukcije. Štaviše, postoji posebna teorija takozvanih *formalnih stepenih redova* koja omogućava nesmetan rad čak i sa stepenim redovima koji nikad ne konvergiraju (sem u 0). Da zaključimo, konvergencija nikad nije bitno pitanje u primenama funkcija generatrisa.

Sada konačno možemo i da kažemo šta je funkcija generatrisa:

Definicija 3.1.2 *Neka je* $(a_0, a_1, a_2, \ldots, a_n, \ldots)$ *niz realnih brojeva. Pod* funkcijom generatrise[2] *ovog niza podrazumeva se stepeni red*

$$a(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n + \ldots.$$

Ako niz $(a_0, a_1, a_2, \ldots, a_n, \ldots)$ ima samo konačno mnogo nenula članova, tada je funkcija generatrise običan polinom. Sada možemo da vidimo da smo na početku ovog odeljka u stvari koristili funkcije generatrise, samo što ih nismo tako zvali.

Uopštena binomna teorema

Već smo videli da se binomna teorema (3.1) može formulisati kao rezultat o koeficijentima polinoma $(1+x)^n$. Za geometrijsku progresiju sa količnikom $-x$ važi

$$1 - x + x^2 + \ldots + (-1)^n x^n + \ldots = \frac{1}{1+x} = (1+x)^{-1}.$$

Za svako $m \in N$ izraz $(1+x)^{-m}$ možemo da posmatramo kao proizvod stepenih redova jednakih $(1+x)^{-1}$. Naravno, ono što bismo voleli da imamo je formula za koeficijent uz x^n u rezultujućem stepenom redu. Ova formula je veoma jednostavna i omogućiće nam da uopštimo binomnu teoremu i na negativne brojeve.

[2]Strogo govoreći, ovo je *obična* funkcija generatrise, s obzirom da postoje i druge vrste funkcija generatrise. Ali kako se njima nećemo baviti, jednostavno ćemo izbaciti reč "obična".

Teorema 3.1.3 *Koeficijent uz x^n u stepenom redu $(1+x)^{-m}$ jednak je*

$$(-1)^n\binom{m+n-1}{n}.$$

Dokaz Da izbegnemo znak minus, posmatraćemo $(1-x)^{-m}$ umesto $(1+x)^{-m}$. Krajnji rezultat dobijamo zamenom x sa $-x$.

Pošto je

$$(1-x)^{-1} = 1 + x + x^2 + \ldots + x^n + \ldots,$$

vidimo da je $(1-x)^{-m}$ proizvod m činilaca, od kojih je svaki jednak stepenom redu $1+x+x^2+\ldots+x^n+\ldots$. Pokazaćemo da je koeficijent uz x^n u proizvodu ovih m činilaca jednak broju neuredjenih izbora n elemenata sa ponavljanjem iz skupa od m elemenata.

Pretpostavimo da svaki činilac ima svoj marker, koji je u početku postavljen na broju 1, i da korak-po-korak pravimo neuredjeni izbor n elemenata sa ponavljanjem iz skupa od ovih m činilaca. Svaki put kada izaberemo odredjeni činilac, njegov marker pomeramo na sledeći član, tako da ako je taj činilac izabran i puta njegov marker će završiti na članu x^i. Prema tome, za svaki od $\binom{m+n-1}{n}$ mogućih izbora mi dobijamo po jedan skup markiranih članova, po jedan iz svakog činioca, čiji je proizvod jednak x^n. Kako svaki od ovih skupova dodaje 1 na koeficijent uz x^n kada se činioci izmnože, zaključujemo da je koeficijent uz x^n jednak $\binom{m+n-1}{n}$.

