Diskretna matematika 1

Luka Horjak (lukahorjak@student.uni-lj.si)

3. april 2022

Kazalo

Uvod

V tem dokumentu so zbrani moji zapiski s predavanj predmeta Diskretna matematika 1 v letu 2021/22. Predavatelj v tem letu je bil prof. dr. Sandi Klavžar.

Zapiski niso popolni. Manjka večina zgledov, ki pomagajo pri razumevanju definicij in izrekov. Poleg tega nisem dokazoval čisto vsakega izreka, pogosto sem kakšnega označil kot očitnega ali pa le nakazal pomembnejše korake v dokazu.

Zelo verjetno se mi je pri pregledu zapiskov izmuznila kakšna napaka – popravki so vselej dobrodošli.

1 Kombinatorika

1.1 Osnovna načela kombinatorike

Trditev 1.1.1 (Načelo produkta)**.** Naj bodo $A_1, \dots, A_n$ končne množice. Tedaj je

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

Trditev 1.1.2 (Načelo vsote)**.** Naj bodo $A_1, \dots, A_n$ končne, paroma disjunktne množice. Tedaj je

$$\left|\bigcup_{i=1}^n A_i\right| = \sum_{i=1}^n |A_i|\,.$$

Trditev 1.1.3 (Načelo enakosti)**.** Če obstaja bijekcija med končnima množicama A in B, je

$$|A| = |B|\,.$$

Definicija 1.1.4. Označimo

$$[n] = \{i \in \mathbb{N} \mid i \leq n\}\,.$$

Trditev 1.1.5. Za *Eulerjev fi*

$$\varphi(n) = |\{i \in [n] \mid (i, n) = 1\}|$$

velja rekurzivna formula

$$\sum_{d|n} \varphi(d) = n.$$

Dokaz. Na dva načina izračunamo moč množice

$$\left\{\frac{i}{n} \;\middle|\; i \in [n]\right\}. \qquad \square$$

Izrek 1.1.6 (Dirichletovo načelo)**.** Če je $n > m$, potem ne obstaja injektivna preslikava $f\colon [n] \to [m]$.

Dokaz. The proof is obvious and need not be mentioned. $\square$

Trditev 1.1.7 (Načelo dvojnega preštevanja)**.** Če dva izraza predstavljata število elementov iste množice, sta enaka.

Definicija 1.1.8. Definiramo padajočo in naraščajočo potenco

$$k^{\underline{n}} = \prod_{i=0}^{n-1} (k - i) \quad \text{in} \quad k^{\overline{n}} = \prod_{i=0}^{n-1} (k + i).$$

Trditev 1.1.9. Za množico N z n elementi in množico K s k elementi velja

i) $\left|K^N\right| = k^n$

ii) $|\{f\colon N \to K \mid f \text{ je injektivna}\}| = k^{\underline{n}}$

iii) Število bijekcij med N in K je $n!$, če je $n = k$, sicer pa 0.

Dokaz. The proof is obvious and need not be mentioned. □

Opomba 1.1.9.1. Če imata končni množici enako moč, je bijektivnost preslikave med njima ekvivalentna tako injektivnosti kot surjektivnosti.

1.2 Binomski koeficienti in binomski izrek

21. februar 2022

Definicija 1.2.1. Naj bo $x \in \mathbb{C}$ in $k \in \mathbb{N}_0$. *Binomski koeficient* števil x in k je število

$$\binom{x}{k} = \frac{x^{\underline{k}}}{k!}.$$

Trditev 1.2.2. Če je $n \in \mathbb{N}_0$ in $k \leq n$, potem je

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

Dokaz. The proof is obvious and need not be mentioned. $\square$

Definicija 1.2.3. Naj bo X končna množica. Označimo

$$\binom{X}{k} = \{A \subseteq X \mid |A| = k\}.$$

Trditev 1.2.4. Za končno množico X velja

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

Dokaz. Na dva načina preštejemo število urejenih k-teric. Dobimo, da je

$$k! \cdot \left|\binom{X}{k}\right| = |X|^{\underline{k}}.$$ $\square$

Trditev 1.2.5. Če je $1 \leq k \leq n$, je

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

Dokaz. Preštejmo število k-elementnih podmnožic $[n]$ na dva načina. Za število 1 imamo dve možnosti – lahko je v podmnožico ali ne. Sedaj preštejemo načine, na katere lahko izmed preostalih $n-1$ elementov izberemo ustrezno število. V prvem primeru dobimo $\binom{n-1}{k-1}$ podmnožic, v drugem pa $\binom{n-1}{k}$. $\square$

