Kombinatorika - zapsiski s predavanj prof. Konvalinke

Domen Vogrin Tomaž Poljanšek Yon Ploj

jesen/zima 2021

Kazalo

1 Osnovni principi kombinatorike

1.1 Funkcije in štetje

Definicija 1.1 (Funkcija)**.**

- injektivna (y je slika največ enega x) ($x_1 \neq x_2 \to f(x_1) \neq f(x_2)$)
- surjektivna (y je slika vsaj enega x) ($\forall y \in Y \exists x \in X : f(x) = y$)
- bijektivna (y je slika natanko enega x) (injektivna in surjektivna)

$$\begin{aligned}
\exists \text{ injekcija } f : X \to Y &\implies |X| \leqslant |Y| \\
\exists \text{ surjekcija } f : X \to Y &\implies |X| \geqslant |Y| \\
\exists \text{ bijekcija } f : X \to Y &\implies |X| = |Y|
\end{aligned}$$

$f : X \to Y$ lahko interpretiramo kot razporejanje kroglic (X) v škatle (Y).
Oznake:

$$\begin{gathered}
\mathbb{N} := \{0, 1, 2, ...\} \\
[n] := \{1, 2, ..., n\}, \quad |[n]| = n \\
2^X := \{A \subseteq X\} (= P(x)) \\
Y^X := \{f : X \to Y\}
\end{gathered}$$

Izrek 1.2 (Binomski)**.**

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

1.2 Osnovna načela

Izrek 1.3 (Dirichletovo načelo)**.**

$$\exists \text{ injektivna } f : X \to Y \implies |X| \leqslant |Y|$$

Ekvivalentno:

$$|X| > |Y| \implies \neg\exists \text{ injektivna } \ f : X \to Y$$

ali z besedami: “če damo n kroglic v k škatel in velja $n > k$, sta v vsaj eni škatli vsaj dve kroglici.”

Izrek 1.4 (Načelo vsote).

$$A \cap B = \emptyset \implies |A \cup B| = |A| + |B|$$

Izrek 1.5 (Načelo vključitev in izkjučitev).

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

Izrek 1.6 (Načelo produkta).

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

Kako uporabljamo ti dve načeli?

- načelo vsote: dve (disjunktni) možnosti, obarvamo vsako posebej, rezultata seštejemo
- načelo produkta: naredimo dve <u>neodvisni</u> izbiri, število možnosti za eno in drugo zmnožimo

Trditev 1.7. $|2^X| = 2^{|X|}$

Dokaz. (Formalen)

$$\Phi = 2^X \to \{0,1\} \times \{0,1\} \times ... \times \{0,1\} \text{ (n-krat)}$$

$$\Phi(A) = (\varepsilon_1, ..., \varepsilon_n), A \subseteq X$$

$$\varepsilon_i = \begin{cases} 0: & x_i \notin A \\ 1; & x_i \in A \end{cases}$$

$$\Psi : \{0,1\}^n \to 2^X$$

$$\Psi(\varepsilon_1, ..., \varepsilon_n) = \{x_i : \varepsilon_i = 1\}$$

$$\Psi \circ \Phi = id_{2^X}$$

$$\Phi \circ \Psi = id_{\{0,1\}^n}$$

$$\implies \Phi \text{ je bijekcija}$$

$$|\{0,1\}^n| = 2^n \text{ po načelu produkta} \implies |2^X| = 2^{|X|}$$

■

Dokaz. (Intuitiven)
Za vsakega od n elementov imamo dve izbiri (damo / ne damo v podmnožico). Izbire so neodvisne, torej imamo $2 \cdot 2 \cdot ... \cdot 2 = 2^n$ izbir. ∎

Trditev 1.8. $|Y^X| = |Y|^{|X|}$

Dokaz. (Formalen)

$$\Phi : Y^X \to Y^{|X|}$$

$$X = \{x_1, ..., x_n\}$$

$$\Phi(f) = (f(x_1), ..., f(x_n))$$

$$\Psi(y_1, ..., y_n) = f$$

$$f(x_i) = y_i$$

∎

Dokaz. (Intuitiven)
Za vsak element iz X imamo $|Y|$ izbir. Izbire so neodvisne, torej imamo $|Y| \cdot |Y| \cdot ... \cdot |Y| = |Y|^{|X|}$ izbir. ∎

Trditev 1.9. Število injektivnih preslikav v Y^X je

$$|Y| \cdot (|Y| - 1) \cdot ... \cdot (|Y| - |X| + 1)$$

Dokaz. Za sliko prvega elementa imamo $|Y|$ izbir, za drugega $(|Y| - 1)$, ...

Opomba. Tu smo uporabili varianto pravila produkta - izbire niso neodvisne, je pa neodvisno število izbir.

Opomba. Velja tudi za $|X| > |Y|(= 0)$

∎

1.3 Permutacije

Definicija 1.10 (Permutacija)**.** Bijektivna preslikava iz X v X se imenuje permutacija. Množico permutacij $[n]$ označimo S_n.

Definicija 1.11 (Relacija)**.** Je množica $R \subseteq X \times Y$. Zapis $(x, y) \in R$ krajšamo kot xRy.

Definicija 1.12 (Preslikava)**.** Relacija f je preslikava, kadar velja:

$$\forall x \in X \; \exists! y \in Y : xfy$$

Pišemo $y = f(x)$.

Trditev 1.13.

$$|S_n| = n!$$

Dokaz. Za sliko 1 imamo n možnosti, za sliko 2 jih je $(n-1)$, ... ■

Primer. Komponiranje permutacij

$$(4\;2\;6\;1\;3\;5) \cdot (3\;6\;1\;2\;5\;4) = (6\;5\;4\;2\;3\;1)$$

Kompozitum je asociativen, a ni komutativen. Ima enoto, $id = (1\;2\;\ldots\;n)$ in inverz, npr. $(4\;2\;6\;1\;3\;5)^{-1} = (4\;2\;5\;1\;6\;3)$.

Definicija 1.14 (Simetrična grupa)**.** Množica permutacij s komponiranjem tvori grupo $(S_n, \cdot)$.

Naj bo $\pi \in S_n$, $i \in [n]$

$$i, \pi(i), \pi^2(i), \pi^3(i), \cdots$$

Po Dirichletovem principu obstajata j in j', $j < j'$, tako da

$$\pi^j(i) = \pi^{j'}(i) \implies i = \pi^{j'-j}(i)$$

$$(i \;\; \pi(i) \;\; \pi^2(i) \;\; \cdots \;\; \pi^{n-1}(i))$$

Trditev 1.15. Permutacijo lahko zapišemo kot produkt disjunktnih ciklov

Primer.

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

2 Podmnožice in načrti

2.1 Binomski koeficienti

Definicija 2.1 (Potenčna množica)**.**

$$2^A := \{B \subseteq A\}$$

Definicija 2.2 (Binomski simbol)**.** Lahko definiramo tudi za množice

$$\binom{A}{k} := \{B \subseteq A : |B| = k\}$$

Beremo "A nad k".

Definicija 2.3 (Binomski koeficient)**.**

$$\binom{n}{k} := \left|\binom{[n]}{k}\right|$$

Beremo "n nad k" ("n choose k").

Izrek 2.4 (Pomen binomskega koeficienta)**.** $\binom{n}{k}$ nam pove število k-elementnih podmnožic množice z n elementi, oziroma število načinov, da izberemo k elementov izmed n elementov.

Primer.

$$\binom{[4]}{2} = \{\{1,2\},\{1,3\},\{1,4\},\{2,3\},\{2,4\},\{3,4\}\}$$

Trditev 2.5.

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

Definicija 2.6 (n na k padajoče)**.** $n^{\underline{k}} := n(n-1)\cdots(n-k+1)$

Definicija 2.7 (n na k naraščajoče)**.** $n^{\overline{k}} := (n)(n+1)\cdots(n+k-1)$

Trditev 2.8.

$$\binom{n}{k} = \frac{n(n-1)...(n-k+1)}{k!} = \frac{n^{\underline{k}}}{k!} = \begin{cases} \frac{n!}{k!(n-k)!} : & 0 \leqslant k \leqslant n \\ 0 : & \text{sicer} \end{cases}$$

Dokaz. (1. način)
Po eno strani lahko izberemo k števil izmed n števil brez ponavljanja, vrstni red je pomemben. Torej: izberemo k-terico različnih števil

$$n(n-1)\cdots(n-k+1)$$

Po drugi strani pa lahko vzamemo $\binom{n}{k}$ (izberemo k-elementno podmnožico v $[n]$), krat $k!$ (izberemo vrstni red)

$$\implies \binom{n}{k}k! = n^{\underline{k}}$$

$$\implies \binom{n}{k} = \frac{n^{\underline{k}}}{k!}$$

■

Dokaz. (2. način)
Če $k < 0$ ali $k > n$, potem očitno $\binom{n}{k} = 0$. Vemo, da je $n!$ število permutacij $[n]$, a vsako k-podmnožico smo šteli $k! \cdot (n-k)!$-krat, zato delimo s tem izrazom.

$$\implies \frac{n!}{k!(n-k)!}$$

■

Trditev 2.9 (Rekurzivna formula)**.**

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

Dokaz. (1. način)
k-elementna podmnožica $[n]$ bodisi vsebuje ali ne vsebuje zadnji element (n).

- vsebuje n: člen $\binom{n-1}{k-1}$ izbere ostalih $k-1$ elementov iz (preostale) $[n-1]$
- ne vsebuje n: člen $\binom{n-1}{k}$ izbere vseh potrebnih k elementov izmed preostalih $[n-1]$.

■

Dokaz. (2. način)

$$\Phi : \binom{[n]}{k} \to \binom{[n-1]}{k-1} \cup \binom{[n-1]}{k}$$

$$\Phi(A) = A \setminus \{n\}$$

$$\text{inverz} : \Psi(B) = \begin{cases} B \cup \{n\} : & |B| = k-1 \\ B : & |B| = k \end{cases}$$

■

Dokaz. (3. način)

$$\binom{n-1}{k-1} + \binom{n-1}{k} = \frac{(n-1)^{\underline{k-1}}}{(k-1)!} + \frac{(n-1)^{\underline{k}}}{k!} = \frac{(n-1)^{\underline{k-1}}(k+n-k)}{k!} = \frac{n^{\underline{k}}}{k!},\ k \geqslant 1$$

■

2.1.1 Pascalov trikotnik

$n=0$							1						
$n=1$						1		1					
$n=2$					1		2		1				
$n=3$				1		3		3		1			
$n=4$			1		4		6		4		1		
$n=5$		1		5		10		10		5		1	
$n=6$	1		6		15		20		15		6		1
	0		1		2		3		4		5		6

Število v n-ti vrstici in k-tem stolpcu pascalovega trikotnika je enako $\binom{n}{k}$. Trikotnik konstruiramo tako, da napišemo zunanji plašč enic, nato pa vsak par sosenjih števil seštejemo in zapišemo vsoto pod niju.

2.2 Binomski izrek

Definicija 2.10.

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

Dokaz. (1. način) - indukcija po n
Baza indukcije, $n=0$: $1 = \binom{0}{0} a^0 b^0 = 1$. OK
Indukcijski korak, $n-1 \Rightarrow n$:

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

$$= \sum_{k=0}^{n-1} \binom{n-1}{k} a^{n-k} b^k + \sum_{k=0}^{n-1} \binom{n-1}{k} a^{n-1-k} b^{k+1} =$$

$$\overset{k'=k+1}{=} \sum_{k=0}^{n-1} \binom{n-1}{k} a^{n-k} b^k + \sum_{k'=1}^{n-1} \binom{n-1}{k'-1} a^{n-k'} b^{k'} =$$

$$\overset{k'=k}{=} \sum_{k=0}^{n} \binom{n-1}{k} a^{n-k} b^k + \sum_{k=0}^{n} \binom{n-1}{k-1} a^{n-k} b^k =$$

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

$$\overset{\text{rekurzija}}{=} \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$

■

Dokaz. (2. način) - isti
Namesto $\sum_{k=0}^{n-1}$ oz. podobno se uporabi kar $\sum_k$ - vsi ostali členi so po definiciji binomskih koeficientov enaki 0. Postopek je podoben, samo vse skupaj je malo hitreje, ker preskočimo vmesne razmiselke. ■

Dokaz. (3. način) - boljši

$$(a+b)\cdot(a+b)\cdot\ldots\cdot(a+b)$$

Po distributivnosti iz vsakega oklepaja izberemo a ali b. Če smo b izbrali k-krat, smo a izbrali $(n-k)$-krat in dobimo $a^{n-k}b^k$. Kolikokrat dobimo $a^{n-k}b^k$? $\binom{n}{k}$-krat, ker izberemo k oklepajev, v katerih izberemo b. ■

2.3 Izbori

Na voljo imamo n oštevilčenih kroglic. Na koliko načinov lahko izberemo k kroglic? Ali dovolimo ponavljanje? Je vrstni red pomemben?

	s ponavljanjem	brez ponavljanja
vrstni red je pomemben	n^k	$n^{\underline{k}}$
vrstni red ni pomemben	$\binom{n+k-1}{k}$	$\binom{n}{k}$

Opomba. V prvi vrstici gre za variacije, v drugi pa za kombinacije.

Primer. Želimo prešteti rešitve tega sistema neenačb.

$$1 \leqslant i_1 \leqslant \ldots \leqslant i_k \leqslant n$$

To so kombinacije s ponavljanjem, $n=4, k=3$.

111	123	222	244
112	124	223	333
113	133	224	334
114	134	233	344
122	144	234	444

Ideja:

$$j_1 = i_1,\ j_2 = i_2 + 1,\ j_3 = i_3 + 2,\ \ldots,\ j_k = i_k + k - 1$$

2.4 Kompozicije

Definicija 2.11 (Kompozicija)**.** Kompozicija naravnega števila n je taka l-terica

$$\lambda = (\lambda_1, \dots, \lambda_l), \quad \lambda_i > 0,$$

da velja

$$\lambda_1 + \lambda_2 + \cdots + \lambda_l = n$$

Lambde imenujemo členi kompozicije, l je dolžina kompozicije, n pa velikost kompozicije.

Primer. $(3, 1, 5, 2)$ je kompozicija števila 11.

Trditev 2.12. Obstaja 2^{n-1} kompozicij števila $n \geqslant 1$ in obstaja $\binom{n-1}{k-1}$ kompozicij števila n s k členi.

Dokaz. Kompozicijo lahko predstavimo s k kroglicami in pregradami:

$$3+1+5+2: \quad \circ\circ\circ | \circ | \circ\circ\circ\circ\circ | \circ\circ$$

$n-1$ prostorov za pregrado $\implies$ 2 izbiri za vsako pregrado ($\exists$, $\nexists$)
$k-1$ pregrad na $n-1$ mestih: $\binom{n-1}{k-1}$ ■

Definicija 2.13 (Šibka kompozicija)**.**

$$\lambda = (\lambda_1, \dots, \lambda_l) \quad \lambda_i \geqslant 0$$

tako da velja

$$\lambda_1 + \cdots + \lambda_l = n$$

Opomba. Šibkih kompozicij števila n je ∞.

Primer. $(0, 0, 3, 1, 0, 5, 0, 2)$

Trditev 2.14. Število šibkih kompozicij n s k členi je $\binom{n+k-1}{k-1}$.

Dokaz. (1. način)
Štejemo rešitve $\lambda_1 + \lambda_2 + \cdots + \lambda_k = n$, zahtevamo $\lambda_1 \geqslant 0$.

$$\mu_i = \lambda_i + 1$$

$$\mu_1 + \cdots + \mu_k = n + k, \quad \mu_i \geqslant 1$$

$$\binom{n+k-1}{k-1} \text{ je rešitev.}$$

■

Dokaz. (2. način)
Šibko kompozicijo predstavino s kroglicami in pregradami.

$$0+0+3+1+0+5+0+2: \quad || \circ \circ \circ | \circ || \circ \circ \circ \circ \circ || \circ \circ$$

Imamo $n+(k-1)$ objektov, izberemo položaje pregrad na $\binom{n+k-1}{k-1}$ načinov - to so kombinacije s ponavljanjem (n kroglic, izberemo jih k).

$$x_i \dots \text{ kolikokrat smo izbrali kroglico } i$$

$$x_i \geqslant 0, \quad i = 1, ..., n$$

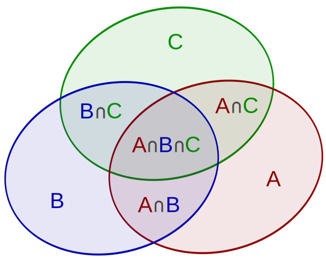
$$x_i + x_2 + ... + x_n = k$$

$\Longrightarrow$ šibke kompozicije k z n členi $= \binom{k+n-1}{n-1} = \binom{n+k-1}{k}$ ■

2.5 Načelo vključitev in izključitev (NVI)

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

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



Izrek 2.15 (NVI)**.**

$$|A_1 \cup \dots \cup A_n| = \sum_{j=1}^{n} (-1)^{j-1} \sum_{1 \leqslant i_1 \leqslant \dots \leqslant i_j \leqslant n} |A_{i_1} \cap A_{i_2} \cap \dots \cap A_{i_j}|$$

Definicija 2.16.

$$A_I := \bigcap_{i \in I} A_i$$

Primer. $A_{\{1,4,6,7\}} = A_1 \cap A_4 \cap A_6 \cap A_7$

Primer. $A_\emptyset = \cap_{i \in \emptyset} A_i = \{a;\ a \in A \ \wedge \ \forall i \in \emptyset \ a \in A_i\} = A$

Izrek 2.17 (Poenostavljen zapis NVI)**.**

$$\left| \bigcup_{i=1}^{n} A_i \right| = \sum_{\emptyset \neq I \subseteq [n]} (-1)^{|I|-1} \left| \bigcap_{i \in I} A_i \right|$$

Izrek 2.18 (Druga oblika NVI)**.**

$$\left|\bigcap_{i=1}^{n} A_i^c\right| = \sum_{I\subseteq[n]} (-1)^{|I|}|A_I|$$

Dokaz. Označimo $A_1, \dots, A_n \subseteq A$ in se spomnimo, da $A_\emptyset = A$

$$\left|\bigcap_{i=1}^{n} A_i^c\right| = \left|(\bigcup_{i=1}^{n} A_i)^c\right| = |A| - \left|\bigcup_{i=1}^{n} A_i\right| = |A_\emptyset| - \sum_{\emptyset\neq I\subseteq[n]} (-1)^{|I|-1}|A_I| = \sum_{I\subseteq[n]} (-1)^{|I|}|A_I|$$

■

Lema 2.19.

$$k \geqslant 1 \implies \sum_{j=0}^{k}(-1)^j\binom{k}{j} = 0$$

Dokaz. V binomski izrek vstavimo $x = -1$

$$(1-1)^n = \sum_{j=0}^{k}\binom{k}{j}x^j = 0$$

■

Opomba. Lema pravi $\sum_{j \text{ sod}}\binom{k}{j} = \sum_{j \text{ lih}}\binom{k}{j}$ oziroma število sodih podmnožic je vedno enako številu lihih podmnožic.