Zamenom x sa $-x$ sada dobijamo rezultat kako je naveden u teoremi. ■

Primer Koeficijent uz x^n u stepenom redu $(1+x)^{-2}$ jednak je

$$(-1)^n\binom{2+n-1}{n} = (-1)^n\binom{n+1}{n} = (-1)^n(n+1).$$

Sada možemo da pišemo

$$(1+x)^{-2} = 1 - 2x + 3x^2 - \ldots + (-1)^n(n+1)x^n + \ldots. \quad ■$$

Definicija 3.1.4 *Za proizvoljan realni broj α i svaki nenegativni broj k, binomni koeficijent $\binom{\alpha}{k}$ se definiše pomoću*

$$\binom{\alpha}{k} = \frac{\alpha(\alpha-1)(\alpha-2)\cdots(\alpha-k+1)}{k!}.$$

Ova definicija je proširenje uobičajene definicije 2.4.2 binomnog koeficijenta, jer kada je α jednako nekom nenegativnom celom broju n, dobijamo istu formulu za $\binom{n}{k}$ kao u definiciji 2.4.2.

Primetimo da kada je $\alpha = -m$ za neki prirodan broj m, tada važi

$$\begin{aligned}\binom{-m}{n} &= \frac{(-m)(-m-1)(-m-2)\cdots(-m-n+1)}{n!} \\ &= (-1)^n\frac{m(m+1)(m+2)\cdots(m+n-1)}{n!} \\ &= (-1)^n\binom{m+n-1}{n}.\end{aligned}$$

Sada uz ovakvu proširenu definiciju binomnog koeficijenta, iz teorema 2.5.4 i 3.1.3 zaključujemo da za proizvoljan ceo broj n važi *uopštena binomna teorema*:

$$(1+x)^n = \binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \ldots + \binom{n}{k}x^k + \ldots. \tag{3.2}$$

Inače, uopštena binomna teorema ostaje da važi i u slučaju kada je n proizvoljan realan broj.

Ovaj opšti oblik je funkcija generatrise, ali kada je n prirodan broj tada važi

$$\binom{n}{k} = 0 \quad \text{za svako } k > n,$$

pa se desna strana jednakosti svodi na polinom.

Zamenom x nekim drugim izrazom u uopštenoj binomnoj teoremi možemo da dobijemo razna njena dalja uopštenja. Mi ćemo za naša razmatranja nekoliko puta da koristimo stepeni red za $(1-\lambda x)^{-m}$, koji je jednak

$$(1-\lambda x)^{-m} = 1 + m\lambda x + \cdots + \binom{m+n-1}{n}\lambda^n x^n + \cdots.$$

Zadaci

3.2 Nalaženje funkcija generatrise

U ovom odeljku bavićemo se nekim važnim operacijama za "sastavljanje" funkcija generatrisa iz već poznatih "delova". Kroz ceo odeljak, neka su $(a_0, a_1, a_2, \ldots)$ i $(b_0, b_1, b_2, \ldots)$ nizovi, a $a(x)$ i $b(x)$ njihove funkcije generatrise.

Sabiranje nizova

Ako nizove sabiramo član po član, odgovarajuća operacija sa funkcijama generatrisa je prosto njihovo *sabiranje*. Tačnije, niz $(a_0+b_0, a_1+b_1, a_2+b_2, \ldots)$ ima funkciju generatrise $a(x)+b(x)$.

Množenje niza realnim brojem

Još jedna prosta operacija je *množenje fiksnim realnim brojem* α. Naime, niz $(\alpha a_0, \alpha a_1, \alpha a_2, \ldots)$ ima funkciju generatrise $\alpha a(x)$.

Pomeranje niza udesno

Ako je n prirodan broj, tada funkcija generatrise $x^n a(x)$ odgovara nizu

$$(\underbrace{0, 0, \ldots, 0}_{n\times}, a_0, a_1, a_2, \ldots).$$

Ovo je veoma korisno kada niz treba *pomeriti udesno* za odredjeni broj mesta.

