Diskretna matematika 1

25. november 2024

1 Kombinatorika

1.1 Osnovna načela kombinatorike

Trditev 1.1 (Načelo produkta). Če sta A, B končni množici, potem je

$$|A \times B| = |A| \cdot |B|.$$

Trditev 1.2 (Posplošeno načelo produkta). Če so A_1, \ldots, A_k končne, potem je

$$|\Pi_{i=1}^k A_i| = \Pi_{i=1}^k |A_i|.$$

Trditev 1.3 (Načelo vsote). Če sta A in B končni in disjunktni množici, potem je

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

Trditev 1.4 (Posplošeno načelo vsote). Če so A_1, \ldots, A_k končne, paroma disjunktne množice, potem je

$$\bigcup_{i=1}^k A_i = \sum_{i=1}^k |A_i|.$$

Trditev 1.5 (Načelo enakosti). Če obstaja bijekcija $A \rightarrow B$, potem je

$$|A| = |B|$$
.

Označimo z $[k] = \{1, 2, ..., k\}.$

Primer. Naj bo A končna množica, |A| = n, $A = \{a_1, a_2, \dots, a_n\}$. Naj bo 2^A potenčna množica. Določi moč 2^A .

Trditev 1.6 (Načelo dvojnega preštevanja). Z njim pokažemo, da sta dva izraza/formuli enaka, če z obema na različna načina preštejemo elemente iste množice.

Primer (Eulorjeva funkcija ϕ). Za $n \in \mathbb{N}$ definiramo $\phi(n) =$ število števil iz [n], ki so tuji z n. Določi $\sum_{d|n} \phi(d)$.

Trditev 1.7 (Dirichletovo načelo). Če sta $n, m \in \mathbb{N}$ in je n > m, potem ne obstaja injektivna preslikava $[n] \to [m]$.

Opomba (Kombinatorična interpretacija). Če n predmetov razporedimo v m predalov in je n > m, potem sta vsaj v enem predalu vsaj dva predmeta.

Primer. Naj bo $X \subset [100], |X| = 10$. Pokaži, da X vsebuje dve disjunktni podmnožici z isto vsoto.

1.2 Število preslikav

Definicija 1.1. Množica $B^A = \{f : A \to B\}$ je množica vseh preslikav iz $A \ v \ B$.

Definicija 1.2. Definiramo:

- $n^{\underline{k}} = \underbrace{n(n-1)\dots(n-k+1)}_{k \text{ faktorjev}}$ je $padajoča \ potenca.$
- $n^{\overline{k}} = n(n+1) \dots (n+k-1)$ je naraščajoča potenca.
- $n! = \frac{n}{n}$ je n fakulteta.
- Množica z n elementi se imenuje n-množica.

Trditev 1.8. Naj bosta N in K končni množici z |N| = n, |K| = k. Tedaj velja:

- 1. $|K^N| = k^n$.
- 2. Število injektivnih preslikav iz N v K je $k^{\underline{n}}$.
- 3. Število bijekcij iz N v K je n!, če n = k in je 0 sicer.

Dokaz. Za 1. in 2. točko uporabimo načelo enakosti. V 3. točki upoštevamo, kadar je preslikava iz končne množice v končno množico bijektivna.

Binomski koeficienti in binomski izrek

Definicija 1.3. Naj bo $x \in \mathbb{C}$. Naj bo $k \in \mathbb{N}_0 = \{1, 2, \ldots\}$. Definiramo $\binom{x}{k} = \frac{x^{\underline{k}}}{k!} = \frac{x(x-1)\dots(x-k+1)}{k!}$. Števila $\binom{x}{k}$ so *binomski koeficienti*. Če je $k \notin \mathbb{N}_0$ definiramo $\binom{x}{k} = 0$.

Trditev 1.9. Če je $n \in \mathbb{N}_0$ in $k \leq n$, $k \in \mathbb{N}_0$, potem je

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

 $\check{S}tevila \binom{n}{k}$ so binomska števila.

Dokaz. Definicija binomskega koeficienta.

