Primož Potočnik

Zapiski predavanj iz Diskretne Matematike I

Ljubljana, marec 2011

Naslov: Zapiski predavanj iz Diskretne Matematike I
Avtor: Primož Potočnik
1. izdaja
Dostopno na spletnem naslovu `www.fmf.uni-lj.si/~potocnik`

CIP – Kataložni zapis o publikaciji
Narodna in univerzitetna knjižnica, Ljubljana

519.11(0.034.2)
519.17(0.034.2)

POTOČNIK, Primož, 1971 –

Zapiski predavanj iz Diskretne Matematike I [Elektronski vir]

Primož Potočnik. - 1. izd. – El. knjiga. – Ljubljana : samozal., 2011

Način dostopa (URL):
http://www.fmf.uni-lj.si/∼potocnik/Ucbeniki/DM-Zapiski2010.pdf

ISBN 978-961-93056-1-4

255519488

Kazalo

1 Osnovna načela preštevanja

1.1 S čim se ukvarja diskretna matematika

Diskretna matematika se pretežno ukvarja s končnimi in številnimi množicami ter relacijami na njih. Na kratko, ukvarja se z različnimi tipi diskretnih struktur. Med bolj poznane naloge, s katerimi se ukvarja *diskretna matematika*, so naloge preštevanja. Delu diskretne matematike, ki obravnave takšne naloge, rečemo *preštevalna kombinatorika*. Poleg preštevalne kombinatorike pa moderna diskretna matematika združuje še vrstno drugih matematičnih področij, kot so: teorija grafov, teorija končnih geometrij, teorija kombinatoričnih načrtov itd.

1.2 Tri načela preštevanja

Če matematik želi prešteti kake objekte s predpisanimi lastnostmi, to običajno stori v dveh korakih: Najprej objekte, ki jih prešteva, združi v množico, nato pa tej množici določi njeno *moč* (tudi kardinalnost). Pri določanju moči dane množice, si večkrat pomagamo z nekaj preprostimi načeli. Navedimo tri izmed njih.

Načelo produkta

Mnogokrat si lahko elemente množice A, ki jo preštevamo, predstavljamo kot urejene n-terice, katerih i-ta komponenta pripada množici A_i. V tem primeru si lahko pomagamo z *načelom produkta*, ki pravi, da je moč kartezičnega produkta danih množic enaka produktu njihovih moči:

$$|\prod_{i=1}^{n} A_i| = \prod_{i=1}^{n} |A_i|.$$

Tipičen zgled uporabe tega načela so naloge z večfaznim izbiranjem. Denimo, da je kombinatorični objekt podan z zaporedjem n izbir, pri čemer v i-tem koraku izbiramo izmed možnostmi v množici A_i. Takšnen kombinatorični objekt lahko enačimo z urejeno n-terico izbir $A_1 \times \ldots \times A_n$. Število vseh takšnih objektov je tedaj enako produktu moči množic A_i. Oglejmo si konkretno nalogo:

Zgled. *Študentsko kosilo je sestavljeno iz predjedi, glavne jedi in sladice. Za predjed si lahko izberemo govejo juho z rezanci ali zelenjavno juho z jušnimi kroglicami. Za glavno jed imamo na razpolago puranji zrezek v gobovi omaki,*

sardele na žaru ali ocvrt sir. Sladica je bodisi jabolko bodisi čokoladna rezina. Koliko različnih kosil si lahko sestavi študent?

REŠITEV: Kosilo lahko opišemo kot urejeno trojico, kjer prva komponenta predstavlja predjed, druga komponenta glavno jed in tretja komponenta sladico. Različnih kosil je tako $2 \cdot 3 \cdot 2 = 12$. ∎

Načelo vsote

Kadar elemente množice A (katere moč želimo določiti) razporedimo v nekaj med seboj disjunktnih podmnožic $A_1, A_2, \ldots, A_n$, katerih moči poznamo, lahko moč množice A določimo na podlagi *načela vsote*, ki pravi, da je moč unije paroma disjunktnih množic enaka vsoti njihovih moči:

$$A_i \cap A_j = \emptyset \text{ za } i \neq j \;\Rightarrow\; |\bigcup_{i=1}^{n} A_i| \;=\; \sum_{i=1}^{n} |A_i|.$$

S tem preprostim načelom lahko na videz zapleteno nalogo (preštevanje elementov množice A) prevedemo na več nekoliko manj zapletenih kombinatoričnih nalog (preštevanje elementov podmnožic A_i).

Zgled. *Varnostno geslo je sestavljeno iz osmih znakov. Vsaj en in največ trije znaki gesla morajo biti številke (med 0 in 9), ostali pa črke slovenske abecede. Koliko različnih gesel lahko sestavimo?*

REŠITEV: Varnostna gesla razdelimo v tri skupine A_1, A_2 in A_3, pri čemer v skupino A_i razvrstimo tista gesla, ki so sestavljena iz i številk in $8-i$ črk. Množice A_1, A_2 in A_3 so paroma disjunktne, njihova unija pa je množica vseh varnostnih gesel. Iskano število je zato enako vsoti moči množic A_1, A_2 in A_3.

Moč množice A_i, $i \in \{1, 2, 3\}$, lahko določimo s pomočjo načela produkta. Mislimo si, da geslo iz množice A_i izberemo v treh fazah. V prvi fazi izberemo i pozicij izmed osmih možnih pozicij za številke v geslu. Kdor je seznanjen s srednješolsko kombinatoriko, ve, da je takšnih izbir $\binom{8}{i}$. V drugi fazi pa izberemo urejeno i-terico številk med 0 in 9, ki jih razvrstimo na i pozicij, ki smo jih izbrali v 1. fazi. Teh izbir je 10^i. Nazadnje izberemo še urejeno $(8-i)$-terico črk, ki jih razvrstimo na preostalih $8-i$ pozicij varnostnega gesla. Takšnih izbir je 25^{8-i}. Vseh varnostnih gesel je zato

$$|A_1|+|A_2|+|A_3| = \binom{8}{1} \cdot 10 \cdot 25^7 + \binom{8}{2} \cdot 10^2 \cdot 25^6 + \binom{8}{2} \cdot 10^3 \cdot 25^5 \approx 1{,}7 \cdot 10^{12}.$$

∎

Načelo enakosti

Iz definicije moči (kardinalnosti) množice sledi, da imata množici A in B enako moč, brž ko med njima obstaja bijektivna preslikava.

$$\exists f\colon A \to B,\ \text{bijekcija} \quad \Rightarrow \quad |A| = |B|.$$

Na tem dejstvu sloni morda najpogosteje uporabljen prijem v kombinatoriki: Če želimo prešteti elemente množice A, je dovolj poiskati bijektivno preslikavo iz množice A v kako množico B, katere moč že poznamo.

Zgled. *Naj bo X množica z n elementi. Koliko podmnožic premore množica X?*

Rešitev: Naloga sprašuje po moči *potenčne množice* $\mathcal{P}X$ množice X. Rešili jo bomo tako, da bomo našli bijektivno preslikavo med množico $\mathcal{P}X$ in množico vseh urejenih n-teric z elementi iz množice $\mathbb{Z}_2 = \{0, 1\}$. Označimo elemente množice X z $x_1, x_2, \ldots, x_n$. Poljubni podmnožici $B \in \mathcal{P}X$ priredimo *karakteristični vektor* $\chi(B) = (a_1, \ldots, a_n) \in \mathbb{Z}_2^n$, za katerega je $a_i = 1$, če je $x_i \in B$, in $a_i = 0$ sicer. Na ta način smo definirali preiskavo $\chi\colon \mathcal{P}X \to \mathbb{Z}_2^n$. Ni se težko prepričati, da je preslikava χ bijektivna, zato je $|\mathcal{P}X| = |\mathbb{Z}_2^n| = 2^n$. Pri slednji enakosti smo seveda uporabili načelo produkta. ∎

2 Izbori

Razdelek pričnimo z naslednjim zgledom. Pri igri loto se v bobnu nahaja 39 kroglic, oštevilčenih s števili $1, 2, \ldots, 39$. Organizator igre iz bobna zaporedoma sedemkrat izvleče po eno kroglico. Na koliko načinov lahko to stori?

Odgovor je odvisen od tega, kako razumemo besedo "način". Osnovni dilemi pri razumevanju naloge sta, ali naj kroglico, ki smo jo v posameznem koraku izvlekli, vrnemo v boben in ali je za nas vrstni red izvlečenih kroglic pomemben. Ti dve dilemi mora seveda razrešiti tisti, ki nam je nalogo zastavil. Od njegovega odgovora je odvisno, kako bomo nalogo reševali.

Kadar je za zastavljalca naloge vrstni red pomemben, bomo preštevali *urejene izbore*, ki jim zaradi zgodovinskih razlogov rečemo tudi *variacije*. Če kroglice vračamo v boben, bomo govorili o variacijah s ponavljanjem, sicer pa o variacijah brez ponavljanja. Če pa vrstni red ni pomemben, bomo šteli *neurejene izbore*, ki jih imenujemo tudi *kombinacije*. Podobno kot prej govorimo o kombinacijah s ponavljanjem in brez ponavljanja – odvisno od tega, ali kroglice vračamo v boben ali ne.

V nadaljevanju si bomo vsako od štirih možnih interpretacij naloge ogledali nekoliko podrobneje. Za lažjo izražavo bomo rezultat vlečenja kroglic imenovali *žreb*. Množico 39 kroglic označimo z $\mathcal{N} = \{1, 2, \ldots, 39\}$.

2.1 Urejeni izbori s ponavljanjem

Denimo, da izvlečene kroglice v boben **vračamo**, vrstni red izvlečenih kroglic pa je **pomemben**. Tedaj lahko rezultat žreba enolično predstavimo z **urejeno sedmerico** elementov množice kroglic $\mathcal{N}$, pri čemer urejeno sedmerico $(a_1, \ldots, a_7)$ razumemo kot tisti žreb, pri katerem v i-tem poskusu izvlečemo kroglico $a_i \in \mathcal{N}$. To nas napelje na idejo, da urejeni izbor s ponavljanjem definiramo na naslednji način.

DEFINICIJA 2.1 *Naj bo N poljubna množica in r poljubno naravno število. Urejeni r-terici $(a_1, a_2, \ldots, a_r)$ elementov množice N rečemo* urejeni izbor elementov množice N dolžine r. *Če želimo poudariti, da so lahko nekateri izmed elementov a_i med seboj tudi enaki, dodamo, da gre za urejeni izbor* s ponavljanjem. *Množico vseh takšnih izborov označimo s simbolom $\overline{\mathcal{V}}(N, r)$.*

OPOMBA. Urejeni izbor elementov n-elementne množice dolžine r v literaturi imenujejo tudi *variacija s ponavljanjem n elementov reda r*.

Ker množica $\overline{\mathcal{V}}(N,r)$ vsebuje *vse* urejene r-terice elementov množice N, je enaka kartezičnemu produktu r kopij množice N:

$$\overline{\mathcal{V}}(N,r) = \underbrace{N \times N \times \ldots \times N}_{r}$$

Od tod (in z upoštevanjem načela produkta) neposredno sledi naslednja trditev.

TRDITEV 2.2 *Naj bo N poljubna množica z n elementi in r poljubno naravno število. Tedaj množica $\overline{\mathcal{V}}(N,r)$ premore n^r izborov.*

2.2 Urejeni izbori brez ponavljanja

Še naprej si mislimo, da je vrstni red izvlečenih kroglic **pomemben**, le da tokrat izbranih kroglic v boben **ne vračamo**. Tako kot prej si žreb, v katerem v i-tem koraku izberemo kroglico a_i, predstavimo z **urejeno sedmerico** $(a_1, \ldots, a_7)$ elementov $a_i \in \mathcal{N}$. Ker kroglic ne vračamo, so elementi a_i **paroma različni**. Po drugi strani pa vsaka sedmerica paroma različnih elementov množice $\mathcal{N}$ predstavlja kak žreb. Možnih žrebov je torej toliko, kot je različnih sedmeric paroma različnih kroglic v bobnu. Povedano povzemimo v naslednjo formalno definicijo *urejenega izbora brez ponavljanja*.

DEFINICIJA 2.3 *Urejeni r-terici paroma različnih elementov množice N rečemo* urejeni izbor elementov množice N dolžine r brez ponavljanja. *Množico vseh takšnih izborov označimo s simbolom $\mathcal{V}(N,r)$.*

Urejenih izborov brez ponavljanja je seveda nekoliko manj kot vseh urejenih izborov. Preden jih preštejemo, vpeljimo naslednji funkciji naravnih števil n in r:

$$n^{\underline{r}} \;=\; n(n-1)\cdots(n-r+1), \quad n! \;=\; n^{\underline{n}} \;=\; n(n-1)\cdots 1$$

in dodatno definirajmo še $n^{\underline{0}} = 0! = 1$ za vsak $n \in \mathbb{N}_0$. Simbolu $n^{\underline{r}}$ rečemo *padajoča potenca* števila n, simbolu $n!$ pa n *fakulteta* (tudi *faktoriela*).

TRDITEV 2.4 *Naj bo N poljubna množica z n elementi in r poljubno naravno število. Tedaj množica $\mathcal{V}(N,r)$ premore $n^{\underline{r}}$ izborov.*

DOKAZ: Formalni dokaz trditve je najlažje izpeljati z indukcijo na dolžino izbora r. Če je $r = 1$, je tipični izbor oblike (a), kjer je a element

množice N. Ker je elementov množice N ravno n, je toliko tudi izborov. Formula torej drži za $r = 1$.

Pa denimo, da za neki k formula drži za vse $r \leq k$. Dokažimo, da velja tudi za $r = k + 1$. Res! Označimo elemente množice N s simboli $a_1, \ldots, a_n$. Izbore iz $\mathcal{V}(N, k+1)$ razvrstimo v n skupin, $\mathcal{R}_1, \ldots, \mathcal{R}_n$, pri čemer v skupino $\mathcal{R}_i$ razvrstimo vse izbore, ki imajo na prvem mestu element a_i. Če izboru $(a_i, x_1, \ldots, x_k)$ iz množice $\mathcal{R}_i$ odrežemo prvo komponento, dobimo "ostanek" $(x_1, \ldots, x_k)$, ki je izbor iz $\mathcal{V}(N \setminus \{a_i\}, k)$. Pri tem se vsak izbor iz $\mathcal{V}(N \setminus \{a_i\}, k)$ pojavi natanko enkrat kot "ostanek" izbora iz skupine $\mathcal{R}_i$. Zato je v vsaki skupini $\mathcal{R}_i$ natanko toliko izborov, kot je izborov v množici $\mathcal{V}(N \setminus \{a_i\}, k)$; teh pa je, kot zagotavlja indukcijska predpostavka, $(n-1)^{\underline{k}}$. Vseh iskanih izborov je tako $n(n-1)^{\underline{k}} = n^{\underline{k+1}} = n^{\underline{r}}$. S tem je indukcijski korak dokazan. ∎

Za razliko od urejenih izborov s ponavljanjem, kjer je dolžina izbora poljubno velika, je dolžina urejenega izbora brez ponavljanja omejena s številom elementov, ki jih izbiramo. Z drugimi besedami,

$$\mathcal{V}(N, r) = \emptyset, \quad \text{brž ko je } \ r > |N|.$$

Urejenim izborom elementov množice N brez ponavljanja najdaljše dopustne dolžine (torej dolžine $r = |N|$) rečemo tudi *permutacija* množice N. Iz trditve 2.4 neposredno sledi naslednje:

TRDITEV 2.5 *Število vseh permutacij n-elementne množice je enako*

$$n^{\underline{n}} = n!.$$

OPOMBA. Permutacijo $(a_1, \ldots, a_n)$ množice N lahko razumemo tudi kot linearno ureditev elementov množice N, pri kateri je a_1 "prvi" element, ki mu "sledi" element a_2 in tako dalje, vse do "zadnjega" elementa a_n. Če pa so elementi množice N že vnaprej podani z nekim vrstnim redom (npr. če je $N = \{1, 2, \ldots, n\}$) pa lahko na permutacijo $(a_1, \ldots, a_n)$ pogledamo tudi kot na bijektivno preslikavo iz množice N vase, ki i-temu elementu množice N priredi element a_i.

2.3 Neurejeni izbori brez ponavljanja

Mislimo si sedaj, da vrstni red izbranih kroglic **ni pomemben**, izbranih kroglic pa **ne vračamo** v boben. V tem primeru lahko izid žreba enolično podamo z **množico** sedmih izžrebanih kroglic. Možnih izidov žreba je torej toliko, kot je vseh sedemelementnih podmnožic množice kroglic $\mathcal{N}$. To nas napelje na naslednjo definicijo.

DEFINICIJA 2.6 *Naj bo N poljubna množica z n elementi in r poljubno nenegativno celo število. Tedaj r-elementni podmnožici množice N rečemo* neurejeni izbor elementov množice N brez ponavljanja dolžine r. *Množico vseh takšnih izborov označimo s simbolom $\mathcal{K}(N,r)$ njihovo število pa s simbolom*

$$\binom{n}{r} = |\mathcal{K}(N,r)|,$$

ki mu pravimo binomski simbol *(tudi* binomski koeficient*) in ga preberemo "n nad r".*

OPOMBA. Za množico $\mathcal{K}(N,r)$ vseh r-elementnih podmnožic množice N je v navadi več različnih simbolov, med drugim tudi simbol $\binom{N}{r}$, ki je morda zaradi svoje podobnosti z binomskim simbolom priročnejši za pomnjenje.

TRDITEV 2.7 *Za poljubni nenegativni celi števili n in r velja enakost*

$$\binom{n}{r} = \frac{n^{\underline{r}}}{r!}.$$

DOKAZ: Naj bo N poljubna n-elementna množica in r poljubno nenegativno celo število. Za $r = 0$ trditev preide v stavek, da poljubna množica premore natanko eno podmnožico z 0 elementi. Ker je prazna množica edina 0-elementna množica, je slednje očitno pravilno. Predpostavimo torej lahko, da je $r \geq 1$.

Trditev bomo dokazali tako, da bomo ponovno prešteli vse urejene izbore brez ponavljanja iz množice $\mathcal{V}(N,r)$. Za $A \in \mathcal{K}(N,r)$ definirajmo naslednjo množico urejenih izborov:

$$\mathcal{R}_A = \{(a_1,\ldots,a_r) : \{a_1,\ldots,a_r\} = A\}.$$

Opazimo, da je $\mathcal{R}_A$ natanko množica vseh permutacij množice A, zato je $|\mathcal{R}_A| = r!$. Ker se vsak izbor iz $\mathcal{V}(N,r)$ pojavi v natanko eni od množic $\mathcal{R}_A$ (namreč tisti, za katere je množica njegovih komponent enaka A), je število vseh takšnih izborov enako $\binom{n}{r}r!$. Iz trditve 2.4 tedaj sledi enakost

$$\binom{n}{r}r! = n^{\underline{r}}.$$

Delimo še z $r!$ in dobimo formulo iz trditve. ∎

2.4 Neurejeni izbori s ponavljanjem

Nazadnje se lotimo še različice naloge, kjer vrstni red izbranih kroglic **ni pomemben**, izžrebane kroglice pa **vračamo** v boben. V tem primeru izida žreba žal ne moremo podati z množico izžrebanih kroglic, saj množica ne dopušča večkratnih pojavitev svojih elementov. Zato za opis žreba potrebujemo matematično strukturo, ki ima podobne lastnosti kot *množica*, dopušča pa večkratno pripadnost kakega elementa. Takšnemu objektu pravimo *multimnožica*. Formalno je multimnožico najlažje opisati kot preslikavo, ki vsakemu potencialnemu elementu priredi njegovo kratnost v multimnožici. Pri tem za elemente, ki jih v multimnožici ni, rečemo, da v njej nastopajo s kratnostjo 0.

DEFINICIJA 2.8 Multimnožica z elementi v množici N *je poljubna preslikava*

$$\mu\colon N \to \mathbb{N}_0.$$

Pri tem številu $\mu(a)$, $a \in N$, *rečemo* kratnost *elementa* a *v multimnožici* μ, *vsoti*

$$\sum_{a \in N} \mu(a)$$

pa moč multimnožice μ.

Neformalno pa lahko multimnožice podajamo tudi kot množice, pri čemer dopuščamo, da se nekateri elementi multimnožice pojavijo več kot enkrat. Pri tem vrstni red elementov, tako kot pri množicah, ni pomemben. Na primer, multimnožico $\mu\colon \{a, b, c, d\} \to \mathbb{N}_0$,

$$\mu(a) = 1,\ \mu(b) = 2,\ \mu(c) = 0,\ \mu(c) = 3,$$

lahko podamo tudi z naštevanjem elementov

$$\mu = [b, c, c, a, c, b] = [c, b, c, b, a, c] = \ldots \quad \text{ali} \quad \mu = [a^1, b^2, c^3].$$

Moč multimnožice μ je 6.

Neurejene izbore s ponavljanjem lahko sedaj opišemo v jeziku multimnožic.

DEFINICIJA 2.9 *Naj bo* N *množica moči* n. *Multimnožici moči* r *z elementi v množici* N *rečemo* neurejeni izbor elementov množice N dolžine r s ponavljanjem. *Množico vseh takšnih multimnožic označimo s simbolom*

$$\overline{\mathcal{K}}(N, r),$$

njihovo število pa s

$$\overline{\mathcal{K}}(n,r).$$

TRDITEV 2.10 *Za poljubni nenegativni števili n in r velja*

$$\overline{\mathcal{K}}(n,r) = \binom{n+r-1}{n-1} = \binom{n+r-1}{r}.$$

DOKAZ: Vzemimo n-elementno množico $N = \{a_1, \ldots, a_n\}$. Trditev dokažemo na strog matematičen način tako, da najdemo bijektivno preslikavo iz množice $\overline{\mathcal{K}}(N,r)$ v množico $\mathcal{K}(\mathbb{N}_{n+r-1}, n-1)$.

Naj bo $\mu\colon N \to \mathbb{N}_0$ multimnožica moči r. Za $k \in \{1, \ldots, n-1\}$ definirajmo

$$b_k = \mu(a_1) + \ldots + \mu(a_k) + k$$

in jih združimo v množico $B_\mu = \{b_1, b_2, \ldots, b_{n-1}\}$. Dokažimo najprej, da je B_μ podmnožica množice $\mathbb{N}_{n+r-1}$ in da premore $n-1$ elementov. Ker je

$$b_{k+1} = b_k + \mu(a_{k+1}) + 1 \qquad (*)$$

za vsak $k \geq 1$, je zaporedje števil b_k strogo naraščajoče. Ker je $b_1 = \mu(a_1) + 1 \geq 1$, so števila b_k pozitivna. Po drugi strani pa je

$$b_{n-1} = \mu(a_1) + \ldots + \mu(a_{n-1}) + n - 1 \leq \sum_{k=1}^{n} \mu(a_k) + n - 1 = r + n - 1.$$

Zato je res B_μ element množice $\mathcal{K}(\mathbb{N}_{n+r-1}, n-1)$. Dokažimo zdaj, da je preslikava

$$\Phi\colon \overline{\mathcal{K}}(N,r) \to \mathcal{K}(\mathbb{N}_{n+r-1}, n-1), \quad \Phi(\mu) = B_\mu,$$

bijekcija. Surjektivnost dokažemo tako, da vzamemo poljubno $(n-1)$-elementno podmnožico $B \subseteq \mathbb{N}_{n+r-1}$, uredimo njene elemente b_k po velikosti, $b_1 < b_2 < \ldots < b_{n-1}$, in določimo števila $\mu(a_k)$ tako, da zadoščajo formuli $(*)$. Dobimo:

$$\mu(a_1) = b_1 - 1, \quad \mu(a_k) = b_k - b_{k-1} - 1 \ \text{ za } \ k \geq 2.$$

Za tako določeno multimnožico $\mu \in \overline{\mathcal{K}}(N,r)$ očitno velja $B_\mu = B$. S tem je surjektivnost preslikave Φ dokazana. Injektivnost sledi iz dejstva, da so števila b_k v formuli $(*)$ natanko določajo vrednosti $\mu(a_k)$. ∎

2.5 Ponovno o igri loto

Na koncu poglavja se vrnimo k naši začetni nalogi o številu možnih žrebov sedmih kroglic. Pri vseh štirih različicah naloge preštevamo izbore elementov množice z $n = 39$ elementi dolžine $r = 7$.