Pomeranje niza ulevo

Šta da radimo ako niz želimo da *pomerimo ulevo* za n mesta kako bismo dobili funkciju generatrisu za niz $(a_n, a_{n+1}, a_{n+2}, \ldots)$? Očigledno, neophodno je da $a(x)$ podelimo sa x^n, ali ne smemo da zaboravimo da pre toga oduzmemo njenih prvih n sabiraka. Funkcija generatrise za gornji niz je

$$\frac{a(x) - (a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1})}{x^n}.$$

Zamena promenljive x sa αx

Neka je α fiksni realni broj i posmatrajmo funkciju $c(x) = a(\alpha x)$. Tada je $c(x)$ funkcija generatrise za niz $(a_0, \alpha a_1, \alpha^2 a_2, \ldots)$.

Na primer, znamo da je $\frac{1}{1-x}$ funkcija generatrise za niz koji sadrži samo jedinice. Prema upravo datom pravilu, tada je $\frac{1}{1-2x}$ funkcija generatrise niza koji se sastoji od stepena broja 2: $(1, 2, 4, 8, \ldots)$.

Ova operacija se takodje koristi u sledećem triku kojim se svi članovi niza na neparnim mestima zamenjuju sa 0: kao što i sam čitalac može lako da proveri, funkcija $\frac{1}{2}(a(x) + a(-x))$ je funkcija generatrise za niz $(a_0, 0, a_2, 0, a_4, 0, \ldots)$.

Zamena promenljive x sa x^n

Još jedna mogućnost je *zamena promenljive x sa x^n*. Ovo daje funkciju generatrisu za niz čiji je član sa rednim brojem nk jednak k-tom članu originalnog niza, dok su ostali članovi niza jednaki 0. Na primer, funkcija $a(x^3)$ generiše niz $(a_0, 0, 0, a_1, 0, 0, a_2, 0, 0, \ldots)$.

Primer Naći funkciju generatrisu za niz

$$(1, 1, 2, 2, 4, 4, 8, 8, \ldots),$$

tj. za niz $a_n = 2^{\lfloor n/2 \rfloor}$.

Rešenje Kao što smo već videli, niz $(1, 2, 4, 8, \ldots)$ ima funkciju generatrisu $\frac{1}{1-2x}$. Zamenom x sa x^2 dobijamo da je $\frac{1}{1-2x^2}$ funkcija generatrisa za niz $(1, 0, 2, 0, 4, 0, 8, 0, \ldots)$. Množenjem sa x dalje dobijamo da je $x\frac{1}{1-2x^2}$ funkcija generatrisa za niz $(0, 1, 0, 2, 0, 4, 0, 8, \ldots)$, a na kraju sabiranjem ove dve funkcije generatrise dobijamo i da je tražena funkcija generatrisa jednaka $\frac{1+x}{1-2x^2}$. ■

Diferenciranje i integracija

Popularne operacije iz matematičke analize, *diferenciranje* i *integracija* funkcija generatrisa imaju sledeće značenje na jeziku nizova.

Izvod $a'(x)$ funkcije $a(x)$ odgovara nizu

$$(a_1, 2a_2, 3a_3, \ldots, (n+1)a_{n+1}, \ldots).$$

Tačnije, član sa rednim brojem k jednak je $(k+1)a_{k+1}$ (stepeni red se diferencira član po član isto kao i polinom).

Funkcija generatrisa $\int_0^x a(t)dt$ odgovara nizu

$$(0, a_0, \frac{1}{2}a_1, \frac{1}{3}a_2, \frac{1}{4}a_3, \ldots, \frac{1}{n}a_{n-1}, \ldots),$$

tj. za sve $k \geq 1$, član sa rednim brojem k jednak je $\frac{1}{k}a_{k-1}$.

Primer Naći funkciju generatrisu za niz kvadrata $(1^2, 2^2, 3^2, \ldots)$, tj. za niz $a_n = (n+1)^2$.

