

# Kombinatorika - zapsiski s predavanj prof. Konvalinka

Domen Vogrin      Tomaž Poljanšek      Yon Ploj

jesen/zima 2021

## Kazalo

<b>1</b>	<b>Osnovni principi kombinatorike</b>	<b>1</b>
1.1	Funkcije in štetje . . . . .	1
1.2	Osnovna načela . . . . .	1
1.3	Permutacije . . . . .	3
<b>2</b>	<b>Podmnožice in načrti</b>	<b>4</b>
2.1	Binomski koeficienti . . . . .	4
2.2	Pascalov trikotnik . . . . .	7
2.3	Binomski izrek . . . . .	7
2.4	Izbori . . . . .	8
2.5	Kompozicije . . . . .	9
2.6	Načelo vključitev in izključitev (NVI) . . . . .	10
2.7	Eulerjeva funkcija $\phi$ . . . . .	12
2.8	Multinomski koeficienti . . . . .	13
2.9	Načrti in t-načrti . . . . .	14
<b>3</b>	<b>Permutacije, razdelitve, razčlenitve</b>	<b>18</b>
3.1	Stirlingova števila prve vrste . . . . .	18
3.2	Stirlingova števila druge vrste . . . . .	20
3.3	Lahova števila . . . . .	22
3.4	Razčlenitve naravnih števil in Eulerjev petkotniški izrek . . . . .	24
3.5	Dvanajstera pot . . . . .	29
<b>4</b>	<b>Rodovne funkcije</b>	<b>30</b>
4.1	Uvod . . . . .	30

4.2	Formalne potenčne vrste . . . . .	32
4.3	Uporaba rodovnih funkcij pri reševanju rekurzivnih enačb . . .	36
4.3.1	Fibonaccijeva rodovna funkcija . . . . .	37
4.4	Binomska vrsta . . . . .	40
4.4.1	Catalanova števila . . . . .	42
4.5	Rodovne funkcije razčlenitev . . . . .	44
4.6	Uporaba rodovnih funkcij . . . . .	46
<b>5</b>	<b>Pólyeva teorija</b>	<b>47</b>
5.1	Orbite, stabilizatorji in negibne točke . . . . .	47
5.2	Burnsidova lema . . . . .	50
5.3	Ciklični indeks . . . . .	52

# 1 Osnovni principi kombinatorike

## 1.1 Funkcije in štetje

**Definicija 1.1** (Funkcija).

- injektivna ( $y$  je slika največ enega  $x$ ) / ( $x_1 \neq x_2 \rightarrow f(x_1) \neq f(x_2)$ )
- 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)

$$\exists \text{ injekcija } f : X \rightarrow Y \implies |X| \leq |Y|$$

$$\exists \text{ surjekcija } f : X \rightarrow Y \implies |X| \geq |Y|$$

$$\exists \text{ bijekcija } f : X \rightarrow Y \implies |X| = |Y|$$

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

$$\mathbb{N} := \{0, 1, 2, \dots\}$$

$$[n] := \{1, 2, \dots, n\}, \quad |[n]| = n$$

$$2^X := \{A \subseteq X\} (= P(X))$$

$$Y^X := \{f : X \rightarrow Y\}$$

**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).

$$\exists f : X \rightarrow Y \implies |X| \leq |Y|$$

Ekvivalentno:

$$|X| > |Y| \implies \neg \exists \text{ inj. } f : X \rightarrow Y$$

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 in produkta).

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

**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 neodvisni izbiri, število možnosti za eno in drugo zmnožimo

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

*Dokaz.* (Formalen)

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

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

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

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

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

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

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

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

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

■

*Dokaz.* (Intuitiven)

Za vsakega od  $n$  elementov imamo dve izbiri (damo / ne damo v podmnožico).