Če je vrstni red izvlečenih kroglic pomemben, kroglice pa vračamo v boben, štejemo urejene izbore s ponavljanjem. Teh je – v skladu s trditvijo 2.2 – natanko

$$39^7 = 137\,231\,006\,679.$$

Če je vrstni red izvlečenih kroglic pomemben, kroglic pa ne vračamo v boben, štejemo urejene izbore brez ponavljanja. Teh je – v skladu s trditvijo 2.4 – natanko

$$39^{\underline{7}} = 77\,519\,922\,480.$$

Če vrstni red izvlečenih kroglic ni pomemben, kroglice pa vračamo v boben, štejemo neurejene izbore s ponavljanjem. Teh je – v skladu s trditvijo 2.10 – natanko

$$\binom{39+7-1}{7} = \binom{45}{7} = 45\,379\,620.$$

Nazadnje si oglejmo še interpretacijo naloge, ki ustreza dejanskim pravilom igre loto, torej, ko vrstni red izvlečenih kroglic ni pomemben in kroglic ne vračamo v boben. Tedaj štejemo neurejene izbore brez ponavljanja, ki jih je – v skladu s trditvijo 2.7 – natanko

$$\binom{39}{7} = \frac{39^{\underline{7}}}{7!} = 15\,380\,937.$$

2.6 Permutacije množic in multimnožic

Že v razdelku o urejenih izborih brez ponavljanja smo definirali pojem permutacije množice. Omenili smo, da si lahko permutacijo dane množice predstavimo kot linearno ureditev njenih elementov. Včasih pa se pojavi potreba po linearnem urejanju elementov multimnožice. Na primer, če želimo prešteti vse besede, ki jih lahko sestavimo s premetavanjem črk besede BANANA, moramo prešteti vse linearne ureditve črk B, treh kopij črke A in dveh kopij črke N, pri čemer kopij posamezne črke med seboj ne ločimo. Takšno linearno ureditev lahko strogo matematično opišemo s pojmom *permutacije multimnožice*.

DEFINICIJA 2.11 *Naj bo $\mu\colon A \to \mathbb{N}_0$ multimnožica moči n. Urejeni n-terici $(x_1, \ldots, x_n)$, v kateri se vsak element $a \in A$ pojavi natanko $\mu(a)$-krat, rečemo* permutacija multimnožice μ.

TRDITEV 2.12 *Naj bo μ multimnožica moči n z elementi $x_1, \ldots, x_k$ in kratnostmi $\mu(x_i) = n_i$. Tedaj je število permutacij multimnožice μ enako*

$$\binom{n}{n_1, \ldots, n_k} = \frac{n!}{n_1! \cdots n_k!}.$$

DOKAZ: Za vsak $i \in \{1, \ldots, k\}$ definirajmo množico $X_i = \{x_i\} \times \mathbb{N}_{n_i}$ ter množice X_i združimo v množico $X = \cup_{i=1}^{k} X_i$. Na elemente množice X lahko pogledamo kot na elemente multimnožice μ, pri čemer pojavitve istega elementa med seboj razlikujemo.

Iz permutacije množice X lahko dobimo permutacijo multimnožice μ tako, da pri vsakem elementu množice X odmislimo njegovo drugo komponento.

Na primer, če je $\mu = \{x_1^1, x_2^3, x_3^2\}$, potem iz permutacije

$$((x_2, 3), (x_1, 1), (x_2, 1), (x_2, 2), (x_3, 2), (x_3, 1))$$

množice X dobimo permutacijo $(x_2, x_1, x_2, x_2, x_3, x_3)$ multimnožice μ.

Vsako permutacijo multimnožice μ lahko na takšen način dobimo iz natanko $n_1! \cdots n_k!$ različnih permutacij množice X. Ker je permutacij množice X natanko $n!$, je permutacij množice μ natanko $n!/n_1! \cdots n_k!$. ∎

OPOMBA. Simbolu $\binom{n}{n_1, \ldots, n_k} = \frac{n!}{n_1! \cdots n_k!}$ rečemo tudi *multinomski simbol*.

2.7 Binomski simboli in Pascalov trikotnik

Oglejmo si nekaj zanimivih lastnosti binomskih simbolov, ki smo jih vpeljali v razdelku 2.3. Začnimo z izrekom, ki pojasni njihovo ime.

TRDITEV 2.13 *V kolobarju polinomov $\mathbb{Q}[x, y]$ za vsako naravno število n velja naslednja, tako imenovana* binomska identiteta.

$$(x + y)^n = \sum_{r=0}^{n} \binom{n}{r} x^{n-r} y^r.$$

DOKAZ: Trditev lahko dokažemo z indukcijo na število n. Zanimivejša pa je naslednja kombinatorična utemeljitev identitete. Potenco $(x + y)^n$ najprej zapišimo kot produkt n faktorjev oblike $x + y$:

$$\underbrace{(x + y)(x + y) \cdots (x + y)}_{n}.$$

Ko s pomočjo distributivnostnega zakona odpravimo vse oklepaje, dobimo vsoto produktov oblike $a_1a_2\ldots a_n$, kjer posamičen faktor a_i izberemo izmed nedoločenk x in y v i-tem oklepaju $(x+y)$ zgornjega produkta:

$$(x+y)^n = \sum_{(a_1,\ldots,a_n)\in\{x,y\}^n} a_1a_2\ldots a_n.$$

Produkt $a_1a_2\ldots a_n$ je torej oblike x^ry^{n-r}, pri čemer r pove, koliko od faktorjev a_i je enakih x. Ker lahko r oklepajev, iz katerih za a_i vzamemo nedoločenko x, izberemo na $\binom{n}{r}$ načinov, se posamični člen x^ry^{n-r} v razvoju potence binoma $(x+y)^n$ pojavi natanko $\binom{n}{r}$-krat. S tem je trditev dokazana. ∎

S pomočjo binomske identitete lahko izpeljemo naslednji zanimivi enakosti. Prva od enakosti je hkrati posledica dejstva, da je število vseh podmnožic n-elementne podmnožice enako 2^n.

TRDITEV 2.14

$$\begin{aligned}\sum_{r=0}^{n}\binom{n}{r} &= 2^n;\\ \sum_{r=0}^{n}(-1)^r\binom{n}{r} &= 0.\end{aligned}$$

DOKAZ: Prvo trditev dobimo, če v binomsko formulo vstavimo $x = y = 1$, drugo pa, če vstavimo $x = 1$ in $y = -1$. ∎

Naslednja trditev pravi, da je binomski simbol $\binom{n}{r}$ neobčutljiv za zamenjavo $r \mapsto n-r$.

TRDITEV 2.15 *Za poljubni števili n, r, $0 \le r \le n$, velja enakost*

$$\binom{n}{n-r} = \binom{n}{r}.$$

DOKAZ: Trditev lahko dokažemo z računskim rokohitrstvom takole: Najprej formulo za binomske koeficiente podamo v naslednji "neokrajšani" obliki,

$$\binom{n}{r} = \frac{n^{\underline{r}}}{r!} = \frac{n!}{r!(n-r)!}.$$

Nato pa v zgornji formuli za r vstavimo $n-r$, in dobimo naslednjo enakost:

$$\binom{n}{n-r} = \frac{n!}{(n-r)!(n-(n-r))!} = \frac{n!}{(n-r)!r!} = \binom{n}{r}.$$

S tem je trditev dokazana.

Za nas pa je zanimivejši naslednji kombinatorični dokaz. Naj bo $\mathcal{N}$ poljubna n-elementna podmnožica. Definirajmo preslikavo, ki vsaki r-elementni podmnožici $A \subseteq \mathcal{N}$ priredimo njen komplement $A^C \subseteq \mathcal{N}$. Ni se težko prepričati, da je takšna preslikava bijekcija med množico $\mathcal{K}(\mathcal{N}, r,)$ vseh r-elementnih podmnožic množice $\mathcal{N}$ in množico $\mathcal{K}(\mathcal{N}, n-r)$ vseh $(n-r)$-elementnih podmnožic množice $\mathcal{N}$. Ker je prvih $\binom{n}{r}$, slednjih pa $\binom{n}{n-r}$, je trditev s tem dokazana. ∎

TRDITEV 2.16 *Za poljubni števili $n, r \in \mathbb{N}_0$, $r \leq n$, velja:*

$$\binom{n+1}{r+1} = \binom{n}{r} + \binom{n}{r+1}.$$

DOKAZ: Navedimo dva dokaza te trditve. Prvi je povsem računski in temelji na formuli iz trditve 2.7. Računajmo:

$$\binom{n}{r} + \binom{n}{r+1} = \frac{n^{\underline{r}}}{r!} + \frac{n^{\underline{r+1}}}{(r+1)!} = \frac{(r+1)n^{\underline{r}} + n^{\underline{r+1}}}{(r+1)!} =$$

$$= \frac{(r+1)n^{\underline{r}} + (n-r)n^{\underline{r}}}{(r+1)!} = \frac{(n+1)n^{\underline{r}}}{(r+1)!} = \frac{n+1^{\underline{r+1}}}{(r+1)!} = \binom{n+1}{r+1}.$$

Drugi dokaz trditve pa je povsem kombinatoričen in upošteva le dejstvo, da je $\binom{n}{r}$ enako številu r-elementnih podmnožic n-elementne množice.

Naj bo $\mathcal{N}$ poljubna $(n+1)$-elementna množica. Brez izgube splošnosti lahko predpostavimo, da je $\mathcal{N} = \{1, 2, \ldots, n, n+1\}$. Množico $(r+1)$-elementnih podmnožic razdelimo v dve skupini: V prvi naj bodo tiste podmnožice, ki vsebujejo element $n+1$, v drugi pa preostale. V drugi skupini so tako pristale ravne vse $(r+1)$-elementne podmnožice množice $\mathcal{N} \setminus \{n+1\}$ – teh je natanko $\binom{n}{r+1}$.

Preštejmo še one iz prve skupine – imenujmo jo R_1. Vsaki podmnožici A iz R_1 priredimo množico $A' = A \setminus \{n+1\}$. Ker A po predpostavki vsebuje element $n+1$, je A' r-elementna podmnožica množice $\mathcal{N} \setminus \{n+1\}$. Predpis $A \mapsto A'$ tako podaja preslikavo med R_1 in $\mathcal{K}(\mathcal{N} \setminus \{n+1\}, r)$. Ni težko videti, da je preslikava, podana s predpisom, $A' \mapsto A' \cup \{n+1\}$ inverz preslikave $A \mapsto A'$. Zato je preslikava $A \mapsto A'$ bijekcija, in množici R_1 ter $\mathcal{N} \setminus \{n+1\}$ sta enako močni. Ker slednja šteje $\binom{n}{r}$ elementov, je to hkrati tudi moč množice R_1. V obeh skupinah skupaj je torej $\binom{n}{r} + \binom{n}{r+1}$ podmnožic. Po

drugi strani pa obe skupini podmnožic skupaj tvorita množico vseh $(r+1)$-elementnih podmnožic $(n+1)$-elementne množice $\mathcal{N}$, za katere pa vemo, da jih je $\binom{n+1}{r+1}$. Enakost je s tem dokazana. ∎

Formula iz trditve 2.16 nosi ime *Pascalova identiteta*. Omogoča nam računati binomske koeficiente rekurzivno s pomočjo sheme, ki ji rečemo *Pascalov trikotnik*. Shema ima obliko enakokrakega trikotnika, ki ga gradimo iz "gornjega" oglišča "navzdol" tako, da na skrajni mesti vsake vrstice najprej vpišemo število 1, "notranjost" vrstice pa zapolnimo tako, da v vsako prazno mesto vpišemo vsoto števili, ki stojita levo in desno diagonalno nad praznim mestom. Pri tem prvo vrstico, v kateri stoji le ena številka, namreč 1, imenujemo 0-to vrstico, naslednje pa prva, druga, tretja itd. Podobno skrajno levemu mestu v vsaki vrstici rečemo 0-to mesto, naslednja pa prvo, drugo, tretje itd. Iz Pascalove identitete tedaj sledi, da se na r-tem mestu n-te vrstice nahaja število $\binom{n}{r}$.

3 Načelo vključitev in izključitev

Načelo vsote nam pove, da je moč unije paroma disjunktnih množic enaka vsoti njihovih moči. Kaj pa, če množice niso paroma disjunktne? Tedaj je moč unije seveda strogo manjša od vsote moči posameznih množic, saj pri seštevanju moči množic elemente, ki nastopajo v presekih dveh ali več množic štejemo več kot enkrat. Načelo vključitev in izključitev podaja zvezo med močjo unije ter močmi posameznih množic ter njihovih presekov.

3.1 Unija dveh množic

Pričnimo s preprostim zgledom unije dveh množic A in B. Če preštejemo najprej elemente množice A, nato pa še elemente množice B, smo prešteli vsak element unije $A \cup B$, pri čemer smo elemente v preseku $A \cap B$ prešteli dvakrat. Zato velja dobro znana formula:

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

3.2 Unija poljubno mnogo množic

Če je množic več, moč njihove unije računamo s pomočjo naslednje trditve.

Trditev 3.1 *Naj bodo $A_1, \ldots, A_n$ poljubne množice. Za $k \in \{1, \ldots, n\}$ naj*

$$S_k = \sum_{\mathcal{J} \in \binom{\mathbb{N}_n}{k}} |\cap_{i \in \mathcal{J}} A_i|$$

označuje vsoto moči presekov vseh k-teric množic A_i. Tedaj je

$$|\cup_{i=1}^{n} A_i| = \sum_{k=1}^{n} (-1)^{k-1} S_k. \qquad (*)$$

Dokaz: Naj bo x element unije $\cup_{i=1}^{n} A_i$. Tedaj je x vsebvan v vsaj eni od množic A_i. Pa denimo, da je x vsebovan v natanko m množicah A_i. Tedaj se za vsak $k \in \{1, \ldots, n\}$ element x pojavi v natanko $\binom{m}{k}$ presekih $\cap_{i \in \mathcal{J}} A_i$ za katere je $|\mathcal{J}| = k$. To pa pomeni, da x za vsak k prispeva k desni strani enakosti $(*)$ natanko $(-1)^{k-1}\binom{m}{k}$, skupaj torej

$$\sum_{k=1}^{n} (-1)^{k-1} \binom{m}{k} = 1 + \sum_{k=0}^{m} (-1)^{k-1} \binom{m}{k} = 1,$$

kjer smo pri zadnji enakosti uporabili trditev 2.16. S tem je trditev dokazana. ∎

Zgled. *Naj bo P_n množica vseh permutacij množice $\mathbb{N}_n$. Elementu $i \in \mathbb{N}_n$ rečemo* fiksna točka permutacije $\pi = (a_1, \ldots, a_n) \in P_n$, *če velja $a_i = i$. Permutaciji brez fiksnih točke rečemo tudi* deranžma. *Koliko deranžmajev v P_n obstaja?*

REŠITEV: Za $i = 1, \ldots, n$ naj bo A_i množica vseh permutacij v P_n, za katere je i fiksna točka. Unija $\cup_{i=1} A_i$ je natanko množica vseh permutacij, ki niso deranžmaji. Nas torej zanima število

$$d_n = |P_n| - |\cup_{i=1}^n A_i| = n! - |\cup_{i=1}^n A_i|.$$

Vzemimo poljubno indeksno množico $\mathcal{J} \in \binom{\mathbb{N}_n}{k}$ in premislimo, koliko elementov premore presek $\cap_{i\in\mathcal{J}} A_i$. Elementi tega preseka so natanko tiste permutacije $(a_1, \ldots, a_n)$, za katere je $a_i = i$ za vsak $i \in \mathcal{J}$, na preostalih mestih $\mathbb{N}_n \setminus \mathcal{J}$ pa se nahaja poljubna permutacija množice $\mathbb{N}_n \setminus \mathcal{J}$. Zato je moč preseka $\cap_{i\in\mathcal{J}} A_i$ enaka $(n-k)!$ in

$$S_k = \sum_{\mathcal{J}\in\binom{\mathbb{N}_n}{k}} |\cap_{i\in\mathcal{J}} A_i| = \binom{n}{k}(n-k)! = \frac{n!}{k!}.$$

Iz načela vključitev in izključitev sledi:

$$|\cup_{i=1}^n A_i| = \sum_{k=1}^{n}(-1)^{k-1} S_k = n! \sum_{k=1}^{n}(-1)^{k-1}\frac{1}{k!}.$$

Opazimo, da zaporedje $\frac{d_n}{n!}$ zelo hitro konvergira k e^{-1}. Verjetnostna interpretacija tega dejstva je, da je verjetnost, da naključno izbrana permutacija nima fiksnih točk, približno enaka $e^{-1} \approx 0{,}37$. ∎

Zgornjo nalogo o deranžmajih lahko srečamo v najrazličnejših preoblekah, med katere sodi tudi spodnja.

Zgled. *V krčmo na Divjem zahodu vstopi druščina n revolverašev. Ker je v salonu prepovedano nositi orožje, pri vratih vsak odda svoj revolver. Zaradi objektivnih okoliščin so v nekem trenutku krčmo prisiljeni na hitro zapustiti, pri čemer vsak na slepo zagrabi enega od n oddanih revolverjev. Kolikšna je verjetnost, da nihče od revolverašev ni zagrabil svojega revolverja.*

REŠITEV: Če revolveraše označimo z naravnimi števili med 1 in n, lahko situacijo po odhodu iz salona opišemo s permutacijo $(a_1, \ldots, a_n)$ množice revolverašev, kjer je a_i zaporedna številka lastnika revolverja, ki ga je ob odhodu zagrabil i-ti revolveraš. Vseh možnih situacij po odhodu je torej $n!$ in vse so enako verjetne. Situacije, kjer nihče od revolverašev ne zagrabi

svojega revolverja, pa ustrezajo natanko deranžmajem. Zato je verjetnost tega dogodka enaka

$$\frac{d_n}{n!} = \sum_{k=0}^{n} (-1)^k \frac{1}{k!}.$$

■

4 Razbitja množic in razčlenitve števil

V tem poglavju bomo preštevali razbitja dane n-elementne množice na k nepraznih podmnožic. Pojasnimo najprej natančno, kaj s tem mislimo.

DEFINICIJA 4.1 Razbitje množice A *je družina* $\mathcal{R} = \{A_1, \ldots, A_k\}$ *nepraznih, paroma disjunktnih podmnožic množice* A*, katerih unija je enaka množici* A*. Množicam* A_i *rečemo tudi* deli razbitja.

Na primer, če je $A = \{a, b, c, d\}$, je $\mathcal{R} = \{\{a\}, \{b, c, d\}\}$ razbitje množice A na 2 neprazni množici. Poleg razbitja $\mathcal{R}$, množica A premore še šest drugih razbitij na 2 neprazni množici. Najprej še tri, kjer je eden od delov moči 1 (in drugi moči 3), nato pa še tri takšna, kjer je sta oba dela razbitja moči 2.

Poleg običajnih razbitij množice, pa bomo obravnavali tudi tako imenovana *urejena razbitja*, kjer elemente vsakega dela razbitja uredimo. Kaj natanko s tem mislimo, bomo pojasnili v nadaljevanju.

4.1 Stirlingova števila druge vrste

Številu vseh razbitij n-elementne množice A na k nepraznih podmnožic rečemo *Stirlingovo število druge vrste* in ga označimo z $S(n, k)$. Množico teh razbitij označimo z $S(A, k)$. Očitno velja naslednje:

$$S(n, k) = 0 \text{ za } k > n, \quad S(n, n) = 1 \text{ in } S(n, 1) = 1. \qquad (*)$$

Dodatno definiramo še $S(n, 0) = 0$ za vsak $n \geq 1$ in $S(0, 0) = 1$.

Ostala števila $S(n, k)$ pa najenostavneje računamo s pomočjo naslednje rekurzivne formule.

TRDITEV 4.2 *Za vsak par* $n, k \in \mathbb{N}$, $1 \leq k \leq n$, *velja*

$$S(n, k) = S(n-1, k-1) + kS(n-1, k).$$

DOKAZ: Naj bo $\mathcal{N} = \{x_1, \ldots, x_n\}$ poljubna n-elementna množica, $\mathcal{R}$ množica vseh razbitij množice $\mathcal{N}$ na k nepraznih podmnožic, $\mathcal{R}_0$ množica tistih razbitij iz $\mathcal{R}$, v katerih nastopa podmnožica $\{x_n\}$ in $\mathcal{R}_1 = \mathcal{R} \setminus \mathcal{R}_0$.

Vzemimo poljubno razbitje $R = \{A_1, \ldots, A_k\} \in \mathcal{R}$. Mislimo si, da element x_n iz množice $\mathcal{N}$ izrežemo. Tedaj razbitje R preide v razbitje $R' = \{A_1 \setminus \{x_n\}, \ldots, A_k \setminus \{x_n\}\}$ množice $\mathcal{N} \setminus \{x_n\}$.

Če razbitje R sodi v skupino $\mathcal{R}_0$, tedaj je ena od množic razbitja R' prazna in mislimo si lahko, da jo iz R' odstanimo. Tako dobimo razbitje

$(n-1)$-elementne množice $\mathcal{N}\setminus\{x_n\}$ na $k-1$ nepraznih podmnožic. Obratno, vsako razbitje $T = \{A'_1, \ldots, A'_{k-1}\}$ množice $\mathcal{N} \setminus \{x_n\}$ na $k-1$ nepraznih podmnožic lahko z vključitvijo množice $\{x_n\}$ dopolnimo do razbitja $R = \{\{x_n\}, A'_1 \ldots, A'_{k-1}\}$ množice $\mathcal{N}$. Ni težko videti, da je R edino razbitje iz $\mathcal{R}_0$, za katero je $R' = T$. S tem smo dokazali, da je preslikava $R \mapsto R'$ bijekcija med množicama $\mathcal{R}_0$ in množico $S(\mathcal{N} \setminus \{x_n\}, k-1)$ nepraznih podmnožic. Po načelu enakosti sledi $|\mathcal{R}_0| = S(n-1, k-1)$.