To lahko pokažemo tudi s sledečo bijekcijo

$$\varphi : \{\text{sode podmnožice } [k]\} \to \{\text{lihe podmnožice } [k]\}$$

$$\varphi(S) = \begin{cases} S \setminus \{k\} : & k \in S \\ S \cup \{k\} : & k \notin S \end{cases}$$

Dokaz. (NVI)

$$a \in \bigcup_{i=1}^{n} A_i,\ a \text{ vsebovana v natanko } k \text{ množicah}$$

Dokazati želimo, da je doprinos a-ju k vsoti na desni enak 1.

$$k - \binom{k}{2} + \binom{k}{3} - \dots + (-1)^{k-1}\binom{k}{k} = \sum_{j=1}^{k}(-1)^{j-1}\binom{k}{j} = -\left(\sum_{j=0}^{k}(-1)^j\binom{k}{j} - 1\right) = 1$$

k … doprinos v prvi vrstici

$\binom{k}{2}$ … doprinos v drugi vrstici

$\sum_{j=0}^{k}(-1)^j\binom{k}{j} = 0$ (po lemi) ■

2.6 Eulerjeva funkcija ϕ

Definicija 2.20 (Eulerjeva funkcija)**.**

$$\phi(n) = \Big|\{i \in [n] : \gcd(i, n) = 1\}\Big|$$

Trditev 2.21.

$$\sum_{a|n} \phi(a) = n$$

(= število števil med 1 in n, ki so tuje n)

Dokaz. Zapišimo $\frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \ldots, \frac{n}{n}$ in jih pokrajšajmo.

$$\begin{array}{cccccccccccc} \frac{1}{12} & \frac{2}{12} & \frac{3}{12} & \frac{4}{12} & \frac{5}{12} & \frac{6}{12} & \frac{7}{12} & \frac{8}{12} & \frac{9}{12} & \frac{10}{12} & \frac{11}{12} & \frac{12}{12} \\ \\ \frac{1}{12} & \frac{1}{6} & \frac{1}{4} & \frac{1}{3} & \frac{5}{12} & \frac{1}{2} & \frac{7}{12} & \frac{2}{3} & \frac{3}{4} & \frac{5}{6} & \frac{11}{12} & \frac{1}{1} \end{array}$$

Ulomkov je n, imenovalci so delitelji števila n, števci so števila, ki so manjša od a in tuja z a. ■

Izrek 2.22 (Formula za ϕ)**.**

$$\phi(n) = n \cdot \prod_{p|n} (1 - \frac{1}{p})$$

Dokaz.

$$A = [n], \quad n = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \quad \alpha_i > 0$$
$$A_i = \{j \in [n] : p_i | j\}$$
$$|A_i| = \frac{n}{p_i}$$
$$|A_i \cap A_j| = \frac{n}{p_i p_j}$$
$$|A_I| = \frac{n}{\prod\limits_{i \in I} p_i}$$

$$\phi(n) = \sum_{I \subseteq [k]} (-1)^{|I|} \frac{n}{\prod\limits_{i \in I} p_i}$$

Kjer je k število praštevilskih faktorjev n (glej prvo vrstico dokaza). Vzemimo za primer $k = 2$:

$$n \cdot (1 - \frac{1}{p_1} - \frac{1}{p_2} + \frac{1}{p_1 p_2}) = n \cdot (1 - \frac{1}{p_1}) \cdot (1 - \frac{1}{p_2})$$

$$\phi(n) \overset{\text{distributivnost}}{=} n \cdot (1 - \frac{1}{p_1}) \cdot (1 - \frac{1}{p_2}) \cdot \ldots \cdot (1 - \frac{1}{p_k})$$

V splošnem torej velja

$$\phi(n) = n \cdot \prod_{p|n} (1 - \frac{1}{p})$$

$\blacksquare$

2.7 Multinomski koeficienti

Spomnimo se na binomske koeficiente

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}, \; 0 \leqslant k \leqslant n$$

Imamo a enic in b ničel. Premešamo jih lahko na

$$\binom{a+b}{a} = \binom{a+b}{b} = \frac{(a+b)!}{a!b!}$$

načinov. Kaj pa če imamo več enakih elementov? Števila $1, 1, 1, 2, 2, 3, 3, 3, 3, 3, 4$ lahko premešamo na.

$$\binom{a_1 + a_2 + \cdots + a_n}{a_1} \cdot \binom{a_2 + a_3 \cdots + a_n}{a_2} \cdot \binom{a_3 + a_4 + \cdots + a_n}{a_3} \cdots$$

načinov. V prvem binomu izberemo enke, v drugem dvojke, v tretjem trojke .... To razpišemo kot

$$\frac{(a_1 + a_2 + ... + a_n)!}{a_1!(a_2 + a_3 + ... + a_n)!} \cdot \frac{(a_2 + a_3 + ... + a_n)!}{a_2!(a_3 + a_4 + ... + a_n)!} \cdot \frac{(a_3 + a_4 + ... + a_n)!}{a_1!(a_4 + a_5 + ... + a_n)!} \cdots \frac{(a_{n-1} + a_n)!}{a_{n-1}!a_n!} =$$

$$= \frac{(a_1 + a_2 + ... + a_n)!}{a_1!a_2!...a_n!} = \frac{(\sum_{i=1}^{n} a_i)!}{\prod_{i=1}^{n} a_i!} = \binom{a_1 + a_2 + ... + a_n}{a_1, a_2, ..., a_n}$$

Alternativno: dodamo indekse $1_1, 1_2, 1_3, 2_1, 2_2, 3_1, 3_2, 3_3, 3_4, 3_5, 4_1$. Premešamo na

$$\frac{(a_1 + a_2 + \cdots + a_n)!}{a_1!a_2! \cdots a_n!}$$

načinov; najprej smo premešali vse na $(a_1 + a_2 + \cdots + a_n)!$ načinov, potem pa z $a_i!$ izbrisali indekse)

Opomba.

$$\binom{a+b}{a,b} = \frac{(a+b)!}{a!b!} = \binom{a+b}{a} = \binom{a+b}{b}$$

Izrek 2.23 (Multinomski izrek)**.**

$$(x_1 + x_2 + \cdots + x_n)^m = \sum_{(a_1,\ldots,a_n) \text{ šibka kompozicija } m} \binom{m}{a_1,\cdots,a_n} x_1^{a_1} \cdots x_n^{a_n}$$

Dokaz.

$$(x_1 + x_2 + \cdots + x_n) \cdot (x_1 + x_2 + \cdots + x_n) \cdot \ldots \cdot (x_1 + x_2 + \cdots + x_n)$$

Iz vsakega oklepaja izberemo x_i, kar skupaj pride $x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$, pri čemer je $\sum_{i=1}^{n} a_i = m$, $a_i \geqslant 0$. Koeficient je očitno $\binom{a_1+a_2+\ldots+a_n}{a_1,a_2,\ldots,a_n}$. ∎

Primer. $x_1 = x_2 = \cdots = x_n$

$$n^m = \sum_{(a_1,\ldots,a_n) \text{šibka kompozicija m}} \binom{m}{a_1,\ldots,a_n}$$

2.8 Načrti in t-načrti

Podjetje proizvaja več različic izdelka, želi jih testirati pri potrošnikih. Vsak potrošnik mora testirati enako število različic, vsako različico mora testirati enako število potrošnikov.

$$1234, 1247, 1357, 2468, 3568, 5678$$

8 različic, 6 potrošnikov, vsak potrošnik testira 4, vsako različico testirajo 3 potrošniki.

Definicija 2.24 (Načrt)**.** $B = \{B_1, \ldots, B_b\}$ je narčt s parametri (v, k, λ), kadar velja

- $B_1, \ldots, B_b \subseteq [v]$
- $|B_1| = \ldots = |B_b| = k$
- vsak $i \in [v]$ se pojavi v natanko λ množicah oz. "blokih".

Primer. Načrt s parametri $(8, 4, 3)$.

Narišemo tabelo

	B_1	$\cdots$	B_b
1			
$\vdots$			
v			

Kljukico damo tam, kjer je $i \in B_j$. V vsakem stolpcu tako dobimo k kljukic, skupaj $k \cdot b$, v vsaki vrstici dobimo λ kljukic, skupaj $\lambda \cdot v$. Iz tega sledi, da $k \cdot b = \lambda \cdot v$, oziroma $b = \frac{\lambda v}{k}$

Velja še b $\leqslant \binom{v}{k}$

$$\frac{\lambda v}{k} \leqslant \frac{v!}{k!(v-k)!}$$

Pokrajšamo $\frac{v}{k}$ na obeh straneh neenačbe in dobimo

$$\lambda \leqslant \frac{(v-1)!}{(k-1)!(v-k)!} = \binom{v-1}{k-1}$$

Izrek 2.25.
Načrt s parametri (v, k, λ) obstaja natanko tedaj, ko velja $k|v \cdot \lambda$ in $\lambda \leqslant \binom{v-1}{k-1}$

Dokaz.
($\Rightarrow$) Že dokazano.
($\Leftarrow$) Izberemo $\frac{\lambda v}{k}$ k-elementnih podmnožic množice $[v]$. To lahko naredimo, ker je $\frac{\lambda v}{k} \leqslant \binom{v-1}{k-1} \cdot \frac{v}{k} = \binom{v}{k}$.

$$v = 8,\ k = 4,\ \lambda = 3$$

$$\frac{\lambda v}{k} = 6 \Rightarrow 1234, 1356, 1567, 1568, 2356, 3457$$

To ni nujno načrt.

$$\lambda_i \ldots \text{v koliko blokih je vsebovan } i$$

$$\lambda_1 = 4,\ \lambda_2 = 2,\ \lambda_3 = 4,\ \lambda_4 = 2,\ \lambda_5 = 5,\ \lambda_6 = 4,\ \lambda_7 = 2,\ \lambda_8 = 1$$

Naredimo isto tabelo kot prej in ugotovimo, da je $\lambda = \frac{\sum_{i=1}^{v} \lambda_i}{v}$.
Če to ni načrt, zagotovo obstajata i, j, da je $\lambda_i > \lambda > \lambda_j$.

Bloki so 4 tipov:

(I) vsebujejo i in j

(II) vsebujejo i, ne pa j

(III) vsebujejo j, ne pa i

(IV) ne vsebujejo ne i ne j

Bloki tipa (I) in (IV) vsebujejo enako i-jev in j-jev.

λ_i = blokov tipa (I) + (II)

λ_j = blokov tipa (I) + (III)

Sledi, da je več blokov tipa (II) kot (III). Iz tega sledi, da obstaja blok tipa (II), tako da po zamenjavi i z n ne dobimo že obstoječega bloka.

$$1234, 1356, 2567, 1568, 2356, 3457$$

V splošnem: $\lambda_i --$, $\lambda_j ++$
Postopek ponovimo, dokler ni $\lambda_1 = \lambda_2 = ... = \lambda_6$

$$1234, 1456, 2567, 1568, 2356, 3457$$

$$1234, 1457, 2567, 1568, 2356, 3457$$

$$1234, 1457, 2678, 1568, 2356, 3457$$

$$1234, 1478, 2678, 1568, 2356, 3457$$

kar je načrt.

Na vsakem koraku se zmanjša $\sum_{i=1}^{v}(\lambda_i - \lambda)$ za 2, po končno korakih je to $= 0$ in dobimo načrt. ■

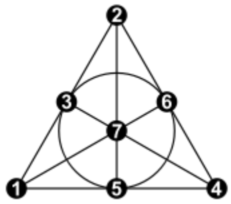
Definicija 2.26 (t-načrt)**.** $B = \{B_1, \ldots, B_b\}$ je t-narčt s parametri (v, k, λ_t), kadar velja

- $B_1, \ldots, B_b \subseteq [v]$
- $|B_1| = \cdots = |B_b| = k$
- vsaka t-elementna podmnožica $[v]$ je vsebovana v točno λ_t blokih.

Opomba. 1-načrt = načrt

Primer. $124, 137, 156, 235, 267, 346, 457$ je 2-načrt $(7, 3, 1)$

Opomba. Tudi načrt s parametri $(7, 3, 3)$ NI 3-načrt!!



Slika 1: Fanova ravnina

Opomba. Fanova ravnina je skica načrta $(7, 3, 3)$.

Izrek 2.27. Če je B t-načrt s parametri (v, k, λ_t), je B tudi $(t-1)$-načrt s parametri (v, k, λ_{t-1}). Velja formula

$$\lambda_{t-1} = \lambda_t \cdot \frac{v - t + 1}{k - t + 1}$$

Dokaz. $S \subseteq [v]$, $|S| = t - 1$. S je vsebovana v λ_s blokih. Narišemo tabelo

	B_1	$\cdots$	B_j	$\cdots$	B_b
1					
$\vdots$					
i			$\checkmark$		
$\vdots$					
v					

$i \notin S$, $S \cup \{i\} \subseteq B_j$.

Skupno je po stolpcih:

- $S \setminus B_j$: 0 kljukic
- $S \subseteq B_j$: $k - t + 1$ kljukic

  skupaj: $\lambda_s \cdot (k - t + 1)$

in po vrsticah:

- $i \in S$: 0 kljukic
- $i \notin S$: λ_t kljukic

  skupaj: $\lambda_t \cdot (v - t + 1)$

$$\implies \lambda_s = \frac{\lambda_t \cdot (v-t+1)}{k-t+1}$$

■

3 Permutacije, razdelitve, razčlenitve

3.1 Stirlingova števila prve vrste

$\pi \in S_n$ lahko zapišemo kot produkt disjunktnih ciklov

$$(1\ 4\ 6\ 3\ 5\ 8\ 2\ 7) = (1)(2\ 4\ 3\ 6\ 8\ 7)(5)$$

Definicija 3.1 (Stirlingovo število prve vrste)**.** Je število permutacij v S_n, ki imajo natanko k ciklov (negibne točke štejemo kot cikle dolžine 1). Označimo $c(n,k)$

Za $c(n,k)$ ni "lepe" formule. Vemo pa naslednje lastnosti

- $c(n,n) = 1$
- $c(n,n-1) = \binom{n}{2}$ (transpozicija)
- $c(n,0) = 0$ (če $n > 0$, oziroma 1, če je $n = 0$)
- $c(n,1) = (n-1)!$
- $c(n,k) = 0$ za $k > n$ ali $k < 0$
- $\sum_k c(n,k) = n!$

Trditev 3.2 (Rekurzivna zveza)**.**

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

Dokaz. Permutacije v S_n s k cikli:

- n je negibna točka: $c(n-1,k-1)$
- n ni negibna točka: $c(n-1,k) \cdot (n-1)$ (izbrišem n, dobim permutacijo v S_{n-1} s k cikli) $\cdot$ (vsako dobimo $(n-1)$-krat)

■

Trditev 3.3 (Formula za $c(n,k)$)**.**

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

$n\backslash k$	0	1	2	3	4	5
0	1	0	0	0	0	0
1	0	1	0	0	0	0
2	0	1	1	0	0	0
3	0	2	3	1	0	0
4	0	6	11	6	1	0
5	0	24	50	36	10	1

Slika 2: Tabela Stirlingovih števil 1. vrste

Opomba. Konstruiramo jo podobno kot Pascalov trikotnik za binomske koeficiente (2.1.1), samo da uporabimo drugo rekurzivno formulo; najprej damo diagonalne elemente na 1, naddiagonalne na 0, nato vse elemente v 1. stoplcu na 0 (razen prvega elementa, ki je že 1), za ostale pa uporabimo rekurzivno forumlo (seštejemo element levo zgoraj in $(n-1)$ krat zgornji).

Dokaz. Indukcija po n:
Baza indukcije: $n = 0 : (1x^0 = x^0)$. OK.
Indukcijski korak: $n-1 \implies n$:

$$x^{\overline{n}} = x^{\overline{n-1}}(x+n-1) = \sum_k c(n-1,k)x^k(x+n-1) =$$

$$= \sum_k c(n-1,k)x^{k+1} + \sum_k c(n-1,k)x^k(n-1) =$$

Pri prvem členu nastavimo $k = k-1$, ker itak seštevamo za vse k.

$$= \sum_k c(n-1,k-1)x^k + \sum_k c(n-1,k)x^k(n-1) =$$

Združimo vsoti in izpostavimo x^k

$$= \sum_k x^k \cdot (c(n-1,k-1) + (n-1)\cdot c(n-1,k)) =$$

Uporabimo rekurzivno zvezo, da dobimo

$$= \sum_k c(n,k)x^k$$

■

Dokaz. Še eno alternativo tega dokaza bomo naredili pri Pólyjevi teoriji (5.18). ■

Definicija 3.4 (Predznačeno Stirlingovo število)**.**

$$s(n,k) := (-1)^{n-k} c(n,k)$$

Trditev 3.5 (Rekurzivna zveza za predznačena Stirlingova števila)**.**

$$\sum_k s(n,k) x^k = x^{\underline{n}}$$

Dokaz. Zamenjajmo x z $-x$ v formuli za $c(n,k)$.

$$\sum_k c(n,k)(-1)^k x^k = (-x)^{\overline{n}}$$

Če na desni izpostavimo $(-1)^n$, se $x^{\overline{n}}$ spremeni v $x^{\underline{n}}$.

$$\sum_k (-1)^{n-k} c(n,k) x^k = x^{\underline{n}}$$

$$\implies \sum_k s(n,k) x^k = x^{\underline{n}}$$

■

3.2 Stirlingova števila druge vrste

Definicija 3.6 (Razdelitev množice)**.** Razdelitev, razbitje ali particija je $\{B_1, \ldots, B_n\}$, pri čemer

- $B_i \neq \emptyset \quad i = 1 \ldots k$
- $B_i \cap B_j = \emptyset$ za $i \neq j$
- $\cup_{i=0}^{k} B_i = A$
- $B_1, \ldots, B_n$ so bloki razdelitve

Primer. $A = [8]$ lahko razdelimo na $\{\{1,4,5\}\{2\}\{3,6,7,8\}\}$, kar lahko zapišemo kot $145 - 2 - 3678$ oziroma urejeno $2 - 415 - 8763$.

Opomba. Če je R je ekvivalenčna relacija nad A (refleksivna, simetrična, tranzitivna), je množica ekvivalenčnih razredov R ravno razdelitev množice A.

Definicija 3.7 (Stirlingovo število druge vrste)**.** $S(n,k)$ je število razdelitev $[n]$ z natanko k bloki.