Izbire so neodvisne, torej imamo  $2 \cdot 2 \cdot \dots \cdot 2 = 2^n$  izbir. ■

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

*Dokaz.* (Formalen)

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

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

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

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

$$f(x_i) = y_i$$

■

*Dokaz.* (Intuitiven)

Za vsak element iz  $X$  imamo  $|Y|$  izbir. Izbire so neodvisne, torej imamo  $|Y| \cdot |Y| \cdot \dots \cdot |Y| = |Y|^{|X|}$  izbir. ■

**Trditev 1.9.** Število injektivnih preslikav v  $Y^X$  je

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

*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,  $id = (1\ 2\ \dots\ n)$  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  $\pi \in S_n$ ,  $i \in [n]$

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

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

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

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

**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.**

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

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

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

**Trditev 2.8.**

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

*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

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

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)

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

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

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

■

*Dokaz.* (3. način)

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

■



## 2.2 Pascalov trikotnik

$$\begin{array}{cccccccc}
n=0 & & & & & & & 1 \\
n=1 & & & & & 1 & 1 & \\
n=2 & & & & 1 & 2 & 1 & \\
n=3 & & & 1 & 3 & 3 & 1 & \\
n=4 & & 1 & 4 & 6 & 4 & 1 & \\
n=5 & 1 & 5 & 10 & 10 & 5 & 1 & \\
n=6 & 1 & 6 & 15 & 20 & 15 & 6 & 1 \\
\hline
& 0 & 1 & 2 & 3 & 4 & 5 & 6
\end{array}$$

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.

## 2.3 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,  $n = 0$  :  $1 = \begin{pmatrix} 0 \\ 0 \end{pmatrix} a^0 b^0 = 1$ . OK

Indukcijski korak,  $n - 1 \Rightarrow n$ :

$$\begin{aligned}
 (a+b)^n &= (a+b)^{n-1}(a+b) = \left(\sum_{k=0}^{n-1} \binom{n-1}{k} a^{n-1-k} b^k\right)(a+b) = \\
 &= \sum_{k=0}^{n-1} \binom{n-1}{k} a^{n-k} b^k + \sum_{k=0}^{n-1} \binom{n-1}{k} a^{n-1-k} b^{k+1} = \\
 &\stackrel{k'=k+1}{=} \sum_{k=0}^{n-1} \binom{n-1}{k} a^{n-k} b^k + \sum_{k'=1}^{n-1} \binom{n-1}{k'-1} a^{n-k'} b^{k'} = \\
 &\stackrel{k'=k}{=} \sum_{k=0}^n \binom{n-1}{k} a^{n-k} b^k + \sum_{k=0}^n \binom{n-1}{k-1} a^{n-k} b^k = \\
 &= \sum_{k=0}^n \left( \binom{n-1}{k} + \binom{n-1}{k-1} \right) a^{n-k} b^k = \\
 &\stackrel{\text{rekurzija}}{=} \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k
 \end{aligned}$$



*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

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

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  $b$ . ■

## 2.4 Izbori

Na voljo imamo  $b$  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.

$$1 \leq i_1 \leq \dots \leq i_k \leq n$$

Želimo prešteti rešitve tega sistema neenačb.

$n = 4, k = 3$

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

Ideja:

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

## 2.5 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

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

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  $n \geq 1$  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).

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

tako da velja

$$\lambda_1 + \dots + \lambda_l = n$$

*Opomba.* Šibkih kompozicij števila  $n$  je  $\infty$ .

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

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

*Dokaz.* (1. način)

Štejemo rešitve  $\lambda_1 + \lambda_2 + \dots + \lambda_k = n$ , zahtevamo  $\lambda_1 \geq 0$ .

$$\mu_i = \lambda_i + 1$$

$$\mu_1 + \dots + \mu_k = n + k, \quad \mu_i \geq 1$$

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

■

*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.

*Opomba.* Kombinacije s ponavljanjem ( $n$  kroglic, izberemo jih  $k$ )

$x_i \dots$  kolikokrat smo izbrali kroglico:

$$x_i \geq 0, \quad i = 1, \dots, n$$

$$x_1 + x_2 + \dots + x_n = k$$

$$\equiv \text{šibke kompozicije } k \text{ z } n \text{ členi} = \binom{k+n-1}{n-1} = \binom{n+k-1}{k} \quad \blacksquare$$

## 2.6 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).

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

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

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

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

**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  $A_\emptyset = A$

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

■

**Lema 2.19.**

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

*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

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

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

*Dokaz.* (NVI)

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

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

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

$k \dots$  doprinos v prvi vrstici

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

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

■

## 2.7 Eulerjeva funkcija $\phi$

**Definicija 2.20** (Eulerjeva funkcija).

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

**Trditev 2.21.**

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

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

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

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

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

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

■

**Izrek 2.22** (Formula za  $\phi$ ).

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

*Dokaz.*

$$A = [n], \quad n = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \quad \alpha_i > 0$$

$$A_i = \{j \in [n] : p_i | j\}$$

$$|A_i| = \frac{n}{p_i}$$

$$|A_i \cap A_j| = \frac{n}{p_i p_j}$$

$$|A_I| = \frac{n}{\prod_{i \in I} p_i}$$

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

$$k = 2$$

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

$$\phi(n) \stackrel{\text{distributivnost}}{=} n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \dots \cdot \left(1 - \frac{1}{p_k}\right)$$

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

■

## 2.8 Multinomski koeficienti

Spomnimo se na binomske koeficiente

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}, \quad 0 \leq k \leq n$$

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.