Če pa razbitje R sodi v skupino $\mathcal{R}_1$, tedaj nobena od množic razbitja R' ni prazna, kar pomeni, da je R' razbitje mnozčie $\mathcal{N} \setminus \{x_n\}$ na k nepraznih podmnožic. Če vzamemo poljubno razbitje $T = \{A'_1, \ldots, A'_k\}$ množice $\mathcal{N} \setminus \{x_n\}$ na k nepraznih podmnožic, lahko z vključitvijo elementa $\{x_n\}$ v katero koli od k množic A'_i dobimo razbitje R iz skupine R_1, za katerega je $R' = T$. Tako dobljena razbitja R so hkrati edina, za katera je $R' = T$, kar pomeni, da je vseh razbitij iz skupine R_1 natanko k-krat toliko, kot je razbitij $(n-1)$-elementne množice $\mathcal{N} \setminus \{x_n\}$ na k-nepraznih podmnožic, torej $kS(n-1, k)$.

Trditev sedaj z lahkoto sledi, saj je $|\mathcal{R}| = |\mathcal{R}_0| + |\mathcal{R}_1| = S(n-1, k-1) + kS(n-1, k)$. ∎

Rekurzivna formula nam omogoča, da Stirlingova števila 2. vrste računamo podobno kot binomske koeficiente. Sestavimo tabelo, v kateri na presečišču n-te vrstice in k-tega stolpca stoji število $S(n, k)$:

$n\|k$	0	1	2	3	4	5	6	7
0	1	0	0	0	0	0	0	0
1	0	1	0	0	0	0	0	0
2	0	1	1	0	0	0	0	0
3	0	1	3	1	0	0	0	0
4	0	1	7	6	1	0	0	0
5	0	1	15	25	10	1	0	0
6	0	1	31	90	65	15	1	0
7	0	1	63	301	350	140	21	1

Iz začetnih pogojev sledi, da so nad glavno diagonalo same ničle, po diagonali same enke, v prvem stolpcu pa, razen pri prvem elementu, zopet same ničle. Število $S(n, k)$ v tabeli dobimo tako, da seštejemo število, ki stoji diagonalno levo nad njim in k-kratnik števila neposredno nad njim. Število 65, ki leži v vrstici 6 in stolpcu 4, smo torej dobili tako, da smo sešteli 25 (levo zgoraj) in $4 \cdot 10$ (smo v stolpcu 4, nad iskanim številom pa stoji 10).

Stirlingova števila 2. vrste imajo zanimivo interpretacijo tudi pri problemih preštevanja funkcij med dvema končnima množicama.

TRDITEV 4.3 *Naj bosta N in K poljubni končni množici moči n in k. Tedaj je število vseh surjektivnih preslikav iz množice N v množico K enako*

$$k!S(n,k).$$

DOKAZ: Naj bodo $b_1, \ldots, b_k$ elementi množice K in $f\colon N \to K$ poljubna surjektivna preslikava. Za vsak $i \in \{1, \ldots, k\}$ definirajmo množico

$$N_i = f^{-1}(b_i) = \{x \in N : f(x) = b_i\}.$$

Tedaj družina $\{N_1, \ldots, N_k\}$ tvori razbitje množice N na k neprazniih delov. Na ta način smo definirali preslikavo Φ iz množice vseh surjektivnih funkcij iz N v K ter množico $S(N,k)$.

Pri tem opazimo, da za razbitje $\mathcal{R} = \{N_1, \ldots, N_k\} \in S(N,k)$ in surjektivno preslikavo $f\colon N \to K$ velja $\Phi(f) = \mathcal{R}$, če in samo če je f definirana s predpisom

$$f(x) = b_i \iff x \in N_{\pi(i)},$$

za neko permutacijo π množice indeksov $\{1, \ldots, k\}$. Od tod sledi, da se v vsako razbitje iz $S(N,k)$ preslika natanko $k!$ različnih surjektivnih preslikav iz N v K. Zato je takšnih surjektivnih preslikavo natanko $k!|S(N,k)| = k!S(n,k)$. ∎

S pomočjo trditve 4.3, rekurzivne formule in načela vključitev in izključitev lahko dokažemo naslednjo zanimivo formulo.

TRDITEV 4.4 *Za poljubni naravni števili n, k, $k \leq n$, velja*

$$S(n,k) = \frac{1}{k!} \sum_{i=1}^{k} \binom{k}{i} (-1)^{k-i} i^n.$$

DOKAZ: Naj bosta N in K, $|N| = n$, $|K| = k$, poljubni množici in naj A označuje množico vseh preslikav iz N v K, ki niso surjektivne. Ker je vseh preslikav iz N v K natanko k^n, je moč množice A enaka $k^n - k!S(n,k)$.

Zdaj pa preštejmo elemente množice A še na drug način. Naj bodo $b_1, \ldots, b_k$ elementi množice K in za vsak $i \in \{1, \ldots, k\}$ naj A_i predstavlja množico vseh tistih funkcij iz N v K, ki elementa b_i nimajo v svoji sliki. Tedaj je množica A očitno unija množic A_i.

Vzemimo poljubno i-elementno podmnožico $\mathcal{J} = \{b_{j_1}, \ldots, b_{j_i}\}$ množice $\{1, \ldots, k\}$. Tedaj presek $\cap_{j \in \mathcal{J}} A_j$ vsebuje natanko vse funkcije iz množice N v množico $K \setminus \{b_{j_1}, \ldots, b_{j_i}\}$ in zato premore natanko $(k-i)^n$ elementov.

Vsota S_i moči presekov $\cap_{j\in\mathcal{J}} A_j$ po vseh i-elementnih podmnožicah $\mathcal{J}$ množice $\{1,\ldots,k\}$ zato znaša

$$\binom{k}{i}(k-i)^n.$$

Trditev sedaj sledi neposredno iz načela vključitev in izključitev. ∎

4.2 Lahova števila

Lahovo število $L(n,k)$ je definirano kot število *linearno urejenih razbitij* n-elementne množice na k nepraznih podmnožic. Neformalno lahko linearno urejeno razbitje množice $A = \{a_1,\ldots,a_n\}$ opišemo kot običajno razbitje, pri čemer vsako množico razbitja linearno uredimo. Dve razbitji na iste množice se pri tem razlikujeta, če se razlikujeta vrstna reda elementov v kateri od množic razbitja.

Razliko med običajnimi in linearno urejenimi razbitji si oglejmo na naslednjem primeru. Naj bo $A = \{a,b,c,d\}$ in poiščimo vsa (običajna) razbitja na množice A na dve podmnožici. Le-ta so

$$\{\{a,b\},\{c,d\}\},\ \{\{a,c\},\{b,d\}\},\ \{\{a,d\},\{b,c\}\},$$

$$\{\{a\},\{b,c,d\}\},\ \{\{b\},\{a,c,d\}\},\ \{\{c\},\{a,b,d\}\},\ \{\{d\},\{a,b,c\}\}.$$

Razbitje $\{\{a,b\},\{c,d\}\}$ porodi štiri različna linearno urejena razbitja:

$$\{(a,b),(c,d)\},\ \{(b,a),(c,d)\},\ \{(a,b),(d,c)\},\ \{(b,a),(d,c)\}.$$

Podobno velja za ostala razbitja na dve enako močni množici. Po drugi strani pa razbitje $\{\{a\},\{b,c,d\}\}$ porodi $3! = 6$ različnih linearno urejenih razbitij – za vsako linearno ureditev elementov $\{b,c,d\}$ po eno. Zato je

$$L(4,2) = 4\cdot 3 + 6\cdot 4 = 36.$$

Za skrajne vrednosti Lahovih števil očitno velja naslednje:

$$L(n,k) = 0 \text{ za } k > n\ , \quad L(n,n) = 1 \ \text{ in } \ L(n,1) = n!.$$

Dodatno definiramo še $L(n,0) = 0$ za vsak $n \geq 1$ in $L(0,0) = 1$.

Podobno kot pri Stirlingovih številih 2. vrste lahko tudi za Lahova števila izpeljemo rekurzivno zvezo. Izpeljava se razlikuje zgolj v tem, da tu pri štetju razbitij iz skupine $\mathcal{R}_1$ iz danega razbitja $T = \{A'_1,\ldots,A'_k\}$ množice $\mathcal{N}\setminus\{x_n\}$ lahko najdemo $n-1+k$ razbitij R iz skupine $\mathcal{R}_1$, za katera je

$R' = T$; izbrisani element x_n lahko namreč vrinemo v katero koli množico A'_i na eno od $|A'_i| + 1$ razpoložljivih mest (za vse elemente množice A'_i ali pa pred kakega od $|A'_i|$ elementov množice A). Element x_n lahko torej vrinemo v razbitje na $(|A_1| + 1) + (|A_2| + 1) + \ldots + (|A_k| + 1)$ načinov, kar znese $n - 1 + k$. Od tod sledi naslednja trditev.

TRDITEV 4.5 *Za $1 \leq k \leq n$ velja*

$$L(n, k) = L(n - 1, k - 1) + (n + k - 1)L(n - 1, k).$$

Z indukcijo na število n in z uporabo rekurzivne formule iz trditve 4.5 lahko izpeljemo tudi eksplicitno formulo, ki Lahova števila izrazi s pomočjo binomskih simbolov.

TRDITEV 4.6 *Za $1 \leq k \leq n$ velja*

$$L(n, k) = \binom{n-1}{k-1} \frac{n!}{k!} = \binom{n}{k} \frac{(n-1)!}{(k-1)!}.$$

Podobno kot pri binomskih simbolih in Stirlingovih številih 2. vrste, lahko tudi Lahova števila računamo s pomočjo sheme, ki izhaja iz rekurzivne zveze. V spodnji tabeli na presečišču n-te vrstice in k-tega stolpca stoji število $L(n, k)$, ki ga dobimo tako, da seštejemo število, ki stoji diagonalno levo nad njim in $(n + k - 1)$-kratnik števila neposredno nad njim. Število 240, ki leži v vrstici 5 in stolpcu 2, smo torej dobili tako, da smo sešteli 24 (levo zgoraj) in $6 \cdot 36$.

$n\|k$	0	1	2	3	4	5	6	7
0	1	0	0	0	0	0	0	0
1	0	1	0	0	0	0	0	0
2	0	2	1	0	0	0	0	0
3	0	6	6	1	0	0	0	0
4	0	24	36	12	1	0	0	0
5	0	120	240	120	20	1	0	0
6	0	720	1800	1200	300	30	1	0
7	0	5040	15120	12600	4200	630	42	1

Poleg običajnih Lahovih števila se v literaturi pojavljajo tudi *predznačena Lahova števila*, definirana s formulo

$$L'(n, k) = (-1)^n L(n, k).$$

4.3 Stirlingova števila prve vrste

Stirlingovo število prve vrste $s(n,k)$ štejeje razbitja n-elementne množice na k nepraznih *ciklično urejenih* množic. Pri tem pojem "ciklično urejena množica" pomeni množico, denimo $A = \{a,b,c,d\}$, skupaj s cikličnim vrstnim redom elementov, denimo

$$[a,b,c,d] = [b,c,d,a] = [c,d,a,b] = [d,a,b,c].$$

Hiter premislek pokaže, da lahko vsako m-elementno množico ciklično uredimo na $(m-1)!$ načinov, saj si lahko ciklično ureditev predstavljamo kot linearno ureditev množice, pri čemer m linearnih ureditev, ki se razlikujejo zgolj za ciklični pomik, štejemo kot isto ciklično ureditev. Ker je linearnih ureditev m-elemente množice $m!$, je zato cikličnih ureditev $\frac{m!}{m} = (m-1)!$.

Stirlingova števila za mejne pare števil n in k zadoščajo enakostim

$$s(n,k) = 0 \text{ za } k > n\ , \quad s(n,n) = 1 \text{ in } s(n,1) = (n-1)!.$$

Dodatno definiramo še $s(n,0) = 0$ za vsak $n \geq 1$ in $s(0,0) = 1$.

Na zelo podoben način kot pri Stirlingovih številih druge vrste in Lahovih številih lahko tudi tu izpeljemo naslednjo rekurzivno formulo.

$$s(n,k) = s(n-1,k-1) + (n-1)s(n-1,k).$$

V tabeli Stirlingovih števil 1. vrste, v kateri na presečišču n-te vrstice in k-tega stolpca stoji število $s(n,k)$, ležijo nad glavno diagonalo same ničle, po diagonali same enke, v prvem stolpcu pa, razen prvega elementa, spet same ničle. V skladu z rekurzivno formulo izračunamo število $s(n,k)$ v tabeli tako, da seštejemo število, ki stoji levo zgoraj nad njim, in $(n-1)$-kratnik števila, ki stoji neposredno nad njim. Na primer, na presečišču vrstice 5 in stolpca 3 dobimo vsoto števila 11 (levo zgoraj) in števila $(5-1)\cdot 6 = 24$, torej 35.

$n\|k$	0	1	2	3	4	5	6	7
0	1	0	0	0	0	0	0	0
1	0	1	0	0	0	0	0	0
2	0	1	1	0	0	0	0	0
3	0	2	3	1	0	0	0	0
4	0	6	11	6	1	0	0	0
5	0	24	50	35	10	1	0	0
6	0	120	274	225	85	15	1	0
7	0	720	1764	1624	735	175	21	1

V literaturi srečamo tudi *predznačena Stirlingova števila prve vrste*, ki so definirana s formulo

$$s'(n,k) = (-1)^{n-k} s(n,k).$$

4.4 Število razčelnitev naravnega števila

Zaporedju (neničelnih) naravnih števil $m_1 \leq m_2 \leq \ldots \leq m_k$, katerih vsota je enaka n, rečemo *razčlenitev naravnega števila n na k členov*. Število vseh takšnih razčlenitev označimo s $p_k(n)$. Očitno je

$$p_k(n) = 0 \text{ za } k > n.$$

Dodatno definiramo $p_0(0) = 1$ in $p_0(n) = 0$ za $n > 0$.

TRDITEV 4.7 *Za vsak par naravnih števil n, k velja*

$$p_k(n) = p_{k-1}(n-1) + p_k(n-k).$$

DOKAZ: Združimo tiste razčlenitve $(m_1, \ldots, m_k)$, za katera je $m_1 = 1$ v množico $\mathcal{R}_0$, tiste, za katera pa je $m_1 > 1$, pa v množico $\mathcal{R}_1$. Če razčlenitvi iz množice $\mathcal{R}_0$ odvzamemo prvi element $m_1 = 1$, dobimo razčlenitev števila $n-1$ na $k-1$ sumandov. Obratno, če razčlenitvi števila $n-1$ na $k-1$ sumandov dodamo na začetek enico, dobimo razčlenitev iz $\mathcal{R}_0$. Zato je $|R_0| = p_{k-1}(n-1)$.

Razčlenitev $(m_1, \ldots, m_k) \in \mathcal{R}_1$ lahko spremenimo v razčlenitev števila $n-k$ na k sumandov, če vsak m_i zmanjšamo za 1. Ker vsako razčlenitev števila $n-k$ na k sumandov dobimo na takšen način natanko enkrat, je $|\mathcal{R}_1| = p_k(n-k)$. Od tod dobimo $p_k(n) = |\mathcal{R}_0| + |\mathcal{R}_1| = p_{k-1}(n-1) + p_k(n-k)$. ∎

Računanje števil $p_k(n)$ si olajšamo, če sestavimo tabelo, v kateri na presečišču n-te vrstice in k-tega stolpca stoji število $p_k(n)$. Začetni pogoji in rekurzivna formula pravijo, da so nad glavno diagonalo same ničle, po diagonali same enke, v prvem stolpcu pa, razen prvega elementa, spet same ničle. Število $p_k(n)$ v tabeli dobimo tako, da seštejemo število, ki stoji levo zgoraj nad njim, in število, ki stoji k vrstic nad iskanim številom. Na primer, na presečišču vrstice 7 in stolpca 3 dobimo vsoto števila 3 (levo zgoraj) in števila 1 (tri vrstice višje).

$n\|k$	0	1	2	3	4	5	6	7
0	1	0	0	0	0	0	0	0
1	0	1	0	0	0	0	0	0
2	0	1	1	0	0	0	0	0
3	0	1	1	1	0	0	0	0
4	0	1	2	1	1	0	0	0
5	0	1	2	2	1	1	0	0
6	0	1	3	3	2	1	1	0
7	0	1	3	4	3	2	1	1

4.5 Prostori polinomov in Stirlingova ter Lahova števila

Za konec razdelka predstavimo presenetljivo interpretacijo Stirlingovih in Lahovih števil v teoriji polinomskih kolobarjev. Naj $\mathbb{Q}[x]$ označuje kolobar polinomov z racionalnimi koeficienti v nedoločenki x. Na kolobar $\mathbb{Q}[x]$ lahko pogledamo tudi kot na neskončno razsežen vektorski prostor nad obsegom $\mathbb{Q}$. Poleg standardne baze

$$\Sigma \;=\; \{1, x, x^2, x^3, \ldots\}$$

prostora $\mathbb{Q}[x]$ definirajmo še bazi

$$\Sigma_p = \{1, x, x^{\underline{2}}, x^{\underline{3}}, \ldots\} \;=\; \{1, x, x(x-1), x(x-1)(x-2), \ldots\},$$
$$\Sigma_n = \{1, x, x^{\overline{2}}, x^{\overline{3}}, \ldots\} \;=\; \{1, x, x(x+1), x(x+1)(x+2), \ldots\}.$$

Ker so vse tri zgoraj naštete množice baze prostora $\mathbb{Q}[x]$, lahko vsak polinom vsake od njih zapišemo kot linearno kombinatocijo polinomov iz vsake druge od njih. Koeficienti takšnih razvojev so tesno povezani s Stirlingovimi ter Lahovimi števili.

Dokažali bomo le trditev, ki podaja razvoj standardnih baznih polonomov iz Σ po polinomih iz Σ_p.

TRDITEV 4.8 *Naj bo n poljubno nenegativno celo število. Tedaj v kolobarju polinomov $\mathbb{Q}[x]$ velja naslednja enakost*

$$x^n = \sum_{k=0}^{n} S(n,k) x^{\underline{k}}.$$

DOKAZ: Trditev lahko dokažemo s pomočjo indukcije na naravno število n in rekurzivne formule za $S(n,k)$ povsem računsko. Mi pa bomo raje navedli kombinatorični dokaz.

Naj bo m poljubno naravno število in $A = \{a_1, \ldots, a_m\}$ poljubna m-elementna množica. Kot vemo, je moč množice A^n vseh urejenih n-teric elementov iz A enaka m^n. Pa preštejmo število elementov množice A^n še na drug način.

Za poljuben element $(x_1, \ldots, x_n) \in A^n$ definirajmo ekvivalenčno relacijo $\sim$ na množici $\mathbb{N}_n = \{1, 2, \ldots, n\}$ s pravilom: $i \sim j$, če in samo če $x_i = x_j$. Ekvivalenčni razredi te relacije tvorijo razbitje množice $\mathbb{N}_n$ na nekaj (vsaj eno in ne več kot n) neprazih podmnožic. Pa naj X_k, $k \in \{1, 2, \ldots, n\}$, predstavlja množico vseh tistih elementov iz A^n, ki na tak način porodijo razbitje z natanko k deli.

Dokazati želimo, da je moč množice X_k enaka $S(n,k)m^{\underline{k}}$. To storimo tako, da najdemo bijekcijo med X_k in množico $S(\mathbb{N}_n,k)\times\mathcal{V}(A,k)$. Ena od takšnih bijekcij je na primer preslikava, ki vsaki m-terici iz X_k priredi par $(\mathcal{R},(y_1,\ldots,y_k))$, kjer je $\mathcal{R}$ razbitje množice $\mathbb{N}_n$ porojeno na zgoraj opisani način z elementi množice X_k, $(y_1,\ldots,y_k)$ pa k-terica, ki jo dobimo iz m-terice $(x_1,\ldots,x_m)$, če pregledujoč z leve proti desni odstranjujemo vse ponovitve elementov, ki smo jih srečali že prej.

Ker je A^n disjunktna unija množic X_k za $k=1,\ldots,n$, od tod sledi

$$m^n=\sum_{k=1}^{n}|X_k|=\sum_{k=1}^{n}S(m,k)m^{\underline{k}}.$$

Ker je $S(m,0)=1$ za $m\geq 1$, lahko k vsoti na desni dodamo še člen s $k=0$.

Tako smo dokazali, da se polinoma na levi in desni strani enakosti iz trditve ujemata pri neskončno mnogo vrednostih spremenljivke x. Ker pa je vsak polinom iz $\mathbb{Q}[x]$ stopnje n enolično določen že z $n+1$ vrednosti v $n+1$ točkah, to pomeni, da sta polinoma iz trditve resnično enaka. ∎

Zgornjo trditev lahko pogojno razumemo tako: Prehodna matrika med bazama Σ in Σ_p je ravno matrika Stirlingovih števil.

Podobne formule, v katerih nastopajo Stirlingova števila 1. vrste in Lahova števila lahko izpeljemo tudi za prehode med preostalimi urejenimi pari baz Σ,Σ_p in Σ_n.

5 Porazdelitve, barvanja in preslikave

Poleg nalog o izborih se v osnovni kombinatoriki pojavljajo tudi naloge o porazdelitvah objektov v skupine. Tipična naloga o porazdelitvah je naslednja:

Kokoši so znesle n jajčk. Na koliko načinov lahko jajčka porazdelimo v k škatel?

Podobno kot pri izborih lahko tudi tu nalogo razumemo na več različnih načinov. Vprašamo se namreč lahko, ali med seboj razlikujemo jajčka in ali razlikujemo med različnimi škatlami. Tako dobimo štiri različice osnovne naloge.

Poleg osnovne naloge nas bosta v vsaki od štirih različic zanimali tudi nekoliko spremenjeni nalogi, pri katerih bomo šteli le tiste porazdelitve, pri katerih so vse škatle zasedene, in tiste porazdelitve, pri katerih je v vsaki škatli največ eno jajce. Število različic se s tem pomnoži s tri, tako da dobimo 12 različnih tipov nalog o porazdelitvah. Tem dvanajstim nalogam včasih slikovito (in nekoliko mistično) rečemo tudi *dvanajstera pot* (angl. *twelfold way*).

Naloge o porazdelitvah imajo tudi nekoliko bolj "barvito" preobleko. Če si mislimo, da je vsaka škatla napolnjena s svojo barvo za barvanje jajčk, si razporejanje jajčk lahko predstavljamo kot barvanje. Namesto o številu razporeditev v k škatel se tako lahko sprašujemo o številu različnih barvanj jajčk s k barvami.

Nazadnje si oglejmo še, kako nalogo o porazdelitvi jajčk oblikovati v strogem matematičnem jeziku. Oglejmo si najprej različico naloge, kjer razlikujemo tako med jajčki kot med škatlami (oz. barvami, če nam je interpretacija z barvami ljubša). V tem primeru lahko jajčka oštevilčimo (navadno s števili med 1 in n), škatle (barve) pa označimo s simboli $c_1, \ldots, c_k$. Porazdelitev jajčk po škatlah lahko sedaj predstavimo s preslikavo iz množice jajčk v množico škatel, ki vsakemu jajčku priredi tisto škatlo, v katero ga razporedimo. Če pri porazdelitvi (barvanju) zahtevamo, da je vsaka škatla zasedena z vsaj enim jajčkom (oz. vsaka barva uporabljena), preštevamo surjektivne preslikave. Če pa zahtevamo, da je v vsaki škatli največ eno jajce (oz. nobeni dve jajci nista iste barve), preštevamo injektivne preslikave.

Kako matematično obravnavati naloge, kjer škatel ali jajčk med seboj ne razlikujemo, bomo videli v nadaljevanju.