Definicija 3.8 (Bellovo število)**.** $B(n)$ je število razdelitev $[n]$. Velja

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

Opomba. $B(n) \neq B_n$. B_n = Bernoulijevo število

Preproste formule za $S(n,k)$ in $B(n)$ nimamo, poznamo pa naslednje identitete:

- $S(n,n) = 1$
- $S(n,n-1) = \binom{n}{2}$
- $S(n,1) = 1 - \delta_{n0}$
- $S(n,0) = \delta_{n0}$
- $S(n,k) = 0$ za $k < 0$ ali $k > n$
- $S(n,k) \leqslant c(n,k)$

Trditev 3.9 (Rekurzivna formula za $S(n)$)**.**

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

Dokaz. Razdelitve $[n]$ s k bloki:

- n je (samostojen) blok: $S(n-1,k-1)$
- n je v bloku velikosti ≥ 1: $k \cdot S(n-1,k)$ (n lahko vstavimo v katerega koli izmed k blokov: n vstavimo nazaj na k načinov)

■

$n \backslash k$	0	1	2	3	4	5	$B(n)$
0	1	0	0	0	0	0	1
1	0	1	0	0	0	0	1
2	0	1	1	0	0	0	2
3	0	1	3	1	0	0	5
4	0	1	7	6	1	0	15
5	0	1	15	25	10	1	52

Opomba. Za konstrukcijo glej Stirlingova števila prve vrste.

Trditev 3.10 (Pomen $S(n)$)**.** $S(n,k)$ je število ekvivalenčnih relacij na $[n]$ s k ekvivalenčnimi razredi. $B(n)$ je število ekvivalenčnih relacij na $[n]$

Trditev 3.11. Število surjekcij $[n] \to [k]$ je $k! \cdot S(n,k)$

Dokaz. Naj bo $f : [n] \to [k]$ surjekcija. Množica $\{f^{-1}(1), f^{-1}(2) \cdots f^{-1}(k)\}$, kjer $f^{-1}(i)$ predstavlja množico praslik i-ja ($= \{j : f(j) = i\}$) je razdelitev $[n]$ s k bloki. Vsaka razdelitev $[n]$ s k bloki nam da $k!$ surjekcij (bloke linearno uredimo).
Ekvivalentno: urejena razdelitev $\equiv$ surjekcija. ■

Posledica 3.12.

$$S(n,k) = \frac{1}{k!}\sum_{j=0}^{k}(-1)^{k-j}\binom{k}{j}j^n = \sum_{j=0}^{k}\frac{(-1)^{k-j}j^n}{j!(k-j)!}$$

Trditev 3.13 (Rekurzivna formula za $S(n)$)**.**

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

Dokaz. (1. način) Z indukcijo (na vajah, sicer je domača naloga) ■

Dokaz. (2. način) Naj bo $x \in \mathbb{N}$. x^n je število preslikav iz $[n]$ v $[k]$. Vsaka preslikava je surjekcija na svojo sliko (zalogo vrednosti).

$$x^n = \sum_T \Big(|T|! \cdot S(n,|T|)\Big) = \sum_k \left(k! \cdot S(n,k) \cdot \binom{x}{k}\right)$$

kjer je T slika preslikave, $\binom{x}{k} = \frac{x^{\underline{k}}}{k!}$ pa predstavlja število k-elementnih podmnožic od $[x]$. ■

Dokaz. (3. način) Dva polinoma stopnje $\leqslant n$, ki se ujemata v $n+1$ točkah, sta enaka (razlika je polonom stopnje $\leqslant n$ z $n+1$ ničlami, torej je ekvivalentna 0)

$\sum_k S(n,k)x^{\underline{k}}$ in x^n sta polinoma stopnje n, ujemata se v neskončno točkah (ker gremo v vsoti po vseh $x \in \mathbb{N}$), torej sta enaka. ■

Velja tudi:

$$\sum_k (-1)^{n-k}S(n,k)x^{\overline{k}} = x^n$$

Trditev 3.14 (Rekurzivna formula za $B(n)$)**.**

$$B(n+1) = \sum_{k=0}^{n}\binom{n}{k}B(k)$$

Dokaz. Izberemo razdelitev $[n+1]$, k pa naj bo število elementov, ki so v istem bloku kot $n+1$

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

$\binom{n}{k}$: izbira elementov, ki so v istem bloku (skupaj z $n+1$).

$B(n-k)$: izberemo razdelitev na preostalih $n-k$ elementih (ta izbira je neodvisna in takih je $B(n-k)$).

Če zamenjamo $n-k$ s k, in uporabimo $\binom{n}{n-k} = \binom{n}{k}$ lahko poenostavimo

$$B(n+1) = \sum_{k=0}^{n} \binom{n}{k} B(k)$$

∎

3.3 Lahova števila

Definicija 3.15 (Lahovo število)**.** $L(n,k)$ je število razdelitev $[n]$ na k linearno urejenih blokov.

Opomba. Spomnimo se: $S(n,k)$ je število razdelitev $[n]$ na k blokov, $c(n,k)$ pa število razdelitev $[n]$ na k ciklično urejenih blokov.

- $L(n,n) = 1$
- $L(n,n-1) = \binom{n}{2} \cdot 2 = n(n-1)$
- $L(n,0) = \delta_{n0}$
- $L(n,1) = n!$
- $L(n,k) = 0$ za $k < 0$ ali $k > n$
- $S(n,k) \leqslant c(n,k) \leqslant L(n,k)$

Trditev 3.16 (Eksplicitna formula za $L(n,k)$)**.**

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

Dokaz. Preštejemo urejene razdelitve $[n]$ s k linearno urejenimi bloki

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

$k!$ - uredimo bloke, $n!$ - premutacija, $\binom{n-1}{k-1}$ - kompozicija ∎

Trditev 3.17.

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

Dokaz. Ekvivalentno kot ostale rekurzije, samo "podrobnost" $(n-1+k)$: n vstavimo za obstoječim številom $(n-1)$ ali pa na začetek bloka (k) ∎

Primerjajmo rekurzije:

- $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$
- $c(n,k) = c(n-1,k-1) + (n-1) \cdot c(n-1,k)$
- $S(n,k) = S(n-1,k-1) + k \cdot S(n-1,k)$
- $L(n,k) = L(n-1,k-1) + (n-1+k) \cdot L(n-1,k)$

Trditev 3.18 (Rekurzivna formula za $L(n,k)$)**.**

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

Dokaz. Dokaz bomo prepustili bralcu za vajo (uporabi indukcijo). ∎

Primerjajmo:

- $\sum_k \binom{n}{k} x^k = (1+x)^n$
- $\sum_k c(n,k)x^k = x^{\overline{n}} \quad \sum_k (-1)^{n-k} c(n,k)x^k = x^{\underline{n}}$
- $\sum_k S(n,k)x^{\underline{k}} = x^n \quad \sum_k (-1)^{n-k} S(n,k)x^{\overline{k}} = x^n$
- $\sum_k L(n,k)x^{\underline{k}} = x^{\overline{n}} \quad \sum_k (-1)^{n-k} L(n,k)x^{\overline{k}} = x^{\underline{n}}$

3.4 Razčlenitve naravnih števil in Eulerjev petkotniški izrek

Definicija 3.19 (Razčlenitev naravnega števila)**.** Razčlenitev ali particija $n \in \mathbb{N}$ je l-terica

$$\lambda = (\lambda_1, \lambda_2, ..., \lambda_l)$$

$$\lambda_1 \geqslant \lambda_2 \geqslant ... \geqslant \lambda_l > 0$$

$$\lambda_1 + \lambda_2 + \cdots + \lambda_l = n$$

λ_i so členi razčlenitve, n je velikost razčlenitve, l je dolžina razčlenitve.

Primer. $(5,4,4,2,1,1)$ je razčlenitev števila 17 s 6 členi.

Opomba. Označimo tudi $5 + 4 + 4 + 2 + 1 + 1$ ali $5\ 4\ 4\ 2\ 1\ 1$.

Razčletnive lahko prikažemo grafično s pomočjo Ferresovih diagramov.

Primer. Diagram za $\lambda = (5, 4, 4, 2, 1, 1)$

$$\begin{array}{ccccc}
\bullet & \bullet & \bullet & \bullet & \bullet \\
\bullet & \bullet & \bullet & \bullet & \\
\bullet & \bullet & \bullet & \bullet & \\
\bullet & \bullet & & & \\
\bullet & & & & \\
\bullet & & & &
\end{array}$$

Definicija 3.20 (Razčlenitve)**.**

- S $p(n)$ označimo število vseh razčlenitev n.
- S $p_k(n)$ označimo število razčlenitev n s k členi.
- S $\overline{p_k}(n)$ označimo število razčlenitev n z $\leqslant k$ členi.

Prvih nekaj števil $p(n) = 1, 1, 2, 3, 5, 7, 11, 15, \ldots$

Opomba. Ni lepe formule za $p(n)$, $p_k(n)$ ali $\overline{p_k}(n)$.

Primer.
$n = 1 : 1$
$n = 2 : 2, 11$
$n = 3 : 3, 21, 111$
$n = 4 : 4, 31, 22, 211, 1111$
$n = 5 : 5, 41, 32, 311, 221, 2111, 11111$
$p_2(5) = 2$
$\overline{p_3}(5) = 5$

Definicija 3.21 (Konjugirana razčlenitev λ')**.** Dobimo s transpozicijo Ferresovega diagrama (stolpce napišemo kot vrstice).

Veljajo naslednje lastnosti:

- $\lambda'_i = |\{i : \lambda_j \geqslant i\}| = \max\{j : \lambda_j \geqslant i\}$
- $\lambda'' = \lambda$
- $\lambda'_1 = l(\lambda)$
- $l(\lambda') = \lambda_1$

Primer. 5 4 4 2 1 1$'$ = 6 4 3 3 1

Trditev 3.22 (Lastnosti $p_k(n)$)**.**

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

Dokaz. Precej trivialno;

1. Izbrišemo prvi stolpec (ima dolžino k)
2. Imamo razčlenitev n s k členi: $\lambda_l = 1$ ($p_{k-1}(n-1)$) in $\lambda_l \geqslant 2$ ($p_k(n-k)$)
3. Razčlenitev s k členi ima lahko strogo manj kot k členov, ali pa natanko k členov.

■

Opomba. Do zdaj obravnavane rekurzivne formule):

- $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$
- $c(n,k) = c(n-1,k-1) + (n-1) \cdot c(n-1,k)$
- $S(n,k) = S(n-1,k-1) + k \cdot S(n-1,k)$
- $L(n,k) = L(n-1,k-1) + (n+k-1) \cdot L(n-1,k)$
- $p_k(n) = p_{k-1}(n-1) + p_k(n-k)$
- $\overline{p_k}(n) = \overline{p_{k-1}}(n) + \overline{p_k}(n-k)$

Tabela za $p_k(n)$:

$n \backslash k$	0	1	2	3	4	5	6	$\sum_k p_k(n) = p(n)$
0	1	0	0	0	0	0	0	1
1	0	1	0	0	0	0	0	1
2	0	1	1	0	0	0	0	2
3	0	1	1	1	0	0	0	3
4	0	1	2	1	1	0	0	5
5	0	1	2	3	1	1	0	7
6	0	1	3	3	2	1	1	11

Za postopek izpolnitve tabele glej Stirlingova števila 1. vrste (2). Uporabi formulo $p_k(n) = p_{k-1}(n-1) + p_k(n-k)$.

Kaj pa rekurzija za $p(n)$?

$$A = \{\text{razčlenitve } n\} = \bigcup_{i=1}^{n} A_i$$

$$A_i = \{\text{razčlenitve } n\text{, ki vsebujejo } i \text{ kot člen}\}$$
$$|A_i| = p(n-i)$$
$$|A_i \bigcap_{i \neq j} A_j| = p(n-i-j)$$
$$|A_I| = p(n - \sum_{i \in I} i)$$

$$\begin{aligned} |\bigcup_{i=1}^{n} A_i| =& |A_1| + ... + |A_n| \\ & - |A_1 \cap A_2| - |A_1 \cap A_3| ... \\ & + |A_1 \cap A_2 \cap A_3| ... \\ & - ... \\ & + ... \end{aligned}$$

$$\begin{aligned} p(n) =& p(n-1) + p(n-2) + \cancel{p(n-3)} + \cancel{p(n-4)} + \cancel{p(n-5)} + ... \\ & - \cancel{p(n-1-2)} - \cancel{p(n-1-3)} - \cancel{p(n-2-3)} - \underline{p(n-1-4)} - ... \\ & + p(n-1-2-3) + p(n-1-2-4) + ... \\ & - p(n-1-2-3-4) - ... \\ & + ... \end{aligned}$$

Torej očitno: $p(n) = \sum_{m=1}^{\infty} ?p(n-m)$.

Relevantne so razčlenitve m z različnimi členi

$$7 = 7 = 6+1 = 5+2 = 4+3 = 4+2+1$$

$\alpha(m)$ ... število razčlenitev m z liho mnogo različnimi členi
$\beta(m)$ ... število razčlenitev m z sodo mnogo različnimi členi
$p(n) = \sum_{m=1}^{\infty} (\alpha(m) - \beta(m) \cdot p(n-m))$

Trditev 3.23.

$$\alpha(m)-\beta(m)=\begin{cases}(-1)^{k-1}: & m=\frac{k(3k\pm1)}{2}\\ 0: & \text{sicer}\end{cases}$$

$$\frac{k(3k-1)}{2}: 1, 5, 12, 22, ...$$
$$\frac{k(3k+1)}{2}: 2, 7, 15, 26, ...$$

Posledica 3.24 (Eulerjev petkotniški izrek)**.**

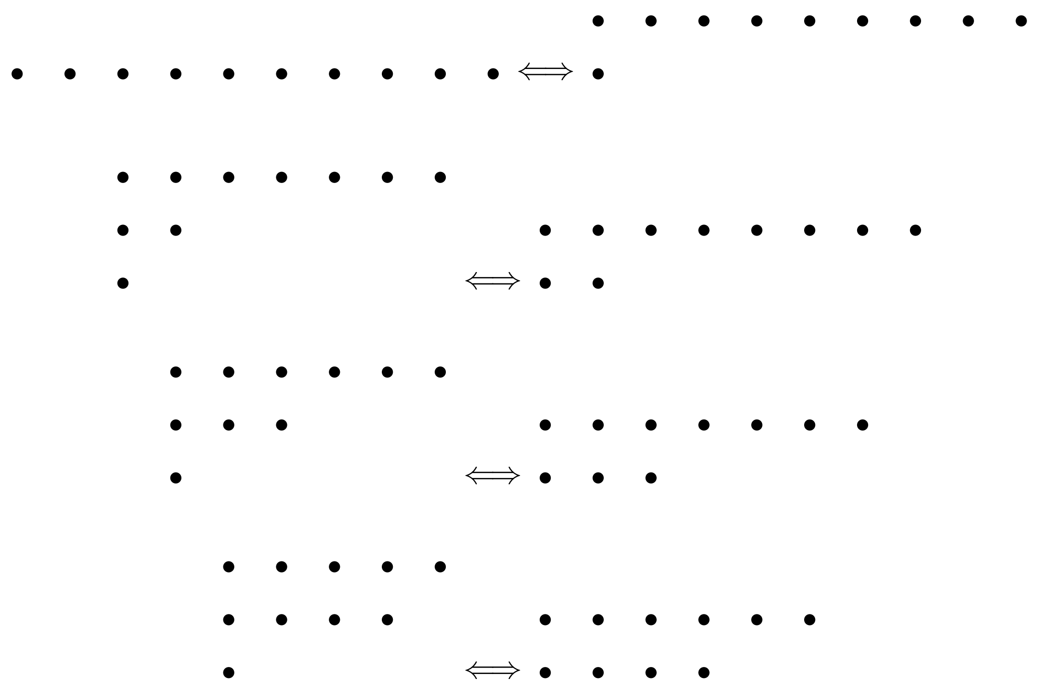
$$p(n)=p(n-1)+p(n-2)-p(n-5)-p(n-7)+p(n-12)+p(n-15)-p(n-22)-p(n-26)\cdots$$

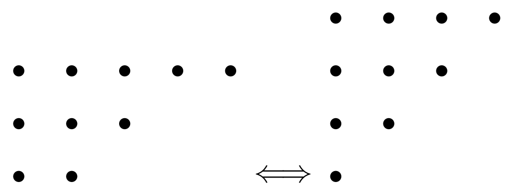
$$p(n)=\sum_{k=1}^{\infty}(-1)^{k-1}(p(n-\frac{k(3k-1)}{2})+p(n-\frac{k(3k+1)}{2}))$$

Dokaz. Iščemo "skoraj bijekcijo"

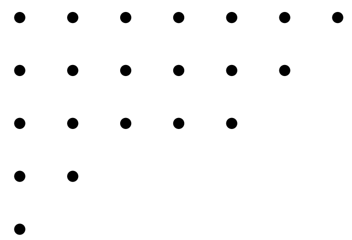
{razčlenitve m z liho mnogo členi} $\Longleftrightarrow$ {razčlenitve m s sodo mnogo členi}

$m=10$:





s(λ) $\coloneqq \lambda_{l(\lambda)}$ najmanjši člen



Recimo diagonali, ki se pojavi ob koncu prvih treh vrstic, **bok**.

$$b(\lambda) \coloneqq \max\{i : \lambda_i = \lambda_1 - i + 1\}$$

1. Če je $s(\lambda) > b(\lambda)$: bok postavimo pod najmanjši člen
2. Če je $s(\lambda) \leqslant b(\lambda)$: najmanjši člen postavimo desno od boka

Zakaj to ni vselej bijekcija? Prvo pravilo ne deluje, če se bok seka z najmanjšim členom, oziroma kadar velja $b(\lambda) = l(\lambda) = s(\lambda)$.

$$(k+1) + (k+2) + \cdots + (k+k) =$$

$$\frac{2k(2k+1)}{2} - \frac{k(k+1)}{2} = \frac{k(3k+1)}{2}$$

Drugo pravilo ne deluje, če

$$b(\lambda) = l(\lambda) = s(\lambda) - 1 = k$$

$$k + (k+1) + (k+2) + \cdots + (k+k-1) =$$

$$\frac{(2k-1)2k}{2} - \frac{(k-1)k}{2} = \frac{k(3k-1)}{2}$$

- če m $\neq \frac{k\cdot(3k\pm1)}{2}$, smo našli bijekcijo, $\alpha(m) - \beta(m) = 0$.
- če m $= \frac{k\cdot(3k\pm1)}{2}$, imamo bijekcijo, če odstavimo eno razčlenitev s k členi.
  * k sod: $\alpha(m) - \beta(m) = -1$

* k lih: $\alpha(m) - \beta(m) = 1$

Torej: $\alpha(m) - \beta(m) = (-1)^{k-1}$

■

3.5 Dvanajstera pot

Imamo $n = |N|$ kroglic in $k = |K|$ škatel. Zanimajo nas razporeditve teh kroglic v škatle, glede na to ali kroglice in škatle med seboj ločimo ali ne.