Rešenje Počinjemo sa nizom koji se sastoji samo od jedinica i čija je funkcija generatrise $\frac{1}{1-x}$. Po prethodnom pravilu, prvi izvod ove funkcije, $\frac{1}{(1-x)^2}$, odgovara nizu $(1, 2, 3, 4, \ldots)$. Po istom pravilu, drugi izvod ove funkcije, $\frac{2}{(1-x)^3}$, odgovara nizu $(2 \cdot 1, 3 \cdot 2, 4 \cdot 3, \ldots)$. Član sa rednim brojem k ima vrednost $(k+2)(k+1) = (k+1)^2 + k + 1$. Pošto mi želimo niz sa opštim članom $a_k = (k+1)^2$, treba još samo da oduzmemo funkciju generatrisu za niz $(1, 2, 3, \ldots)$. Dobijamo da je tražena funkcija generatrise jednaka

$$\frac{2}{(1-x)^3} - \frac{1}{(1-x)^2}. \quad \blacksquare$$

Množenje funkcija generatrisa

Množenje funkcija generatrisa je ujedno i najzanimljivija operacija. Proizvod $a(x)b(x)$ je funkcija generatrisa za niz $(c_0, c_1, c_2, \ldots)$, gde su koeficijenti c_k dati pomoću:

$$\begin{aligned} c_0 &= a_0 b_0 \\ c_1 &= a_0 b_1 + a_1 b_0 \\ c_2 &= a_0 b_2 + a_1 b_1 + a_2 b_0 \\ &\vdots \end{aligned}$$

i uopšte možemo da pišemo

$$c_k = \sum_{i=0}^{k} a_i b_{k-i}.$$

Ovo se lako pamti—koeficijenti proizvoda $a(x)b(x)$ sve do k-tog su isti kao i proizvodu polinoma $(a_0 + a_1 x + \ldots + a_k x^k)$ i $(b_0 + b_1 x + \ldots + b_k x^k)$.

Napomena Operacije koje smo naveli u ovom odeljku nisu korisne samo za nalaženje funkcije generatrise koja odgovara datom nizu, već i za nalaženje niza koji odgovara datoj funkciji generatrise. U principu, ovaj problem se uvek može rešiti pomoću Taylorovog reda, tj. ponovljenim diferenciranjem, ali ova tehnika u praksi retko daje dobre rezultate.

Ovaj odeljak završavamo primerom primene funkcija generatrise. Dalji primeri su dati u zadacima, a neki važniji problemi će biti obradjeni u sledećim odeljcima.

Primer Kutija sadrži 30 crvenih, 40 plavih i 50 belih lopti. Lopte iste boje se ne razlikuju medjusobno. Na koliko načina se može izabrati 70 lopti iz kutije?

Rešenje Kao što već znamo iz prethodnog odeljka, broj koji tražimo je jednak koeficijentu uz x^{70} u proizvodu

$$(1+x+x^2+\ldots+x^{30})(1+x+x^2+\ldots+x^{40})(1+x+x^2+\ldots+x^{50}).$$

Ovaj izraz nećemo da množimo. Umesto toga pišemo

$$1+x+x^2+\ldots+x^{30}=\frac{1-x^{31}}{1-x},$$

što je već poznati zbir konačne geometrijske progresije. Ceo proizvod se sada može prepisati kao

$$\frac{1-x^{31}}{1-x}\frac{1-x^{41}}{1-x}\frac{1-x^{51}}{1-x}=\frac{1}{(1-x)^3}(1-x^{31})(1-x^{41})(1-x^{51}).$$

Činilac $(1-x)^{-3}$ može da se razvije u stepeni red prema uopštenoj binomnoj teoremi (3.2). U proizvodu preostalih činilaca $(1-x^{31})(1-x^{41})(1-x^{51})$, dovoljno je naći koeficijente stepena do x^{70}, što je sasvim lako. Stoga dobijamo proizvod

$$\left(\binom{2}{2}+\binom{3}{2}x+\binom{4}{2}x^2+\cdots\right)(1-x^{31}-x^{41}-x^{51}+\cdots),$$

gde $\cdots$ u drugom paru zagrada stoje za stepene veće od x^{70}. Koeficijent uz x^{70} u ovom proizvodu jednak je $\binom{70+2}{2}-\binom{70+2-31}{2}-\binom{70+2-41}{2}-\binom{70+2-51}{2}=1061$.
■