5.1 Preslikave

V tem razdelku nas bo zanimalo, koliko funkcij iz n-elementne množice N v k-elementno množico K obstaja. V nadaljevanju bomo elemente množice N označevali z $a_1, \ldots, a_n$, elemente množice K pa s $c_1, \ldots, c_k$.

Naj K^N označuje množico vseh preslikav iz N v K, $(K^N)_i$ množico vseh injektivnih preslikav in $(K^N)_s$ množico vseh surjektivnih preslikav iz N v K.

Vsako preslikavo $f \in K^N$ lahko enolično predstavimo z n-terico

$$(f(a_1), \ldots, f(a_n)) \in K^n$$

njenih slik. V tem smislu smemo na preslikave iz N v K gledati kot na urejene izbore elementov množice K dolžine n. Pri tem injektivnim preslikavam utrezajo izbori brez ponavljanja. Od tod sledita prvi dve formuli spodnje trditve. Formulo o številu surjektivnih preslikav pa smo dokazali že v razdelku o Stirlingovih številih 2. vrste.

TRDITEV 5.1 *Naj bo N poljubna n-elementna množica in K poljubna k-elementna množica. Tedaj velja*

$$|K^N| = k^n, \qquad |(K^N)_i| = k^{\underline{n}}, \qquad |(K^N)_s| = k!S(n,k).$$

5.2 Ekvivalenčni razredi preslikav - dvanajstera pot

S pomočjo permutacij bomo v tem razdelku na množici preslikav iz množice N v množico K uvedli tri ekvivalenčne relacije. V definiciji spodaj smo množico vseh permutacij množice A (gledanih kot bijektivne preslikave iz A v A) označili s simbolom $\mathrm{Sym}(A)$.

DEFINICIJA 5.2 *Naj bosta N in K poljubni neprazni množici in $f, g \in K^N$ poljubni preslikavi. Tedaj pišemo*

$$\begin{aligned} f \sim_K g &\Leftrightarrow \exists \lambda \in Sym(K) : \ g = \lambda \circ f; \\ f \sim_N g &\Leftrightarrow \exists \rho \in Sym(N) : \ g = f \circ \rho; \\ f \sim_{N,K} g &\Leftrightarrow \exists \lambda \in Sym(K),\ \rho \in Sym(N) : \ g = \lambda \circ f \circ \rho. \end{aligned}$$

Vsaka od teh treh ekvivalenčnih relacij razbije množico N^K na ekvivalenčne razrede. Ni težko videti, da ekvivalenčni razred kake surjektivne preslikave vsebuje le surjektivne preslikave, ekvivalenčni razred injektivne preslikave pa le injektivne preslikave. Zato tudi množici $(N_K)_s$ in $(N_K)_i$ razpadeta na ekvivalenče razrede glede na te tri ekvivalenčne relacije. Osrednje vprašanje tega razdelka je, koliko je teh ekvivalenčnih razredov. Preden odgovorimo na to vprašanje, pa si oglejmo zgled.

Zgled. *Naj bo* $N = \{1, \ldots, 5\}$, $K = \{c_1, c_2, c_3\}$ *in* $f\colon N \to K$,

$$f(1) = f(2) = c_1,\ f(3) = f(4) = c_2,\ f(5) = c_3.$$

S katerimi funkcijami je f *v relaci* $\sim_K$ *(oz.* $\sim_N$ *in* $\sim_{N,K}$*).*

REŠITEV: Preslikava f je v relaciji $\sim_N$ z natanko tistimi preslikavami, pri katerih se elementa c_1 in c_2 pojavita med slikami dvakrat, element c_3 pa enkrat.

Nadalje, preslikava f je v relaciji $\sim_K$ s tistimi preslikavami g, za katere je

$$g(1) = g(2),\ g(3) = g(4),$$

elementi $g(1), g(3)$ in $g(5)$ pa so paroma različni.

Nazadnje, preslikava f je v relaciji $\sim_{N,K}$ z vsemi tistimi funkcijami, pri katerih se dva izmed treh elementov $\{c_1, c_2, c_3\}$ pojavita med slikami dvakrat, tretji pa enkrat. ∎

TRDITEV 5.3 *(Dvanajstera pot) Naj bo* N *poljubna* n*-elementna množica in* K *poljubna* k*-elementna množica. Tedaj je število ekvivalenčnih razredov, na ketere razpadejo množice* K^N, $(K^N)_i$ *in* $(K^N)_s$ *pri relacijah* $=$, $\sim_N$, $\sim_K$ *in* $\sim_{N,K}$ *enako številom v spodnji tebeli.*

relacija	K^N	$(K^N)_i$	$(K^N)_s$
$=$	k^n	$k^{\underline{n}}$	$k!S(n,k)$
$\sim_N$	$\binom{n+k-1}{n}$	$\binom{k}{n}$	$\binom{n-1}{n-k}$
$\sim_K$	$\sum_{i=1}^{k} S(n,i)$	1, *za* $k \geq n$, 0 *sicer*	$S(n,k)$
$\sim_{N,K}$	$\sum_{i=1}^{k} p_i(n)$	1, *za* $k \geq n$, 0 *sicer*	$p_k(n)$

DOKAZ: Naj bo $N = \{a_1, \ldots, a_n\}$ in $K = \{c_1, \ldots, c_k\}$. Pravilnost prve vrstice (kjer štejemo kar preslikave in N v K, saj vsak ekvivalenčni razred glede na relacijo enakosti vsebuje natanko en element) sledi iz trditve 5.1.

Oglejmo si sedaj relacijo $\sim_N$. Množico ekvivalenčnih razredov množice K^N označimo s $[K^N]_N$. Vzemimo preslikavo $f\colon N \to K$ in ji priredimo multimnožico

$$\mu = [f(a_1), \ldots, f(a_n)]$$

moči n z elementi iz K. Multimnožica, ki pripada ekvivalentni preslikavi $g = f \circ \rho$, $\rho \in \mathrm{Sym}(N)$, je enaka $\mu' = [f(\rho(a_1)), \ldots, f(\rho(a_n))]$. Ker vrstni

red pri navajanju elementov multimnožice ni pomemben, je $\mu = \mu'$. Zato lahko definiramo preslikavo

$$\varphi\colon [K^N]_N \to \overline{\mathcal{K}}(K,n), \qquad \varphi([f]) = [f(a_1),\ldots,f(a_n)].$$

Bijektivnost preslikave φ dokažemo tako, da ji poiščemo inverzno preslikavo ψ, ki multimnožico $[b_1,\ldots,b_n]$ moči n z elementi iz K preslika v ekvivalenčni razred preslikave $f\colon N \to K$, $f(a_i) = b_i$ za $i = 1,\ldots,n$. Bralcu prepuščamo, da preveri, da sta φ in ψ vzajemno inverzni preslikavi. S tem smo dokazali:

$$|[K^N]_N| = |\overline{\mathcal{K}}(K,n)| = \binom{k+n-1}{n}.$$

Preslikava $f\colon N \to K$ je injektivna, če in samo če je kratnost vsakega elementa multimnožice $\varphi([f])$ enaka 1, se pravi, natanko tedaj, ko je $\varphi([f])$ v resnici podmnožica množice K moči n. Zato je ekvivalenčnih razredov injektivnih preslikav natanko toliko kot n-elementnih podmnožic množice K.

$$|[(K^N)_s]_N| = |\binom{K}{n}| = \binom{k}{n}.$$

Število ekvivalenčnih razredov surjektivnih preslikav določimo tako, da multimnožici $\mu\colon K \to \mathbb{N}_0$, ki pripada preslikavi $f \in (K^N)_s$, priredimo multimnožico $\mu'\colon K \to \mathbb{N}_0$, $\mu'(c) = \mu(c)-1$. Opazimo, da pravilo $\mu \mapsto \mu'$ podaja bijektivno preslikavo med multimnožicami μ moči n z lastnostjo $\mu(c) \geq 1$ za vsak $c \in K$ in multimnožicami moči $n-k$. Zato je

$$|[(K^N)_s]_N| = |\{\mu\colon K \to \mathbb{N}_0; |\mu| = n, \mu \geq 1\}| = |\overline{\mathcal{K}}(K,n-k)| = \binom{n-1}{n-k}.$$

Osredotočimo se sedaj na relacijo $\sim_K$. Množico ekvivalenčnih razredov množice K^N glede na to relacijo označimo s $[K^N]_K$. Vzemimo preslikavo $f\colon N \to K$ in ji priredimo razbitje

$$\{f^{-1}(c) : c \in \mathrm{Im}(f)\}$$

množice N na $|\mathrm{Im}(f)|$ paroma disjunktnih nepraznih podmnožic. Opazimo, da poljubna ekvivalentna preslikava $g = \lambda \circ f$, $\lambda \in \mathrm{Sym}(K)$, porodi isto razbitje množice N. Zato lahko za vsak $i \in \{1,\ldots,k\}$ definiramo preslikavo, ki slika iz množice ekvivalenčnih razredov preslikav $f\colon N \to K$ z i-elementno sliko $\mathrm{Im}(f)$ v množico razbitij množice N na i nepraznih podmnožic, po pravilu $[f] \mapsto \{f^{-1}(c) : c \in \mathrm{Im}(f)\}$. Ni težko preveriti, da je ta preslikava

bijektivna. Od tod neposredno sledita formuli za število ekvivalenčnih razredov na množicah K^N in $(K^N)_s$.

Razbitje, ki pripada injektivni preslikavi, je natanko razbitje množice N na enoelementne množice. Zato je ekvivalenčni razred injektivnih funkcij en sam, če seveda kašna injketivna preslikava iz N v K obstaja – sicer je število ekvivalenčnih razredov enako 0.

Podobno razmislimo tudi situacijo v primeru relacije $\sim_{N,K}$. Tu vlogo razbitij množice N nadomestijo razbitja naravnega števila n. Podrobnosti izpuščamo. ■

6 Delovanja grup in preštevanje orbit

6.1 Permutacije

Bijektivno preslikavo iz množice Ω v množico Ω imenujemo tudi *permutacija* množice Ω. Ker lahko takšno bijektivno preslikavo enolično predstavimo z urejeno n-terico njenih, paroma različnih slik, je permutacij n-elementne množice natanko toliko kot je vseh takšnih n-teric, torej $n!$.

Množico vseh permutacij množice Ω bomo označili s $\mathrm{Sym}(\Omega)$, identično preslikavo iz Ω v Ω pa z id_Ω. Za zapis permutacij uporabljamo več različnih načinov, za nas pa bo najprimernejši *ciklični zapis permutacije*, ki ga bomo predstavili na naslednjem primeru.

Naj bo $\Omega = \{1, 2, 3, 4, 5, 6\}$ in naj bo $\pi\colon \Omega \to \Omega$ permutacija podana s

$$\pi(1) = 3,\ \pi(2) = 6,\ \pi(3) = 5,\ \pi(4) = 4,\ \pi(5) = 1,\ \pi(6) = 2.$$

Tedaj je ciklični zapis permutacije π enak

$$\pi = (1, 3, 5)(2, 6)(4).$$

Pri tem števila v prvem oklepaju beremo kot: "1 se preslika v 3, 3 se preslika v 5 in 5 se preslika v 1". Drugi oklepaj bi pomenil: "2 se preslika v 6 in 6 se preslika v 2". Zadnji oklepaj pa se bere kot: "4 se preslika v 4". Pri tem posameznim "oklepajem" rečemo *cikli permutacije*, številu elementov v posameznem oklepaju pa *dolžina cikla*.

Seveda ciklični zapis permutacije ni enolično določen: permutacijo π bi prav tako lahko zapisali na naslednje načine:

$$\pi = (5, 1, 3)(2, 6)(4) = (3, 5, 1)(6, 2)(4) = (6, 2)(3, 5, 1)(4) = (6, 2)(4)(3, 5, 1).$$

Kratek premislek pokaže, da lahko permutacijo π zapišemo v ciklični obliki na $(3 \cdot 2) \cdot 3! = 18$ načinov.

Kadar je iz konteksta razvidno, katere elemente permutacija permutira, cikle dolžine 1 iz cikličnega zapisa permutacije navadno izpuščamo. Tako je običajnejši zapis permutacije π naslednji:

$$\pi = (1, 3, 5)(2, 6).$$

Domenimo se še, da bomo sliko $\pi(x)$ elementa x pri permutaciji π označavali v "eksponenti" obliki:' x^π.

6.2 Množenje permutacij in simetrična grupa

Naj bo Ω končna množica, in $\mathrm{Sym}(\Omega)$ množica vseh permutacij množice Ω. Obstajata dva standardna načina, kako definirati množenje na $\mathrm{Sym}(\Omega)$:

Ker so permutacije preslikave, jih lahko *komponiramo*, kot smo to vajeni pri preslikavah. Na primer, če je $\Omega = \{1,2,3,4,5\}$, $g = (1,3,4)(2,5)$ in $h = (2,4,5)$, potem je

$$g \circ h = (1,3,4,2) \quad \text{in} \quad h \circ g = (1,3,5,4).$$

Poleg operacije komponiranja $\circ\colon \mathrm{Sym}(\Omega)\times\mathrm{Sym}(\Omega) \to \mathrm{Sym}(\Omega)$, $\circ\colon (g,h) \mapsto g\circ h$ pa lahko na množici $\mathrm{Sym}(\Omega)$ definiramo še binarno operacijo imenovano *komponiranje z desne*:

$$\cdot : \mathrm{Sym}(\Omega) \times \mathrm{Sym}(\Omega) \to \mathrm{Sym}(\Omega), \qquad \cdot : (g,h) \mapsto h \circ g.$$

Medtem ko je navadno komponiranje uglašeno z običajnim zapisom permutacij, saj velja $(g \circ h)(\alpha) = g(h(\alpha))$, pa je desno komponiranje uglašeno z eksponentnim zapisom permutacij, saj je

$$\alpha^{(g\cdot h)} = (\alpha^g)^h, \quad \text{vendar} \quad (g \cdot h)(\alpha) = (h(g(\alpha)).$$

Operacijama $\circ$ in $\cdot$ rečemo tudi *levo množenje* in *desno množenje* permutacij.

Vaja. Preveri:

- $(1,4,3)(2,5) \circ (1,2)(4,5) = (1,5,3)(2,4)$.
- $(1,4,3)(2,5) \cdot (1,2)(4,5) = (1,5)(2,4,3)$.
- $(1,3,5) \cdot (2,4) = (1,3,5)(2,4) = (1,3,5) \circ (2,4)$.
- $(1,3,4) \cdot (4,5) \neq (1,3,4) \circ (4,5)$.

Ker za vsako permutacijo $g \in \mathrm{Sym}(\Omega)$ velja $\mathrm{id}_\Omega \circ g = g \circ \mathrm{id}_\Omega = g$ in $\mathrm{id}_\Omega \cdot g = g \cdot \mathrm{id}_\Omega = g$ ter ker sta obe množenji (tako levo kot desno) asociativni, postane množica $\mathrm{Sym}(\Omega)$, skupaj z vsako od njiju, grupa, v kateri vlogo enote igra permutacija id_Ω.

Definicija 6.1 *Grupi* $(Sym(\Omega), \circ)$ *in* $(Sym(\Omega), \cdot)$ *imenujemo* leva simetrična grupa *in* desna simetrična grupa *množice* Ω *in ju označimo s simboloma* $Sym_L(\Omega)$ *in* $Sym_D(\Omega)$.

Ker smo se odločili za eksponentni zapis permutacij, nam bosta ljubša desno množenje in desna simetrična grupa. Zato bomo grupo $\mathrm{Sym}_D(\Omega)$ označevali kar z S_Ω, pikico pri desnem množenju pa, kot je to običajno, izpuščali.

Podgrupi grupe S_Ω rečemo *permutacijska grupa* na množici Ω.

6.3 Delovanja grup

Dve permutaciji na množici Ω predstavljata isti element grupe $\mathrm{Sym}(\Omega)$ natanko tedaj, ko elemente slikata na enak način. V kombinatoriki pa je velikokrat smiselno opazovati grupe, katerih elementi sicer permutirajo množico Ω, vendar tako, da smeta dva, sicer različna elementa grupe "delovati" na množici Ω na enak način. Da bomo lahko obravnavali tudi takšne situacije, vpeljimo pojem "delovanja grupe".

Naj bo G grupa in Ω množica. Delovanje grupe G na množici Ω je poljubna preslikava

$$\Phi\colon \Omega \times G \to \Omega, \qquad (\omega, g) \mapsto \omega^g,$$

ki zadošča pogojema:

- $\omega^1 = \omega$ za vse $\omega \in \Omega$;
- $\omega^{(gh)} = (\omega^g)^h$ za vse $\omega \in \Omega$ in $g, h \in G$.

Delovanje grupe G na Ω pa lahko opišemo tudi kot homomorfizem iz G v simetrično grupo S_Ω na naslednji način. Naj bo $\Phi\colon \Omega \times G \to \Omega$ delovanje. Definirajmo preslikavo

$$\bar{\Phi}\colon G \to S_\Omega, \qquad \bar{\Phi}(g) = (\omega \mapsto \omega^g).$$

Ni se težko prepričati, da je $\bar{\Phi}$ je homomorfizm group

Obratno, naj bo $\Psi\colon G \to S_\Omega$ poljuben homomorfizem grup. Definirajmo delovanje grupe G na Ω:

$$\bar{\Psi}\colon \Omega \times G \to \Omega, \qquad (\omega, g) \mapsto \omega^{\bar{\Psi}(g)}.$$

Pri tem velja naslednje: Če pričnemo z delovanjem Φ, mu priredimo homomorfizem $\bar{\Phi}$ in temu homomorfizmu spet priredimo delovanje $\bar{\bar{\Phi}}$, dobimo natanko začetno delovanje Φ.

$$\bar{\bar{\Phi}} = \Phi.$$

To kaže na to, da lahko delovanje grup enakovredno definiramo tako, kot smo to storili v teh zapiskih, ali pa kot homomorfizem v simetrično grupo.

Če delovanje grupe G na Ω predstavimo kot homomorfizem $\Psi\colon G \to S_\Omega$, potem sliki homomorfizma Ψ rečemo *permutacijska reprezentacija* grupe G in jo označimo z G^Ω. Opazimo, da je G^Ω permutacijska grupa, ki vsebuje natanko tiste permutacije množice Ω, ki permutirajo tako, kot permutira kakšen element iz g.

Množici vseh $g \in G$, ki pribijejo vsak element množice Ω se imenuje *jedro delovanja*. Če na delovanje pogledamo kot na homomorfizem $\Psi\colon G \to S_\Omega$, potem je jedro delovanja ravno jedro homorfizma Ψ.

$$\mathrm{Ker}(\Psi) = \{g \in G : \Psi(g) = \mathrm{id}\}.$$

Iz 1. izreka o homomorfizmih iz teorije grup tedaj sledi $G^\Omega \cong G/\mathrm{Ker}(\Psi)$.

Če jedro delovanja vsebuje le nedelavni element grupe, potem je delovanje *zvesto*. Če G deluje zvesto na Ω, potem je pripadajoči homomorfizem $G \to S_\Omega$ injektiven, in zato $G^\Omega = G$. V tem smislu lahko zvesta delovanja enačimo s pripadajočimi permutacijskimi grupami.

6.4 Stabilizatorji in orbite delovanja

Naj grupa G deluje na množici Ω in naj bo ω poljuben element množice Ω. Množici

$$G_\omega = \{g \in G : \omega^g = \omega\}$$

vseh elementov grupe G, ki element ω pribijejo, rečemo *stabilizator* elementa ω v grupi G, množici slik

$$\omega^G = \{\omega^g : g \in G\}$$

pa rečemo *orbita* elementa ω pri delovanju grupe G.

Za zgled si oglejmo klasični primer iz teorije grup. Za poljubno grupo G in elementa $g, h \in G$ definirajmo

$$h^g = g^{-1}hg.$$

Z lahkoto se prepričamo, da smo s tem definirali delovanje grupe G na množici $\Omega = G$, ki ga imenujemo *delovanje grupe G na sebi s konjugacijo*. Stabilizator G_h elementa h pri tem delovanju vsebuje vse tiste elemente $g \in G$, za katere velja $g^{-1}hg = h$, torej tiste $g \in G$, ki komutirajo s h. Podobno, element $g \in G$ leži v jedru tega delovanja, če in samo če velja $g^{-1}hg = h$ za vsak $h \in H$, torej če in samo če leži g v centru grupe G. Orbite h^G imenujemo *konjugiranostni razredi elementov grupe G*.

Definiramo lahko tudi delovanje grupe G na množici $\Omega = \{H : H \leq G\}$ vseh njenih podgrup s predpisom:

$$H^g = g^{-1}Hg = \{g^{-1}hg : h \in H\}.$$

Grupi H^g pri tem rečemo konjugiranka grupe H. Stabilizator G_H podgrupe $H \in \Omega$ je enak normalizatorju grupe H v G.

TRDITEV 6.2 *Naj grupe G deluje na množici Ω. Tedaj za poljubna elementa $g \in G$ in $\omega \in \Omega$ velja*

$$G_{(\omega^g)} = (G_\omega)^g.$$

Stabilizatorja dveh elementov množice Ω, ki ležite v isti orbiti grupe G, sta torej konjugirana.

DOKAZ: Vzemimo poljuben element $h \in G$. Tedaj trditev neposredno sledi iz naslednje verige ekvivalenc:

$$h \in G_\omega \Leftrightarrow \omega^h = \omega \Leftrightarrow \omega^{gg^{-1}hg} = \omega^g \Leftrightarrow g^{-1}hg \in G_{(\omega^g)}.$$

∎

TRDITEV 6.3 *Množica orbit pri delovanju grupe G na množici Ω predstavlja razbitje množice Ω.*

DOKAZ: Ker vsak element množice ω leži v orbiti ω^G, je unija vseh orbit pri delovanju grupe G enaka Ω. Naj bosta ω^G in β^G orbiti z nepraznim presekom. Dokazati moramo, da sta tedaj enaki. Res. Naj bo $\gamma \in \omega^G \cap \beta^G$ in naj bo δ poljuben element orbite ω^G. Tedaj obstajajo elementi $g, h, t \in G$, da je $\gamma = \omega^g = \beta^h$ in $\delta = \omega^t$. Sledi $\delta = \omega^t = (\beta^{hg^{-1}})^t = \beta^{hg^{-1}t}$. S tem smo dokazali, da je $\omega^G \subseteq \beta^G$. Če zamenjamo vlogi ω in β, dokažemo vsebovanost še v drugo smer in s tem enakost orbit ω^G in β^G. Orbite pri delovanju grupe G torej res tvorijo razbitje množice Ω. ∎

TRDITEV 6.4 *Naj grupa G deluje na množici Ω in naj bo ω poljuben element množice Ω. Tedaj velja enakost*

$$|G_\omega|\,|\omega^G| \;=\; |G|.$$

DOKAZ: Označimo z $G(\omega \mapsto \beta)$ množico elementov grupe G, ki preslikajo točko ω v izbrano točko β množice Ω. Če β ni element orbite ω^G, potem je množica $G(\omega \mapsto \beta)$ prazna. Predpostavimo sedaj, da je $\beta \in \omega^G$, izberimo element $g \in G(\omega \mapsto \beta)$ in definirajmo preslikavo $f\colon G(\omega \mapsto \beta) \to G$ s predpisom $f(h) = hg^{-1}$. Z lahkoto se prepričamo, da je preslikava f injektivna in da je njena slika enaka stabilizatorju G_ω. Zato je moč množice $G(\omega \mapsto \beta)$ enaka redu stabilizatorja G_ω, brž ko β pripada orbiti ω^G, in je enaka 0, če leži β zunaj ω^G.