Opomba. Tudi $\binom{0}{0} = 1$. Razlaga: 0! = 1 je število bijektivnih preslikav iz \emptyset v \emptyset .

Opomba. Če je $0 \le k \le n$, potem $\binom{n}{k} = \binom{n}{n-k}$.

Definicija 1.4. Naj bo N množica. Definiramo $\binom{N}{k} = \{A \in P(N) \mid |A| = k\}.$

Trditev 1.10. Če je N n-množica in je $0 \le k \le n$, potem je

$$\left| \binom{N}{k} \right| = \binom{n}{k}.$$

Dokaz. Definiramo $X = \{(n_1, n_2, \dots, n_k); n_i \in \mathbb{N} \text{ paroma različni}\}$. Označimo $X_{n,k} = \binom{N}{k}$. Preštejemo elementi množici X na 2 načina.

Trditev 1.11. Za $n \in \mathbb{N}$ in $1 \le k \le n$ velja:

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

Dokaz. Naj bo N n-množica. Naj bo $x \in N$ poljuben fiksen element. Definiramo $\mathcal{A} = \left\{A \in \binom{N}{k}; \ x \in A\right\}$ in $\mathcal{B} = \left\{B \in \binom{N}{k}; \ x \notin B\right\}$. Potem $\binom{N}{k} = \mathcal{A} \cup \mathcal{B}$. Uporabimo prejšnjo trditev in načelo vsote.

Definicija 1.5. Pascalov trikotnik je trikotnik oblike

Opomba. S pomočjo Paskalovega trikotnika se lahko spomnimo rekurzivno formulo za $\binom{n}{k}$ (n je številka vrstice, k je številka diagonale, ki jo gledamo z leve proti desni). Šteteti vrstice in diagonale začnemo z 0.

Izrek 1.12 (Binomski izrek). Za vsak $n \in \mathbb{N}_0$ velja:

$$(a+b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}.$$

Dokaz. Izberimo k-krat a izmed n oklepajev.

Opomba. V izreku sta a in b elementi poljubnega komutativnega kolobarja.

1.4 Izbori

Naj bo N n-mnižica. Opazujemo izbori k-elementov.

- 1. Izbor je urejen (važno v kakšnem vrstnem redu izberimo elementi):
 - 1.1 Elementi si lahko ponavljajo: n^k .
 - 1.2 Elementi se ne smejo ponavljati: $n^{\underline{k}}$.
- 2. Izbor je neurejen:
 - 2.1 Elementi si lahko ponavljajo [trditev]: $\binom{n+k-1}{k}$.
 - 2.2 Elementi se ne smejo ponavljati: $\binom{n}{k}$.

Trditev 1.13. Število neurejenih izborov s ponavljanjem dolžine k iz n-množice N je

$$\binom{n+k-1}{k}$$
.

Dokaz. Naj bo $N = \{x_1, x_2, ..., x_n\}.$

Neurejenemu izboru
$$\underbrace{x_1 \dots x_1}_{k_1} \underbrace{x_2 \dots x_2}_{k_2} \dots \underbrace{x_n \dots x_n}_{k_n}$$
 priredimo niz $\underbrace{1 \dots 1}_{k_1} \underbrace{0 \dots 1}_{k_2} \underbrace{0 \dots 0}_{k_n} \underbrace{1 \dots 1}_{k_n}$.

1.5 Permutacije in permutacije s ponavljanjem

Definicija 1.6. Naj bo A n-množica. Permutacija množice A je bijektivna preslikava $\pi: A \to A$.

Množico vseh permutacij velikosti n (permutacij na [n]) označimo z S_n . Množico vseh permutacij množice A označimo z S_A .

Trditev 1.14. $|S_n| = n!$.

$$Dokaz$$
. Z indukcijo pokažemo, da je $|S_n| = n|S_{n-1}|$ in $|S_1| = 1$.

Trditev 1.15. Vsako permutacijo lahko zapišemo kot produkt disjunknih ciklov.

Definicija 1.7. Naj bo $\pi \in S_n$. Par je *inverzija*, če velja: i < j in $\pi(i) > \pi(j)$.