Spomnimo se na definiciji injektivnosti in surjektivnosti

- injektivna razporeditev: v vsaki škatli je največ ena kroglica
- surjektivna razporeditev: v vsaki škatli je vsaj ena kroglica

N	K	vse	injektivne	surjektivne
Ločimo	Ločimo	k^n	$k^{\underline{n}}$	$k! \cdot S(n,k)$
Ne ločimo	Ločimo	$\binom{n+k-1}{k-1}$	$\binom{k}{n}$	$\binom{n-1}{k-1}$
Ločimo	Ne ločimo	$\sum_{i \leqslant k} S(n,i)$	$k \geqslant n \ ? \ 1 : 0$	$S(n,k)$
Ne ločimo	Ne ločimo	$\overline{p_k}(n)$	$k \geqslant n \ ? \ 1 : 0$	$p_k(n)$

4 Rodovne funkcije

4.1 Uvod

Na kakšne načine lahko predstavimo zaporedje?

1. Z eksplicitno formulo

$$a_n = 2^n \quad b_n = n! \quad F_n = \frac{1}{\sqrt{5}}((\tfrac{1+\sqrt{5}}{2})^{n+1} - (\tfrac{1-\sqrt{5}}{2})^{n+1})$$

2. Z rekurzivno zvezo

$$a_n = F_{n \geqslant d}(a_{n-1}, a_{n-2}, ...) + \text{začetni členi } a_0, ...a_{d-1}$$

$$a_n = 2a_{n-1}, \quad a_0 = 1$$
$$b_n = nb_{n-1}, \quad n \geqslant 1, \quad b_0 = 1$$
$$F_n = F_{n-1} + F_{n-2}, \quad n \geqslant 2, \quad F_0 = 1, \quad F_1 = 1$$

3. Z asimptotsko formulo

$$F_n \sim \frac{1}{\sqrt{5}}(\frac{1+\sqrt{5}}{2})^{n+1}$$

$$n! \sim \sqrt{2\pi n}(\frac{n}{e})^n$$

Definicija 4.1 (Asimptotska enakost)**.** $a_n \sim b_n := \lim_{n\to\infty} \frac{a_n}{b_n} = 1$

Opomba. $\sqrt{2\pi n}(\frac{n}{e})^n$ smatramo za preprostejšo formulo kot $n!$, saj je prejšnja bolj uporabna pri računanju.

Za izračun potence a^b potrebujemo $log_2(b)$ operacij, računanje $n!$ pa je izjemno počasno.

Primer. $2^{64} = (((((2^2)^2)^2)^2)^2)^2$

Primer. $2^{100} = ((2^{24} \cdot 2)^2)^2$

Ponavadi zaporedja poenostavimo tako, da jih ocenimo s pribižkom, ki ima splošni člen oblike $a_n \sim An^BC^n$.

4. Z rodovno funkcijo

Spomnimo se iz analize: $\sum_{n=0}^{\infty} a_n x^n$ je potenčna vrsta, ki konvergira na $x \in (-R, R)$, divergira pa na $x \in (-\infty, -R) \cup (R, \infty)$, kjer je $R \in [0, \infty]$ (lahko je tudi ∞) konvergenčni polmer. V $x = \pm R$ ne moremo zagotovo trditi ničesar.

$$R = \lim_{n\to\infty} |\frac{a_n}{a_{n+1}}|, \text{ če limita obstaja}$$

$$R = \frac{1}{\limsup\limits_{n\to\infty} \sqrt[n]{|a_n|}} \in [0, \infty]$$

Za $\sum_{n=0}^{\infty} a_n z^n$, z $\in \mathbb{C}$ velja podobno: konvergira za $|z| < R$, divergira za $|z| > R$.

Primer. $\sum_{n=0}^{\infty} 2^n x^n$, $R = \lim_{n\to\infty}(\frac{2^n}{2^{n+1}}) = \frac{1}{2}$, $\frac{1}{\limsup\limits_{n\to\infty} \sqrt[n]{|2^n|}} = \frac{1}{2}$

Primer. $\sum_{n=0}^{\infty} n! x^n$, $R = \lim_{n\to\infty}(\frac{n!}{(n+1)!}) = 0$, divergira za $x \neq 0$

Primer. $e^x = \sum_{n=0}^{\infty} \frac{1}{n!} x^n$

Vzemimo sedaj zaporedje $a_n = 2^n = 1, 2, 4, 8, \ldots$ in ga zapišimo kot polinom, nato pa uporabimo formulo za potenčno vrsto.

$$1 + 2x + 4x^2 + 8x^3 + \cdots = \sum_{n=0}^{\infty} 2^n x^n = \frac{1}{1-2x}, \quad |x| < \frac{1}{2}$$

Zaporedje lahko na ta način "zakodiramo" v funkcijo.

$$a_n = n! \to \sum_{n=0}^{\infty} n! \cdot x^n$$

Ampak tega (za primer $a_n = n!$) žal ne znamo izračunati. Zato bomo vpeljali eksponentno rodovno funkcijo.

- $\sum_{n=0}^{\infty} a_n \cdot x^n$ je (običajna) rodovna funkcija $(a_n)_n$
- $\sum_{n=0}^{\infty} a_n \cdot \frac{x^n}{n!}$ je eksponentna rodovna funkcija $(a_n)_n$

$$\sum_{n=0}^{\infty} n! \cdot \frac{x^n}{n!} = \sum_{n=0}^{\infty} x^n = \frac{1}{1-x}$$

$$\sum_{n=0}^{\infty} 2^n \cdot \frac{x^n}{n!} = e^{2x}$$

$$\sum_{n=0}^{\infty} F_n \cdot x^n = \frac{1}{1-x-x^2}$$

Zadnji primer bomo izpeljali kasneje.

4.2 Formalne potenčne vrste

Definicija 4.2 (Polinom)**.**

$$\mathbb{R}[x] = \{a_0 + a_1 x + a_2 x^2 + ... + a_n x^n : a_0, ..., a_n \in \mathbb{R}\}$$

Množica realnih ($\mathbb{R}[x]$) oziroma kompleksnih ($\mathbb{C}[x]$) polinomov tvori polje za seštevanje in množenje (v resnici tudi $\mathbb{Q}[x]$, $\mathbb{Z}_p[x]$ in ostali obsegi).

$$\sum_{i=0}^{n} a_i x^i + \sum_{j=0}^{m} b_j x^j = \sum_{i=0}^{max(n,m)} (a_i + b_i) x^i$$

$$(a_i = 0 : i > n; b_j = 0, j > m)$$

Ker se želimo ukvarjati zgolj s poljem polinomov (ne s funkcijami), bomo polinom definirali drugače

Definicija 4.3 (Polinom kot zaporedje)**.**

$$\mathbb{R}[x] = \{(a_0, a_1, ...) : a_i \in \mathbb{R}. \text{ Le končno mnogo } a_i \neq 0\}$$

$(\mathbb{R}[x], +, \cdot)$ je (neskončnorazsežen) vektorski prostor (za $\cdot$ množenje s skalarjem)

$\mathbb{R}_n[x] = \{a_0+a_1x+...+a_nx^n : a_0, ..., a_n \in \mathbb{R}\}$ (polinomi stopnje $\leqslant n$) je $(n+1)$-dimenzionalen vektorski prostor. Njegova baza je npr. $1, x, x^2, ..., x^n$, lahko pa tudi $1, x^{\underline{1}}, x^{\underline{2}}, ..., x^{\underline{n}}$ ali $1, x^{\overline{1}}, x^{\overline{2}}, ..., x^{\overline{n}}$. Prehodni matriki bi bili $[c(n,k)]$ in $[S(n,k)]$.

$$\sum_k c(n,k)x^k = x^{\overline{n}} \qquad \sum_k S(n,k)x^{\underline{k}} = x^n$$

Definicija 4.4 (Konvolucijsko množenje)**.** Produkt polinomov po pravilu "vsak z vsakim".

$$\sum_n a_n x^n \cdot \sum_n b_n x^n = \sum_n \Big(\sum_{k=0}^{n} (a_k b_{n-k}) \Big) x^n$$

Primer. $(a_0 + a_1x + ... + a_nx^n)(b_0 + b_1x + ... + b_mx^m) = a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + (a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0)x^3 + ... + a_nb_mx^{n+m}$

Koeficienti pri x^k so

$$a_0b_k + a_1b_{k-1} + ... + a_kb_0 = \sum_{i=0}^{k} a_ib_{k-i} = \sum_{\substack{i,j \geqslant 0 \\ i+j=k}} a_ib_j$$

$(\mathbb{R}[x], +, \cdot)$ je sedaj komutativen kolobar (kjer je $\cdot$ konvolucijski produkt). $\mathbb{R}[x]$, z vsemi temi operacijami tvori komutativno algebro. Lahko bi za kolobar vzeli tudi $\mathbb{C}([0,1])$. Če vzamemo polinome fiksne stopnje $\mathbb{R}^{n\times n}$, dobimo nekomutativno algebro.

Definicija 4.5 (Algebra)**.** Algebraična struktura $((F, +, \cdot), (V, +, \circ))$ je algebra, če je $((F, +, \cdot), (V, +))$ vektorski prostor in $\circ$ produkt med vektorji, za katerega velja distributivnost.

Definicija 4.6 (Algebra formalnih potenčnih vrst)**.** $\mathbb{R}[[x]]$ je komutativna algebra zaporedij v $\mathbb{R}$.

$$\mathbb{R}[[x]] = \{(a_0, a_1, a_2, ...) : a_i \in \mathbb{R}\} = \{f : \mathbb{N} \to \mathbb{R}\} = \mathbb{R}^{\mathbb{N}}$$

Za operacije

$$(a_n)_n + (b_n)_n = (a_n + b_n)_n$$

$$\lambda(a_n)_n = (\lambda a_n)_n \quad \lambda \in \mathbb{R}$$

$$(a_n)_n(b_n)_n = (\sum_{k=0}^{n} a_k b_{n-k})_n$$

Namesto $(a_n)_n$ ali $a_0, a_1, a_2, \ldots$ pišemo $\sum_{n=0}^{\infty} a_n x^n$ oziroma $a_0+a_1x+a_2x^2+\ldots$. V tem primeru x ni spremenljivka, x^n ni potenciranje, $\cdot$ ni množenje in $+$ ni seštevanje, temveč so samo oznake, da ločimo med členi.

Z izrazom "formalna potenčna vrsta" se nanašamo na neko zaporedje. "Rodovna funkcija zaporedja" (ang. "generating function") je v bistvu tudi formalna potenčna vrsta (torej zaporedje), ampak ponavadi s tem mislimo bolj na zaporedje kot celoto, t.j. na funkcijski zapis, npr. $\frac{1}{1-2x}$.

Enota za množenje je $1 = 1+0x+0x^2+\ldots$. Velja tudi $(1+x+x^2+...)(1-x) = 1$, torej je $(1-x)$ multiplikativni inverz za $(1+x+x^2+...)$. To poznamo kot formulo za potenčno vrsto.

$$\sum_{n=0}^{\infty} x^n = \frac{1}{1-x}$$

Trditev 4.7. $\sum_{n=0}^{\infty} a_n x^n$ ima inverz za množenje natanko tedaj, ko $a_0 \neq 0$.

Dokaz. $(\Rightarrow)$

$$\sum_{n=0}^{\infty} a_n x^n \cdot \sum_{n=0}^{\infty} b_n x^n = 1$$

$$\begin{aligned} a_0b_0 &= 1 \\ a_0b_1 + a_1b_0 &= 0 \\ a_0b_2 + a_1b_1 + a_2b_0 &= 0 \\ ... &= 0 \end{aligned}$$

$(\Leftarrow)$ Skonstruirajmo inverz za $\sum_{n=0}^{\infty} b_n x^n$

$$\begin{aligned} b_0 &= \frac{1}{a_0} \\ b_1 &= -\frac{a_1b_0}{a_0} \\ b_2 &= -\frac{a_1b_1 + a_2b_0}{a_0} \\ &... \end{aligned}$$

■

Vpeljimo nekaj oznak, ki jih bomo uporabljali v nadaljevanju.

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

$[x^n]F(x) \coloneqq a_n$ (n-ti člen zaporedja)

$F(0) \coloneqq [x^0]F(x)$

$(F \cdot G)(0) \coloneqq F(0) \cdot G(0)$

Definicija 4.8 (Odvod formalne potenčne vrste)**.** Definiramo po zgledu odvajanja polinomov pri analizi.

$$F(x) = \sum_n a_n x^n \implies F'(x) \coloneqq \sum_n (n+1) a_{n+1} x^n$$

$$(a_0, a_1, a_2, ...) \longmapsto (a_1, 2a_2, 3a_3, ...)$$

Trditev 4.9 (Odvod produkta)**.** Deluje enako kot pri analizi.

$$(F(x)G(x))' = F'(x)G(x) + F(x)G'(x)$$

Dokaz. Preverimo, da se koeficienti ujemajo pri splošnem členu $[x^n]$. Na levi imamo

$$(n+1)(a_0 b_{n+1} + a_1 b_n + ... + a_{n+1} b_0)$$

Na desni pa

$$a_1 b_n + 2a_2 b_{n-1} 3a_3 b_{n-2} + ... + (n+1) a_{n+1} b_0 + a_0 (n+1) b_{n+1} + a_1 n b_n + a_2 (n-1) b_{n-1} + ... + a_n b_1$$

kar lahko zapišemo kot

$$(0+n+1)(a_0 b_{n+1}) + (1+n)(a_1 b_n) + (2+n-1)(a_2 b_{n-1}) + ... + (n+1)(a_n b_1) + (n+1+0)(a_{n+1} b_0)$$

Od tod neposredno sledi naša formula. ■

Definicija 4.10.

$$e^{\lambda x} \coloneqq \sum_n \frac{\lambda^n}{n!} x^n$$

Trditev 4.11. Velja $e^{\lambda x} \cdot e^{\mu x} = e^{(\lambda + \mu) x}$

Dokaz. Uporabimo formulo za splošni člen konvolucijskega produkta

$$e^{\lambda x} \cdot e^{\mu x} = \sum_{k=0}^{n} \frac{\lambda^k}{k!} \frac{\mu^{n-k}}{(n-k)!} \stackrel{?}{=} \frac{(\lambda + \mu)^n}{n!} = e^{(\lambda + \mu) x}$$

Če enakost z vprašajem pomnožimo z $n!$, dobimo

$$\sum_{k=0}^{n} \binom{n}{k} \lambda^k \mu^{n-k} = (\lambda + \mu)^n$$

kar pa drži po binomskem izreku. ■

Opomba. Ni nujno, da se omejimo na realne polinome. Tudi $\mathbb{C}$[[x]] in $\mathbb{Q}$[[x]] tvorita algebri. Splošneje, vzamemo lahko poljuben $K[[x]]$, kjer je K komutativen obseg, $(K, +)$ abelova grupa, $(K \setminus \{0\}, \cdot)$ abelova grupa in med operacijama velja distributivnost. To vključuje tudi končna polja, npr. $\mathbb{Z}_p$, kjer je p praštevilo.

Izrek 4.12. Polje velikosti n obstaja natanko tedaj, ko je n potenca praštevila ($n = p^k$). Za nek n obstaja samo eno tako polje (do izomorfizma natančno).

Definicija 4.13 (Karakteristika)**.** Je najmanjše tako število k, da velja $\underbrace{1 + 1 + \cdots}_{k\text{-krat}} = id$.

Obseg ima karakteristiko 0, če $1 + 1 + ... + 1 \neq 0$.

Primer. V $\mathbb{Z}_5$ velja $1 + 1 + 1 + 1 + 1 = 0$, torej $\mathbb{Z}_5$ ima karakteristiko 5.

Primer. $\mathbb{Q}$, $\mathbb{R}$ in $\mathbb{C}$ imajo karakteristiko 0.

Končna polja imajo karakteristiko p, če so velikosti p^k.

V $\mathbb{Z}_5$ za vsa števila večja od 5 velja $5! = 6! = ... = 0$. V obsegu s karakteristiko > 0 zato izraz $\frac{1}{n!}$ ni nujno definiran. Zato se omejimo na obsege s karakteristiko 0.

4.3 Uporaba rodovnih funkcij pri reševanju rekurzivnih enačb

Opomba. Dejanski primeri v tem poglavju niso vključeni.

Spomnimo se na dekompozicijo parcialnih ulomkov.

$$\frac{x + 1}{(1 - 2x)(1 - x)} = \frac{A}{1 - 2x} + \frac{B}{1 - x}$$

Opomba (Parcialna dekompozicija z metodo prekrivanja). V zgornjem primeru obe strani pomnožimo z $(1 - 2x)$, nato pa vstavimo $x = \frac{1}{2}$. Ostane samo $A = 3$. Pomnožimo še z $(1-x)$ in vstavimo $x = 1$. Dobimo $B = -2$. Požvižgamo se na deljenje z nič, ker deluje.

Pozor! Ta metoda deluje samo takrat, ko imamo v imenovalcu samo enostavne ničle. Če imamo tudi ničle višjih stopenj, lahko enostavne ničle izračunamo z metodo prekrivanja, ostale pa ročno.

Ugotovili smo, da $\frac{x+1}{(1-2x)(1-x)}$, kar je v bistvu $\frac{3}{1-2x} - \frac{2}{1-x}$ lahko interpretiramo kot $a_n = 3 \cdot 2^n - 2$.

Spomnimo se še na kvadratno enačbo.

$$ax^2 + bx + c = a(x - x_1)(x - x_2),\ x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Pri kombinatoriki jo bomo nekoliko obrnili.

$$c + bx + ax^2 = c(1 - y_1 x)(1 - y_2 x)$$

$\frac{1}{y_1}$ in $\frac{1}{y_2}$ sta ničli našega polinoma $c + bx + ax^2$.

$$c + b\frac{1}{y} + a\frac{1}{y^2} = 0 \quad / \cdot y^2$$

$$a + by + cy^2 = 0$$

$y_{1,2}$ sta torej ničli obratnega polinoma.

Trditev 4.14.

$$\frac{1}{(1-x)^k} = \sum_{n=0}^{\infty} \binom{n+k-1}{k-1} x^n$$

Dokaz.

$$\frac{1}{1-x} \cdot \frac{1}{1-x} \cdot \dots \cdot \frac{1}{1-x} = (1+x+x^2+\cdots)(1+x+x^2+\cdots)\cdots(1+x+x^2+\cdots)$$

Tako na levi kot na desni strani je k členov. Vzemimo za primer $k = 3$ in analizirajmo člen $[x^5]$:

$$x^5 \cdot x^0 \cdot x^0, \quad x^3 \cdot x^1 \cdot x^1, \quad x^1 \cdot x^2 \cdot x^2, \quad \dots$$

Ugotovimo, da delamo šibke kompozicije moči k, teh pa je ravno $\binom{n+k-1}{k-1}$. ∎

Dokaz. (Z indukcijo) Dokaz z indukcijo je bralcu prepuščen za vajo. ∎

Primer. $\frac{1}{1-x} = \sum_n x^n$.