Zadaci

3.3 Rekurentne jednačine

- Rešavanje homogenih linearnih rekurentnih jednačina, Nešetril 10.3 i Biggs 18.5
- Fibonacci-jevi brojevi kao primer
- Primeri nehomogenih rekurentnih jednačina

3.4 Particije prirodnih brojeva

- Particije prirodnih brojeva i njihova funkcija generatrise, Biggs 19.3
- Komentar o Hardy-jevoj i Ramanujan-ovoj proceni za p_n
- Funkcija generatrise za ograničene particije, Biggs 19.4

3.5 Catalan-ovi brojevi

- Definicija pozicionih binarnih stabala
- Prebrojavanje pomoću funkcija generatrisa (obe stvari kao u Nešetril-u)
- Definicija Catalan-ovih brojeva
- Korektni nizovi zagrada
  (bijekcija: “Stablo” ¡-¿ “(Levo_podstablo) Desno_podstablo”)
- Problem izlaza sa steka
- Medju probleme stavi direktan dokaz jednačine za korektne nizove zagrada i preostale probleme iz Nešetril-ove knjige

3.6 Metod zmijskog ulja

- Metod zmijskog ulja, Wilf
- Primeri, Wilf

Glava 4

Teorija grafova

4.1 Šta je graf?

Pojam grafa

- Izbor modela i problema iz stvarnog sveta gde se pojavljuju grafovi (Westova knjiga?)
- Definicija (jednostavnog neorijentisanog) grafa
- Crteži grafova (sa primerima)
- Posebne klase grafova (K_n, C_n, P_n, $K_{m,n}$)
- Definicija matrice susedstva i matrice incidentnosti
- Definicija izomorfizma grafova sa primerom
- Invarijante grafova
- Problem postojanja izomorfizma
- Definicije susedstva $N_G(v)$, stepena $d_G(v)$, regularnosti, $\delta(G)$ i $\Delta(G)$
- Prva teorema iz teorije grafova
- Lema o rukovanju

Podgrafovi

- Definicija podgrafa i indukovanog podgrafa i primer (rečenica da je graf nadgraf svojih podgrafa)
- Oznake za podgrafove i $G - v$, $G - e$, kao i $G + v$, $G + e$
- Definicija komplementa, kompletnog podgrafa i nezavisnog skupa čvorova

Povezanost

- Putevi i konture u grafu (dužina puteva i kontura, dijametar; radijus u problemima)
- Definicija povezanosti pomoću puteva izmedju čvorova
- Primer povezanog i nepovezanog grafa
- Šetnje u grafovima (ovde ukljuciti i definiciju "trail"-ova, kao u knjizi D.West-a), svaka šetnja sadrži put (West, lemma 1.2.6, p.16), svaka neparna zatvorena šetnja sadrži neparan ciklus (West, lemma 1.2.7, p.17)
- Relacija povezanosti izmedju čvorova, definicija komponenti (povezanosti) kao klasa ekvivalencije i opažanje da su komponente maksimalni povezani podgrafovi
- Primer komponenti iz prethodnog primera nepovezanih grafova
- Teorema o povezanosti
- Definicija mostova i artikulacionih čvorova

Rastojanje

- Definicija rastojanja izmedju čvorova
- Opažanje da je rastojanje metrika na čvorovima grafa i da ima još dve osobine (celobrojne vrednosti, unutrašnji čvor), kao i da su takve metrike obavezno metrike grafova (zadatak)

Bipartitni grafovi

- Definicija bipartitnosti
- Teorema da je graf G bipartitan ako i samo ako ne sadrži neparne konture