Definicija 1.8. Permutacija $\pi \in S_n$ je soda (oz. liha), če ima sodo mnogo inverzij (oz. liho mnogo inverzij).

1.5.1 Multimnožice

Definicija 1.9. Multimnožica z elementi v množici S je preslikava $\mu: S \to \mathbb{N}_0$. Pri tem številu $\mu(a), a \in S$, rečemo kratnost elementa a v multimnožici μ , vsoti $\sum_{a \in S} \mu(a)$ pa moč multimnožice μ . Multimnožica je končna, če je njena moč končna.

Opomba. Multimnožico M formalno podamo z urejenim parom (S, μ) . Namesto da elemente zapišemo večkrat, lahko kratnost označimo tudi s formalno potenco: $M = \{a, a, b, c, c, c\} = \{a^2, b, c^3\}$.

Multimnožica je isto kot neurejen izbor s ponavljanjem. Tojer obstaja $\binom{n+k-1}{k}$ k-elementnih multimnožic v množici z n elementi.

1.5.2 Permutacije multimnožic

Permutacija multimnožice $M=(S,\mu)$ moči n je zaporedje (x_1,\ldots,x_n) , kjer je $x_i\in S$ in se vsak $a\in S$ v zaporedju pojavi $\mu(a)$ -krat.

Trditev 1.16. Število permutacij multimnožice $M = \{1^{\alpha_1}, 2^{\alpha_2}, \dots, k^{\alpha_k}\}$ moči $n = \alpha_1 + \dots + \alpha_k$ je

$$\frac{n!}{\alpha_1!\alpha_2!\dots\alpha_k!}$$

Dokaz. Najprej izberimo položaje elementa 1, nato izberimo položaje elementa 2 itd.

Definicija 1.10. Številu $\frac{n!}{\alpha_1!\alpha_2!...\alpha_k!}$ rečemo *multinomski koeficient* in ga označimo z $\binom{n}{\alpha_1,\alpha_2,...,\alpha_k}$.

Opomba. Multinomski koeficient je posplošitev binomskega koeficienta.

Trditev 1.17 (Multinomski izrek). Velja

$$(x_1 + \ldots + x_k)^n = \sum \binom{n}{\alpha_1, \alpha_2, \ldots, \alpha_k} x_1^{\alpha_1} \ldots x_k^{\alpha_k},$$

kjer vsota teče po vseh izbirah naravnih števil $\alpha_1, \ldots, \alpha_k$, katerih vsota je n.

Dokaz. Število permutacij multimnožice moči n, kjer je S množica indeksov.

1.6 Kompozicije naravnega števila

Definicija 1.11. Kompožicija naravnega števila n je zaporedje pozitivnih naravnih števil $\lambda = (\lambda_1, \ldots, \lambda_l)$, za katero velja $\lambda_1 + \ldots + \lambda_l = n$. Dolžina kompozicije λ , $l(\lambda)$ je število elemetnov zaporedja, številu n pa rečemo velikost kompozicije. Števila $\lambda_1, \ldots, \lambda_l$ imenujemo členi kompozicije.

Trditev 1.18. Naj bo $n \ge 1$.

- 1. Število kompožicij števila n je enako 2^{n-1} .
- 2. Število kompožicij dolžine k števila n je enako $\binom{n-1}{k-1}$.

Dokaz. Število n lahko si predstavljamo kot zaporedje n kgoglic, kompozicijo pa s pregradami med kroglicami: $\bullet \mid \bullet \bullet \mid \bullet$.

Opomba. Lahko razumemo kompozicijo števila n s k členi kot rešitev enačbe $x_1 + \ldots + x_k = n$, kjer so $x_i \in \mathbb{N}$.

1.6.1 Šibke kompozicije

Šibka kompozicija števila n ima isto definicijo kot kompozicija, le da dovolimo med členi tudi ničle.

Trditev 1.19. *Število šibkih kompozicij števila n s k členi je* $\binom{n+k-1}{k-1} = \binom{n+k-1}{n}$.

Dokaz. 1. način. Rešujemo enačbo $x_1 + \ldots + x_k = n$, kjer so $x_i \in \mathbb{N}_0$.