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

Primer. $\frac{1}{(1-x)^3} = \sum_n \binom{n+2}{2} x^n$.

4.3.1 Fibonaccijeva rodovna funkcija

Poskusimo sestaviti rodovno funkcijo za Fibonaccijevo zaporedje $1, 1, 2, 3, 5, 8, \ldots$. Uporabili bomo oznaki $F_n = n$-ti člen Fibonaccijevega zaporedja in $F(x) = \sum_{k=0}^{\infty} F_n \cdot x^n$, t.j. Fibonaccijeva formalna potenčna vrsta.

$$
\begin{aligned}
F_n &: 1, 1, 2, 3, 5, 8, 13, 21, \ldots \\
F_{n-1} &: 0, 1, 1, 2, 3, 5,\ 8, 13, \ldots = x \cdot F(x) \\
F_{n-2} &: 0, 0, 1, 1, 2, 3,\ 5,\ 8, \ldots = x^2 \cdot F(x)
\end{aligned}
$$

Opazimo, da velja $F(x) = 1 + x \cdot F(x) + x^2 \cdot F(x)$. Če ta izraz malo uredimo, dobimo

$$F(x)(1 - x - x^2) = 1$$

$$F(x) = \frac{1}{1 - x - x^2}$$

Kar je rodovna funkcija za Fibonaccijevo zaporedje.

Primer. $a_n = 2a_{n-1}$, $a_0 = 1$. Pomnožimo rekurzivno formulo z x^n in seštejmo $\sum_{n=1}^{\infty}$.

$$\sum_{n=1}^{\infty} a_n x^n = \sum_{n=1}^{\infty} 2a_{n-1} x^n$$

Leva stran je $F(x) - 1$, ker seštevamo od $n = 1$ namesto od $n = 0$. Na desni strani nesemo pred vsoto 2 in izpostavimo en x, da imamo pri a isto številko.

$$F(x) - 1 = 2x \sum_{n=1}^{\infty} a_{n-1} x^{n-1} = 2x \sum_{n=0}^{\infty} a_n x^n = 2xF(x)$$

Izpostavimo $F(x)$ kot prej

$$F(x)(1 - 2x) = 1 \implies F(x) = \frac{1}{1 - 2x}$$

Če želimo, lahko to pretvorimo še v eksplicitno formulo.

$$F(x) = \frac{1}{1 - 2x} = \sum_{n=0}^{\infty} 2^n x^n \implies a_n = 2^n$$

Primer. $a_n = 3a_{n-1} - 2a_{n-2}$, $a_0 = 1$, $a_1 = 4$. Primer je prepuščen bralcu. Rešitev je $F(x) = \frac{1+x}{1-3x+2x^2}$ oziroma $a_n = 3 \cdot 2^n - 2$

Poskusimo posplošiti zgornji postopek za poljubno homogeno linearno rekurzivno enačbo.

Izrek 4.15 (Recept za reševanje homogene linearne rekurzivne enačbe s konstantnimi koeficienti)**.**

$$c_d a_n + c_{d-1} a_{n-1} + \cdots + c_0 a_{n-d} = 0 \quad n \geqslant d$$

Zapišimo karakteristični polinom

$$c_d \lambda^d + c_{d-1} \lambda^{d-1} + \cdots + c_0 \quad (c_d, c_0 \neq 0, c_i \in \mathbb{C})$$

kjer so $\lambda_1, \ldots, \lambda_k$ ničle z večkratnostmi $\alpha_1, \ldots \alpha_k$.

$$a_n = \sum_{i=1}^{k} p_i(n) \lambda_i^n, \quad deg(p_i) < \alpha_i$$

Dokaz. Pomnožimo vrsto z x^n in seštejmo od d do ∞.

$$c_d a_n + c_{d-1} a_{n-1} + \cdots + c_0 a_{n-d} = 0 \quad /x^n / \sum_{n=d}^{\infty}$$

$$\begin{aligned}
0 = & \, c_d(F(x) - a_0 - a_1 x - \cdots - a_{d-3} x^{d-3} - a_{d-2} x^{d-2} - a_{d-1} x^{d-1}) \\
& + c_{d-1} x (F(x) - a_0 - a_1 x - \cdots - a_{d-3} x^{d-3} - a_{d-2} x^{d-2}) \\
& + c_{d-2} x^2 (F(x) - a_0 - a_1 x - \cdots - a_{d-3} x^{d-3}) \\
& + \cdots \\
& + c_1 x^{d-1} (F(x) - a_0) \\
& + c_0 x^d F(x)
\end{aligned}$$

$F(x)(c_d + c_{d-1} x + c_{d-2} x^2 + \cdots + c_1 x^{d-1} + c_0 x^d) = P(x)$ polinom stopnje $<$ d

$$F(x) = \frac{P(x)}{c_d + c_{d-1} x + c_{d-2} x^2 + \cdots + c_1 x^{d-1} + c_0 x^d}$$

Karakteristični polinom: $c_d \lambda^d + c_{d-1} + \lambda^{d-1} + \cdots + c_0$ z ničlami $\lambda_1, \ldots, \lambda_k$

$$\begin{aligned}
F(x) &= \frac{P(x)}{c_d \prod_{i=1}^{k} (1 - \lambda_i x)^{\alpha_i}} = \\
&= \sum_{i=1}^{k} \sum_{j=1}^{\alpha_i} \frac{A_{i,j}}{(1 - \lambda_i x)^j} = \\
&= \sum_{i=1}^{k} \sum_{j=1}^{\alpha_i} A_{ij} \sum_{n=0}^{\infty} \binom{n+j-1}{j-1} \lambda_i^n x^n
\end{aligned}$$

$$a_n = \sum_{i=1}^{k}(\sum_{j=1}^{\alpha_i} A_{ij}\binom{n+j-1}{j-1})\lambda_i^n = \sum_{i=1}^{k} p_i(n)\lambda_i^n$$

$$\binom{n+j-1}{j-1} = \frac{(n+j-1)(n+j-2)...(n+1)}{(j+1)!}$$

$$\text{polinom stopnje (j - 1)} \implies deg(p_i) < \alpha_i$$

■

Izrek 4.16 (Reševanje nekaterih nehomogenih rekurzivnih enačb)**.**

$$c_d a_n + c_{d-1}a_{n-1} + ... + c_0 a_{n-d} = q(n)\lambda^n$$

Rešitev je vsota rešitve homogene enačbe in partikularne rešitve, ki jo poiščemo z nastavkom

$$a_n = n^\alpha r(n)\lambda^n$$

$\deg(r(n)) \leqslant \deg(q)$, α-kratnost λ v karakterističnem polinomu,

$$\alpha \geqslant 0, \quad \alpha = 0 \iff \lambda \text{ ni ničla}$$

Dokaz. Prepuščen bralcu. ■

4.4 Binomska vrsta

Spomnimo se biomskega koeficienta za $n, k \in \mathbb{N}$

$$\binom{n}{k} = \left|\binom{[n]}{k}\right| = \frac{n^{\underline{k}}}{k!} = \begin{cases} \frac{n!}{k!(n-k)!} : 0 \leqslant k \leqslant n \\ 0 : k > n \end{cases}$$

Definicija 4.17 (Posplošeni binomski koeficient)**.** Zahtevamo samo $n \in \mathbb{N}$.

$$\binom{\lambda}{n} = \frac{\lambda^{\underline{n}}}{n!} = \frac{\lambda \cdot (\lambda-1)\cdots(\lambda-n+1)}{n!}$$

Kjer je $\lambda \in K$, K konvergentni obseg s karakteristiko 0, npr $\mathbb{R}^2$ ali $\mathbb{C}^2$.

Primer. $\binom{\frac{5}{2}}{3} = \frac{\frac{5}{2}\cdot\frac{3}{2}\cdot\frac{1}{2}}{6} = \frac{5}{16}$

Primer. $\binom{i}{2} = \frac{i(i-1)}{2} = \frac{-1-i}{2}$

Primer. $\binom{-1}{n}\frac{(-1)(-2)...(-n)}{n!} = (-1)^n$

Primer. $k \in \mathbb{N}$:

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

$$= \frac{(-1)^n(n+l+k-1)!}{n!(k-1)!} = (-1)^n\binom{n+k-1}{k-1}$$

Primer.

$$\binom{\frac{1}{2}}{n} = \frac{\frac{1}{2}\cdot(-\frac{1}{2})\cdot(-\frac{3}{2})\cdots(\frac{1}{2}-n+1)}{n!} = \frac{(-1)^{n-1}\cdot 1\cdot 3\cdot 5\cdots(2n-3)}{2^n\cdot n!}$$

Uporabimo simbol !!. Velja $7!! = 1\cdot3\cdot5\cdot7$ oziroma za soda števila: $6!! = 2\cdot4\cdot6$. Pri sodih številih pa lahko izpostavimo 2, da dobimo $6!! = 2^3\cdot 3!$.

$$\frac{(-1)^{n-1}(2n-3)!!}{2^n\cdot n!}\cdot\frac{(2n-2)!!}{(2n-2)!!} = \frac{(-1)^{n-1}(2n-2)!}{2^n\cdot n!\cdot 2^{n-1}(n-1)!} = \frac{(-1)^{n-1}}{2^{2n-1}\cdot n}\binom{2n-2}{n-1}$$

Če smo malo previdni, opazimo, da to deluje samo pod pogojem $n \geqslant 1$, sicer je $\binom{\frac{1}{2}}{n} = 0$.

Definicija 4.18 (Binomska vrsta)**.** Naj bo K obseg in $\lambda \in K$.

$$B_\lambda(x) = \sum_{n=0}^{\infty}\binom{\lambda}{n}x^n$$

$$= 1 + \lambda x + \frac{\lambda(\lambda-1)}{2}x^2 + \frac{\lambda(\lambda-1)(\lambda-2)}{6}x^3 + ...$$

Opomba. Zapis $B_\lambda(x) = \sum_{n=0}\binom{\lambda}{n}x^n$ je napačen! Lahko je bodisi $\sum_{n\in\mathbb{N}_0}$, $\sum_{n=0}^{\infty}$ ali $\sum_{n=0}^{\lambda}$.

Primer. Če za λ vzamemo $n \in \mathbb{N}$, dobimo binomski izrek.

$$B_n(x) = \sum_{k=0}^{\infty}\binom{n}{k}x^k = \sum_{k=0}^{n}\binom{n}{k}x^k = (1+x)^n$$

Primer. Če za λ vzamemo $-k$, $k \in \mathbb{N}$, dobimo

$$B_{-k}(x) = \sum_{n=0}^{\infty}\binom{-k}{n}x^n = \sum_{n=0}^{\infty}(-1)^n\binom{n+k-1}{k-1}x^n = (1+x)^{-k}$$

Zadnjo enakost smo dokazali v prejšnjem razdelku (glej 4.14).

Opazimo očiten vzorec. Ali bi lahko posplošili pravilo $B_\lambda(x) = (1+x)^\lambda$? Natančneje, če bi definirali npr. $(1+x)^{\frac{1}{2}}$ tako, da velja $((1+x)^{\frac{1}{2}})^2 = 1$, ali lahko pričakujemo, da je $B_{\frac{1}{2}} = (1+x)^{\frac{1}{2}}$? Vse to in še več bomo lahko trdili, ko dokažemo $B_\lambda(x) \cdot B_\mu(x) = B_{\lambda+\mu}(x)$.

Lema 4.19 (Binomski izrek s črtico)**.**

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

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

Dokaz. Z indukcijo.
Baza indukcije: $n = 0$, $1 = 1$ ✓
Indukcijski korak: $n-1 \implies n$

$$\begin{aligned}(\lambda+\mu)^{\underline{n}} &= (\lambda+\mu)^{\underline{n-1}}(\lambda+\mu-n+1) = \\ &\overset{IP}{=} \sum_k \binom{n-1}{k} \lambda^{\underline{k}} \mu^{\underline{n-1-k}} (\lambda - k + \mu + k - n + 1) = \\ &= \sum_k \binom{n-1}{k} \lambda^{\underline{k+1}} \mu^{\underline{n-1-k}} + \sum_k \binom{n-1}{k} \lambda^{\underline{k}} \mu^{\underline{n-k}} = \\ &= \sum_k \binom{n-1}{k-1} \lambda^{\underline{k}} \mu^{\underline{n-k}} + \sum_k \binom{n-1}{k} \lambda^{\underline{k}} \mu^{\underline{n-k}} = \\ &= \sum_k \binom{n}{k} \lambda^{\underline{k}} \mu^{\underline{n-k}}\end{aligned}$$

Dokaz za naraščajoče potence prepustimo bralcu. ■

4.4.1 Catalanova števila

Definicija 4.20 (Catalanovo število)**.** C_n je število pravilnih postavitev oklepajev na nizu $n+1$ števil $(t_0\ t_1\ t_2\ \ldots\ t_n)$.

Prvih nekaj Catalanovih števil (od $n = 0$ dalje): $1, 1, 2, 5, 14, 42, \ldots$.

$n = 0$	(t_0)				
$n = 1$	$(t_0 t_1)$				
$n = 2$	$(t_0 t_1) t_2$	$t_0 (t_1 t_2)$			
$n = 3$	$((t_0 t_1) t_2) t_3$	$(t_0 t_1)(t_2 t_3)$	$t_0 (t_1 (t_2 t_3))$	$(t_0 (t_1 t_2)) t_3$	$t_0 ((t_1 t_2) t_3)$

Poiščimo rekurzivno zvezo za C_n. Za rekurzivni korak bomo izbrali lokacijo zadnjega množenja (stik najbolj zunanjih oklepajev).

Primer. Pri $((t_0t_1)t_2)t_3$ je "zadnje množenje" med $((t_0t_1)t_2)$ in t_3, pri $(t_0t_1)(t_2t_3)$ pa med (t_0t_1) in (t_2t_3).

V splošnem, $(t_0t_1\dots t_k)\cdot(t_{k+1}\dots t_{n+1})$, kjer velja $0 \leqslant k \leqslant n$. Ostane nam še izbira oklepajev med k členi in $(n+1)-(k+1)=n-k$ členi.

Izrek 4.21 (Rekurzivna zveza za C_n)**.**

$$C_{n+1}=\sum_{k=0}^{n} C_k C_{n-k} \qquad n \geqslant 0$$

Ker smo kul matematiki, se ne bomo zadovoljili zgolj z rekurzivno zvezo.

Izrek 4.22 (Eksplicitna formula za C_n)**.**

$$C_n=\frac{1}{n+1}\binom{2n}{n}$$

Dokaz. Definirajmo $F(x)=\sum_{n=0}^{\infty} C_n x^n$. Pomnožimo rekurzijo z x^{n+1} in seštejmo člene $\sum_{n=0}^{\infty}$, kot smo to počeli pri linearnih rekurzijah.

$$\sum_{n=0}^{\infty} C_{n+1}x^{n+1}=\sum_{n=0}^{\infty}(\sum_{k=0}^{\infty} C_k C_{n-k})x^{n+1}$$

Levo stran izrazimo kot $F(x)-1$, na desni strani pa opazimo konvolucijo $F(x)$ s samim sabo. Dobimo torej $xF^2(x)$. Če enakost preoblikujemo, dobimo $xF^2(x)-F(x)+1=0$.

Kaj pa zdaj? No, ko vidimo kvadratno enačbo, nas ima, da bi jo rešili. Poskusimo s kvadratno enačbo

$$F(x)=\frac{1\pm\sqrt{1-4x}}{2x}$$

Sedaj pa se vprašajmo, če je ta izraz kaj smiseln. Če začnemo s členom $\sqrt{1-4x}$, lahko uporabimo binomsko vrsto.

$$\begin{aligned}
\sqrt{1+x}&=1-2\sum_{n=1}^{\infty}\frac{(-1)^n}{2^{2n}n}\binom{2n-2}{n-1}x^n\\
\sqrt{1-4x}&=1-2\sum_{n=1}^{\infty}\frac{\cancel{(-1)^n}}{\cancel{2^{2n}}n}\binom{2n-2}{n-1}(-4x)^n\\
&=1-2\sum_{n=1}^{\infty}\frac{1}{n}\binom{2n-2}{n-1}x^n
\end{aligned}$$

Nadaljujemo tako, da izračunano vstavimo v prvotno ničlo.

$$\frac{1+\sqrt{1-4x}}{2x} = \frac{2-2\sum_{n=1}^{\infty}\frac{1}{n}\binom{2n-2}{n-1}x^n}{2x} \qquad \notin k[[x]]$$

To na žalost ni formalna potenčna vrsta, saj delimo neko vrsto z x-om, ki se ne more izpostaviti.

Po drugi strani, če vzamemo drugo ničlo, se nam člen 1 krajša, ostane pa lepa formalna potenčna vrsta.

$$\frac{1-\sqrt{1-4x}}{2x} = \sum_{n=1}^{\infty}\frac{1}{n}\binom{2n-2}{n-1}x^{n-1}$$

Ta vrsta tudi reši našo kvadratno enačbo.

$$x\Big(\frac{1-\sqrt{1-4x}}{2x}\Big)^2 - \frac{1-\sqrt{1-4x}}{2x} + 1 \underset{\sqrt{1-4x}^2=1-4x}{=} 0$$

Zato je to naša rešitev.

$$F(x) = \sum_{n=0}^{\infty}\frac{1}{n+1}\binom{2n}{n}x^n$$

$\blacksquare$

Primer. $C_3 = \frac{1}{4}\binom{6}{3} = \frac{\cancel{6}\cdot 5\cdot\cancel{4}}{\cancel{4}\cdot\cancel{6}} = 5$

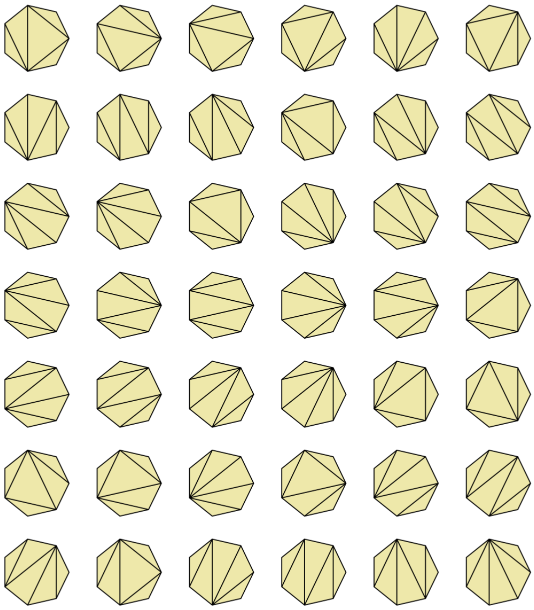
Primer. $C_5 = \frac{1}{6}\binom{10}{5} = \frac{\overset{\cancel{2}}{\cancel{2}}\cdot\overset{3}{\cancel{9}}\cdot\overset{2}{\cancel{8}}\cdot 7\cdot\cancel{6}}{\cancel{6}\cdot\cancel{5}\cdot\cancel{4}\cdot\cancel{3}\cdot\cancel{2}} = 42$

Catalanova števila so zelo pogosta v kombinatoriki. Dva primera uporabe sta:

- Dyckove poti dolžine n. To so poti od $(0,0)$ do $(2n,0)$ s koraki diagonalno gor $(1,1)$ in diagonalno dol $(1,-1)$, a nikoli ne grejo pod x os.
- Triangulacije $(n+2)$-kotnika. To pomeni dodajanje diagonal $(n+2)$-kotniku, dokler nimamo samih trikotnikov.