Seštejemo sedaj moči množic $G(\omega \mapsto \beta)$ po vseh $\beta \in \Omega$ in vsoto označimo z S. K vsoti S prispevajo le tisti elementi β, ki ležijo v orbiti ω^G – vsak

takšen natanko $|G_\omega|$. Zato je ta vsota enaka $|G_\omega|\,|\omega^G|$. Po drugo strani pa vsak element g grupe G leži v natanko eni množici $G(\omega \mapsto \beta)$, namreč tisti pri kateri je $\beta = \omega^g$. Zato je vsota S enaka tudi $|G|$. S tem je dokaz končan. ∎

OPOMBA. Prijemu, ki smo ga uporabili v zgornjem dokazu, v kombinatoriki pogosto rečemo *računovodsko pravilo* (angl. *counting principle*). Računovodsko pravilo pravi, da je vsota elementov dane matrike enaka tako vsoti njenih vrstičnih vsot kot tudi vsoti njenih stolpčnih vsot. Pravilo lahko v zgornjem dokazu uporabimo na sledeč način: Definiramo matriko, katere vrstice so indeksirane z elementi množice Ω, stolpci z elementi grupe G, na presečišču vrstice $\beta \in \Omega$ ter stolpca $g \in G$ pa stoji 0 ali 1, odvisno od tega ali je $g \in G(\omega \mapsto \beta)$ ali ne. Vrstična vsota pri elementu $\beta \in \Omega$ je tedaj enaka $|G(\omega \mapsto \beta)|$, vse stolpčne vsote pa so enake 1.

DEFINICIJA 6.5 *Delovanje grupe G na množici Ω je* tranzitivno, *če je $\omega^G = \Omega$ za nek (in tedaj vsak) $\omega \in \Omega$.*

6.5 Preštevanje orbit in Cauchy-Frobeniusova lema

Pri preštevanju kombinatoričnih objektov nam je velikokrat v pomoč preprosta, vendar uporabna formula za izračun števila orbit grupe, ki se v literaturi pogosto pojavlja z imenom *Burnsidova lema*, ali pa (zgodovinsko pravilneje) *Cauchy-Frobeniusova lema*. Poglejmo, kaj pravi.

IZREK 6.6 (Cauchy-Frobeniusova lema) *Naj grupa G deluje na množici Ω in naj m označuje število orbit tega delovanja. Za element $g \in G$ naj $Fix(g) = \{\omega : \omega^g = \omega\}$ predstavlja množico elementov Ω, ki jih element g pribije. Tedaj velja enakost*

$$m|G| = \sum_{g \in G} |Fix(g)|.$$

DOKAZ: Naj bodo $\Omega_1, \ldots, \Omega_m$ orbite delovanja grupe G na Ω. Oglejmo si množico

$$\mathcal{M} = \{(a, g) : a \in \Omega, g \in G_a\}$$

in preštejmo njene elemente na dva načina. Najprej opazimo, da je moč množice $\mathcal{M}$ enaka vsoti moči stabilizatorjev G_a po vseh $a \in \Omega$. Vemo tudi, da je moč stabilizatoja $|G_a|$ enaka $|G|/|\Omega_i|$, kjer je Ω_i tista orbita, ki vsebuje element a. Zato

$$|\mathcal{M}| = \sum_{a \in \Omega} |G_a| = \sum_{i=1}^{m} \sum_{a \in \Omega_i} \frac{|G|}{|\Omega_i|} = \sum_{i=1}^{m} |G| = m|G|.$$

Po drugi strani pa lahko elemente množice $\mathcal{M}$ preštejemo tako, da seštejemo moči množic

$$\mathcal{M}_g = \{(a, g) : a \in \Omega, g \in G_a\} = \{(a, g) : a \in \mathrm{Fix}(g)\}.$$

Zato

$$|\mathcal{M}| = \sum_{g \in G} |\mathcal{M}_g| = \sum_{g \in G} |\mathrm{Fix}(g)|.$$

S tem je izrek dokazan. ∎

6.6 Delovanje grupe na funkcijah

Pričnimo z zgledom. Oglišča pravilnega šestkotnika bi radi pobarvali s tremi barvami: belo, rdečo in modro. Na koliko načinov lahko to storimo, če štejemo dve barvanji kot enaki, brž ko lahko iz enega preidemo v drugega s pomočjo vrtenja šestkotnika okoli njegovega središča?

Prevedimo nalogo v matematični jezik. Označimo oglišča šestkotnika s števili $1, \ldots, 6$, začenši z 1 in nadaljujoč v pozitivni smeri z 2, 3 itd. Barvanje šestkotnika si lahko predstavljamo kot funkcijo iz množice oglišč $N = \{1, \ldots, 6\}$ v množico barv $K = \{\mathrm{B}, \mathrm{R}, \mathrm{M}\}$.

Naj bo G grupa vrtenj šestkotnika, predstavljena kot permutacijska grupa na množici oglišč. Če barvanje $\varphi\colon N \to K$ "zavrtimo" z rotacijo $g \in G$, potem dobimo načeloma drugačno barvanje $\varphi^g\colon N \to K$ določeno s pravilom $\varphi^g(a) = \varphi(a^{g^{-1}})$. Dve barvanji $\varphi_1, \varphi_2\colon N \to K$ sta torej "enaki", če obstaja permutacija $g \in G$, za katero je $\varphi_2 = {\varphi_1}^g$. Ni težko videti, da je preslikava $K^N \times G \to K^N$, $(\varphi, g) \mapsto \varphi^g$, delovanje grupe G na množici K^N. Iz zgoraj povedanega sledi, da sta dve barvanji šestkotnika "enaki" natanko tedaj, ko sta v isti orbiti tega delovanja. Če želimo rešiti zastavljeno nalogo, moramo torej prešteti število orbit induciranega delovanja grupe G na K^N. Odgovor ponuja naslednja posledica Cauchy-Frobeniusove leme.

IZREK 6.7 *Naj bosta N in K končni množici in naj končna grupa G deluje na množici N. Za vsak $g \in G$ naj $c(g)$ označuje število orbit grupe $\langle g \rangle$ na množici N. Tedaj je število orbit delovanja grupe G pri njenem naravnem delovanju na množici preslikav K^N enako*

$$\frac{1}{|G|} \sum_{g \in G} |K|^{c(g)}.$$

Dokaz: Spomnimo se, da grupa G deluje na množici K^N funkcij iz N v K v skladu z naslednjim predpisom:

$$\varphi^g(a) = \varphi(a^{g^{-1}}),\ \varphi \in K^N,\ g \in G,\ a \in N.$$

Ni težko videti, da element $g \in G$ pribije funkcijo $\varphi\colon N \to K$ natanko tedaj, ko je φ konstantna na vsaki orbiti grupe $\langle g\rangle$. Takšna funkcija je enolično določena z naborom $c(g)$ elementov iz K. Zato je funkcij, ki so konstantne na vsaki orbiti grupe $\langle g\rangle$ natanko $|K|^{c(g)}$. Z drugimi besedami, $\mathrm{Fix}(g) = |K|^{c(g)}$. Če označimo število orbit grupe G na K^N z m in uporabimo Cauchy-Frobeniusovo lemo (Izrek 6.6), dobimo

$$m|G| = \sum_{g\in G} \mathrm{Fix}(g) = \sum_{g\in G} |K|^{c(g)}.$$

Zgornjo enakost delimo z $|G|$ in dobimo enakost, ki jo dokazujemo. ∎

Vrnimo se k nalogi o barvanju oglišč pravilnega šestkotnika. Grupa G vrtenj šestkotnika vsebuje naslednje permutacije:

$$\mathrm{id},\ s = (1,2,3,4,5,6),\ s^2 = (1,3,5)(2,4,6),$$

$$s^3 = (1,4)(2,5)(3,6),\ s^4 = (1,5,3)(2,6,4),\ s^5 = (1,6,5,4,3,2),$$

ki imajo naslednje število orbit:

$$c(\mathrm{id}) = 6,\ c(s) = 1,\ c(s^2) = 2,\ c(s^3) = 3,\ c(s^4) = 2,\ c(s^5) = 1.$$

Zato je iskano število različnih barvanj pravilnega šestkotnika z dvema barvama enako:

$$\frac{1}{6}(3^6 + 3^1 + 3^2 + 3^3 + 3^2 + 3^1) = 130.$$

6.7 Ciklični indeks delovanja grupe

Nalogo o barvanju oglišč pravilnega šestkotnika s tremi barvami lahko nekoliko otežimo in vprašamo, koliko izmed 130 barvanj je takšnih, da so natanko 3 oglišča bela, 2 oglišči rdeči in 1 oglišče modro. Pri tem barvanj, ki so v isti orbiti delovanja grupe vrtenj šestkotnika še vedno ne ločimo med seboj. Na tovrstna vprašanja nam odgovarja *teorija Pólya in Redfielda*. Pričnimo s pojmom, ki na videz nima velike zveze z našo nalogo.

Naj grupa G deluje na množici N. Vzemimo poljuben element $g \in G$ in s $k_i(g)$, $i = 1,\ldots,n$, označimo število orbit grupe $\langle g\rangle$ dolžine i. Če je $\bar{g}$ permutacija množice N, porojena z delovanjem elementa g, tedaj $k_i(g)$

ustreza številu ciklov dolžine i v cikličnem zapisu permutacije $\bar{g}$. Zato n-terici $(k_1(g), k_2(g), \ldots, k_n(g))$ rečemo *ciklična struktura* elementa g.

Elementu $g \in G$ s ciklično strukturo $(k_1, k_2, \ldots, k_n)$ priredimo element $z_g(x_1, \ldots, x_n) = {x_1}^{k_1} {x_2}^{k_2} \cdots {x_n}^{k_n}$ kolobarja $\mathbb{Q}[x_1, x_2, \ldots, x_n]$.

Vsoto

$$Z_G(x_1, \ldots, x_n) = \frac{1}{|G|} \sum_{g \in G} z_g(x_1, \ldots, x_n)$$

imenujemo *ciklični indeks* delovanja grupe G.

Zgled. *Izračunaj ciklični indeks naravnega delovanja ciklične grupe C_6 na množici $\{1, 2, 3, 4, 5, 6\}$.*

REŠITEV: Sestavimo tabelo elementov grupe C_6 in njihovih cikličnih struktur:

g	cikl. strukt.	$z_g(x_1, x_2, x_3, x_4, x_5, x_6)$
id	$(6, 0, 0, 0, 0, 0)$	${x_1}^6$
$(1, 2, 3, 4, 5, 6)$	$(0, 0, 0, 0, 0, 1)$	x_6
$(1, 3, 5)(2, 4, 6)$	$(0, 0, 2, 0, 0, 0)$	${x_3}^2$
$(1, 4)(2, 5)(3, 6)$	$(0, 0, 0, 3, 0, 0)$	${x_2}^3$
$(1, 5, 3)(2, 6, 4)$	$(0, 0, 2, 0, 0, 0)$	${x_3}^2$
$(1, 6, 5, 4, 3, 2)$	$(0, 0, 0, 0, 0, 1)$	x_6

Ciklični indeks grupe A_4 lahko prečitamo iz zadnjega stolpca:

$$Z_{C_6}(x_1, x_2, x_3, x_4, x_5, x_6) = \frac{1}{6}\left({x_1}^6 + {x_2}^3 + 2{x_3}^2 + 2x_6\right).$$

■

6.8 Izrek Redfielda in Pólya

Zvezo med cikličnim indeksom delovanja in številom neekvivalentnih barvanj s predpisanim številom objektov dane barve podaja *izrek Redfielda in Pólya*.

IZREK 6.8 *(Redfield 1927, Pólya 1937) Naj grupa G deluje na množici N moči n in naj bo $K = \{c_1, \ldots, c_k\}$ poljubna množica moči k. Ciklični indeks delovanja grupa G na množici N označimo z $Z_G(x_1, \ldots, x_n)$. Definirajmo polinom*

$$p(t_1, \ldots, t_k) = Z_G(\sum_{i=1}^{k} t_i, \sum_{i=1}^{k} t_i^2, \ldots, \sum_{i=1}^{k} t_i^n) \in \mathbb{Q}[t_1, \ldots, t_k].$$

Tedaj je koeficient v polinomu p pri monomu $t_1^{\alpha_1} t_2^{\alpha_2} \cdots t_k^{\alpha_k}$ enak številu tistih orbit φ^G induciranega delovanja grupe G na množici preslikav K^N, za katere je $\varphi^{-1}(c_i) = \alpha_i$ za vsak $i \in \{1, \ldots, k\}$.

S pomočjo zgornjega izreka rešimo nalogo z začetka razdelka takole. V ciklični indeks ciklične grupe C_6 vstavimo namesto nedoločenke x_i, $i = 1, \ldots, 6$, vsoto ${t_1}^i + {t_2}^i + {t_3}^i$. Dobimo:

$$\frac{1}{6}\big({x_1}^6 + {x_2}^3 + 2{x_3}^2 + 2x_6\big) =$$

$$\frac{1}{6}\big((t_1 + t_2 + t_3)^6 + (t_1^2 + t_2^2 + t_3^2)^3 + 2(t_1^3 + t_2^3 + t_3^3)^2 + 2(t_1^6 + t_2^6 + t_3^6)\big) =$$

Zanima nas koeficient pri monomu $t_1^3 t_2^2 t_3$. Le-ta se pojavi le pri členu $(t_1 + t_2 + t_3)^6$ in tu s koeficientom

$$\binom{6}{3, 2, 1} = \frac{6!}{3! \cdot 2!} = 60.$$

Iskano število neekvivalentnih barvanj je torej enako $\frac{60}{6} = 10$.

7 Rekurzivne enačbe

OPOMBA. Zapiski teh predavanj so nekoliko zgoščeni. Pomagate si lahko tudi z razlago v [3].

7.1 Fibonaccijevo zaporedje

Oglejmo si dobro znani zgled zaporedja števil $F_0, F_1, F_2, \ldots$, ki je definirano rekurzivno s predpisom

$$F_0 = 0,\ F_1 = 1,\ F_{n+2} = F_{n+1} + F_n \text{ za vse } n \in \mathbb{N}_0.$$

tako definirano zaporedje imenujemo *Fibonaccijevo zaporedje*, število F_n pa n-to Fibonaccijevo število. Tip vprašanja, s katerim se bomo ukvarjali v tem razdelku, je, kako izračunati n-to Fibonaccijevo število, ne da bi pred tem izračunali vsa predhodna Fibonaccijeva števila.

Zgornjo nalogo lahko nekoliko posplošimo. Naj bodo $c_0, \ldots, c_d$ poljubna kompleksna števila in naj bo $f\colon \mathbb{N}_0 \to \mathbb{C}$ poljubna funkcija. Iščemo zaporedje kompleksnih števil $a_0, a_1, a_2, \ldots$, katerega prvih d členov je enakih v naprej predpisanim vrednostim $b_0, \ldots, b_{d-1} \in \mathbb{C}$,

$$a_0 = b_0,\ a_1 = b_1,\ \ldots,\ a_{d-1} = b_{d-1} \tag{1}$$

in ki za vsak $n \in \mathbb{N}_0$ zadošča enakosti

$$c_d a_{n+d} + c_{d-1} a_{n+d-1} + \ldots + c_1 a_{n+1} + c_0 a_n = f(n) \tag{2}$$

Pri tem bomo predpostavili, da je $c_0, c_d \neq 0$, saj bi sicer lahko s preoštevilčenjem dobili enakost istega tipa, vendar z manj členi na levi strani enakosti. Z deljenjem z vodilnim koeficientom c_d lahko predpostavimo celo, da je $c_d = 1$.

Izrazu (2) rečemo *linearna rekurzivna enačba s konstantnimi koeficienti*, enakostim (1) pa *začetni pogoji enačbe* (1). Če je funkcija $f(n)$ na desni strani enakosti konstantno enaka nič, pristavimo še besedico *homogena*. Neznanka v enačbi (2) je simbol $(a_n)_{n\in\mathbb{N}_0}$, ki predstavlja neznano zaporedje (in ne neznano število, kot smo vajeni pri običajnih enačbah iz srednješolske matematike).

Linearno rekurzivno enačbo s konstantnimi koeficienti lahko rešujemo s pomočjo linearne algebre, in sicer v kontekstu vektorskega prostora vseh zaporedij, ki si ga bomo ogledali v naslednjem razdelku.

7.2 Prostor zaporedij

Naj bo $\mathbb{F}$ poljuben obseg. Preslikavi

$$a\colon \mathbb{N}_0 \to \mathbb{F}$$

rečemo *zaporedje* s členi v obsegu $\mathbb{F}$. Vrednosti $a(n)$, $n \in \mathbb{N}_0$, rečemo *člen zaporedja* in ga navadno označimo z a_n. Zaporedje a pa navadno označimo s simbolom $(a_n)_{\mathbb{N}_0}$, včasih pa tudi površno s simbolom $(a_1, a_2, a_3, \ldots)$. Množico vseh zaporedij s členi v $\mathbb{F}$ označimo z $\mathbb{F}^{\mathbb{N}_0}$.

Če množico $\mathbb{F}^{\mathbb{N}_0}$ opremimo z operacijami seštevanja, množenja in množenja s skalarjem po komponentah, dobimo algebrsko strukturo, ki zadošča aksiomom algebre. Mi se bomo v nadaljevanju omejili na operaciji seštevanja in množenja s skalarjem, ter tako na množico $\mathbb{F}^{\mathbb{N}_0}$ gledali kot na vektorski prostor.

Spomnimo se, da za vsak vektorski prostor V nad obsegom $\mathbb{F}$ množico vseh linearnih preslikav iz V v V označimo z $\mathrm{End}(V)$. Če množico $\mathrm{End}(V)$ opremimo z operacijama seštevanja in množenja s skalarjem po komponentah, dobimo vektorski prostor. Če pa na množici $\mathrm{End}(V)$ definiramo še množenje kot komponiranje preslikav, postane vektorski prostor $\mathrm{End}(V)$ algebra. Nas bo še posebej zanimal element množice $\mathrm{End}(V)$, ki mu rečemo *preslikava pomika* in je definiran s predpisom:

$$E\colon \mathbb{F}^{\mathbb{N}_0} \to \mathbb{F}^{\mathbb{N}_0}, \quad E(a_0, a_1, a_2, \ldots) = (a_1, a_2, a_3, \ldots).$$

7.3 Linearne rekurzivne enačbe s konstantnimi koeficienti

Oglejmo si sedaj, v kakšni zvezi so linearne rekurzivne enačbe s prostorom zaporedij in endomorfizmi nad njimi. Naj bo

$$Q(x) = x^d + c_{d-1}x^{d-1} + \ldots + c_1 x + c_0, \quad c_0 \neq 0,$$

polinom s koeficineti v obsegu $\mathbb{F}$. Če namesto nedoločenke x vstavimo preslikavo E, dobimo nov element algebre $\mathrm{End}(\mathbb{F}^{\mathbb{N}_0})$. Oglejmo si, kdaj je neko zaporedje $(a_n)_{n\in\mathbb{N}_0}$ v njegovem jedru. Opazimo, da velja naslednje:

$$(a_n)_{n\in\mathbb{N}_0} \in \mathrm{Ker}(Q(E)) \Leftrightarrow \ldots \Leftrightarrow$$

$$a_{n+d} + c_{d-1}a_{n+d-1} + \ldots + c_1 a_{n+1} + c_0 a_n = 0 \text{ za vsak } n \in \mathbb{N}_0. \qquad (3)$$

Ugotovili smo, da je jedro endomorfizma $Q(E)$ natanko množica vseh rešitev enačbe (3). Polinomu $Q(x)$ pri tem rečemo *karakteristični polinom* enačbe (3).

Pričnimo z reševanjem homogene enačbe (3). V nadaljevanju bomo predpostavili, da je $\mathbb{F} = \mathbb{C}$. Če želimo enačbo rešiti, moramo poiskati jedro endomorfizma $Q(E)$.

Karakteristični polinom $Q(x)$ najprej razcepimo na linearne faktorje:

$$Q(x) = (x - \lambda_1)^{s_1} \cdots (x - \lambda_k)^{s_k}.$$

Iz linearne algebre se spomnimo naslednjega izreka.

IZREK 7.1 *Če sta $p(x)$ in $q(x)$ tuja polinoma in je A endomorfizem vektorskega prostora V, potem je jedro endomorfizma $p(A)q(A)$ enako direktni vsoti jeder endomorfizmov $p(A)$ in $q(A)$.*

Z indukcijo lahko zgornji izrek posplošimo na poljubno število paroma tujih polinomov. Iz tega sledi naslednje:

$$\mathrm{Ker}(Q(E)) = \mathrm{Ker}((E - \lambda_1 I)^{s_1}) \oplus \ldots \oplus \mathrm{Ker}((E - \lambda_k I)^{s_k})$$

Zadošča torej, da ugotovimo, kaj je jedro $K = \mathrm{Ker}((E-\lambda I)^s)$ za poljuben $\lambda \neq 0$ in $s \in \mathbb{N}$. Premislimo najprej, da je razsežnost takšnega jedra enaka s. V resnici dokažemo nekoliko splošnejšo trditev.

TRDITEV 7.2 *Naj bo $p(x) = x^s + \ldots + c_1 x + c_0$ poljuben polinom stopnje s. Tedaj je razsežnost jedra $Ker(p(E))$ enaka s.*

DOKAZ: Definirajmo preslikavo

$$\Phi\colon \mathrm{Ker}(p(E)) \to \mathbb{F}^s, \quad (a_n)_{n\in\mathbb{N}_0} \mapsto (a_0, a_1, \ldots, a_{s-1}).$$

Ta preslikava je očitno linearna in injektivna. Je pa tudi surjektivna, saj lahko za vsak nabor začetnih členov $a_0, \ldots, a_{s-1}$ iz enakosti

$$a_{n+s} = -c_{s-1}a_{n+s-1} - \ldots - c_0 a_n$$

rekurzivno izračunamo člene $a_s, a_{s+1}, \ldots$, za katere bo zaporedje $(a_n)_{n\in\mathbb{N}_0}$ ležalo v jedru operatorja $p(E)$. Vektorska prostora $\mathrm{Ker}(p(E))$ in $\mathbb{F}^s$ sta torej izomorfna. S tem je trditev dokazana. ∎

Zdaj vemo, da je razsežnost jedra K enaka s. Zadošča torej najti s linearno neodvisnih zaporedij iz K. Z neposrednim računom se prepričamo, da zaporedja

$$(\lambda^n)_{n\in\mathbb{N}_0},\ (n\lambda^n)_{n\in\mathbb{N}_0},\ (n^2\lambda^n)_{n\in\mathbb{N}_0},\ \ldots,\ (n^{s-1}\lambda^n)_{n\in\mathbb{N}_0}$$

ležijo v jedru K, in ker so očitno linearno neodvisna, tvorijo njegovo bazo. Vsako zaporedju v jedru K je torej neka linearna kombinacija zgornjih zaporedij. Če so $\alpha_0, \ldots, \alpha_{s-1}$ koeficienti takšne linearne kombinacije, ima ustrezno zaporedje obliko $(A(n)\lambda^n)_{n\in\mathbb{N}_0}$, kjer je

$$A(n) = \alpha_0 + \alpha_1 n + \ldots + \alpha_{s-1} n^{s-1}.$$

S tem smo dokazali:

Trditev 7.3 *Zaporedje leži v jedru operatorja $(E - \lambda I)^s$, če in samo če je oblike $(A(n)\lambda^n)_{n\in\mathbb{N}_0}$, kjer je $A(n)$ kak polinom stopnje največ $s-1$.*

Če povzamemo vse do sedaj povedano, ugotovimo, da se splošna rešitev homogene enačbe (3) glasi:

$$a_n = A_1(n)\lambda_1^n + A_2(n)\lambda_2^n + \ldots + A_k(n)\lambda_k^n,$$

kjer je $A_i(n)$ poljuben polinom stopnje največ $s_i - 1$.