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

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

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

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

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

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

načinov; najprej smo premešali vse na  $(a_1 + a_2 + \dots + a_n)!$  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).

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

*Dokaz.*

$$(x_1 + x_2 + \dots + x_n) \cdot (x_1 + x_2 + \dots + x_n) \cdot \dots \cdot (x_1 + x_2 + \dots + x_n)$$

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

*Primer.*  $x_1 = x_2 = \dots = x_n$

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

## 2.9 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).  $B = \{B_1, \dots, B_b\}$  je načrt s parametri  $(v, k, \lambda)$ , kadar velja



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

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

	$B_1$	$\dots$	$B_b$
Narišemo tabelo	1		
	$\dots$		
	$v$		

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

Velja še  $b \leq \binom{v}{k}$

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

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

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

### Izrek 2.25.

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

*Dokaz.*

$(\Rightarrow)$  Že dokazano.

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

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

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

To ni nujno načrt.

$\lambda_i \dots$  v koliko blokih je vsebovan  $i$

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

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.

$$\lambda_i = \text{blokov tipa (I) + (II)}$$

$$\lambda_j = \text{blokov tipa (I) + (III)}$$

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  $\lambda_1 = \lambda_2 = \dots = \lambda_6$

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).  $B = \{B_1, \dots, B_b\}$  je  $t$ -načrt s parametri  $(v, k, \lambda_t)$ , kadar velja

- $B_1, \dots, B_b \subseteq [v]$
- $|B_1| = \dots = |B_b| = k$

- vsaka  $t$ -elementna podmnožica  $[v]$  je vsebovana v točno  $\lambda_t$  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!!

Fanova ravnina:

**Izrek 2.27.** Če je  $B$   $t$ -načrt s parametri  $(v, k, \lambda_t)$ , je tudi  $(t - 1)$ -načrt s parametri  $(v, k, \lambda_{t-1})$ . 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  $\lambda_s$  blokih. Narišemo tabelo

	$B_1$	$\cdots$	$j$	$\cdots$	$B_b$
1					
$\vdots$					
$i$			✓		
$\vdots$					
$v$					

$i \notin S$ ,  $S \cup \{i\} \subseteq B_j$ . Skupno je po stolpcih:

- $S \setminus B_j$ : 0 kljukic
  - $S \subseteq B_j$ :  $k - t + 1$  kljukic
- skupaj:  $\lambda_s(k - t + 1)$

in po vrsticah:

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

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

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

■

### 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) · (vsako dobimo  $(n-1)$ -krat))

■

Tabela Stirlingovih števil 1. vrste:

$n \backslash k$	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

Konstruiramo podobno kot Pascalov trikotnik za binomske koeficiente (2.2), samo da uporabimo drugo rekurzivno formulo; najprej damo diagonalne elemente na 1, naddiagonalne na 0, 1. stoplec na 0 (razen prvega elementa, ki je že 1), za ostale pa uporabimo rekurzivno formulo (seštejemo element levo zgoraj in  $(n-1)$  krat zgornji).

**Trditev 3.3** (Rekurzivna zveza).

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

*Dokaz.* Indukcija po  $n$ :

Baza indukcije:  $n = 0 : (1x^0 = x^0)$ . OK.