Te dve uporabi lahko dokažete bodisi tako, da najdete bijekcijo med želenimi konstrukcijami in postavljanjem oklepajev, bosidi pokažete, da ima konstrukcija isto rekurzivno zvezo.

V knjigi Enumerative Combinatorics je 66 matematičnih struktur, ki jih preštevajo Catalanova števila. Na spletni strani Richarda Stanlyja jih je še več kot 100.



Slika 3: Triangulacije sedemkotnika

Slika 4: Dyckova pot

4.5 Rodovne funkcije razčlenitev

Spomnimo se na razčlenitve in števila $p_k(n), \overline{p_k}(n), p(n)$.

Primer. $n = 5, k = 3 : (3\ 2), (3\ 1\ 1), (2\ 2\ 1), (2\ 1\ 1\ 1), (1\ 1\ 1\ 1\ 1)$

Ugotovili smo že, kako izračunati koeficient pri $[x^5]$ pri izrazu kot je $(1+x+x^2+\ldots)(1+x+x^2+\ldots)\ldots$. Kaj pa če koeficienti niso povsod enaki?

$$(1+x+x^2+\ldots)(1+x^2+x^4+\ldots)(1+x^3+x^6+\ldots) \qquad [x^5]$$

Izberemo nekaj iz prvega oklepaja, prištejemo 2· nekaj iz drugega in 3· nekaj iz tretjega.

$$x^5 = x^{0\cdot1}\cdot x^{1\cdot2}\cdot x^{1\cdot3} = x^{2\cdot1}\cdot x^{0\cdot2}\cdot x^{1\cdot3} = x^{1\cdot1}\cdot x^{2\cdot2}\cdot x^{0\cdot3} = x^{3\cdot1}\cdot x^{1\cdot2}\cdot x^{0\cdot3} = x^{5\cdot1}\cdot x^{0\cdot2}\cdot x^{0\cdot3}$$

To je enak problem, kot če bi hoteli zapisati število 5 kot vsoto števil 1, 2 in

3. Zgoraj bi to izgledalo (z enakim vrstnim redom)

$$5 = 2 + 3 = 1 + 1 + 3 = 1 + 2 + 2 = 1 + 1 + 1 + 2 = 1 + 1 + 1 + 1 + 1$$

Trditev 4.23.

$$\sum_{n=0}^{\infty} \overline{p_k}(n) x^n = \prod_{i=1}^{k} \frac{1}{1 - x^i}$$

Dokaz. Koeficient na obeh straneh je število rešitev enačbe

$$a_1 \cdot 1 + a_2 \cdot 2 + \ldots + a_k \cdot k = n$$

$$\sum_n p_k(n) x^n = (1 + x + x^2 + \ldots)(1 + x^2 + x^4 + \ldots) \ldots (1 + x^k + x^{2k} + \ldots)$$

$p_k(n) =$ število razčlenitev n s k členi $\leqslant k$, kjer je vsaj en člen $= k$. ∎

Trditev 4.24.

$$\sum_n p_k(n) x^n = \frac{x^k}{\prod_{i=1}^{k}(1 - x^i)}$$

Trditev 4.25.

$$\sum_n p(n) x^n = \prod_{i=1}^{\infty} \frac{1}{1 - x^i}$$

Pri $[x^n] : (1+x+x^2+\ldots)(1+x^2+x^4+\ldots) \ldots (1+x^n+x^{2n}+\ldots)\underbrace{(1 + x^{n+1} + x^{2n+2} + \ldots) \ldots}_{\text{ignoriramo}}$

$$\Longrightarrow \overline{p_n}(n) = p(n)$$

Primer. $o(n)$ je število razčlenitev n s samimi lihimi členi

$$\sum_n o(n) x^n = \prod_{i=0}^{\infty} \frac{1}{1 - x^{2i-1}}$$

Primer. $d(n)$ je število razčlenitev n z različnimi členi

$$\begin{aligned} \sum_n d(n) x^n &= \prod_{i=1}^{\infty} (1 + x^i) \cdot \frac{\prod_{i=1}^{\infty}(1 - x^i)}{\prod_{i=1}^{\infty}(1 - x^i)} \\ &= \frac{\prod_{i=1}^{\infty}(1 - x^{2i})}{\prod_{i=1}^{\infty}(1 - x^i)} \\ &= \prod_{i=1}^{\infty} \frac{1}{1 - x^{2i-1}} \\ &\Longrightarrow o(n) = d(n) \end{aligned}$$

4.6 Uporaba rodovnih funkcij

(1) Rodovna funkcija je pogosto "lepa", tudi če za zaporedje nimamo "lepe" formule.

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

(2) Rodovno funkcijo se da pogosto zapisati iz kombinatoričnega problema (več pri Kombinatoriki 2).

Primer. i_n je število involucij v S_n, torej $\pi^2 = id$, $\sum i_n \frac{x^n}{n!} = e^{x+\frac{x^2}{2}}$. Pomen: e na nekaj sestavljeno iz x (cikli dolžine 1) in $\frac{x^2}{2}$ (cikli dolžine 2).

(3) V rodovni funkciji so "skriti" vsi drugi zapisi zaporedja.

Primer. $\sum_n F_n x^n = \frac{1}{1-x-x^2} \to (1-x-x^2)\sum_n F_n x^n = 1$.

$$[x^n] : F_n - F_{n-1} - F_{n-2} = 0$$

asimptotika: vzamemo singularnost (x_0), ki je najbližje izhodišču

$$F_n \sim An^B(\frac{1}{x_0})^n$$

(4) Iz rodovnih funkcij lahko izračunamo še drugo: povprečje, varianco ... npr. koliko elementov ima v povprečju podmnožica $[n]$?

$$\frac{\sum_{S\subseteq[n]}|S|}{2^n} = \frac{\sum_k k\cdot\binom{n}{k}}{2^n} = \frac{n2^{n-1}}{2^n} = \frac{n}{2}$$

5 Pólyeva teorija

Primer. Koliko je ogrlic z n koraldami k barv? Dve ogrlici sta enaki, če eno iz druge dobimo z rotacijo.

Primer. Koliko je zapestnic z n koraldami r barvami? Dve zapestnici sta enaki, če eno iz druge dobimo z rotacijo ali zrcaljenjem.

Nekateri objekti so ekvivalentni, zanima nas število ekvivaletnih razredov barvanj.

Definicija 5.1 (Permutacijska grupa)**.** je grupa $G \leqslant S_n$

Izrek 5.2 (Cayleyev)**.** Vsaka grupa je izomorfna neki permutacijski grupi.

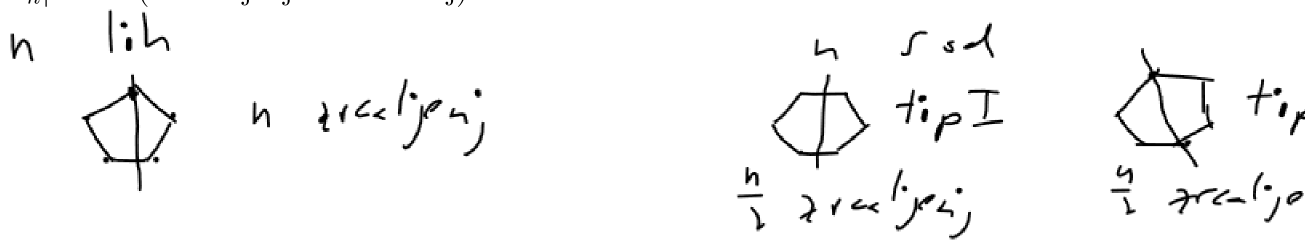
Dokaz. Naj bo G poljubna grupa in $g \in G$. Definirajmo $T_g : G \to G$:

$$T_g(x) = gx$$

T_g je permutacija množice G.
$H = \{T_g : g \in G\}$ je grupa za komponiranje.
$H \cong G$ ■

Primer (Ciklična grupa). $C_n = \{(1\ 2\ 3\ \dots\ n)^i : 0 \leqslant i < n\} \leqslant S_n$
$C_n \cong \mathbb{Z}_n$
$\phi : \mathbb{Z}_n \to C_n := i \to (1\ 2\ \dots\ n)^i$

Primer (Diedrska grupa). $D_n = \{\text{rotacije + zrcaljenja}\} \leqslant S_n$
$|D_n| = 2n$ (n zrcaljenj in n rotacij)



Definicija 5.3 ($x \sim y$)**.** $\exists g \in G : g \cdot x = y$

Trditev 5.4. $\sim$ je ekvivalenčna relacija.

X z operacijo $\sim$ razpade na ekvivalenčne razrede, ki jih imenujemo orbite. Orbito elementa x v G označimo Gx ($\neq G_x$!!).

5.1 Orbite, stabilizatorji in negibne točke

Definicija 5.5 (Orbita)**.**

$$Gx = g \cdot x : g \in G$$

Opomba 5.6. Koncept orbit spominja na leve (desne) odseke, a ni isto. Pri odsekih imamo podgrupo, tukaj pa x niti ni element G. Pomembna posledica je, da so orbite lahko različno velike, odseki pa so po moči vedno enaki ($|aH| = |bH|$).

Primer. Za $G = C_n, D_n$ ali S_n velja $Gx = X$ (samo ena orbita).

Primer.

$$G = \{\text{id, zrcaljenje}\} \leqslant S_n$$

$$\text{število orbit} = \begin{cases} \frac{n+1}{2}; & n \text{ lih} \\ \frac{n}{2}; & n \text{ sod, zrcaljenje tipa 1} \\ \frac{n}{2}+1; & n \text{ sod, zrcaljenje tipa 2} \end{cases}$$

Množico orbit označimo z X/G.

Opomba. Na enak način smo označili tudi faktorske grupe (množice odsekov), a koncept ni isti, ker orbita $\neq$ odsek (glej opombo 5.6).

Definicija 5.7 (Stabilizator)**.**

$$G_x = \{g \in G : g \cdot x = x\}$$

Elemente G_x ($\neq Gx$!!) imenujemo stabilizatorji x-a.

Definicija 5.8 (Negibna točka)**.**

$$X_g = \{x \in X : g \cdot x = x\}$$

Elemente X_g imenujemo negibne točke g-ja.

Izrek 5.9.

$$G_x \leqslant G$$

Dokaz.

$$id \in G_x$$

$$\begin{aligned} g, h \in G_x &\implies g \cdot x = x, h \cdot x = x \\ &\implies (g \cdot h) \cdot x = g \cdot (g \cdot x) = g \cdot x = x \\ &\implies g \cdot h \in G_x \\ g \in G_x &\implies g \cdot x = c \implies g^{-1} \cdot x = g^{-1} \cdot g \cdot x = x \\ &\implies g^{-1} \in G_x \end{aligned}$$

∎

Primer. $G = C_n$
$G_x = \{id\}$
$X_g = \begin{cases} x : g = id \\ \emptyset : g \neq id \end{cases}$

Primer. $G = D_n$
$G_x = \{id, \text{zrcaljenje}\}$
$$X_g = \begin{cases} n : g = id \\ 0 : (g \text{ rotacija}) \text{ ali } (g \text{ zrcaljenje tipa 1 in } n \text{ sod}) \\ 1 : g \text{ zrcaljenje, } n \text{ lih} \\ 2 : g \text{ zrcaljenje tipa 2, } n \text{ sod} \end{cases}$$

Trditev 5.10.
$$|G| = |G_x| \cdot |Gx| \quad \forall x \in X$$

Dokaz. Spomnimo se levih odsekov ...

$$H \leqslant G \models g \cdot H = \{g \cdot h : h \in H\} \quad \text{je levi odsek v } G$$

$$g = e \implies g \cdot H = H$$

$g \cdot H$ in $g' \cdot H$ sta bodisi enaka, bodisi disjunktna. G torej razpade na leve odseke, ki imajo enako moč ($H \to gH$ je bijekcija; inverz $g \to g^{-1}h$).
... in kvocientnih množic

$$G/H = \{gH : g \in G\}$$

$$|G/H| = \frac{|G|}{|H|} \quad (\text{torej } |H| \text{ deli } |G|)$$

Uporabimo za $H = G_x$ Vemo, da velja

$$|G/G_x| = \frac{|G|}{|G_x|}$$

Definirajmo
$$\phi : Gx \to G/G_x \quad \text{kot} \quad g \cdot x \to gG_x$$

ϕ je očitno bijekcija, torej imata Gx in G/G_x enako moč. Velja torej

$$|G_x| \cdot |Gx| = |G_x| \cdot |G/G_x| = |G_x| \cdot \frac{|G|}{|G_x|} = |G|$$

Pozor! g ni enolično določen. Pokažimo, da je ϕ dobro definirana (za nek vhod dobimo enoličen izhod).

$$g \cdot x = h \cdot x \iff h^{-1} \cdot g \cdot x = x \iff h^{-1} \cdot g \in G_x \iff h^{-1} \cdot g \cdot G_x = G_x \iff g \cdot G_x = h \cdot G_x$$

Hkrati smo pokazali, da je injektivna (ker so vmes ekvivalence, ne samo implikacije). Pokažimo še, da je surjektivna:

$$gG_x = \phi(g \cdot x)$$

$$\implies |G_x| = \frac{G}{G_x}$$

■

Primer. Preštej simetrije tetraedra.
$|G| = |G_x||Gx| = 3 \cdot 4 = 12$
id + rotacije za $120°$ + rotacije za $180°$
$1 + 4 \cdot 2 + 3 = 12$

Primer. Preštej simetrije kocke.
$|G| = |G_x||Gx| = 3 \cdot 8 = 24$

5.2 Burnsidova lema

Lema 5.11 (Burnsidova)**.** Število orbit je enako povprečnemu številu negibnih točk.

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X_g|$$

Dokaz.

$$\sum_{g\in G} |X_g| = \sum_{g\in G} \sum_{x \in X_g} 1 = \sum_{g \in G} \sum_{\substack{x\in X \\ g\cdot x = x}} 1 = \sum_{x\in X} \sum_{\substack{g\in G \\ g\cdot x = x}} 1 = \sum_{x \in X} \sum_{g \in G_x} 1 = \sum_{x\in X} |G_x|$$

Opomba. Ta del bi lahko utemeljili tudi s tabelco: v vrstice napišemo elemente X, v stolpce elemente G. Na polju (g, x) naredimo kljukico ntk. $g \cdot x = x$. Število kljukic po vrsticah je $\sum_{x\in X} |G_x|$, število kljukic po stolpcih pa $\sum_{g\in G} |X_g|$.

$$\sum_{g\in G} |X_g| = \sum_{x\in X} |G_x| = \sum_{x\in X} \frac{|G|}{|Gx|} = |G| \sum_{x \in X} \frac{1}{|Gx|}$$

Analizirajmo pomen faktorja $\sum_{x\in X} \frac{1}{|Gx|}$. Za vsak x iz naše množice vzamemo inverz moči njegove orbite. Ker vsak x pripada natanko eni orbiti, in ker ima vsaka orbita natanko toliko x-ov, kolikor je njena moč, dobimo sledečo sliko

$$\underbrace{\frac{1}{2} + \frac{1}{2}}_{=1} + \underbrace{\frac{1}{1}}_{=1} + \underbrace{\frac{1}{4} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4}}_{=1} + \ldots = \text{število orbit}$$

oziroma računsko (oznaka σ = orbita)

$$\sum_{x\in\sigma} \frac{1}{|\sigma|} = |\sigma| \cdot \frac{1}{|\sigma|} = 1$$

kar lahko uporabimo, da poenostavimo

$$|G| \sum_{x \in X} \frac{1}{|Gx|} = |G| \sum_{\sigma \in X/G} \sum_{x \in \sigma} \frac{1}{|\sigma|} = |G| \sum_{\sigma \in X/G} 1 = |G| \cdot |X/G|$$

■

Primer. $G = C_n$. $|X/G|$ je očitno 1, saj lahko iz ene točke z rotacijami v ciklu pridemo kamorkoli, torej imamo samo eno orbito. Ko seštevamo števila negibnih točk, ugotovimo, da jih je pri identiteti n, pri ostalih $n-1$ ciklih pa nobene.

$$1 = \frac{1}{n}(n + (n-1) \cdot 0)$$

Primer. $G = D_n$. Spet imamo očitno samo 1 orbito. Na desni strani pa štejemo: n negibnih točk pri identiteti, $(n-1)$ pravih rotacij, ki nimajo nobene negibne točke, n zrcaljenj z 1 negibno točko če je n lih, sicer pa še $\frac{n}{2}$ zrcaljenj preko simetrale stranic (0 negibnih točk) in $\frac{n}{2}$ zrcaljenj preko diagonale (2 negibni točki).

$$n \text{ lih:} \quad 1 = \frac{1}{2n}(n + (n-1) \cdot 0 + n \cdot 1)$$

$$n \text{ sod:} \quad 1 = \frac{1}{2n}(n + (n-1) \cdot 0 + \frac{n}{2} \cdot 0 + \frac{n}{2} \cdot 2)$$

Primer. $G = \{\text{id}, \text{zrcaljenje}\}$. Ločimo primera glede na parnost n-ja in tip zrcaljenja.

$$n \text{ lih, zrcaljenje preko točke:} \quad 1 + \frac{n-1}{2} = \frac{1}{2}(n+1)$$

$$n \text{ sod, zrcaljenje preko točk:} \quad 2 + \frac{n-2}{2} = \frac{1}{2}(n+2)$$

$$n \text{ sod, zrcaljenje preko stranice:} \quad \frac{n}{2} = \frac{1}{2}(n+0)$$

Primer. $G = S_n$.

$$1 = \frac{1}{n!} \sum_{\pi \in S_n} \#\text{negibnih točk } \pi$$

Ugotovili smo, da je vsota števil negibnih točk vseh permutacij enaka $n!$. To ni povsem očitno, ampak lahko sami preverite.