Posledica 1.2.5.1. Binomski koeficienti so ravno števila v *Pascalovem trikotniku*:

$$\begin{array}{ccccccccc} & & & & 1 & & & & \\ & & & 1 & & 1 & & & \\ & & 1 & & 2 & & 1 & & \\ & 1 & & 3 & & 3 & & 1 & \\ 1 & & 4 & & 6 & & 4 & & 1 \end{array} \quad = \quad \begin{array}{ccccccccc} & & & & \binom{0}{0} & & & & \\ & & & \binom{1}{0} & & \binom{1}{1} & & & \\ & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & \\ & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & \\ \binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4} \end{array}$$

Izrek 1.2.6 (Binomski)**.** Za vse $n \in \mathbb{N}_0$ za $a, b \in K$, kjer je K komutativen kolobar, velja

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

Dokaz. Uporabimo distributivnost in preštejemo število pojavitev vsakega monoma. $\square$

1.3 Izbori

Definicija 1.3.1. Naj bo N množica z n elementi.

i) *Urejen izbor s ponavljanjem* je vsaka urejena k-terica elementov N.

ii) *Urejen izbor brez ponavljanja* je vsaka k-terica paroma različnih elementov N.

iii) *Neurejen izbor brez ponavljanja* je vsaka podmnožica k elementov množice N.

iv) *Neurejen izbor s ponavljanjem* je vsaka multimnožica s k elementi iz N.

Opomba 1.3.1.1. Urejenim izborom pravimo tudi *variacije*, neurejenim pa *kombinacije*.

Trditev 1.3.2. Število neurejenih izborov s ponavljanjem je enako

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

Dokaz. Uporabimo strategijo pik in pregrad. Naj x_k označuje število pojavitev elementa k v multimnožici.[1] Tedaj lahko vsak izbor predstavimo kot

$$\underbrace{\bullet\bullet\cdots\bullet}_{x_1} \mid \underbrace{\bullet\bullet\cdots\bullet}_{x_2} \mid \cdots \mid \underbrace{\bullet\bullet\cdots\bullet}_{x_n}.$$

Vsak izbor natanko ustreza enemu zapisu s pikami in pregradami, teh pa je ravno $\binom{n+k-1}{k}$. Izmed $n+k-1$ elementov moramo namreč izbrati k pik, preostalih $n-1$ mest pa zasedejo pregrade. $\square$

[1] Definicija v naslednjem razdelku.

1.4 Permutacije in permutacije s ponavljanjem

Definicija 1.4.1. *Permutacija* množice A je bijekcija $f\colon A \to A$. Označimo

$$S_A = \{f\colon A \to A \mid f \text{ je bijekcija}\},$$

v posebnem primeru

$$S_n = S_{[n]}.$$

Definicija 1.4.2. *Multimnožica* je urejen par (U, μ), kjer je U množica in $\mu\colon U \to \mathbb{N}_0$.

28. februar 2022

Definicija 1.4.3. *Permutacija multimnožice* $M = (U, \mu)$ je vsako zaporedje elementov $(x_1, \dots, x_n)$, kjer so vsi $x_i \in U$ in se vsak element $x \in U$ v zaporedju pojavi $\mu(x)$ krat.