- 2. način. Kroglice in pregrade.
- 3. način. Neurejeni izbori s ponavljanjem.

1.7 Razčlenitve naravnega števila

Definicija 1.12. Razčlenitev naravnega števila n je zaporedoje pozitivnih naravnih števil $\lambda = (\lambda_1, \ldots, \lambda_l)$, kjer je $\lambda_1 \geq \ldots \lambda_l$ in $\lambda_1 + \ldots + \lambda_l = n$. Dolžina razčlenitve λ , $l(\lambda)$ je število elemetnov zaporedja, številu n pa rečemo velikost razčlenitve. Števila $\lambda_1, \ldots, \lambda_l$ imenujemo členi razčlenitve. Razčlenitvam rečemo tudi particije.

Definicija 1.13. Naj bo $\lambda = (\lambda_1, \dots, \lambda_l)$ račlenitev naravnega števila n. Ferrersov diagram λ je seznam vrstic oblike:

1. vrsta:
$$\underbrace{\circ \circ \circ \dots \circ}_{\lambda_1 \text{ krožcev}}$$

2. vrsta:
$$\underbrace{\circ \circ \ldots \circ}_{\lambda_2 \text{ krožcev}}$$

:

k. vrsta:
$$\underbrace{\circ \dots \circ}_{\lambda_l \text{ krožcev}}$$

Definicija 1.14. Naj bo $\lambda = (\lambda_1, \dots, \lambda_l)$ račlenitev naravnega števila n. Konjugirana razčlenitev $\overline{\lambda}$ je razčlenitev, ki ima transponiran Ferrersov diagram.

Uvedemo oznake:

- p(n) je število razčlenitev števila n. Funkciji p(n) rečemo tudi razčlenitvena funkcija.
- $p_k(n)$ je število razčlenitev števila $n \le k$ členi.
- $\overline{p}_k(n)$ je število razčlenitev števila n z največ k členi.

Trditev 1.20. Za naravni števili n in k velja:

- 1. $p_k(n) = p_{k-1}(n-1) + p_k(n-k)$.
- 2. $p_k(n) = \overline{p}_k(n-k)$.
- 3. $\overline{p}_k(n) = \overline{p}_{k-1}(n) + \overline{p}_k(n-k)$.

Dokaz. Pomagamo si z Ferrersovim diagramom.

- 1. Razbijemo razčlinitve na tiste, ki vsebujejo 1 in tiste, ki jo ne vsebujejo.
- 2. Odštejemo od prvega stolpca 1.
- 3. Razčlenitev n z največ k členi ima bodisi natanko k členov bodisi kvečjemi k-1 členov.

1.8 Stirlingova števila I. vrste

Definicija 1.15. Naj bo $1 \le k \le n$. Stirlingovo število I. vrste C(n,k) je število permutacij množice [n], ki se zapišejo kot produkt k disjunktnih ciklov. Velja: C(n,0) = 0, n > 0 in C(0,0) = 1.

Primer. Izračunaj C(n,n), C(n,1), C(4,2).

Trditev 1.21. Naj bo $1 \le k \le n$. Velja:

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

Dokaz. Permutacije [n] s k cikli razdelimo takole:

- 1. tiste, kjer je n negibna točka in
- 2. ostale.

Za izračun C(n,k) lahko si pomagamo s Stirlingovo matriko I. vrste, ki jo dobimo s pomočjo rekurzivne zveze.

Trditev 1.22. $x^{\overline{n}} = \sum_{k=0}^{\infty} C(n,k) x^k$.

Dokaz. Indukcija po n.

Primer. Izračunaj $x^{\overline{4}}$.

1.9 Stirlingova števila II. vrste in Bellova števila

Definicija 1.16. Razdelitev množice X je družina podmnožic $\{X_i\}_{i\in I}$ za katero velja:

- $1. \bigcup_{i=I} X_i = X,$
- 2. $X_i \cap X_j = \emptyset$ za vsaka $i, j \in I, i \neq j$.