Primer. 3×3 mreža z 2 luknjama. Koliko različnih konfiguracij obstaja, če konfiguraciji smatramo za enaki ntk. lahko eno dobimo iz druge z rotacijami in zrcaljenji?
Vzemimo za X množico vseh izbir lukenj na plošči ($|X| = \binom{9}{2} = 36$). Na tej množici deluje D_4 ($|D_4| = 8$). Pri identiteti imamo torej 36 negibnih točk, pri rotacijah za 90° vedno 0, pri rotacijah za 180° lahko izberemo katerkoli nasprotni par lukenj (4 možne izbire), pri vodoravnih in navpičnih zrcaljenjih $6+6$, pri diagonalnih zrcaljenjih pa še $2 \cdot 6$ izbir.

$$\frac{1}{8}(36 + 0 + 4 + 12 + 12) = 8$$

Opomba. Če tu ne dobimo naravnega števila, smo falili.

5.3 Ciklični indeks

Naj bo $G \leqslant S_n$ permuatacijska grupa, $n = |X|$. $g \in G$ je permutacija elementov iz X, ki jo seveda lahko enolično zapišemo g kot produkt disjunktih ciklov.

Definicija 5.12 (Ciklični indeks)**.** Označimo z $\alpha_i(g)$ število ciklov dolžine i. Ciklični indeks $Z_G(t_1, \ldots, t_n)$ definiramo kot

$$Z_G(t_1, \ldots, t_n) = \frac{1}{|G|} \sum_{g \in G} t_1^{\alpha_1(g)} t_2^{\alpha_2(g)} \cdots t_n^{\alpha_n(g)}$$

Primer. $G = C_4$. $|G| = 4$. Za vsak element grupe pogledamo kakšna je ciklična struktura. id ima 4 cikle dolžine 1, torej dobimo člen $(t_1)^4$. Rotacija za 180° ima 2 cikla dolžine 2 ((1 2 3 4) in (1 4 3 2)), torej $(t_2)^2$, vsaka od dveh rotacij za 90° pa je cikel dolžine 4, torej $2 \cdot (t_4)^1$.

$$Z_{C_4}(t_1, t_2, t_3, t_4) = \frac{1}{4}((t_1)^4 + (t_2)^2 + 2 \cdot t_4)$$

Primer. $G = D_4$. Imamo identiteto, rotacijo za 180°, dve rotaciji za 90°, 4 zrcaljenja (vodoravno, navpično in dve diagonalni). $Z_{D_4}(t_1, t_2, t_3, t_4) = \frac{1}{8}((t_1)^4 + (t_2)^2 + 2t_4 + 2(t_2)^2 + 2(t_1)^2 t_2)$.

Izrek 5.13 (Ciklični indeks C_n)**.**

$$Z_{C_n}(t_1, \ldots, t_n) = \frac{1}{n} \sum_{d|n} \phi(d) \cdot (t_{\frac{n}{d}})^d$$

Izrek 5.14 (Ciklični indeks D_n).

$$Z_{D_n} = \frac{1}{2} Z_{C_n} + \begin{cases} \frac{1}{2} t_1 t_2^{\frac{n-1}{2}} & : n \text{ lih} \\ \frac{1}{4} t_2^{\frac{n}{2}} + \frac{1}{4} t_1^2 t_2^{\frac{n}{2}-1} & : n \text{ sod} \end{cases}$$

Opomba (Formula za Eulerjevo funkcijo).

$$\phi(n) = n \prod_{\substack{p|n \\ p \in \mathbb{P}}} (1 - \frac{1}{p})$$

Dokaz. Ciklična grupa je sestavljena iz dolgega cikla in vseh njegovih potenc. $C_n = \{(1\ \dots\ n)^i : 0 \leqslant i \leqslant n-1\}$. Kakšnega tipa je dolg cikel na neko potenco?

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

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

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

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

Opazimo, da velja

$$d|n \implies (1\ 2\ \dots\ n)^d = (1\ \ (d{+}1)\ \ (2d{+}1)\ \ \dots)(2\ \ (d{+}2)\ \ (2d{+}2)\ \ \dots)\cdots$$

Kar pomeni, da je $(1\ 2\ \dots\ n)^d$ produkt d ciklov dolžine $\frac{n}{d}$. Hkrati, če $d \perp n$, je $(1\ 2\ \dots\ n)^d$ en sam cikel dolžine d.

Vzemimo $d = \gcd(n, i)$, $n = d \cdot n'$, $i = d \cdot i'$. Vemo, da $\gcd(n', i') = 1$. Po prejšnjih ugotovitvah velja

$$(1\ 2\ \dots\ n)^i = ((1\ 2\ \dots\ n)^d)^{i'}$$

Ker je $(1\ 2\ \dots\ n)^d$ produkt d ciklov dolžine n' in ker sta si n' in i' tuji, je rezultat še vedno produkt d ciklov dolžine $n' = \frac{n}{d}$. Doprinos k cikličnemu indeksu bo $(t_{\frac{n}{d}})^d$. Kolikokrat pa dobimo ta člen? Tolikokrat, kolikor je i-jev, da je $\gcd(n, i) = d$. To nam pove Eulerjeva funkcija $\phi(\frac{n}{d})$. ∎

Opomba. d lahko zamenjamo z $\frac{n}{d}$. Dobimo popolnoma ekvivalentno formulo

$$Z_{C_n}(t_1, \dots, t_n) = \frac{1}{n} \sum_{d|n} \phi(d) \cdot (t_d)^{\frac{n}{d}}$$

Dokaz. Še za D_n.

$$Z_{D_n} = \frac{1}{2} Z_{C_n} + \begin{cases} \frac{1}{2} t_1 t_2^{\frac{n-1}{2}} & : n \text{ lih} \\ \frac{1}{4} t_2^{\frac{n}{2}} + \frac{1}{4} t_1^2 t_2^{\frac{n}{2}-1} & : n \text{ sod} \end{cases}$$

Prvi del so rotacije, ki jih je enako kot pri C_n (deliti moramo z $\frac{1}{2}$, ker ima D_n dvakrat več elementov; na začetku delimo z $2n$ namesto z n). Prišteti moramo le še zrcaljenja.

Če je n lih, so vsa zrcaljenja istega tipa. Takih zrcaljenj je n. Ko delimo s številom elemenotov ($2n$), je to $\frac{1}{2}$. Doprinos od enega zrcaljenja je 1 negibna točka in $\frac{n-1}{2}$ parov točk, ki se izmenjajo.

Če je n sod, ločimo na $\frac{n}{2}$ zrcaljenj prek točke in $\frac{n}{2}$ zrcaljenj prek stranice. Spet delimo še z $2n$, ostane $\frac{1}{4}$. Pri zrcaljenju čez simetralo stranic dobimo $\frac{n}{2}$ 2-ciklov. Pri zrcaljenju čez točki imamo 2 negibni točki, nato pa ostalih $n-2$ oglišč razdelimo v pare. ■

5.4 Število neekvialentnih barvanj

V tem razdelku bomo ugotovili pravo uporabnost Burnsidove leme in cikličnega indeksa.

Definicija 5.15 (Barvanje)**.** Če je R množica barv, je barvanje $b \in R$ preslikava iz množice korald v množico barv $b : X \to R$. R^X je tedaj množica barvanj.

Namesto da permutiramo koralde, lahko G razumemo tudi kot grupo permutacij barvanj (podgrupo S_{R^X}). Ker je g permutacija korald, moramo posebej definirati, kako uporabimo $g \in G$ na barvnju $b \in R^X$.

Definicija 5.16 (Permutacija barvanja)**.** $g \cdot b(x) := b(g^{-1} \cdot x)$

S tem smo dobili izomorfno permutacijsko grupo. Ne bom bolj natančno povedal, kaj s tem mislim.

Nas zanima število neekvivalentnih barvanj naše ogrlice. To je ravno število orbit naše grupe permutacij barvanj ($G = C_n$ za število barvanj ogrlic, $G = D_n$ za število barvanj zapestnic). Po Burnsidovi lemi moramo izračunati povprečno število negibnih točk.

Primer. $n = 6$, $r = 2$, g je rotacija za 120°. Koliko je negibnih točk za barvanje? Pozor: za permutacijo korald pri taki rotaciji nimamo negibnih točk. Mi štejemo negibne točke barvanj. Take negibne točke so: barvanje, kjer so vse koralde bele/črne in barvanje kjer je vsaka druga koralda bela/črna. Imamo torej 4 negibne točke.

Primer. Če bi v prejšnjem primeru vzeli rotacijo za $60°$, bi imeli 2 negibni točki. Če bi vzeli rotacijo za $180°$, bi imeli 8 negibnih točk.

V splošnem: iščemo permutacij barvanj, kjer je $b = g \cdot b$, oziroma $g \cdot b(x) = b(g^{-1} \cdot x) = b(x)$ za vsak $x \in X$. Drugače rečeno, iščemo število g-jev, kjer sta x in $g^{-1} \cdot x$ vedno iste barve. Za vsak tak g velja, da so tudi $gx, g^2x, g^3x, \ldots$ iste barve.

Ugotovimo, da je edina zahteva, da mora biti vsak cikel g v celoti iste barve. Torej je število negibnih barvanj enako $r^{c(g)}$, kjer je $c(g)$ število ciklov v g, oziroma $c(g) = \sum\limits_i \alpha_i(g)$.

Izrek 5.17 (Pólyev izrek)**.** Število neekvivalentnih barvanj je enako

$$\frac{1}{|G|} \sum_{g \in G} r^{c(g)} = Z_g(r, \ldots, r)$$

Primer. Število ogrlic z n koraldami in r barvami je $\frac{1}{n} \sum_{d|n} \phi(d) \cdot r^{\frac{n}{d}}$.

Primer. Število zapestnic z n koraldami in r barvami je

$$\frac{1}{2n} \sum_{d|n} \phi\Big(\frac{n}{d}\Big) r^d + \begin{cases} \frac{1}{2} r^{\frac{n+1}{2}}; n \text{ lih} \\ \frac{1}{4} r^{\frac{n}{2}} + \frac{1}{4} r^{\frac{n}{2}+1}; n \text{ sod} \end{cases}$$

Primer. Na koliko načinov lahko pobarvamo oglišča tetraedra z r (različnimi) barvami? Izračunajmo ciklični indeks grupe rotacij tetraedra.

$$\underset{\substack{\uparrow \\ \text{grupa rotacij tetraedra}}}{Z_G}(t_1, t_2, t_3, t_4) = \frac{1}{12}(t_1^4 + 8t_1t_3 + 3t_2^2)$$

nato le še vstavimo $t_1 = t_2 = t_3 = t_4 = r$.

Primer 5.18. Naj bo $G = S_n$. Barvanji sta v tem primeru ekvivalentni natanko tedaj, ko imata enako število korald iste barve. Število možnih barvanj torej dobimo kot šibke kompozicije n (št. korald) z r (št. barv) členi.

$$\binom{n+r-1}{r-1}$$

Po drugi strani bi lahko to zapisali po Pólyevem izreku.

$$\frac{1}{n!}\sum_{\pi\in S_n} r^{c(\pi)} = \frac{1}{n!}\sum_k c(n,k)r^k$$

Tukaj smo uporabili razmislek, da permutacija s k cikli doprinese člen r^k, pojavi pa se ravno $c(n,k)$-krat (definicija Stirlingovih števil prve vrste).

Če enačimo rezultata obeh metod, se nam nekaj členov krajša.

$$\binom{n+r-1}{r-1} = \frac{(n+r-1)!}{(r-1)!n!} = \frac{(n+r-1)\cdots r\cdot(r-1)\cdots 1}{((r-1)\cdot(r-2)\cdots 2\cdot 1)\cdot n!} = r^{\overline{n}}\cdot\frac{1}{n!}$$

$$\implies \sum_k c(n,k)r^k = r^{\overline{n}}$$

Opomba. To formulo smo že dokazali z indukcijo - glej rekurzivna zveza za $c(n,k)$ (3.3).

Recimo, da nas zanima, koliko je možnih barvanj zapestnic s točno določenim številom korald za vsako barvo. Imamo srečo, da so to pred nami želeli tudi nekateri pametni matematiki.

Primer. Enumerator barvanj

$$u_1^4 + u_1^3u_2 + 2u_1^2u_2^2 + u_1u_2^3 + u_2^4$$

Definicija 5.19 (Enumerator barvanj)**.**

$$E_G(u_1,\ldots,u_r) = \sum_{Gb\in R^x/G} \Pi_{i=1}^r u_i^{|b^{-1}(i)|}$$

Opomba. R^x/G je množica vseh neekvivalentnih barvanj.

Izrek 5.20 (Posplošitev Pólyevega izreka)**.**

$$E_G(u_1,\ldots,u_r) = Z_G(u_1+\cdots+u_r, u_1^2+\cdots+u_r^2, u_1^3+\cdots+u_r^3,\ldots,u_1^n+\cdots+u_r^n)$$

Dokaz. Brez dokaza. Namig: Burnsidova lema na množici barvanj s fiksnimi $|b^{-1}(i)|$. ∎

Opomba. Če v posplošitev Pólyevega izreka vstavimo $u_i = 1$, dobimo Pólyev izrek.

Primer. Poglejmo si ogrlico s 4 koraldami in 2 barvama. Grupa bo torej $G = C_4$.

$$Z_{C_4}(t_1, t_2, t_3, t_4) = \frac{1}{4}(t_1^4 + t_2^2 + 2t_4)$$

$$Z_{C_4}(u_1 + u_2, u_1^2 + u_2^2, u_1^3 + u_2^3, u_1^4 + u_2^4) = u_1^4 + u_1^3 u_2 + 2u_1^2 u_2^2 + u_1 u_2^3 + u_2^4$$

Koeficient pred $u_1^3 u_2$ je 1, kar pomeni da imamo 1 neekvivalentno barvanje ogrlice s 3 belimi in 1 črno koraldo. Koeficient pred $u_1^2 u_2^2$ je 2, kar pomeni da imamo 2 neekvivalentni barvanji ogrlice z 2 belima in 2 črnima koraldama.

Opomba. Polinom, ki ga dobimo s tem izrekom bo očitno vedno simetričen (koeficient pred $u_1^n \cdots u_r^m$ bo enak ne glede na to, kako permutiramo eksponente).

Primer. Koliko je neekvivalentnih zapestnic s 6 koraldami, če imamo 1 črno, 3 bele in 2 rdeči koraldi? Parametri so torej $n = 6$, $r = 3$, $G = D_6$.

$$Z_{D_6}(t_1, \ldots, t_6) = \frac{1}{12}(t_1^6 + t_2^3 + 2t_3^2 + 2t_6) + \frac{1}{4}(t_2^3 + t_1^2 t_2^2)$$

$$[u_1 u_2^3 u_3^2] \left(Z_{D_6}(u_1 + u_2 + u_3, \ldots, u_1^6 + u_2^6 + u_3^6) \right) = 6$$

Izračunajte sami, pomagajte si z multinomskim koeficientom, da ne računate vseh potenc.

6 Trije klasični izreki iz teorije delno urejenih množic

Definicija 6.1 (Delno urejena množica)**.** Množica opremljena z relacijo delne urejenosti $(P, \leqslant)$.

Opomba. Izraz "delno urejena množica" bomo krajšali z "DUM", ampak izgovorimo s celim izrazom. V angleščini delno urejenim množicam pravimo "partially ordered sets", krajšamo "poset" in okrajšano tudi izgovarjamo.

Definicija 6.2 (Relacija delne urejenosti)**.** Relacija, za katero veljajo naslednje lastnosti

- refleksivnost $x \leqslant x$
- antisimetričnost $x \leqslant y \wedge y \leqslant x \implies x = y$
- tranzitivnost $x \leqslant y \wedge y \leqslant z \implies x \leqslant z$

Primer. Označujemo $\underline{n} \coloneqq ([n], \leqslant)$, kjer je $\leqslant$ običajna relacija manjše ali enako.

Primer. Boolova algebra $B_n \coloneqq (2^{[n]}, \subseteq)$. To je algebra za operaciji $\cup$, $\cap$. V računalništvu pogosto srečamo dvoelementno Boolovo algebro $B_1 = \{0, 1\}$.

Primer. $D_n \coloneqq (\{\text{delitelji } n\}, |)$. Za množico bi lahko vzeli tudi $\mathbb{N}_{>0}$

Definicija 6.3 (Stroga neenakost)**.**

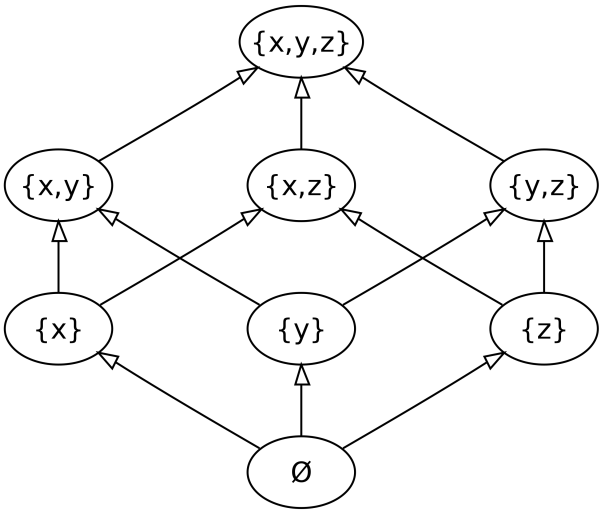
$$x < y \iff x \leqslant y \wedge x \neq y$$

Definicija 6.4 (Predhodnik)**.** x je predhodnik y, če sta v relaciji $\lessdot$

$$x \lessdot y \iff x < y \wedge \nexists z : x < z < y$$

Primer. $B_3 = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$. $A \in B_3$ je predhodnik elementov $A \cup \{i\}$ za vsak $i \notin A$.

Definicija 6.5 (Hassejev diagram)**.** Graf (V, E), kjer so vozlišča $V = P$ (elementi naše množice), robovi pa $E = \{(x, y); x \lessdot y \vee y \lessdot x\}$. Običajno narišemo tako, da je y nad x, če je $x < y$.

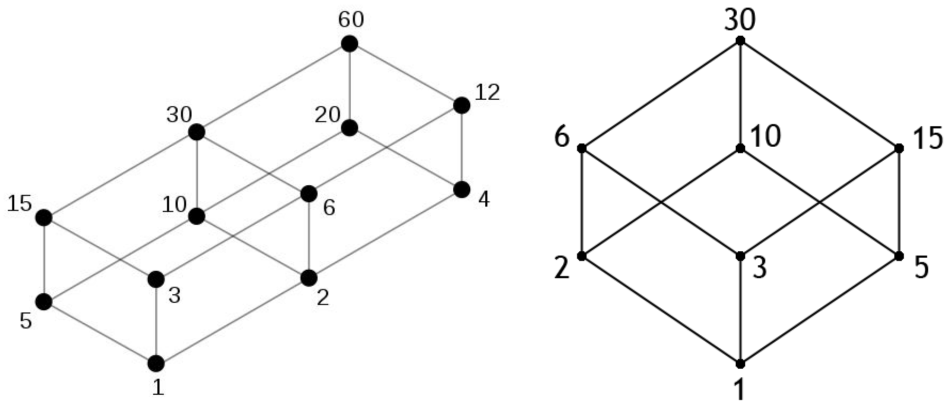


Slika 5: Hassejev diagram B_3

Trditev 6.6. Hassejev diagram B_n je hiperkocka Q_n.