Trditev 1.4.4. Število permutacij multimnožice $\{1^{\alpha_1}, \dots, k^{\alpha_k}\}$, kjer je $\alpha_1 + \dots + \alpha_k = n$, je natanko

$$\frac{n!}{\alpha_1! \cdots \alpha_k!}.$$

Dokaz. Velja

$$\prod_{i=1}^{n} \binom{n - \alpha_1 - \dots - \alpha_{i-1}}{\alpha_i} = \frac{n!}{\alpha_1! \cdots \alpha_k!}.$$ □

Opomba 1.4.4.1. Zgornjemu številu pravimo *multinomski koeficient* in ga označimo z

$$\frac{n!}{\alpha_1! \dots \alpha_k!} = \binom{n}{\alpha_1, \dots, \alpha_k}.$$

Izrek 1.4.5 (Multinomski)**.** Za $n \geq 0$ velja

$$\left(\sum_{i=1}^{k} x_i\right)^n = \sum_{\alpha_1 + \dots + \alpha_k = n} \binom{n}{\alpha_1, \dots, \alpha_k} \prod_{i=1}^{k} x_i^{\alpha_i}.$$

Dokaz. Enak kot pri binomskem. □

1.5 Kompozicije in razčlenitve

Definicija 1.5.1. *Kompozicija* naravnega števila n je zaporedje $\lambda = (\lambda_1, \dots, \lambda_l)$, kjer so $\lambda_i \in \mathbb{N}$ in velja

$$\sum_{i=1}^{l} \lambda_i = n.$$

Trditev 1.5.2. Število kompozicij števila n je 2^{n-1}. Število kompozicij dolžine k je $\binom{n-1}{k-1}$.

Dokaz. Pike in pregrade. □

Definicija 1.5.3. *Šibka kompozicija* naravnega števila n je kompozicija, v kateri dovolimo, da so nekateri členi enaki 0.

Trditev 1.5.4. Število šibkih kompozicij števila n dolžine k je $\binom{n+k-1}{k-1}$.

Dokaz. Pike in pregrade. □

Definicija 1.5.5. *Razčlenitev* števila $n \in \mathbb{N}$ je vsaka padajoča kompozicija števila n. Število razčlenitev dolžine k označimo z $p_k(n)$, število razčlenitev dolžine največ k pa z $\overline{p}_k(n)$.

Trditev 1.5.6. Veljajo naslednje zveze:

i) $p_k(n) = \overline{p}_k(n-k)$

ii) $\overline{p}_k(n) = \overline{p}_{k-1}(n) + \overline{p}_k(n-k)$

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

Dokaz. The proof is obvious and need not be mentioned. □

1.6 Stirlingova števila

Definicija 1.6.1. Za $1 \leq k \leq n$ je *Stirlingovo število 1. vrste* $c(n,k)$ število permutacij S_n, ki jih lahko zapišemo kot produkt k ciklov. Posebej naj bo $c(n,0) = 0$ za $n \geq 1$ in $c(0,0) = 1$.

Trditev 1.6.2. Velja rekurzivna formula

$$c(n,k) = c(n-1,k-1) + (n-1) \cdot c(n-1,k).$$

Dokaz. Permutacij, v katerih je x fiksna točka, je $c(n-1,k-1)$, drugače pa na $n-1$ načinov izberemo element, v katerega se preslika x, nato pa jih razporedimo v k ciklov. □

Izrek 1.6.3. Velja

$$x^{\overline{n}} = \sum_k c(n,k)x^k.$$

Dokaz. Indukcija po n. □

Definicija 1.6.4. Družina nepraznih množic $\{X_i\}_{i \in I}$ je *razdelitev*, če za vse različne $i, j \in I$ velja $X_i \cap X_j = \emptyset$ in

$$\bigcup_{i \in I} X_i = X.$$

Množicam X_i pravimo *blok razdelitve*

Definicija 1.6.5. Za $1 \leq k \leq n$ je *Stirlingovo število 2. vrste* $S(n,k)$ število razdelitev n-množice v k blokov.