7.4 Linearne nehomogene enačbe s konstantnimi koeficienti

Splošna rešitev nehomogene enačbe

$$c_d a_{n+d} + c_{d-1} a_{n+d-1} + \ldots + c_0 a_n = f(n)$$

ima obliko

$$a_n = z_n + b_n\,,$$

kjer je b_n kaka (imenujmo jo posebna) rešitev zgornje enačbe in z_n rešitev pripadajoče homogene enačbe

$$c_d z_{n+d} + c_{d-1} z_{n+d-1} + \ldots + c_0 z_n = 0\,.$$

Kadar je funkcija $f(n)$ oblike

$$f(n) = p(n)\alpha^n\,, \qquad (*)$$

kjer je $p(n)$ polinom stopnje r in α s-kratna ničla karakterističnega polinoma $Q(x)$ (lahko je tudi $s = 0$), rešitev b_n poiščemo z nastavkom

$$b_n = n^s P(n)\alpha^n\,,$$

kjer je $P(n)$ polinom stopnje r z nedoločenimi koeficienti.

Kadar je nehomogeni del $f(n)$ enak vsoti funkcij oblike $(*)$, $f(n) = f_1(n) + f_2(n) + \ldots + f_k(n)$, je posebna rešitev b_n vsota posebnih rešitev nehomogenih enačb $c_d a_{n+d} + c_{d-1} a_{n+d-1} + \ldots + c_0 a_n = f_i(n)$, $1 \le i \le k$.

Zgled. *Poišči splošno rešitev rekurzivne enačbe*

$$a_{n+2} - 2a_{n+1} + a_n = 3n + 1\,.$$

REŠITEV: Karakteristični polinom $Q(x) = (x-1)^2$ ima $\alpha = 1$ za dvojno ničlo. Zato posebno rešitev b_n poiščemo z nastavkom $b_n = n^2(An + B)1^n$. Nastavek vstavimo v enačbo in dobimo

$$A(n+2)^3 + B(n+2)^2 - 2A(n+1)^3 - 2B(n+1)^2 + An^3 + Bn^2 = 3n + 1\,.$$

Odpravimo oklepaje in primerjamo koeficiente pri potencah n. Dobimo sistem linearnih enačb za koeficienta A in B:

$$\begin{aligned} 6A &= 3\,, \\ 2B + 6A &= 1\,. \end{aligned}$$

Sistem rešimo in dobimo posebno rešitev $b_n = \frac{1}{2}n^3 - n^2$. Rešimo še pripadajočo homogeno enačbo, rešitev je $z_n = C + Dn$, ter obe rešitvi seštejemo: $a_n = C + Dn - n^2 + \frac{1}{2}n^3$. ∎

8 Osnovno o grafih

Opomba. Ta razdelek v veliki meri sledi prvemu poglavju knjige [3].

8.1 Definicija in osnovni pojmi

Naj bo V (običajno končna) neprazna množica in E poljubna družina dvoelementnih podmnožic množice V. Paru $\Gamma = (V, E)$ pravimo *graf* na *množici točk* (tudi *vozlišč*) $V = V(\Gamma)$ in z *množico povezav* $E = E(\Gamma)$. Če je $\{u, v\}$ povezava grafa Γ, tedaj pravimo, da sta točki u in v *sosednji* in pišemo $u \sim v$. Hkrati pravimo, da sta točki u in v krajišči povezave $\{u, v\}$. Povezavo $\{u, v\}$ včasih pišemo krajše kot uv ali vu.

Opomba. Včasih dopuščamo tudi grafe, ki imajo med nekaterimi pari točk več povezav (*vzporedne povezave*) ali pa imajo povezave, ki imajo obe krajišči enaki (*zanke*). Takim grafom bomo rekli *multigrafi*. Če definiramo, da zanka prispeva 2 k stopnji točke, potem lema 8.1 velja tudi za multigrafe. Kadar želimo poudariti, da govorimo o (multi)grafih brez zank in vzporednih povezav, takim grafom rečemo *enostavni grafi*.

Poleg multigrafov je grafom sorodna stuktura *usmerjeni graf*. Neformalno si ga lahko predstavljamo kot graf (ali celo kot multigraf), kjer vsako povezavo usmerimo. Namesto krajišč povezave v tem primeru govorimo kot o začetku in koncu povezave (repu in glavi povezave). Če je u rep in v glava povezave uv, potem napišemo $u \to v$ in rečemo, da je uv usmerjena povezava grafa Γ.

Grafe si radi tudi narišemo. To storimo tako, da vozlišča grafa predstavimo kot točke ravnine, povezavo med sosednjima vozliščema pa kot krivuljo (običajno kar kot daljico) s krajiščema v točkah ravnine, ki ustrezata krajiščema povezave.

Stopnja točke (tudi *valenca točke*) u v grafu Γ, označimo jo z $\deg_\Gamma(u)$, je enaka številu povezav grafa Γ, ki imajo točko u za svoje krajišče. Točkam stopnje 0 pravimo *izolirane točke*. Graf Γ je *regularen*, če obstaja tako število k, da velja $\deg_\Gamma(u) = k$ za vsak $u \in V(\Gamma)$. V tem primeru rečemo tudi, da je graf Γ k-regularen, oziroma, da je regularen stopnje k.

Stopnje točk in število povezav grafa veže naslednja enakost:

Lema 8.1 (O rokovanju). *Za vsak graf Γ velja*

$$\sum_{v \in V(\Gamma)} deg(v) = 2 \cdot |E(\Gamma)| .$$

DOKAZ: Uporabili bomo tako imenovano računovodsko pravilo. Naj bo $\mathcal{M}$ množica vseh urejenih parov $(u, e) \in V(\Gamma) \times E(\Gamma)$, za katere je u krajišče povezave e. Preštejmo elemente množice $\mathcal{M}$. Po eni strani velja

$$|\mathcal{M}| = \sum_{u \in V(\Gamma)} \deg(u),$$

po drugi strani pa

$$|\mathcal{M}| = \sum_{e \in E(\Gamma)} 2 = 2 \cdot |E(\Gamma)|.$$

S tem je trditev dokazana. ∎

POSLEDICA 8.2 *Vsak graf ima sodo mnogo točk lihe stopnje.*

OPOMBA. V usmerjenih grafih namesto stopnje $\deg(v)$ definiramo *vhodno stopnjo* $\deg^-(v)$ in *izhodno stopnjo* $\deg^+(v)$ točke v, pri čemer prva predstavlja število točk u grafa Γ, za katere je uv usmerjena povezava grafa Γ, druga pa število točk u grafa Γ, za katere je vu usmerjena povezava grafa Γ. V kontekstu grafov lema o rokovanju preide v enakost

$$\sum_{v \in V(\Gamma)} \deg^-(v) = \sum_{v \in V(\Gamma)} \deg^+(v) = |E|.$$

Graf Γ' je *podgraf* grafa Γ, če velja $V(\Gamma') \subseteq V(\Gamma)$ in $E(\Gamma') \subseteq E(\Gamma)$. Podgraf Γ' je *vpet*, če velja $V(\Gamma') = V(\Gamma)$, in je *induciran* z množico točk $U \subseteq V(\Gamma)$, če velja $V(\Gamma') = U$ in $E(\Gamma') = \{uv \in E(\Gamma) \mid u, v \in V(\Gamma')\}$. V tem primeru pišemo tudi $\Gamma' = \Gamma[U]$.

Graf Γ je *dvodelen*, če lahko množico točk $V(\Gamma)$ zapišemo kot disjunktno unijo dveh podmnožic $A, B \subseteq V(\Gamma)$ tako, da je za vsako povezavo $uv \in E(\Gamma)$ ena od točk u, v vsebovana v množici A, druga pa v množici B. Množici A in B imenujemo množici *dvodelnega razbitja* grafa Γ.

8.2 Metrične lastnosti

Zaporedje točk $v_0 v_1 \dots v_k$ grafa Γ je *sprehod* dolžine k, če $v_i \sim v_{i+1}$ za $0 \leq i < k$. Sprehod je *enostaven*, če so vse povezave na njem različne. Sprehod je *sklenjen*, če je $v_0 = v_k$. Sprehod, na katerem so vse točke različne, je pot, enostaven sklenjen sprehod z vsaj eno povezavo, na katerem sta enaki le prva in zadnja točka, pa je cikel grafa. Zaradi enostavnosti dopuščamo tudi sprehode dolžine 0, tj. sprehode oblike v_0. Sprehod dolžine 0 je seveda hkrati tudi pot, domenimo pa se, da ga ne bomo imeli za cikel.

LEMA 8.3 *Če med točkama grafa obstaja sprehod dolžine k, potem med njima obstaja tudi pot dolžine največ k.*

DOKAZ: Naj bosta u in v poljubni točki grafa Γ med katerima obstaja sprehod. Če je $u = v$, tedaj med njima obstaja pot dolžine 0 in trditev očitno velja. Predpostavimo torej, da je $u \neq v$. Med vsemi sprehodi med u in v izberimo najkrajšega, denimo $S = v_0 v_1 \dots v_m$, $u = v_0$, $v = v_m$. Dovolj je dokazati, da je S pot. Pa denimo, da temu ni tako. Tedaj obstajata v zaporedju $v_0, v_1, \dots, v_m$ kaka točka ponovi, denimo $v_i = v_j$ za $0 \leq i < j \leq m$. Vendar tedaj je tudi $S' = v_0 v_1 \dots v_i v_{j+1} \dots v_m$ sprehod med u in v, ki pa je očitno krajši od sprehoda S. To pa nasprotuje naši izbiri sprehoda S in dokazuje, da je S pot. ∎

Za dve točki u in v rečemo, da sta v isti *povezani komponenti*, če med njima obstaja sprehod. Ni težko videti, da je relacija "biti v isti povezani komponenti" ekvivalenčna. Njenim ekvivalenčnim razredom rečemo *povezane komponente grafa*. Graf je *povezan*, če ima eno samo povezano komponento.

Razdaljo $d_\Gamma(u, v)$ med točkama u in v v grafu Γ definiramo kot dolžino najkrajše poti od u do v v Γ. (Če taka pot ne obstaja, za razdaljo vzamemo vrednost ∞.) Kot pove lema 8.3, bi lahko razdaljo ekvivalentno definirali tudi kot dolžino najkrajšega sprehoda med danima točkama.

S tako definirano razdaljo postane množica točk povezanega grafa metrični prostor. Največji razdalji med parom točk grafa pravimo *premer* (tudi *diameter*) grafa,

$$\operatorname{diam}(\Gamma) = \max\{d_\Gamma(u, v) \mid u, v \in V(\Gamma)\}\,.$$

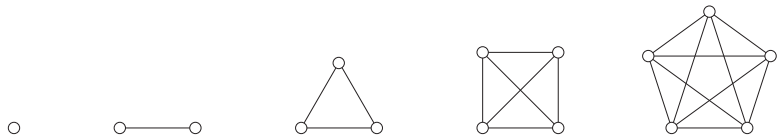
Dolžini najkrajšega cikla v grafu pravimo tudi *notranji obseg* (ali *ožina*) grafa.

8.3 Nekatere družine grafov

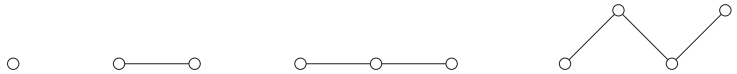
V tem razdelku si bomo ogledali nekaj družin grafov, ki jih pogosto srečujemo v zgledih in nalogah.

Polni grafi K_n: $V(K_n) = \mathbb{Z}_n$, $E(K_n) = \{uv \mid u, v \in \mathbb{Z}_n, u \neq v\}$. Polni graf K_n ima n točk in $\binom{n}{2} = \frac{n(n-1)}{2}$ povezav. Je $(n-1)$-regularen graf in je dvodelen le za $n = 1$ in 2.

Poti P_n: $V(P_n) = \mathbb{Z}_n$, $E(P_n) = \{u(u+1) \mid u = 0, 1, \dots, n-2\}$. Pot P_n ima n točk in $n-1$ povezav (njena *dolžina* je $n-1$). Za $n = 1$ in $n = 2$ je enaka grafu K_n. Vse poti so dvodelni grafi.

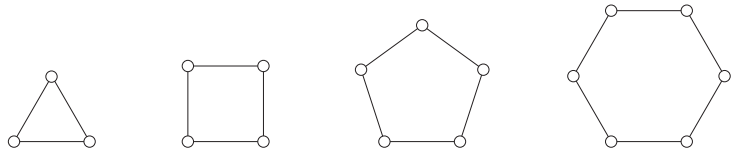


Slika 1: Polni grafi K_1, K_2, K_3, K_4 in K_5.



Slika 2: Poti P_1, P_2, P_3 in P_4.

Cikli C_n $(n \geq 3)$: $V(C_n) = \mathbb{Z}_n$, $E(C_n) = \{u(u+1) \mid u \in \mathbb{Z}_n\}$. Kadar dopuščamo tudi multigrafe, sta definirana še cikla C_1 (zanka) in C_2 (par vzporednih povezav). Cikel C_n ima n točk in n povezav. Je 2-regularen graf in je dvodelen natanko tedaj, ko je n sodo število. Vsak 2-regularen graf je disjunktna unija enega ali več ciklov. Cikel C_3 imenujemo tudi *trikotnik*.

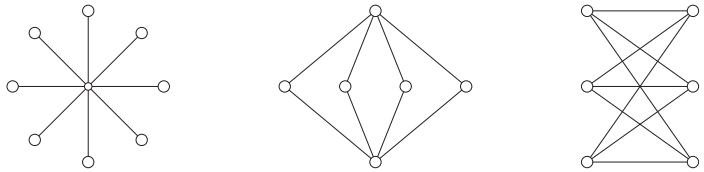


Slika 3: Cikli C_3, C_4, C_5 in C_6.

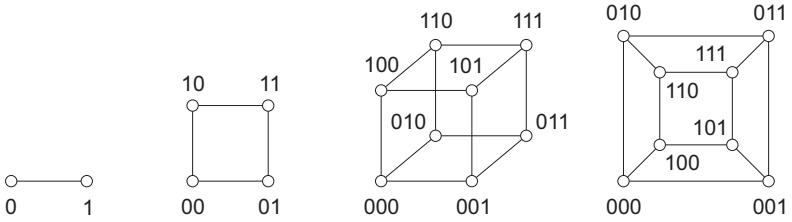
Polni dvodelni grafi $K_{m,n}$: $V(K_{m,n}) = A \cup B$, kjer velja $|A| = m$, $|B| = n$ in $A \cap B = \emptyset$, $E(K_{m,n}) = \{uv \mid u \in A, v \in B\}$. Polni dvodelni graf $K_{m,n}$ ima $m + n$ točk in mn povezav. Graf $K_{m,n}$ je regularen natanko tedaj, ko je $m = n$. Vsi grafi $K_{m,n}$ so dvodelni. Grafom $K_{1,n}$ pravimo tudi *zvezde*.

Hiperkocke Q_d: $V(Q_d) = \{(u_1, u_2, \ldots, u_d) \mid u_i \in \{0,1\}\}$, $E(Q_n) = \{uv \mid u, v \in V(Q_d) : \sum_{i=1}^{d} |u_i - v_i| = 1\}$. Običajno med hiperkocke štejemo tudi 0-razsežno kocko $Q_0 = K_1$. Hiperkocka Q_d (skelet d-razsežne kocke) ima 2^d točk in $d \cdot 2^{d-1}$ povezav. Je d-regularen graf. Vse hiperkocke so dvodelni grafi (za množici dvodelnega razbitja vzamemo množico točk, ki imajo sodo mnogo komponent enakih 0, in množico točk, ki imajo liho mnogo komponent enakih 0).

Kolesa W_n $(n \geq 3)$: $V(W_n) = \mathbb{Z}_n \cup \{\infty\}$, $E(W_n) = \{u(u+1), u\infty \mid u \in \mathbb{Z}_n\}$. Graf W_n ima $n + 1$ točk in $2n$ povezav. Za kolesa velja $\delta(W_n) = 3$ in $\Delta(W_n) = n$. Edino regularno kolo je $W_3 \simeq K_4$. Nobeno kolo ni dvodelen

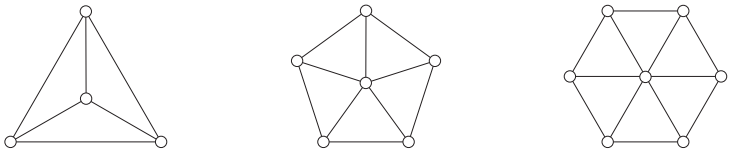


Slika 4: Polni dvodelni grafi $K_{1,8}$, $K_{2,4}$ in $K_{3,3}$.



Slika 5: Hiperkocki Q_1 in Q_2 ter dve sliki hiperkocke Q_3.

graf.



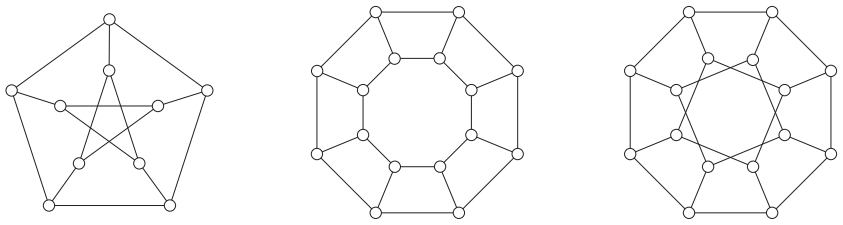
Slika 6: Kolesa W_3, W_5 in W_6.

Posplošeni Petersenovi grafi $P_{n,k}$ ($n \geq 3$ in $0 < k < n$): $V(P_{n,k}) = \{u_i, v_i \mid i \in \mathbb{Z}_n\}$, $E(P_{n,k}) = \{u_iu_{i+1}, u_iv_i, v_iv_{i+k} \mid i \in \mathbb{Z}_n\}$. Posplošeni Petersenov graf $P_{n,k}$ ima $2n$ točk. Če je $n \neq 2k$, ima $3n$ povezav in je kubičen graf, za $n = 2k$ pa ima $\frac{5n}{2}$ povezav. Graf $P_{n,k}$ je dvodelen natanko tedaj, ko je število n sodo in število k liho. Družina ima ime po *Petersenovem grafu* $P_{5,2}$.

Krožni grafi $\mathrm{Cir}(n; S)$: Naj bo S poljubna podmnožica grupe $\mathbb{Z}_n$, ki ne vsebuje elementa 0 in ki z vsakim elementom $s \in S$ vsebuje tudi nasprotni element $n - s$. *Krožni graf* $\Gamma = \mathrm{Cir}(n; S)$ na n točkah in s *simbolom* S je določen takole:

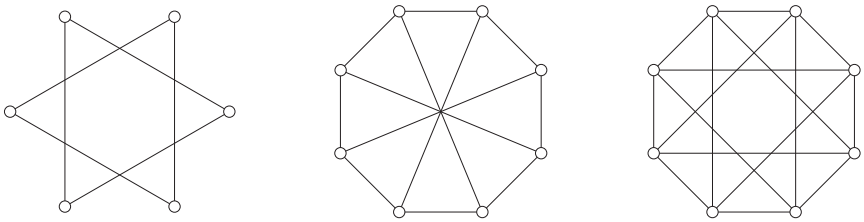
$$V(\Gamma) = \mathbb{Z}_n \qquad \text{in} \qquad E(\Gamma) = \{uv \mid v - u \in S\}\,.$$

Med krožne grafe spadajo polni grafi in cikli: $K_n = \mathrm{Cir}(n; \{1, 2, \ldots, n-1\})$ in $C_n = \mathrm{Cir}(n; \{1, n-1\})$.



Slika 7: Petersenov graf in posplošena Petersenova grafa $P_{8,1}$ in $P_{8,2}$.

Krožni graf $\mathrm{Cir}(n;S)$ ima n točk in $\frac{n|S|}{2}$ povezav. Je $|S|$-regularen graf. Naj bo $S = \{s_1, \ldots, s_d\}$, kjer je $d \geq 1$. Če je $\gcd(n, s_1, \ldots, s_d) = 1$, potem je krožni graf $\mathrm{Cir}(n;S)$ dvodelen natanko tedaj, ko je število n sodo, vsa števila s_i, $1 \leq i \leq d$, pa so liha.



Slika 8: Krožni grafi $\mathrm{Cir}(6;\{2,4\})$, $\mathrm{Cir}(8;\{1,4,7\})$ in $\mathrm{Cir}(8;\{1,3,5,7\})$.

Cayleyjevi grafi $\mathrm{Cay}(G;S)$: Cayleyjevi grafi so posplošitev krožnih grafov. Naj bo G končna grupa in S poljubna podmnožica grupe G, ki ne vsebuje enote grupe G in ki z vsakim elementom $s \in S$ vsebuje tudi nasprotni element s^{-1}. *Cayleyjev graf* $\Gamma = \mathrm{Cay}(G;S)$ grupe G in s *simbolom* S je določen takole:

$$V(\Gamma) = G \qquad \text{in} \qquad E(\Gamma) = \{uv \mid uv^{-1} \in S\}\,.$$

Med cayleyjeve grafe spadajo tudi hiperkocke, saj lahko graf Q_d predstavimo kot cayleyjev graf grupe $\mathbb{Z}_2^d$ s simbolom $S = \{(1,0,\ldots,0),(0,1,\ldots,0),\ldots,(0,0,\ldots,1)\}$. Cayleyjevi grafi so $|S|$-regularni grafi.

9 Izomorfizmi in avtomorfizmi

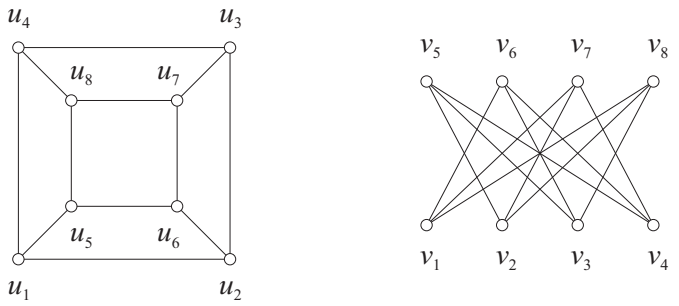
OPOMBA. Ta razdelek v veliki meri sledi drugemu poglavju knjige [3].