Trditev 6.7. Če je n produkt različnih praštevil, je Hassejev diagram D_n hiperkocka.

Definicija 6.8 (Izomorfnost)**.** Delno urejeni množici P in Q sta izomorfni, če obstaja bijekcija $\phi : P \to Q$, da velja $a \leqslant b \iff \phi(a) \leqslant \phi(b)$.



Slika 6: Hassejeva diagrama za D_{30} in D_{60}

Definicija 6.9 (Kartezični produkt)**.** $P \times Q$ je delno urejena množica z elementi (x, y), $x \in P, y \in Q$, in relacijo $(x, y) \leqslant (x', y') \iff x \leqslant x' \land y \leqslant y'$.

Dokaz. Bralec lahko za zabavo dokaže, da je kartezični produkt delno urejenih množic tudi delno urejena množica. ■

Primer. $\underline{2} \times \underline{2} \times \cdots \times \underline{2} \cong B_n$. Izomorfizem dokažemo z $\phi(A) := (\varepsilon_1, \ldots, \varepsilon_n)$.

Primer. $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. Opazimo, da je D_n izomorfen $[0, \alpha_1] \times [0, \alpha_2] \cdots \times [0, \alpha_k]$, kjer smo z $[0, \alpha_i]$ označili $\underline{\alpha_i} \cup \{0\}$.

Iz zgornjih dveh primerov je razvidno, da če je n produkt različnih praštevil, je D_n izomorfen B_k, kjer je k moč faktorizacije n. Iz tega sledi zgornja trditev o Hassejevih diagramih D_n (6.7).

Definicija 6.10 (Veriga)**.** Naj bo $(P, \leqslant)$ delno urejena množica. Tedaj je $(C \subseteq P, \leqslant)$ veriga, če velja $\forall x, y \in C : x \leqslant y \lor y \leqslant x$ (vsi elementi so med seboj primerljivi).

Primer. $\{\emptyset, \{1, 3\}, \{1, 3, 4\}\} \subseteq B_4$ je veriga.

Definicija 6.11 (Antiveriga)**.** Naj bo $(P, \leqslant)$ delno urejena množica. Tedaj je $(C \subseteq P, \leqslant)$ antiveriga, če velja $\forall x, y \in C : \neg(x \leqslant y \lor y \leqslant x)$ (nobena dva elementa nista primerljiva).

Primer. $\{\{1, 3\}, \{2, 4\}, \{1, 2\}\} \subseteq B_5$ je antiveriga.

Definicija 6.12 (Višina delno urejene množice)**.** Velikost najdaljše verige.

Definicija 6.13 (Širina delno urejene množice)**.** Velikost najdaljše antiverige.

Primer.

množica	višina	širina
$\underline{n}$	n	1
B_n	$n+1$	$\binom{n}{\lfloor \frac{n}{2} \rfloor}*$
D_n	$\alpha_1 + \cdots + \alpha_k + 1$	?

Opomba. * To je malo težje dokazati, ampak bomo pokazali kasneje (Spernerjev izrek).

Definicija 6.14 (Maksimalni element)**.** Tak x, da velja $\nexists y : x \leqslant y$.

Definicija 6.15 (Največji element)**.** Tak x, da velja $\forall y : x \geqslant y$.

Opomba. Če je x največji, potem je x maksimalen. Obratno ne velja.

Opomba. Če je P končna, obstaja maksimalen element.

Opomba. Obstaja največ en največji element.

Izrek 6.16 (Minskyjev izrek)**.** Naj bo $(P, \leqslant)$ končna delno urejena množica, M dolžina najdaljše verige (višina), m pa najmanjše število antiverig, s katerimi lahko pokrijemo P. Tedaj velja $M = m$.

Dokaz. Očitno velja $M \leqslant m$, saj bo vsak element najdaljše verige moral imeti svojo antiverigo. $m \leqslant M$ bomo pokazali z indukcijo po moči P.
Baza indukcije: $|P| = 1$. $m = M = 1$.
Indukcijski korak: definirajmo $A \coloneqq \{\text{maksimalni elementi v } P\}$. Vemo, da je višina $P \setminus A$ je zagotovo $M - 1$ (vsaka najdaljša veriga ima natanko en maksimalen element). Po indukcijski predpostavki jo zato lahko pokrijemo z $M-1$ antiverigami. Ker je A antiveriga, lahko P pokrijemo z M antiverigami. ∎

Opomba. Ta dokaz služi tudi kot algoritem za iskanje antiverig.

6.1 Dilworthov izrek

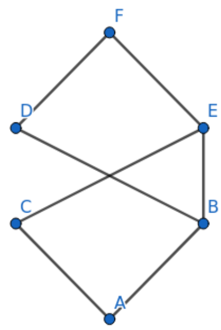
Izrek 6.17 (Dilworthov izrek)**.** Naj bo $(P, \leqslant)$ končna delno urejena množica, M dolžina najdaljše antiverige (širina), m pa najmanjše število verig, s katerimi lahko pokrijemo P. Tedaj velja $M = m$.

Dokaz. Podobno kot pri Minskyjevem izreku, opazimo da $M \leqslant m$, ker mora vsak element najdaljše antiverige imeti svojo verigo v pokritju. $m \leqslant M$ bomo pokazali z indukcijo po moči P.

Baza indukcije: $|P| = 1$. $m = M = 1$.

Indukcijski korak: definirajmo $C :=$ katerakoli najdaljša veriga v P. Problem nastane (za razliko od dokaza Minskyjevega), ker $P \setminus C$ nima nujno manjše širine kot P.

Če je se širina zmanjšala, lahko (enako kot pri Minskyjevem) $P \setminus C$ pokrijemo z $\leqslant M - 1$ verigami, torej lahko P pokrijemo z $\leqslant M$ verigami.



Slika 7: Primer DUM, kjer se širina ne zmanjša, če odstranimo najdaljšo verigo $\{A, B, E, F\}$ (najdaljša antiveriga je potem $\{C, D\}$).

Če se širina ni zmanjšala, izberimo neko najdaljšo antiverigo $A = \{a_1, \ldots, a_n\}$ iz $P \setminus C$. Definirajmo

- $S^+ := \{x \in P; \exists i : x \geqslant a_i\}$
- $S^- := \{x \in P; \exists i : x \leqslant a_i\}$

Pokažimo nekaj lastnosti glede S^+ in S^-.

1. $S^+ \cap S^- = A$

   Dokaz. A je očitno vsebovan v obeh množicah zaradi refleksivnosti ($\forall a \in A \exists i : a \leqslant a_i$). Če je $x \in S^+ \cap S^-$, potem $a_i \leqslant x \leqslant a_j$, zaradi tranzitivnosti pa $a_i \leqslant a_j$. Ker sta a_i in a_j iz iste antiverige, mora veljati $i = j$, kar pomeni da je $x = a_i$ in zato $x \in A$. ■

2. $S^+ \cup S^- = P$

   Dokaz. Očitno je, da je unija vsebovana v P. Če $x \notin S^+$ in $x \notin S^-$, potem $\forall i : x \ngeqslant a_i \wedge x \nleqslant a_i$, kar pomeni da je $A \cup \{x\}$ antiveriga, ki je večja od A, kar je v nasprotju z definicijo A. ■

3. $S^+ \neq P$

   Dokaz. Najmanjši element v C zagotovo ni v S^+; če bi obstajal i, da $x \geqslant a_i$, bi $C \cup \{a_i\}$ bila daljša veriga kot C. Pomembno je opaziti, da $x \neq a_i$, ker je A sestavljena iz elementov $P \setminus C$. ■

4. $S^- \neq P$

   Dokaz. Iz istega razloga kot zgoraj največji element C zagotovo ni v S^-. ■

Z drugimi besedami, S^+ ima širino M, a je njena moč strogo manjša od $|P|$. Po indukcijski predpostavki lahko S^+ pokrijemo z M verigami $C_1^+, \ldots, C_M^+$, S^- pa z $C_1^-, \ldots, C_M^-$. Vsak element A mora imeti svojo verigo C_i^+. Brez škode za splošnost privzemimo $a_i \in C_i^+$ in $a_i \in C_i^-$. Naše pokritje Pja sestavljajo $C_i = C_i^+ \cup C_i^-$. ■

6.2 Spernerjev izrek

Lema 6.18. $\forall k : \binom{n}{k} \leqslant \binom{n}{\lfloor \frac{n}{2} \rfloor}$. Povedano z besedami: trdimo, da je največji binomski koeficient neke vrstice vedno v njeni sredini.

Dokaz. Oglejmo si zaporedna binomska koeficienta in izračunajmo kriterij, kdaj je naslednji večji od prejšnjega.

$$\binom{n}{k} \leqslant \binom{n}{k+1}$$

$$\frac{\binom{n}{k}}{\binom{n}{k+1}} \leqslant 1$$

$$\frac{n!(k+1)!(n-k-1)!}{k!(n-k)!n!} \leqslant 1$$

$$\frac{k+1}{n-k} \leqslant 1$$

$$k+1 \leqslant n-k$$

$$2k+1 \leqslant n$$

$$k \leqslant \frac{n-1}{2}$$

■

Opomba. Zaporedje, za katerega velja $a_0 \leqslant a_1 \leqslant \cdots \leqslant a_k \geqslant a_{k+1} \geqslant \cdots$ imenujemo unimodalno.

Izrek 6.19 (Spernerjev)**.** Širina B_n je $\binom{n}{\lfloor \frac{n}{2} \rfloor}$.

Dokaz. Če vzamemo $A = \binom{[n]}{\lfloor \frac{n}{2} \rfloor}$ je to ravno antiveriga velikosti $\binom{n}{\lfloor \frac{n}{2} \rfloor}$. S tem smo fiksirali minimalno vrednost širine. Dokažimo, da ne obstaja daljša antiveriga.

Naj bo A poljubna antiveriga v B_n. Naj bo a_i število elementov A, ki so i-elementne množice. Očitno je $a_0 + a_1 + \cdots + a_n = |A|$.

Preštejmo maksimalne verige v B_n

- Vse: $n!$

  Dokaz. Verigo $\emptyset \subseteq \{i_1\} \subseteq \{i_1, i_2\} \subseteq \cdots \subseteq [n]$ dobimo tako, da izberemo nek vrstni red dodajanja elementov proti $[n]$. ■

- Tiste, ki vsebujejo izbrano podmnožico $S \in B_n$ velikosti k: $k!(n-k)!$

  Dokaz. Dobimo jih tako, da konstruiramo verigo do S ($k!$ načinov), nato pa dodajamo še ostalih $n-k$ elementov do $[n]$. ■

- Tiste, ki vsebujejo katerikoli element iz A: $\sum_{k=0}^{n} a_k k!(n-k)!$

  Dokaz. Vsak element A ima lahko med 0 in n elementov. Če za vsako od teh števil dodamo seštejemo število verig, ki vsebuje ta element (teh je dokazano $k!(n-k)!$), dobimo ravno naš rezultat. Nobene verige nismo šteli dvakrat, ker vsaka od naših verig vsebuje natanko en element A-ja (A je antiveriga, zato ne sme obstajati veriga med dvema elementoma iz A). ■

Zaključimo lahko, da je $\sum_{k=0}^{n} a_k k!(n-k)! \leqslant n!$, saj je množica maksimalnih verig, ki vsebujejo elemente iz A pomnožica vseh maksimalnih verig. Če delimo z $n!$, dobimo

$$\sum_{k=0}^{n} \frac{a_k}{\binom{n}{k}} \leqslant 1$$

$$1 \geq \sum_{k=0}^{n} \frac{a_k}{\binom{n}{k}} \geq \sum_{k=0}^{n} \frac{a_k}{\binom{n}{\lfloor \frac{n}{2} \rfloor}} = \frac{1}{\binom{n}{\lfloor \frac{n}{2} \rfloor}} \sum_{k=0}^{n} a_k$$

$$\binom{n}{\lfloor \frac{n}{2} \rfloor} \geq \sum_{k=0}^{n} a_k$$

$$\binom{n}{\lfloor \frac{n}{2} \rfloor} \geq |A|$$

■

Posledica 6.20 (Dilworth-Sperner)**.** B_n lahko pokrijemo z $\binom{n}{\lfloor \frac{n}{2} \rfloor}$ verigami.

6.3 Hallov izrek

Definicija 6.21 (Prirejanje)**.** Naj bo $G = (V, E)$ graf. $M \subseteq E$ je prirejanje, če velja $e \cap f = \emptyset$ za vsaka $e, f \in M$.

Če pobarvamo povezave iz M z rdečo barvo, potem nobeno vozlišče iz G nima več kot ene rdeče povezave.

Definicija 6.22 (Popolno prirejanje)**.** Naj bo M prirejanje grafa G. M je popolno prirejanje, če velja $\forall v \in V : \exists e \in M : v \in e$.

Opomba. Angleško: "matching" in "perfect matching".

Opomba. Če ima G popolno prirejanje, je $|V|$ sodo.

Definicija 6.23 (Popolno prirejanje iz X v Y)**.** Naj bo G dvodelen graf na particiji X in Y. Prirejanje M je popolno prirejanje iz X v Y če velja $\forall x \in X : \exists e \in M : x \in e$.

Opomba. Če obstaja popolno prirejanje iz X v Y, je $|X| \leqslant |Y|$. Popolno prirejanje namreč deluje kot injekcija.

Definicija 6.24 (Soseščina A)**.** $N(A) = \{v \in V : \exists u \in A : u \sim v\}$

Opomba 6.25. Če obstaja popolno prirejanje iz X v Y, je $|A| \leqslant |N(A)|$. Popolno prirejanje je v tem primeru injekcija $A \to N(A)$.

Definicija 6.26 (Alternirajoča pot)**.** Pot, v kateri se izmenjujejo rdeče in črne povezave (tj. povezave, ki so element prirejanja in povezave, ki niso).

Izrek 6.27 (Hall)**.** Naj bo G dvodelen graf na particiji X in Y. Tedaj obstaja popolno prirejanje iz X v Y natanko tedaj, ko $|A| \leqslant |N(A)|$ za vsak $A \subseteq X$.

Opomba. Če predpostavimo Dilworthov izrek, je Hallov izrek zelo lahko dokazati. Velja tudi obratno.

Opomba. Hallov izrek nam poda ekvivalenco oblike $\exists \iff \forall$. Tako ekvivalenco imenujemo dobra karakterizacija. Kadar imamo tako ekvivalenco, lahko dokažemo ali ovržemo trditev na levi ali desni strani s tem da dokažemo obstoj največ enega objekta.

Dokaz. Dokaz v desno smo že razmislili (6.25). Začnimo s poljubnim prirejanjem in predpostavimo $|A| \leqslant |N(A)|$. Če je to prirejanje popolno iz X v Y, potem smo končali. Sicer poskusimo to prirejanje povečati. To bomo lahko ponavljali, dokler ne pridemo do popolnega prirejanja.

Po predpostavi (naše prirejanje ni popolno) obstaja neko vozlišče $a \in X$, ki ni v nobeni povezavi v prirejanju (ni element rdeče povezave). Definirajmo
$A \coloneqq \{x \in X; \exists \text{ alternirajoča pot od } a \text{ do } x\}$ in
$B \coloneqq \{y \in Y; \exists \text{ alternirajoča pot od } a \text{ do } y\}$.

Zagotovo velja $a \in A$. Pokažimo, da je $N(A) \subseteq B$.

$$y \in N(A) \implies \exists x \in A : x \sim y \implies \exists \text{ alternirajoča pot od } a \text{ do } x, x \sim y$$

Ker smo v dvodelnem grafu in ker a nima rdečih povezav, bo zadnja povezava v alternirajoči poti do x rdeča (v Y vedno pridemo po črni in v X vedno pridemo po rdeči). Če je povezava xy črna, potem jo lahko dodamo k alternirajoči poti in dobimo alternirajočo pot od a do y, torej je $y \in B$. Če pa je xy rdeča, mora biti y predzadnje vozlišče naše poti od a do x, ker ima x lahko največ eno rdečo povezavo (tisto, po kateri smo prišli do njega). Torej je $y \in B$.

Po predpostavki in pravkaršnji ugotovitvi, imamo

$$|A| \leqslant |N(A)| \leqslant |B|$$

Iz A gre $|A| - 1$ rdečih povezav (vsi elementi razen a morajo imeti natanko eno rdečo povezavo, ker so del alternirajoče poti). To pomeni, da v B obstaja vozlišče b, ki nima nobene rdeče povezave (ker je $|A| \leqslant |B|$). Če vsem povezavam v poti od a do b zamenjamo barvo, ne bomo pokvarili prirejanja; vsako vozlišče bo imelo še vedno največ eno rdečo povezavo. Ker se alternirajoča pot od a do b začne in konča s črno, smo s to inverzijo hkrati povečali število rdečih povezav za 1.

Postopek ponavljamo dokler ne dosežemo popolnega prirejanja. ■

Opomba. To je algoritem, ki bodisi poišče popolno prirejanje, bodisi dokaže, da le-to ne more obstajati (če slučajno naletimo na primer, ko $|A| > |N(A)|$).

Posledica 6.28. Naj bo G dvodelni graf na X in Y. Tedaj velja

$$\forall x \in X : \forall y \in Y : \deg(x) \geqslant \deg(y) \implies \exists \text{ popolno prirejanje } X \to Y$$

Dokaz. Želimo pokazati, da je $|A| \leqslant |N(A)|$. Označimo število povezav med A in B kot $e(A,B)$ in $B \coloneqq N(A)$. Naj bo d neko število, ki je med $\deg(x)$ in $\deg(y)$ za vsaka x in y (d obstaja po naši predpostavki).

$$d \cdot |B| \geqslant \sum_{y \in B} \deg(y) \geqslant e(A,B) = \sum_{x \in A} \deg(x) \geqslant d \cdot |A|$$
$$\implies |A| \leqslant |B|$$

Po Hallovem izreku je to vse, kar moramo pokazati. ■

Posledica 6.29. Naj bo G biregularen (stopnja vsakega vozlišča na levi/desni strani je enaka) dvodelen graf. Tedaj obstaja popolno prirejanje iz X v Y ali iz Y v X.

Dokaz.

$$|E| = \sum_{x \in X} \deg(x) = r \cdot |X|$$
$$|E| = \sum_{y \in Y} \deg(y) = s \cdot |Y|$$
$$|X| \leqslant |Y| \iff r \geqslant s \iff \exists \text{ popolno prirejanje } X \to Y$$
$$|X| \geqslant |Y| \iff r \leqslant s \iff \exists \text{ popolno prirejanje } Y \to X$$

■