Trditev 1.6.6. Velja rekurzivna zveza

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

Dokaz. Če je element x v nekem bloku sam, imamo $S(n-1,k-1)$ možnosti, drugače pa na k načinov izberemo blok, v katerega ga dodamo. □

Izrek 1.6.7. Velja

$$x^n = \sum_k S(n,k) \cdot x^{\underline{k}}.$$

Dokaz. Dovolj je izrek dokazati za naravna števila. Naj bo $A = [x]^n$. Velja $|A| = x^n$. Po drugi strani pa lahko A razdelimo glede na število različnih elementov k, teh pa je $S(n,k) \cdot x^{\underline{k}}$. □

Trditev 1.6.8. Število surjekcij $f \in K^N$ je

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

Dokaz. The proof is obvious and need not be mentioned. □

Definicija 1.6.9. *Bellovo število* $B(n)$ je število vseh razdelitev množice z n elementi v bloke, oziroma

$$B(n) = \sum_k S(n,k).$$

Trditev 1.6.10. Velja rekurzivna formula

$$B(n+1) = \sum_k \binom{n}{k} B(k).$$

Dokaz. Naj bo x v bloku velikosti $k+1$. Tedaj je razdelitev natanko

$$\binom{n}{k} \cdot B(n-k).$$

□

Definicija 1.6.11. Za $1 \leq k \leq n$ je *Lahova števila* $L(n,k)$ število razdelitev n-množice v k linearno urejenih blokov.

Trditev 1.6.12. Velja rekurzivna zveza

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

Dokaz. Podobno kot prejšnji. □

Izrek 1.6.13. Velja

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

Dokaz. Elemente uredimo na $n!$ načinov, nato pa izberemo $k-1$ elementov, ki so prvi v svojem bloku. Pri tem smo vsako razdelitev šteli $k!$-krat. □

Izrek 1.6.14. Velja

$$x^{\overline{n}} = \sum_k L(n,k) x^{\underline{k}}.$$

1.7 Dvanajstera pot

Izrek 1.7.1. Tabela al neki idk, idgaf, this is bs

14. marec 2022

Tabela 1: Kill me pls

$f: N \to K$	Poljubna	Injektivna	Surjektivna
Ločimo elemente N in K	k^n	$k^{\underline{n}}$	$k! \cdot S(n,k)$
Ločimo elemnete K	$\binom{n+k-1}{n}$	$\binom{k}{n}$	$\binom{n-1}{k-1}$
Ločimo elemente N	$\sum_{i=1}^{k} S(n,i)$	$\begin{cases} 1, & n \leq k \\ 0, & n > k \end{cases}$	$S(n,k)$
Ne ločimo elementov	$\overline{p}_k(n)$	$\begin{cases} 1, & n \leq k \\ 0, & n > k \end{cases}$	$p_k(n)$

Dokaz. The proof is obvious and need not be mentioned. □

1.8 Načelo vključitev in izključitev

Izrek 1.8.1 (Načelo vključitev in izključitev)**.** Velja

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{\substack{X \in \mathcal{P}([n]) \\ X \neq \emptyset}} (-1)^{|X|+1} \cdot \left|\bigcap_{i \in X} A_i\right|.$$

Dokaz. Vsak element štejemo natanko

$$\sum_{i=1}^{k} (-1)^{i+1} \binom{k}{i} = 1$$

krat. □

Izrek 1.8.2. Velja

$$\varphi(n) = n \cdot \prod_{p \mid n} \left(1 - \frac{1}{p}\right).$$

Dokaz. The proof is obvious and need not be mentioned. □

1.9 Rekurzivne enačbe

Izrek 1.9.1. Naj bo zaporedje $(a_n)_{n=0}^{\infty}$ podano z rekurzivno zvezo

$$a_n = Aa_{n-1} + Ba_{n-2}.$$

Naj bosta α in β ničli karakterističnega polinoma.

i) Če je $\alpha \neq \beta$, obstajata taki konstanti K_1 in K_2, da je

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

ii) Če je $\alpha = \beta$, obstajata taki konstanti K_1 in K_2, da je

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

Dokaz. Dokažemo, da taka K_1 in K_2 obstajata za a_0 in a_1, nato pa z indukcijo dokažemo še, da je to splošen predpis. □

Izrek 1.9.2. Zaporedje $(a_n)_{n=0}^{\infty}$ reši homogeno rekurzivno enačbo natanko tedaj, ko je oblike

$$a_n = \sum_{i=1}^{k} A_i(n)\lambda_i^n,$$

kjer so λ_i ničle karakterističnega polinoma, A_i pa polinomi, katerih stopnja je manjša od večkratnosti pripadajoče ničle.