Vzemimo grafa Γ in Γ'. Bijektivni preslikavi $\varphi : V(\Gamma) \to V(\Gamma')$, za katero je $uv \in E(\Gamma)$ natanko tedaj, ko je $\varphi(u)\varphi(v) \in E(\Gamma')$, pravimo *izomorfizem grafov*. Grafa Γ in Γ' sta *izomorfna*, oznaka $\Gamma \simeq \Gamma'$, če med njima obstaja kakšen izomorfizem. Pri delu z grafi izomorfnih grafov med seboj običajno ne ločimo (npr. pravimo, da graf vsebuje cikel, kar pomeni, da vsebuje podgraf, ki je izomorfen nekemu ciklu). V primeru, ko je graf Γ' kar enak grafu Γ, izomorfizmu grafov pravimo *avtomorfizem* grafa. Če množico avtomorfizmov danega grafa Γ opremimo z operacijo komponiranja preslikav, dobimo grupo, ki ji pravimo *grupa avtomorfizmov* grafa Γ in jo označimo z $\mathrm{Aut}(\Gamma)$. Kadar za poljubni točki grafa obstaja avtomorfizem, ki prvo preslika v drugo, pravimo, da je graf *tranzitiven po točkah*. Vsi cayleyjevi grafi so tranzitivni po točkah.

9.1 Izomorfnost grafov

Lastnosti grafa, ki jo imajo poleg grafa samega tudi vsi z njim izomorfni grafi, pravimo *invarianta* grafa. Osnovni način, s katerim dokažemo, da grafa nista izomorfna, je, da poiščemo grafovsko invarianto, v kateri se obravnavana grafa ločita. Preproste invariante so: število točk in povezav, število podgrafov izbrane vrste (npr. trikotniki), stopnje točk, dvodelnost, itn. Izomorfnost običajno dokažemo tako, da konstruiramo izomorfizem. Včasih si delo lahko poenostavimo, če upoštevamo, da sta grafa izomorfna natanko tedaj, ko sta izomorfna njuna komplementarna grafa.

Zgled. *Dokažimo, da sta grafa* Γ_1 *in* Γ_2 *s slike 9 izomorfna, grafa* Γ_3 *in* Γ_4 *s slike 10 pa ne.*



Slika 9: Grafa Γ_1 in Γ_2.

REŠITEV: Graf Γ_2 je dvodelen z razbitjem $C = \{v_1, v_2, v_3, v_4\}$, $D = \{v_5, v_6, v_7, v_8\}$. Hitro tudi opazimo, da množici $A = \{u_1, u_3, u_6, u_8\}$ in $B = \{u_2, u_4, u_5, u_7\}$ tvorita dvodelno razbitje grafa Γ_1. Izomorfizem $\varphi : \Gamma_2 \to \Gamma_1$ mora dvodelno razbitje seveda ohranjati. Poskusimo preslikati točko v_1 v u_2. Ker je v_5 edina točka v množici D, ki točki v_1 ni sosednja, in točka u_8 edina točka v množici B, ki točki u_2 ni sosednja, mora izomorfizem φ preslikati točko v_5 v točko u_8.

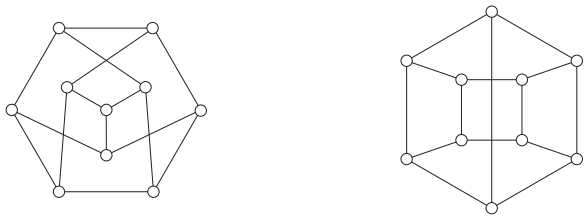
Pri sliki točke v_2 imamo spet nekaj svobode, pa se odločimo za točko u_4. S tem smo, enako kot zgoraj, določili sliko točke v_6, ki se mora preslikati v točko u_6. Nadaljujemo podobno in dobimo preslikavo φ, ki se nam zdi primeren kandidat za izomorfizem:

x	v_1	v_2	v_3	v_4	v_5	v_6	v_7	v_8
$\varphi(x)$	u_2	u_4	u_5	u_7	u_8	u_6	u_3	u_1

Sedaj moramo preveriti, ali preslikava φ povezave grafa Γ_2 res preslika bijektivno na povezave grafa Γ_1. Za vsak $xy \in E(\Gamma_2)$ poglejmo sliko $\varphi(x)\varphi(y)$:

xy	v_1v_6	v_1v_7	v_1v_8	v_2v_5	v_2v_7	v_2v_8	v_3v_5	v_3v_6	v_3v_8	v_4v_5	v_4v_6	v_4v_7
$\varphi(x)\varphi(y)$	u_2u_6	u_2u_3	u_2u_1	u_4u_8	u_4u_3	u_4u_1	u_5u_8	u_5u_6	u_5u_1	u_7u_8	u_7u_6	u_7u_3

V spodnji vrstici smo dobili natanko vse povezave grafa G_1, kar pomeni, da je preslikava φ res izomorfizem. Omenimo še, da je graf Γ_1 prikazan kot 3-kocka Q_3, graf Γ_2 pa kot polni dvodelni graf $K_{4,4}$ brez štirih neodvisnih povezav, $K_{4,4} - 4K_2$.



Slika 10: Grafa Γ_3 in Γ_4.

Oglejmo si sedaj grafa Γ_3 in Γ_4. Vidimo, da graf Γ_4 vsebuje cikel dolžine 4, graf Γ_3 pa ne. Podobno vsebuje graf Γ_4 le dva cikla dolžine 5, Γ_3 pa mnogo več. Grafa tako nista izomorfna. Graf Γ_3 je izomorfen Petersenovemu grafu, graf Γ_4 pa 5-strani prizmi $C_5 \square K_2$. ∎

9.2 Avtomorfizmi grafov

Izomorfizmu grafa vase rečemo tudi *avtomorfizem grafa*. Avtomorfizem grafa Γ je torej permutacija točk grafa, ki vsak par sosednjih vozlišč preslika v par sosednjih vozlišč. (Pozor: če bi dovoljevali tudi neskončne grafe, bi morali zahtevati tudi, da se par nesosednjih vozlišč preslika v par nesosednjih vozlišč.) Avtomorfizem grafa Γ lahko torej razumemo kot element simetrične grupe $\mathrm{Sym}(V(\Gamma))$.

Ker je produkt dveh avtomorfizmov grafa očitno spet avtomorfizem grafa (in ker je identiteta tudi avtomorfizem vsakega grafa), tvori množica vseh avtomorfizmov grafa podgrupo grupe $\mathrm{Sym}(V(\Gamma))$. To množico označimo s simbolom $\mathrm{Aut}(\Gamma)$ in jo imenujemo *grupa avtomorfizmov grafa* Γ.

Določati grupo avtomorfizmov grafa je načeloma težak problem, za nekatere posebne družine grafov, pa je naloga dokaj lahka. Poglejmo si nekaj primerov:

- $\mathrm{Aut}(K_n) = S_n$;
- $\mathrm{Aut}(C_n) = D_n$;
- $\mathrm{Aut}(K_{m,n}) \cong S_m \times S_n$, če $m \neq n$;
- $\mathrm{Aut}(K_{n,n}) = (S_n \times S_n) \rtimes S_2$.

Nekoliko zanimivejše je določanje grupe avtomorfizmov Petersenovega grafa.

Zgled. *Dokaži, da je grupa avtomorfizmov Petersenovega grafa izomorfna grupi S_5.*

REŠITEV: Najprej opazimo, da lahko Petersenov graf predstavimo takole:

$$V(\mathrm{Pet}) = \{\{i,j\} : i,j \in \mathbb{Z}_5, i \neq j\}, \quad \{i,j\} \sim \{s,t\} \Leftrightarrow \{i,j\} \cap \{s,t\} = \emptyset.$$

Sedaj je očitno, da vsaka permutacija $\sigma \in \mathrm{Sym}(\mathbb{Z}_5)$ porodi avtomorfizem grafa $\tilde{\sigma}$, ki je definiran s predpisom $\{i,j\}^{\tilde{\sigma}} = \{i^\sigma, j^\sigma\}$. Na ta način smo grupo $\mathrm{Sym}(\mathbb{Z}_n) \cong S_5$ vložili v grupo $\mathrm{Aut}(\Gamma)$. Dokazati moramo le še, da Petersenov graf ne premore drugih avtomorfizmov. To storimo z naslednjim premislekom.

Naj bo $v = \{0,1\} \in V(\mathrm{Pet})$ in $G = \mathrm{Aut}(\mathrm{Pet})$. Najprej opazimo, da S_5 (in zato tudi $\mathrm{Aut}(\mathrm{Pet})$) deluje tranzitivno na točkah Petersenovega grafa. Zato nam lema o orbiti in stabilizatorju pove

$$|G| = 10 \cdot |G_v|.$$

Podobno vidimo, da G_v deluje tranzitivno na soseščini $\{\{2,3\},\{3,4\},\{2,4\}\}$ vozlišča v, saj vozlišče $u = \{2,3\}$ preslikamo v vozlišče $\{3,4\}$ z avtomorfizmom $\tilde{\alpha} \in G_v$ za $\alpha = (0)(1)(3)(2,4) \in S_5$ in v vozlišče $\{2,4\}$ z avtomorfizmov $\tilde{\alpha}$ za $\alpha = (0)(1)(2)(3,4)$. Zato je

$$|G| = 10 \cdot |G_v| = 10|G_{vu}||u^{G_v}| = 10 \cdot 3 \cdot |G_{vu}|.$$

Poglejmo si sedaj orbito elementa $z = \{3,4\}$ pri delovanju grupe G_{vu}. Ker je z sosed v, se lahko z elementom iz G_{vu} preslika zgolj v soseda v. Očitno se ne more preslikati v u, saj se tja preslika že u sam. Po drugi stani pa avtomorfizem $\tilde{\alpha} \in G_{vu}$ za $\alpha = (0)(1)(2,3)(4)$ preslika z v tretjega soseda, $\{2,4\}$, vozlišča v. Zato je $z^{G_{vu}} = \{z, \{2,4\}\}$, in zato

$$|G| = 30 \cdot |G_{vu}| = 30 \cdot |G_{vuz}||z^{G_{vu}}| = 60 \cdot |G_{vuz}|.$$

Nazadnje poglejmo še orbito $w^{G_{vuz}}$ vozlišča $w = \{1,2\}$. Ker je w sosed točke z, se z elementom iz G_{vuz} preslika bodisi v samega sebe bodisi v $\{0,2\}$, ne pa tudi v tretjega soseda, u, točke z, saj se v u preslika že u sam. Po drugi strani pa res obstaja permutacija $\alpha = (0,1)(2)(3)(4) \in S_5$, za katero je $\tilde{\alpha} \in G_{vuz}$ in je $w^{\tilde{\alpha}} = \{0,2\}$. Zato je

$$|G| = 60 \cdot |G_{vuz}| = 60 \cdot |G_{vuzw}||w^{G_{vuz}}| = 120 \cdot |G_{vuzw}|.$$

Nazadnje pa premislimo še, da je G_{vuzw} trivialna grupa. Namreč poljuben avtomorfizem Petersenovega grafa, ki pribije točke u, v, z in w pribije tudi peto točko, $t = \{4,5\}$ petcikla $uvzwt$. Vsaka od preostalih petih točk pa je sosednja kaki izmed petih že pribitih točk tega petcikla. Zato takšno točko element iz G_{vuzw} tudi pribije. S tem smo dokazali, da je $|G| = 120$ in zato

$$\mathrm{Aut}(\mathrm{Pet}) \cong S_5.$$

■

10 Drevesa

V povezanem grafu med poljubnima dvema točkama obstaja vsaj ena pot. Grafu, v katerem med poljubnima dvema točkama obstaja natanko ena pot, rečemo *drevo*.

TRDITEV 10.1 *Za graf* Γ *so ekvivalentne naslednje trditve:*

(1) Γ *je drevo;*

(2) Γ *je povezan, ampak z odstranitvijo poljubne povezave postane nepovezan;*

(3) Γ *je povezan in* $|E(\Gamma)| = |V(\Gamma)| - 1$.

(4) Γ *ne vsebuje cikla in* $|E(\Gamma)| = |V(\Gamma)| - 1$.

(5) Γ *je povezan in ne vsebuje cikla.*

DOKAZ: Dokaz poteka z indukcijo na število točk. Trditev očitno drži za vse grafe na dveh točkah (takšna grafa sta samo dva, K_2 in njegov komplement). Denimo, da trditev drži za vse grafe na manj kot n točkah. Dokažimo, da tedaj velja tudi za graf Γ na n točkah.

(1) $\Rightarrow$ (2): Denimo, da je Γ drevo. Tedaj je povezan po deficiji. Naj bo $e = uv$ poljubna povezava grafa Γ. Tedaj je (u, v) **edina** pot med u in v. To pa pomeni, da v grafu $\Gamma - e$ ni nobene poti, kar pomeni, da Γ ni povezan.

(2) $\Rightarrow$ (3): Predpostavimo, da je Γ povezan, odstranitev poljubne povezave pa ga razbije. Dokazujemo enakost $|E(\Gamma)| = |V(\Gamma)| - 1$. Izberi povezavo e. Tedaj je $\Gamma - e$ unija povezanih komponent X in Y (premisli, da sta povezani komponenti dve in ne morda tri ali več). Grafa X in Y sta povezana, če pa odstanimo kakšno povezavo, razpadeta (saj če ne bi razpadla, ne bi ob odstranitvi te iste povezave razpadel niti graf Γ). Uporabimo indukcijo in dobimo $|E(X)| = |V(X)| - 1$ and $|E(Y)| = |V(Y)| - 1$. Tedaj

$$|E(\Gamma)| = |E(X)| + |E(Y)| + 1 = (|V(X)| - 1) + (|V(Y)| - 1) + 1 = |V(\Gamma)| - 1.$$

(3) $\Rightarrow$ (4): Predpostavljamo, da je Γ povezan in da zadošča pogoju $|E(\Gamma) = |V(\Gamma)| - 1$. Dokazujemo, da Γ nima ciklov. Pa recimo, da obstaja cikel C. Za vsak $v \in V(\Gamma)$ poiščemo prvo povezavo e_v na kaki najkrajši poti med v in C. Premislek pokaže, da je $e_v \neq e_u$ za poljubni različni točki $u, v \in V(\Gamma) \setminus V(C)$. Zato je

$$|E(\Gamma) \geq |E(C)| \cup |\{e_v : v \in V(\Gamma) \setminus V(C)\}| = V(\Gamma),$$

kar je protislovje.

(4) $\Rightarrow$ (5): Predpostavljamo, da je Γ brez ciklov in da velja$|E(\Gamma)| = |V(\Gamma)| - 1$. Dokazati moramo, da je Γ povezan. Naj bodo $X_1, \ldots, X_k$ komponente za povezanost in denimo, da je $k \geq 2$. Vsak izmed grafov X_i zadošča (5), zato po indukcijski predpostavki X_i zadošča tudi (4). Tedaj pa je $|E(X_i)| = |V(X_i)| - 1$. Po drugi strani:

$$|E(\Gamma)| = \sum_{i=1}^{k} |E(X_i)| = \sum_{i=1}^{k} |V(X_i)| - k.$$

Ker je $|E(\Gamma)| = |V(\Gamma)| - 1$, sledi $k = 1$, in Γ je povezan.

(5) $\Rightarrow$ (1): Predpostavljamo, da je Γ povezan in brez ciklov. Dokazujemo, da obstaja med poljubnima točkama natanko ena pot. Zaradi povezanoti obstaja vsaj ena pot. Če bi bili dve, bi dobili cikel – protislovje. ∎

POSLEDICA 10.2 *Drevo z vsaj dvema točkama vsebuje dve točki stopnje* 1.

DOKAZ: Naj bo Γ graf, v katerem ima vsaj $|V(\Gamma)| - 1$ točk stopnjo vsaj 2 (označimo množico teh točk z U). Preostala točka ima stopnjo vsaj 1, saj bi sicer tvorila komponentno za povezanost. Tedaj je

$$|E(\Gamma)| = \frac{1}{2}(\sum_{v \in U} \deg(v) + 1) \geq \frac{1}{2}(|V(\Gamma)| \cdot 2 + 1) = |V(\Gamma)| + \frac{1}{2}.$$

Pri tem smo pri prvi neenakosti uporabili lemo o rokovanju. Sedaj pa iz trditve 10.1 sledi, da Γ ni drevo, kar je protislovje ∎

OPOMBA. Točki stopnje 1 rečemo tudi *list* grafa. Zgornja posledica torej pravi, da ima drevo vsaj dva lista. Če ima drevo natanko dva lista, potem se neenakost v dokazu zgornje trditve izide le, če ima vsaka druga točka stopno natanko 2. Ni se težko prepričati, da je povezan graf, ki ima dva lista, ostale točke pa imajo stopnjo 2, izomorfen poti.

10.1 Vpeta drevesa

Vpet podgraf grafa Γ, ki je drevo, se imenuje *vpeto drevo* grafa Γ.

TRDITEV 10.3 *Graf je povezan, če in samo če vsebuje vpeto drevo.*

DOKAZ: Če graf Γ vsebuje vpeto drevo, obstaja pot med poljubnima dvema točkama že v drevesu. Zato je Γ povezan. Naj bo sedaj Γ povezan graf. Če je Γ drevo, je trditev dokazana. Sicer obstaja povezava e, za katero je $\Gamma - e$ povezan. Odstranimo e iz Γ in postopek nadaljujemo, dokler ne dobimo (vpetega) drevesa. ∎

Povezan graf, ki ni drevo, ima več kot eno vpeto drevo. *Število vpetih dreves* v grafu Γ označimo s $\tau(\Gamma)$.

Pri računanju števila $\tau(\Gamma)$ je priročno razširiti naš horizont na družino multigrafov. Za povezavo e multigrafa Γ na $\Gamma - e$ označuje multigraf, ki ga dobimo iz Γ z odstranitvijo povezave e, Γ/e pa multigraf, ki ga dobimo iz Γ, če povezavo e *skrčimo*, tj. identificiramo njeni krajišči, zanko, ki nastane iz e ob tako nastali novi točki, pa odstranimo. Nasploh lahko v naslednjem izreku v multigrafih, ki nastopajo, brišemo vse zanke, ki se morebiti pojavijo.

TRDITEV 10.4 *Naj bo e poljubna povezana multigrafa Γ. Tedaj velja*

$$\tau(\Gamma) = \tau(\Gamma - e) + \tau(G/e).$$

DOKAZ: Vpetih dreves multigrafa Γ, ki povezave e ne vsebujejo, je natanko toliko kot vpetih dreves multigrafa $\Gamma - e$. Po drugi strani pa iz vpetega drevesa multigrafa Γ, ki vsebuje povezavo e, s skrčitvijo te povezave dobimo vpeto drevo multigrafa Γ/e. Ta postopek nam očitno da bijekcijo med vpetimi drevesi multigrafa Γ, ki vsebujejo povezavo e, z vpetimi drevesi multigrafa Γ/e. ∎

OPOMBA. Število vpetih dreves pa lahko izračunamo tudi s pomočjo linearne algebre, natančneje, s pomočjo Laplaceove matrike grafa.

DEFINICIJA 10.5 *Laplacova matrika $L(\Gamma)$ (multi)grafa Γ je kvadratna matrika, katere stoplci in vrstice so indeksirane s točkami grafa, v presečišču vrstice u in stoplca v leži negativno število povezav med u in v, diagonalni element točke v pa je enak stopnji točke v.*

TRDITEV 10.6 *Število vpetih dreves (multi)grafa Γ je enako absolutni vrednosti determinante matrike, ki jo dobimo iz $L(\Gamma)$ tako, da odstanimo poljubno vrstico in poljuben stolpec.*

S pomočjo te trditve (in nekaj spretnosti pri računanju determinant) lahko dokažemo tako imenovano Cayleyjevo formulo za število vpetih dreves polnega grafa, ki pravi $\tau(K_n) = n^{n-2}$.

11 Eulerjevi in hamiltonovi grafi

OPOMBA. Ta razdelek v veliki meri sledi četrtemu poglavju knjige [3].

11.1 Eulerjevi grafi

Sprehod v grafu (ali multigrafu) je enostaven, če vsebuje vsako povezavo grafa največ enkrat. Enostaven sprehod, je *eulerjev*, če vsebuje vse povezave grafa (vsako natanko enkrat). Multigraf je *eulerjev*, če vsebuje eulerjev obhod, torej sklenjen sprehod, ki vsebuje vsako povezavo multigrafa natanko enkrat. Eulerjevih multigrafov ni težko prepoznati.

IZREK 11.1 *Multigraf Γ brez izoliranih točk je eulerjev, če in samo če je povezan in so vse njegove točke sode stopnje.*

DOKAZ: Naj bo Γ graf brez izoliranih točk. Denimo, da je Γ eulerjev. Tedaj je očitno povezan, saj vsaka točka leži na eulerjevem sprehodu. (Tu smo uporabili dejstvo, da Γ nima izoliranih točk.) Vsakič, ko eulerjev sprehod obišče kako točko, porabi dve povezavi – eno za vstop v točko, drugo za izhod iz nje. Ker eulerjev obhod pri vsaki točki porabi vse povezave, mora biti stopnja vsake točke soda.

Denimo sedaj, da je Γ povezan, vsaka njegova točka pa ima sodo stopnjo. Naj bo W najdaljši med enostavnimi obhodi v Γ in naj bo Γ' multigraf, ki ga dobimo iz Γ, če odstranimo vse povezave obhoda W. Če Γ ni eulerjev, potem Γ' premore kakšno povezavo. Po drugi strani ima vsaka točka multigrafa Γ' sodo stopnjo, saj smo stopnjo točke z odstranjevanjem povezavav iz W zmanjšali za sodo število. Še več, ker je Γ povezan, ima vsaj ena točka na sprehodu W v grafu Γ' stopnjo večjo ali enako 2. V takšni točki lahko torej začnemo sprehod v grafu Γ', ki ga nadaljujemo poljubno ter končamo šele, ko se vrnemo v začetno točko (ker ima v grafu Γ' vsaka točka sodo stopnjo, takšen sprehod resnično slej ko prej zopet vrne v začetno točko). Če ta novi sklenjeni sprehod vrinemo v sprehod W, dobimo sklenjeni sprehod v Γ, ki je daljši od W. To pa je protislovje. ∎

11.2 Hamiltonovi grafi

Pot P v grafu Γ je *hamiltonova*, če velja $V(P) = V(\Gamma)$. Cikel C v grafu Γ je *hamiltonov*, če velja $V(C) = V(\Gamma)$. Hamiltonova pot in cikel sta torej vpeta pot oziroma vpet cikel. Graf je *hamiltonov*, če ima hamiltonov cikel.

Znan ni noben preprost, hitro preverljiv potreben in hkrati zadosten pogoj za hamiltonost grafa. Preprost potreben pogoj je podan v naslednji trditvi. Pri njej je uporabljena oznaka $\Omega(\Delta)$ za število povezanih komponent grafa Δ.

TRDITEV 11.2 *Naj bo $S \subset V(\Gamma)$ neprazna množica točk grafa Γ. Če je $\Omega(\Gamma - S) > |S|$, potem Γ nima hamiltonovega cikla.*

DOKAZ: Naj bodo $\Gamma_1, \ldots, \Gamma_k$ povezane komponente grafa $\Gamma - S$ in naj bo $C = v_0 v_2 \ldots v_{n-1} v_0$ hamiltonov cikel grafa Γ. Dokazati moramo, da je $|S| \geq k$. Brez škode za splošnost lahko privzamemo, da $v_{n-1} \in S$.