Definicija 1.17. Naj bo $1 \le k \le n$. Stirlingovo število II. vrste S(n,k) je število razdelitev množice [n] v k nepraznih razredov. Velja: S(n,0) = 0, n > 0 in S(0,0) = 1.

Primer. Izračunaj S(n,n), S(n,1), S(n,2).

Definicija 1.18. Bellovo število $B(n) = \sum_{k=0}^{\infty} S(n,k)$ je število vseh razdelitev n-množice v neprazne razrede.

Trditev 1.23. Naj bo $1 \le k \le n$. Velja:

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

Dokaz. Vzemimo množico [n]. Razdelitve v k razredov razdelimo takole:

- 1. tiste, ki imajo $\{n\}$ kot samostojni del in
- 2. ostale.

Za izračun S(n,k) lahko si pomagamo s Stirlingovo matriko II. vrste, ki jo dobimo s pomočjo rekurzivne zveze.

Trditev 1.24. $x^n = \sum_{k=0}^{\infty} S(n,k) x^{\underline{k}}$.

Dokaz. TODO

Opomba. Če dva polinoma stopnje n ujemata v n+1 točk, potem sta enaka.

Izrek 1.25. Število surjekcij iz n-množice v k-množico je enako

k!S(n,k).

Dokaz. Vsaka surjekcija določa razdelitev n-množice v k nepraznih razredov.

Trditev 1.26. $B(n+1) = \sum_{k=0}^{\infty} {n \choose k} B(k)$.

Dokaz. TODO

Definicija 1.19. Naj bo $1 \le k \le n$. Lahovo število L(n,k) je število razdelitev n-množice v k linearno urejenih kosov.

1.10 Dvajnastera pot

Naj bo N n-množica (predmetov) in K k-množica (predalov). Gledamo "funkcijo" $f: N \to K$, ki predmeti razporedi po predalih.

Imamo 12 možnosti: predmeti in predali lahko bodisi ločimo med seboj bodisi ne ločimo med seboj, funkcija lahko poljubna, inkjektivna (vsak predal ima kvečjemu 1 predmet) ali surjektivna (noben predal ni prazen).

Izrek 1.27 (Dvajnastera pot). Velja:

ločimo predmeti/predali	poljubna	ig injektivna	surjektivna
DA/DA	k^n	$k^{\underline{n}}$	k!S(n,k)
DA/NE	$\sum_{i \le k} S(n, i)$	$\begin{cases} 1; & n \le k \\ 0; & sicer \end{cases}$	S(n,k)
NE/DA	$\binom{n+k-1}{k-1}$	$\begin{cases} \binom{k}{n}; & n \le k \\ 0; & sicer \end{cases}$	$\binom{n-1}{k-1}$
NE/NE	$\overline{p}_k(n)$	$\begin{cases} 1; & n \le k \\ 0; & sicer \end{cases}$	$p_k(n)$

Dokaz. Uporabimo že znane rezultate (kompozicije, razčlenitve) itd.

1.11 Načelo vključitev in izključitev

Recimo, da sta A, B poljubni množici, potem $|A \cup B| = |A| + |B| - |A \cap B|$.

Primer. Koliko so števil v [30] ni tujih s 30? Koliko so tujih?

Izrek 1.28 (Načelo vključitev in izključitev). Naj bo A_1, \ldots, A_n množice. Velja:

$$\left| \bigcup_{i=1}^{n} A_i \right| = \sum_{j=1}^{n} (-1)^{j+1} \sigma_j,$$

$$kjer\ je\ \sigma_j = \sum_{I \in \binom{[n]}{i}} \left| \bigcap_{i \in I} A_i \right|.$$

Dokaz. Pokažemo, da če $x \in \bigcup_{i=1}^n A_i$, potem prispeva natanko 1 k formuli.

Primer. Na koliko načinov lahko razporedimo n označenih predmetov v k označenih predalov, če je vsaj en predal prazen?

Posledica 1.28.1. Če je X N-množica in so $A_1, \ldots, A_n \subset X$, potem je število elementov množice X, ki niso v nobeni izmed množic A_1, \ldots, A_n enako

$$N + \sum_{j=1}^{n} (-1)^j \sigma_j.$$

Definicija 1.20. Premestitev množice [n] je permutacija $\pi \in S_n$ brez negibnih točk.