Dokaz. Naj bo Q karakteristični polinom, $E\colon \mathbb{C}^{\mathbb{N}_0} \to \mathbb{C}^{\mathbb{N}_0}$ pa endomorfizem vektorskih prostorov, ki deluje po predpisu $E\colon (a_0, a_1, \dots) \mapsto (a_1, a_2, \dots)$. Tedaj je tudi $Q(E)$ endomorfizem, zaporedje a pa je v jedru endomorfizma natanko tedaj, ko zadošča rekurzivni enačbi. Naj bo sedaj $\varphi\colon \ker(Q(E)) \to \mathbb{C}^d$ preslikava, ki deluje po predpisu

$$\varphi(a_0, a_1, \dots) = (a_0, \dots, a_{d-1}).$$

Opazimo, da je φ linearna in bijektivna. Sledi, da je $\dim\ker(Q(E)) = d$.

Naj bo sedaj

$$Q(x) = \prod_{i=1}^{k}(x - \lambda_i)^{s_i}.$$

Sledi, da je

$$\ker(Q(E)) = \bigoplus_{i=1}^{k} \ker((E - \lambda_i I)^{s_i}).$$

Ni pa težko opaziti, da je

$$\left\{ n^k\lambda^n \;\middle|\; 0 \le k < s \right\}$$

baza $\ker((E - \lambda)^s)$, saj vsaka iteracija zmanjša stopnjo polinoma. □

Opomba 1.9.2.1. Nehomogene linearne rekurzivne enačbe rešujemo tako, da z nastavkom poiščemo partikularno rešitev enačbe, nato pa ji prištejemo homogeno rešitev.

1.10 Rodovne funkcije

28. marec 2022

Definicija 1.10.1. *Formalna potenčna vrsta* zaporedja $(a_n)_{n=1}^{\infty}$ je zapis

$$F(x) = \sum_{n=0}^{\infty} a_n x^n.$$

S seštevanjem in množenjem s skalarjem po komponentah ter množenjem

$$A(x) \cdot B(x) = \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} a_k b_{n-k} \right) x_n$$

postanejo formalne potenčne vrste algebra.

Trditev 1.10.2. Formalna potenčna vrsta je obrnljiva natanko tedaj, ko je njen prosti člen različen od 0.

Dokaz. Če je $AB = 1$, je $a_0 b_0 = 1$, zato je prosti člen neničeln. Če pa je $a_0 \neq 0$, lahko induktivno definiramo $b_0 = a_0^{-1}$ in

$$b_n = - \left(\sum_{k=1}^{n} a_k b_{n-k} \right) a_0^{-1}. \qquad \square$$

Definicija 1.10.3. *Odvod* formalne potenčne vrste je vrsta

$$A'(x) = \sum_{n=0}^{\infty} (n+1) a_{n+1} x^n.$$

Opomba 1.10.3.1. Za odvod velja

$$(A+B)' = A' + B', \quad (AB)' = A'B + AB' \quad \text{in} \quad (A^{-1})' = \frac{-A'}{A^2}.$$

2 Dodatek

A Število izborov z omejitvami

Tabela 2: Število izborov k elementov iz množice z n elementi

	S ponavljanjem	Brez ponavljanja
Urejen izbor	n^k	$n^{\underline{k}}$
Neurejen izbor	$\binom{n+k-1}{k}$	$\binom{n}{k}$

B Stirlingova števila prve vrste

Tabela 3: Stirlingova števila prve vrste

$n \setminus k$	0	1	2	3	4	5	6
0	1						
1	0	1					
2	0	1	1				
3	0	2	3	1			
4	0	6	11	6	1		
5	0	24	50	35	10	1	
6	0	120	274	225	85	15	1

C Stirlingova števila druge vrste

Tabela 4: Stirlingova števila druge vrste

$n \setminus k$	0	1	2	3	4	5	6
0	1						
1	0	1					
2	0	1	1				
3	0	1	3	1			
4	0	1	7	6	1		
5	0	1	15	25	10	1	
6	0	1	31	90	65	15	1

Stvarno kazalo