Ekstremni grafovi

- Teorema o najvecem broju grana u grafu bez trouglova
- Turanova teorema

4.2 Stabla

- Definicija stabala
- Primedba o njihovom značaju u računarskim naukama i drugim granama nauke; primer
- Teorema o karakterizaciji
- Posledica da svako stablo ima bar dva lista
- Definicija ekscentriciteta
- Primer stabla sa ekscentricitetima
- Definicija centra
- Teorema o centru stabla
- Fundamentalne konture:
- Definicija kostabla, njegovih tetiva i fundamentalnih kontura
- Definicija binarne sume i vektorskog prostora kontura (vektorski prostor zatvorenih šetnji; linearna nezavisnost vektora pod binarnom sumom)
- Teorema da fundamentalne konture predstavljaju bazu ovog vektorskog prostora
- Posledice o dimenziji ovog prostora i ciklomatički broj
- Preseci idu u probleme!

Da li treba spojiti ovu sekciju sa fundamentalnim ciklusima? Ima vremena za takvu odluku ...

4.3 Prebrojavanje razapinjućih stabala

- Problem prebrojavanja razapinjućih stabala
- Cayley-jeva teorema
- Dokaz pomoću Prüfer-ovog koda
- Najnoviji dokaz iz "Proofs from THE BOOK"
- U zadatke ubaciti: Generatingfunctionology, p. 163, problem 18
- Matrix-tree teorema
- Definicija usmerenog stabla iz S. Even-ove knjige
- Dokaz pomoću determinanti?
- Još dva dokaza Cayley-jeve teoreme pomoću stepenog niza će se naći medju problemima

4.4 Ojlerovi i Hamiltonovi grafovi

- Definicija originalnog, Königsberg-skog problema mostova i njegovo svodjenje na problem crtanja graf pomoću jedne zatvorene linije
- Teorema da je G Ojlerov graf ako i samo ako je povezan i svaki čvor ima paran stepen
- U zadacima stavi verziju teoreme sa Ojlerovim putem
- Definicija Hamiltonovog puta i konture, i nekoliko osnovnih teorema koje garantuju njihovo postojanje. BEZ HAMILTONOVOG ZATVORENJA!

4.5 Sparivanja u bipartitnim grafovima

Po knjizi R.Diestel-a, sekcije 2.1 i 2.2, uz pomoc knjige N.Biggs-a, sekcije 10.4—10.6: Malo više reći na početku o uvećavajućim putevima, pa tek onda preći na Diestel-ove rezultate. Zadržati se samo na bipartitnim grafovima. Priča o transverzalama (sistemima različitih predstavnika).

Dakle:

- primeri problema
- Holova teorema, deficijencija
- uvećavajući putevi, definicija, teorema, kako ih primeniti
- transverzale

4.6 Jača povezanost

Po knjizi R.Diestel-a:

Definicije iz sekcije 1.4

Struktura 2-povezanih grafova iz sekcije 3.1

Menger-ove teoreme iz sekcije 3.3 (bez uvodjenja fanova)

4.7 Spektar grafa

Moje vidjenje, potpomognuto knjigom D.West-a:

Karakteristični polinom i definicija spektra

Broj setnji preko matrice susedstva

Osvrt na nekoliko neophodnih rezultata iz linearne algebre, uključujući minimalni polinom

Povezanost i spektri, onako!

Bipartitnost grafa

Dijametar grafa ograničen brojem sopstvenih vrednosti

Teorema o preplitanju

Rejlijev odnos
Najveća sopstvena vrednost je izmedju $\delta(G)$ i $\Delta(G)$
Najveća sopstvena vrednost regularnog grafa
Najveća sopstvena vrednost neregularnog grafa?

Glava 5

Algoritmi na grafovima

Osim navedenih sekcija, ova glava bi trebalo da sadrži i uvodni tekst o kompleksnosti algoritama i uporedjivanju funkcija. Mislim da to treba objasniti što je jednostavnije moguće, tako da ću kratku priču o tome staviti unutar prvog poglavlja, zajedno sa pričom o DFS i BFS.