Primer. Izračunaj število premestitev množice [n].

Izrek 1.29. Če je $n = p_1^{e_1} \dots p_r^{e^r}$ razcep $n \in \mathbb{N}$ na prafaktorji, potem je

$$\phi(n) = n(1 - \frac{a}{p_1}) \dots (1 - \frac{1}{p_r})$$
 (Eulorjeva funkcija).

Dokaz. TODO

1.12 Rekurzivne enačbe

Primer. Na koliko načinov lahko prehodimo n stopnic, če vsakič pregodimo 1 ali 2?

Primer. Koliko je dvojiških dreves s korenom z n vozlišč?

Izrek 1.30. Naj bo zaporedje $(a_n)_{n\geq 0}$ podano takole:

$$a_0 = b_0$$
, $a_1 = b_1$, $a_n = Aa_{n-1} + Ba_{n-2}$, $n \ge 2$,

kjer so b_0, b_1, A, B fiksna števila. Naj bosta α in β korena <u>karakteristične enačbe</u> $x^2 = Ax + B$. Tedaj velja:

1. Če je $\alpha \neq \beta$, potem obstajata konstanti K_1, K_2 , tako da je

$$a_n = K_1 \alpha^n + K_2 \beta^n.$$

2. Če je $\alpha = \beta$, potem obstajata konstanti K_1, K_2 , tako da je

$$a_n = (K_1 + K_2 n)\alpha^n.$$

Splošen primer

Zaporedje $(a_n)_{n>0}$ je podano takole:

- 1. $a_0=b_0, a_1=b_1,\dots,a_{d-1}=d_{d-1},$ kjer so b_0,b_1,\dots,b_{d-1} fiksna števila.
- 2. $c_d a_{n+d} + c_{d-1} a_{n+d-1} + \ldots + c_1 a_{n+1} + c_0 a_n = f(n)$ (*), kjer so c_d, \ldots, c_0 fiksna števila, $f(n) : \mathbb{N}_0 \to \mathbb{C}$.

Definicija 1.21. (*) je <u>d-člena linearna rekurzija s konstantnimi koeficienti</u>. Če je $f(n) \equiv 0$, potem rečemo, da je rekurzija (*) homogena.

Kako rešemo homogeno rekurzijo?

TODO

Izrek 1.31. $(a_n)_{n\geq 0}\in \ker((E-\lambda I)^s)\Leftrightarrow a_n \ je \ oblike \ a_n=P(n)\lambda^n, \ kjer \ je \ P(n) \ polinom \ stopnje \ kvečjemu \ s-1.$

Izrek 1.32. Splošna rešitev enačbe

$$c_d a_{n+d} + c_{d-1} a_{n+d-1} + \ldots + c_1 a_{n+1} + c_0 a_n = 0$$

je oblike

$$A_1(n)\lambda_1^n + \ldots + A_k(n)\lambda_k^n$$

kjer so λ_i ničla karakterističnega polinoma kratnosti s_i , in je $A_i(n)$ polinom stopnje k večjemu $s_i - 1$ za vse $i \in [k]$.

Kako rešemo nehomogeno rekurzijo?

Rešitev nehomogene enačbe

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

je oblike

$$z_n + b_n$$

kjer je z_n splošna rešitev ustrezne homogene enačne in je b_n neka partikularna rešitev enačbe (*). Pri tem b_n praviloma iščemo z ustreznim nastavkom, pri čemer upoštevamo, da če je f(n) aditivna, torej

$$f(n) = f_1(n) + \ldots + f_t(n),$$

potem b_n lahko dobimo kot vsoto partikularnih rešitev od

$$c_d a_{n+d} + c_{d-1} a_{n+d-1} + \ldots + c_1 a_{n+1} + c_0 a_n = f_i(n).$$

Primer. Pri začetnih pogojah $a_0 = 0$, $a_1 = 1$, reši enačbo $a_n = 4a_{n-1} - 4a_{n-2} - 2n + 5 \cdot 3^n$.