Za $i = 1, \ldots, k$ naj bo n_i največji indeks, za katerega je $v_{n_i} \in V(\Gamma_i)$. Točka v_{n_i} je torej zadnja točka na ciklu C, ki še leži v komponenti Γ_i. Naslednja točka, v_{i+1}, je element množice S. Točke $v_{n_1+1}, v_{n_2+1}, \ldots, v_{n_k+1}$ so torej (paroma različni) elementi množice S, in zato $|S| \geq k$. ∎

Zgornji potrebni pogoj za hamiltonost grafa žal ni tudi zadostni, kot kaže primer Petersenovega grafa. V Petersenovem grafu Pet za vsako neprazno množico $S \subseteq V(\mathrm{Pet})$ velja $\Omega(\Gamma - S) \leq |S|$, vendar graf vseeno ni hamiltonov.

Dobrih zadostnih pogojev za hamiltonost grafa ni enostavno najti. Navedimo jih nekaj.

TRDITEV 11.3 *Naj bosta u in v takšni nesosednji točki grafa Γ, da velja $deg(u)+deg(v) \geq |V(\Gamma)|$. Če je graf $\Gamma + uv$ hamiltonov, potem je hamiltonov tudi graf Γ.*

DOKAZ: Naj bo $n = |V(\Gamma)|$. Denimo, da je graf $\Gamma + uv$ hamiltonov. Potem obstaja hamiltonova pot $uv_1v_2 \ldots v_{n-2}v$ v grafu Γ. Naj bo U množica indeksov sosed točke u ter V množica indeksov sosed točke v v grafu Γ. Če je za kak $i \in U$ velja $i - 1 \in V$, tedaj je $v_0 v_1 \ldots v_{i-1} v_{n-1} v_{n-2} \ldots v_i v_0$ hamiltonov cikel v grafu Γ. Predpostavimo torej lahko, da takšnega indeksa i ni. Z drugimi besedami, $V \subseteq \{0, 1, \ldots, n-2\} \setminus (U - 1)$, kjer smo z $U - 1$ označili množico $\{i - 1 : i \in U\}$. Od tod sledi neenakost $\deg(v) = |V| \leq n - 1 - |U| = n - 1 - \deg(u)$, kar je v prostislovju z našo predpostavko o vsoti stopenj točk u in v. ∎

Od tod z lahkoto izpeljemo naslednji posledici.

IZREK 11.4 (Ore). *Če za vsak par nesosednjih točk u, v grafa Γ velja $deg(u)+deg(v) \geq |V(\Gamma)|$, potem je graf Γ hamiltonov.*

IZREK 11.5 (Dirac). *Če ima graf Γ vsaj 3 točke in velja $\delta(\Gamma) \geq \frac{|V(\Gamma)|}{2}$, potem je graf G hamiltonov.*

12 Povezanost in Mengerjev izrek

OPOMBA. Ta razdelek v veliki meri sledi petemu poglavju knjige [3].

Točka v grafa Γ je *prerezna točka*, če ima graf $\Gamma - v$ več komponent kot graf Γ. Podobno je povezava $e \in E(\Gamma)$ *prerezna povezava*, če ima graf $\Gamma - e$ več komponent kot graf Γ. Prerezni povezavi pravimo tudi *most*.

Graf Γ je *k-povezan*, če ima vsaj $k+1$ točk, za vsako množico točk $U \subset V(\Gamma)$, ki ima manj kot k točk, pa je graf $G - U$ povezan. Če je graf Γ k-povezan, je tudi ℓ-povezan za vsako število $\ell \leq k$. Največje število k, za katero je graf Γ k-povezan, imenujemo *povezanost* grafa Γ in ga označimo s $\kappa(\Gamma)$.

- $\kappa(C_n) = 2$,
- $\kappa(K_n) = n - 1$
- $\kappa(K_{m,n}) = \min\{m, n\}$.
- Za vsak graf Γ je $\kappa(\Gamma) \leq \delta(G)$.

12.1 Mengerjev izrek

Vzemimo $A, B \subseteq V(\Gamma)$. Poti v grafu Γ, ki se začne v točki iz A in konča v točki iz B, pravimo *(A, B)-pot*. Množica $S \subseteq V(\Gamma)$ je *(A, B)-prerez* v Γ, če vsaka (A, B)-pot vsebuje kako točko iz S. Če (A, B)-prerez odstranimo iz grafa Γ, se preostanek množice A (če ga je kaj) znajde v drugi povezani komponenti kot preostanek množice B. Vsak (A, B)-prerez vsebuje vse točke iz $A \cap B$.

IZREK 12.1 (Menger). *Naj bo Γ graf in $A, B \subseteq V(\Gamma)$. Največje število disjunktnih (A, B)-poti v Γ je enako najmanjši moči (A, B)-prereza v Γ.*

Množica S *loči* točki $u, v \in V(\Gamma)$, če u in v ležita v različnih komponentah grafa $\Gamma - S$. Velikokrat srečamo Mengerjev izrek v naslednji obliki:

POSLEDICA 12.2 *Naj bosta $u, v \in V(\Gamma)$, $u \neq v$, nesosednji točki grafa Γ. Potem je največje število notranje disjunktnih (u, v)-poti v Γ enako najmanjši moči množice, ki loči točki u in v.*

Mengerjev izrek nam omogoča tudi drugačen pogled na k-povezanost.

POSLEDICA 12.3 (Opis k-povezanih grafov). *Naj bo Γ graf z vsaj $k+1$ točkami. Graf Γ je k-povezan natanko tedaj, ko za vsak par različnih točk $u, v \in V(\Gamma)$ obstaja vsaj k notranje disjunktnih (u, v)-poti.*

12.2 2-povezani grafi in bloki

Blok grafa Γ je maksimalen povezan podgraf brez prereznih točk (t.j. povezan podgraf brez prereznih točk, ki ni vsebovan v nobenem večjem takšnem podgrafu). Blok grafa je bodisi izolirana točka bodisi prerezna povezava (skupaj s krajiščema) bodisi maksimalen 2-povezan podgraf.

TRDITEV 12.4 (Opis 2-povezanih grafov). *Naj bo Γ graf z vsaj tremi točkami. Naslednje trditve so enakovredne:*

1. *Γ je 2-povezan.*
2. *Γ ima en sam blok.*
3. *Vsak par točk grafa Γ leži na skupnem ciklu (oziroma med vsakim parom točk grafa Γ obstaja par notranje disjunktnih poti).*
4. *$\delta(\Gamma) \geq 1$ in vsak par povezav grafa Γ leži na skupnem ciklu.*

Različna bloka grafa imata skupno največ eno točko, ki mora biti prerezna točka grafa. Različni povezavi e_1, e_2 grafa pripadata istemu bloku natanko tedaj, ko ležita na skupnem ciklu.

Grafu Γ priredimo *graf blokov* $B(\Gamma)$ takole: Naj bodo $B_1, \ldots, B_k$ bloki grafa Γ in $v_1, \ldots, v_p$ prerezne točke v Γ. Potem vzamemo

$$V(B(\Gamma)) = \{B_1, \ldots, B_k, v_1, \ldots, v_p\} \quad \text{in} \quad E(B(\Gamma)) = \{v_i B_j \mid v_i \in V(B_j)\}\,.$$

Če je graf Γ povezan, je $B(\Gamma)$ drevo.

13 Ravninski grafi in Eulerjeva formula

Kot smo že omenili v uvodu, grafe radi rišemo v ravnini tako, da vozlišče grafa predstavimo kot točko ravnine, povezo med vozliščema pa kot ravno (ali pa tudi krivo) črto s krajišči v točkah, ki ustrezata krajiščema povezave. Pri tem pazimo, da povezava (oziroma, natančneje, črta, ki ponazarja povezavo) ne seka same sebe in ne poteka skozi nobeno drugo vozlišče kot le svoje krajišče. Seveda ima lahko dani graf več različnih risb.

Če obstaja risba grafa, pri kateri se nobeni dve povezavi med seboj ne sekata (razen morda v svojih krajiščih), rečemo, da je graf *ravninski*, takšni risbi pa *ravniska risba grafa*. Tako so, na primer, ravninski vsi cikli C_n, vse poti P_n, vsa drevesa, pa tudi polni grafi K_3 in K_4 ter polni dvodelni grafa $K_{2,n}$, $n \in \mathbb{N}$. Kasneje pa bomo videli, da polni grafi K_n za $n \geq 5$ in polni dvodelni grafi $K_{m,n}$ za $m, n \geq 3$ niso ravninski.

OPOMBA. Formalno definicijo risbe in ravninskosti grafa lahko opišemo takole: *Vložitev* multigrafa Γ v metrični prostor Σ je določena z injektivno preslikavo $\varphi\colon V(\Gamma) \to \Sigma$, ki vsaki točki multigrafa priredi točko prostora Σ, in tako družino zveznih preslikav $\varphi_e\colon [0,1] \to \Sigma$ (tu smo povezavo e predstavili z zaprtim intervalom $[0,1]$), da velja: $\varphi_e(0)$ je slika enega, $\varphi_e(1)$ pa slika drugega krajišča povezave e, $\varphi_e|_{(0,1)}$ je injektivna in njena slika ne vsebuje nobene točke, ki bi bila slika točke grafa ali pa del slike kake druge povezave grafa. Graf, ki premore vložitev v ravnino, se imenuje *ravninski graf*.

Dokazati, da je neki graf ravninski, je načeloma enostavno – najti moramo njegovo ravninsko risbo. Precej težje pa je dokazati, da graf ni ravninski, saj bi morali pregledati vse možne njegove risbe in preveriti, da nobena ni ravninska. Ker je to seveda nemogoče, je za dokazovanje neravninskosti grafov potrebno razviti kakšne drugačne prijeme. Eden takšnih je *Eulerjeva formula*.

13.1 Eulerjeva formula

Zamislimo si ravninsko risbo ravninskega grafa Γ. Če iz ravnine izrežemo vse črte in točke, ki predstavljajo povezave in vozlišča grafa, dobimo nekaj med seboj ločenih povezanih območij, ki jih imenujemo *lica*. Eno od teh območij je neomejeno in obdaja celotno risbo grafa, ostala območja pa so omejena. Množico vsej lic tako narisanega grafa Γ označimo z $F(\Gamma)$.

Na prvi pogled ni videti nobenega razloga, zakaj bi število lic grafa ne bilo odvisno od konkretne ravniske risbe le-tega. Zato je toliko presenetljivejša naslednja trditev, iz katere med drugim sledi, da je število lic ravninskega grafa neodvisno od konkretne ravninske risbe.

IZREK 13.1 (Eulerjeva formula) *Naj bo Γ ravninski graf z množico vozlišč V in množico povezav E. Naj bo F množica lic kake ravninske slike grafa Γ in Ω množica komponent za povezanost grafa Γ. Tedaj velja naslednja enakost:*

$$|V| - |E| + |F| = 1 + |\Omega|.$$

Zgornji izrek navadno dokazujemo z indukcijo na število povezav grafa. Pri tem si pomagamo tudi s formulo o številu povezav v drevesu z n točkami. Podrobnosti dokaza bomo izpustili. Namesto tega raje izpeljimo naslednjo pomembno posledico Eulerjeve formule.

TRDITEV 13.2 *Naj bo Γ povezan ravninski graf z vsaj tremi točkami. Tedaj je*

$$|E(\Gamma)| \leq 3|V(\Gamma)| - 6.$$

DOKAZ: Izberimo kako ravninsko sliko grafa Γ in z F označimo množico pripadajočih lic, z $\vec{E}$ pa množico vseh usmerjenih povezav grafa Γ (tj. množico vseh parov (u, v), $u, v \in V(\Gamma)$, za katere je $u \sim v$).

Če rob lica prehodimo v smeri urinega kazalca, dobimo sklenjen sprehod v grafu, ki ga bomo imenovali kar *usmerjeni rob lica*. Za razliko od omejenih lic se domenimo, da je usmerjeni rob neomejenega lica obhod, ki ga dobimo, če robne povezave zunanjega lica prehodimo v smeri, ki je nasprotna urinemu kazalcu. Opazimo, da vsaka usmerjena povezava leži na natanko enem robu lica (namreč na robu tistega lica, ki leži desno od nje, če gledamo v smeri usmeritve povezave). Hkrati pa vsak rob lica vsebuje vsako usmerjeno povezavo največ enkrat.

Število usmerjenih povezav, ki jih vsebuje rob lica $f \in F$, označimo z $\deg(f)$. Enostaven premislek pokaže, da iz $\deg(f) \leq 2$ sledi, da je graf Γ izomorfen K_1 ali K_2, kar pa je v protislovju s predpostavko, da je $|V(\Gamma)| \geq 3$. Zato je $\deg(f) \geq 3$ za vsak $f \in F$.

Oglejmo si množico parov $\mathcal{M} = \{(e, f) : e \in \vec{E}, f \in F, e \text{ leži na robu } f\}$. Elemente množice $\mathcal{M}$ preštejmo na dva načina:

$$|\mathcal{M}| = \sum_{e \in \vec{E}} 1 = |\vec{E}| = 2|E|.$$

Po drugi strani:

$$|\mathcal{M}| = \sum_{f \in F} \deg(f) \geq \sum_{f \in F} 3 = 3|F|.$$

Od tod sledi $|F| \leq \frac{2}{3}|E|$. Vstavimo to v enakost $|F| = 2 - |V| + |E|$, ki sledi iz Eulerjeve fornule. Dobimo $2 - |V| + |E| \leq \frac{2}{3}|E|$, od koder dobimo

$\frac{1}{3}|E| \leq |V| - 2$. To neenakost še pomnožimo s 3 in dobimo, kar smo trdili. ∎

Podobno kot zgornjo trditev lahko dokažemo tudi naslednje.

TRDITEV 13.3 *Naj bo* Γ *povezan ravninski graf z vsaj štirimi točkami. Če* Γ *ne vsebuje cikla dolžine* 3*, tedaj je*

$$|E(\Gamma)| \leq 2|V(\Gamma)| - 4.$$

Iz zgornjih dveh rezultatov neposredno sledi naslednje.

TRDITEV 13.4 *Grafa* K_5 *in* $K_{3,3}$ *nista ravninska.*

DOKAZ: Graf K_5 ima 5 vozlišč in 10 povezav. Če bi bil ravninski, bi veljalo $10 \leq 3 \cdot 5 - 6$, kar pa očitno ni res. Zato graf K_5 ni ravninski. Podobno, graf $K_{3,3}$ ima 6 vozlišč in 9 povezav ter ne vsebuje ciklov dolžine 3. Če bi bil ravninski, bi veljalo $9 \leq 2 \cdot 6 - 4$. Ker to ni res, graf $K_{3,3}$ ni ravninski.

13.2 Izreka Wagnerja in Kuratowskega

V tem razdelku si bomo ogledali nekaj operacij na grafih, ki ohranjajo lastnost "biti ravninski". Prva od takih operacij je operacija "podgraf". Očitno namreč velja naslednje:

TRDITEV 13.5 *Če je graf* Γ *ravninski, tedaj je ravniski tudi vsak njegov podgraf* Γ'*.*

Naslednja operacija, ki ohranja ravninskost, je operacija *subdivizije*, ki jo bomo sedaj opisali. Naj bo $e = u_0v_0$ poljubna povezava grafa Γ. Z Γ' označimo graf, ki ga dobimo iz Γ tako, da na sredi povezave e dodamo novo točko (stopnje 2). (Formalno bi lahko Γ' definirali kot graf z množico točk $V(\Gamma) \cup \{e\}$, kjer sta dve točki $u, v \in V(\Gamma)$, $uv \neq e$, sosednji v Γ', če sta bili sosednji v Γ, "nova točka" e je sosednja svojima krajiščema u_0 in v_0 v grafu Γ, točki u_0 in v_0 pa v grafu Γ' nista sosednji.) Grafu Γ' tedaj rečemo *graf, dobljen iz* Γ *s subdivizijo povezave* e. Vsakemu grafu, ki ga dobimo iz Γ z zaporednim subdividiranjem povezav, rečemo *subdivizija grafa* Γ. Ni se težko prepričati, da velja naslednje.

TRDITEV 13.6 *Naj bo* Γ' *poljubna subdivizija grafa* Γ*. Tedaj je* Γ *ravninski, če in samo če je ravninski* Γ'*.*

Če združimo zgornji dve trditvi s Trdtivijo 13.4, ugotovimo, da Γ, ki vsebuje kak podgraf Γ', ki je subdivizija grafa K_5 ali pa grafa $K_{3,3}$, ni ravninski. Presenetljivo pa je, da je ta potrebni pogoj za ravninskost hkrati tudi zadostni. Velja namreč naslednji globok in netrivialen izrek, ki nosi ime poljskega matematika Kazimierza Kuratowskega.

Izrek 13.7 *(Kuratowski) Graf Γ je ravninski, če in samo če noben od njegovih podgrafov ni subdivizija niti grafa K_5 niti grafa $K_{3,3}$.*

Za konec definirajmo še tretjo operacijo, ki ohranja ravninskost. Naj bo Γ' graf, dobljen iz kakega podgrafa grafa Γ z odstranjevanjem in krčenjem povezav (na vsakem koraku lahko odstranimo dobljene zanke, vzporedne povezave pa združimo v eno samo povezavo – tako ves čas ostajamo v razredu enostavnih grafov). Tedaj grafu Γ' rečemo *minor* grafa Γ. Ni se težko prepričati, da velja naslednje.

Trditev 13.8 *Če je graf Γ ravninski, tedaj je ravninski tudi vsak njegov minor Γ'.*

S pomočjo Trditve 13.4 lahko zato sklenemo, da graf, ki premore kak minor, izomorfen grafu K_5 ali grafu $K_{3,3}$, ni ravninski. Podobno kot v primeru subdivizij, pa velja ta implikacija tudi v obratni smeri. Karakterizaciji ravninskih grafov, ki jo tako dobimo, rečemo *Wagnerjev izrek*.

Izrek 13.9 *(Wagner) Graf Γ je ravninski, če in samo če ne premore minorja, izomorfnega K_5 ali $K_{3,3}$.*

14 Barvanja grafov

OPOMBA. Ta razdelek v veliki meri sledi sedmemu poglavju knjige [3].

Preslikavi $c\colon V(\Gamma) \to \{1, 2, \ldots, k\}$ pravimo *k-barvanje* točk grafa Γ. Barvanje točk c je *dobro* (tudi *pravilno*), če so sosednje točke obarvane z različnimi barvami, tj. $u \sim v \Rightarrow c(u) \neq c(v)$. Najmanjše število k, za katero obstaja dobro k-barvanje točk grafa Γ, imenujemo *kromatično število* (tudi *barvnost*) grafa G; oznaka $\chi(\Gamma)$.

Podobno preslikavi $c'\colon E(\Gamma) \to \{1, 2, \ldots, k\}$ pravimo *k-barvanje povezav* multigrafa brez zank Γ. Barvanje povezav c' je *dobro* (tudi *pravilno*), če so povezave, ki imajo kako skupno krajišče, obarvane z različnimi barvami. Najmanjše število k, za katero obstaja dobro k-barvanje povezav multigrafa brez zank Γ, imenujemo *kromatični indeks* multigrafa Γ; oznaka $\chi'(G)$.

14.1 Barvanje točk

Če je $\Gamma' \subseteq \Gamma$, potem je $\chi(\Gamma') \leq \chi(\Gamma)$. Naj bo $\omega(\Gamma)$ velikost največjega polnega podgrafa grafa Γ (velikost *maksimalne klike*) in $\Delta(\Gamma)$ maksimalna stopnja kakega vozlišča v Γ. Tedaj velja $\omega(\Gamma) \leq \chi(\Gamma) \leq \Delta(\Gamma) + 1$. Spodnja meja je očitna, saj za pravilno barvanje točk polnega grafa na n točkah potrebujemo n barv, zgornjo mejo pa z lahkoto dokažemo, če poskusimo točke pobarvati kar po požrešni metodi.

Nekoliko težje pa je dokazati, da je ta zgornja meja dosežena le pri lihih ciklih in polnih grafih. Prav to pravi Brooksov izrek.

IZREK 14.1 (Brooks). *Naj bo Γ povezan graf. Če Γ ni lih cikel in ni poln graf, potem je $\chi(\Gamma) \leq \Delta(\Gamma)$.*

Določanje kromatičnega števila konkretnega grafa je običajno sestavljeno iz dveh delov: iskanja spodnje meje (pri preprostih nalogah najdemo podgraf, za katerega poznamo kromatično število, npr. $\chi(K_n) = n$, $\chi(C_n) = 2$ za sode n in 3 za lihe n, $\chi(\Gamma) \leq 2$ natanko tedaj, ko je Γ dvodelen graf, itn.) in konstrukcije barvanja, ki dokaže, da je spodnjo mejo res moč doseči (večkrat si lahko pomagamo tudi z Brooksovim izrekom).

Včasih si delo lahko poenostavimo z naslednjim znamenitim izrekom:

IZREK 14.2 (Izrek štirih barv). *Za vsak ravninski graf Γ je $\chi(\Gamma) \leq 4$.*

Zgled. *Poišči kromatično število Petersenovega grafa Pet.*

Rešitev: Ker Pet vsebuje cikel dolžine 5, je $\chi(\text{Pet}) \geq \chi(C_5) = 3$. Ker je Pet kubičen graf, iz Brooksovega izreka dobimo $\chi(\text{Pet}) \leq 3$. Torej $\chi(\text{Pet}) = 3$. ■

14.2 Barvanje povezav

Tudi za barvanja povezav velja, da iz $\Gamma' \subseteq \Gamma$ sledi $\chi'(\Gamma) \leq \chi'(\Gamma)$. Najpomembnejši izrek o barvanju povezav grafov je:

Izrek 14.3 (Vizing). *Za vsak graf G velja $\Delta(\Gamma) \leq \chi'(\Gamma) \leq \Delta(\Gamma) + 1$.*

Graf Γ je *razreda* 1, če je $\chi'(\Gamma) = \Delta(\Gamma)$, sicer je *razreda* 2. Če je n sod, sta grafa C_n in K_n razreda 1, za lihe n-je pa sta razreda 2. Pomembna družina grafov razreda 1 so dvodelni grafi. Natančneje:

Izrek 14.4 (König). *Za dvodelni multigraf Γ velja $\chi'(\Gamma) = \Delta(\Gamma)$.*

Za multigrafe je kromatični indeks lahko večji od maksimalne stopnje točk plus ena.

Izrek 14.5 (Vizing; Shannon). *Naj bo Γ multigraf brez zank, v katerem ne obstaja več kot μ paroma vzporednih povezav (za grafe vzamemo $\mu = 1$). Potem je $\Delta(\Gamma) \leq \chi'(\Gamma) \leq \min\{\Delta(\Gamma) + \mu, \frac{3}{2}\Delta(\Gamma)\}$.*

Literatura

[1] V. Batagelj: *Kombinatorika*, samozaložba, Ljubljana, 1997.

[2] V. Batagelj, S. Klavžar: *DS2, algebra in teorija grafov, naloge*, DMFAS, Ljubljana, 1992.

[3] M. Juvan, P. Potočnik: *Kombinatorika s teorijo grafov: primeri in rešene naloge*, DMFAS, Ljubljana, 2000.

[4] J. H. van Lint, R. M. Wilson: *A Course in Combinatorics*, Cambridge University Press, Cambridge, 1993.

[5] D. Veljan: *Kombinatorika s teorijom grafova*, Školska knjiga, Zagreb, 1989.

[6] R. J. Wilson, J. J. Watkins: *Uvod v teorijo grafov*, DMFAS, Ljubljana, 1997.