Uvod za DFS i BFS: Većina grafovskih algoritama zahteva sistematičan metod za obilaženje čvorova grafa. U sekcijama 5.1.1 i 5.1.2 opisaćemo dva popularna metoda koja su pogodna za mnoge probleme. Takodje ćemo dati primere jednostavnih algoritama koji koriste ove metode.

Matrična reprezentacija grafova će se naći još u prvom poglavlju prethodne glave, dok ce se teorema o stepenima matrice susedstva naci u poglavlju o spektrima grafova.

- Poziv na definiciju matrice susedstva A
- Definicija liste susedstva T
- Primer oba pojma na istom grafu S (može da bude iz S. Even-ove knjige)
- Poziv na teoremu o stepenima matrice susedstva

5.1 Obilazak čvorova grafa

5.1.1 DFS i povezanost

- Opis DFS, definicija isturenih i uvučenih grana (forward i backward grane)
- Algoritam u pseudo-kodu, primer na istom grafu S
- Teorema 1.6 iz Gibbons-a

- Kompleksnost DFS
- Primena na povezanost (broj komponenti) sa dokazom korektnosti

5.1.2 BFS i najkraći putevi

- Opis BFS
- Algoritam u pseudo-kodu, primer na istom grafu S
- Kompleksnost BFS
- Primena na odredjivanje najkraćih puteva u običnim grafovima sa dokazom korektnosti (Koristi rečenicu: BFS takodje može da se koristi za proveru povezanosti grafa kao i DFS. Ovde ćemo opisati drugu jednostavnu primenu BFS-a.)

5.1.3 Nalaženje blokova grafa

Primena DFS-a za nalaženje blokova grafa.

5.2 Orijentisani grafovi

5.2.1 Tranzitivno zatvorenje

Proveri Sedgewick-a Glava 32.

- Definicija orijentisanog grafa, slabe i jake povezanosti, promena u DFS razapinjućoj šumi, efektima na reprezentaciju grafa u računaru
- Postavka problema tranzitivnog zatvorenja
- Algoritam u pseudo-kodu
- Primer
- Povezanost (jaka?)
- Dokaz korektnosti

5.2.2 Topološko sortiranje

Problem topološkog sortiranja acikličnih orijentisanih grafova.

5.2.3 Jake komponente povezanosti

Primena DFS-a na nalaženje jakih komponenti povezanosti.

5.3 Težinski grafovi

5.3.1 Najkraći putevi

- Definicija težinskih grafova, korišćenje za modeliranje praktičnih problema, efekti na reprezentaciju u računaru
- Nalaženje najkraćih puteva u težinskom grafu kao primer praktičnog problema
- Dijkstra-in algoritam (kao u Gibbons-u): opis i pseudo kod, primer, dokaz korektnosti, kompleksnost $O(n^2)$
- Warshall-ov algoritam (Gibbons, str. 19-20). Koristi rečenicu: Ako želimo da nadjemo rastojanja izmedju svih parova čvorova, tada možemo da koristimo Dijkstra-in algoritam za svaki čvor ponaosob. Ali, postoji mnogo jednostavniji algoritam koji ćemo sada opisati.

  Prisećanje na teoremu o stepenima matrice susedstva,
  opis Warshall-ovog algoritma,
  dokaz korektnosti,
  pseudo-kod i kompleksnost.
- Primeri za Dijsktra-in i Warshall-ov algoritam, Gibbons str. 15

5.3.2 Najmanja razapinjuća stabla

- Motivacioni problem na povezanim mrežama
- Kruskal-ov algoritam
- Primer na istom grafu kao za Prim-ov algoritam
- Dokaz korektnosti sa kompleksnošću
- Prim-ov algoritam
- Primer na istom grafu kao za Kruskal-ov algoritam
- Dokaz korektnosti sa kompleksnošću