Indukcijski korak:  $n-1 \implies n$ :

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

■

*Dokaz.* Alternativno, lahko gremo tudi v obratni smeri.

$$x \leftrightarrow -x$$

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

$s(n, k) := (-1)^{n-k} c(n, k)$  predznačeno stirlingovo število prve vrste

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

■

## 3.2 Stirlingova števila druge vrste

**Definicija 3.4** (Razdelitev množice). Razdelitev, razbitje ali particija je  $\{B_1 \cdots B_n\}$ , pri čemer

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

*Primer.*

$$A = [8] : \{\{1, 4, 5\}\{2\}\{3, 6, 7, 8\}\} \equiv 145 - 2 - 3678 \equiv 2 - 415 - 8763$$

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

**Definicija 3.5** (Stirlingovo število druge vrste).  $S(n, k)$  je število razdelitev  $[n]$  z natanko  $k$  bloki.

**Definicija 3.6** (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  $k > n$
- $S(n, k) \leq c(n, k)$

**Trditev 3.7** (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  $\geq 1$ :  $k \cdot S(n-1, k)$  ( $n$  lahko vstavimo v katerega koli izmed  $k$  blokov:  $n$  vstavimo nazaj na  $k$  načinov)

■

$n \setminus k$	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 3.8** (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 3.9.** Število surjekcij  $[n] \rightarrow [k]$  je  $k! \cdot S(n, k)$

*Dokaz.* Naj bo  $f : [n] \rightarrow [k]$  surjekcija. Množica  $\{f^{-1}(1), f^{-1}(2) \dots f^{-1}(k)\}$ , kjer  $f^{-1}(i)$  predstavlja množico praslík  $i$ -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 3.10.**

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

**Trditev 3.11** (Rekurzivna formula za  $S(n)$ ).

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

*Dokaz.* (1. način) Z indukcijo (na vajah, DN?)

■

*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).

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

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

Dva polinoma stopnje  $\leq n$ , ki se ujemata v  $n + 1$  točkah, sta enaka (razlika je polinom stopnje  $\leq n$  z  $n + 1$  ničlami, torej je ekvivalentna 0)

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

Velja tudi:

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

**Trditev 3.12** (Rekurzivna formula za  $B(n)$ ).

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

*Dokaz.* Izberemo razdelitev  $[n+1]$  ( $k$  je 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  $B(n-k)$ ).

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

■

### 3.3 Lahova števila

**Definicija 3.13** (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.

- $L(n, n) = 1$
- $L(n, n-1) = 2$
- $\binom{n}{2} = n(n-1)$



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

**Trditev 3.14** (Rekurzivna 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,  $n!$  - permutacija,  $\binom{n-1}{k-1}$  - kompozicija ■

**Trditev 3.15.**

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

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

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

*Dokaz.* Dokaz bomo prepustili bralcu za vajo ■

Primerjajmo:

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

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

### 3.4 Razčlenitve naravnih števil in Eulerjev petkotniški izrek

**Definicija 3.17** (Razčlenitev naravnega števila). Razčlenitev ali particija  $n \in \mathbb{N}$  je  $l$ -terica

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

$$\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_l > 0$$

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

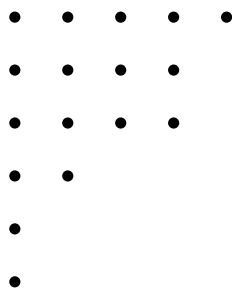
$\lambda_i$  so členi razčlenitve,  $n$  je velikost razčlenitve,  $l$  je dolžina razčlenitve.

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

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

Razčlenitve lahko prikažemo grafično s pomočjo Ferresovih diagramov.

*Primer.* Diagram za  $\lambda = (5, 4, 3, 2, 1, 1)$



**Definicija 3.18** (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  $\leq k$  členi.

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

*Primer.*

$$n = 0 : (), p(0) = 1, p_0(0) = 1$$

$$n = 1 : 1$$

$$n = 2 : 2, 11$$

$$n = 3 : 3, 21, 111$$

$$n = 4 : 4, 31, 22, 211, 1111$$

$$n = 5 : 5, 41, 32, 311, 221, 2111, 11111$$

$$p(n) : 1, 1, 2, 3, 5, 7, 11, 15, \dots$$

$$p_2(5) = 2$$

$$\overline{p}_3(5) = 5$$

**Definicija 3.19** (Konjugirana razčlenitev  $\lambda'$ ). Dobimo s transpozicijo Ferrerovega diagrama (stolpce napišemo kot vrstice).

Veljajo naslednje lastnosti:

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

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

**Trditev 3.20** (Lastnosti  $p_k(n)$ ).

1.  $p_k(n) = \overline{p}_{k-1}(n - k)$
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 / dodamo prvi stolpec / stolpec dolžine  $k$
2. Imamo razčlenitev  $n$  s  $k$  členi:  $\lambda_l = 1$  ( $p_{k-1}(n-1)$ ) in  $\lambda_l \geq 2$  ( $p_k(n-k)$ )
3. Očitno

■

*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 (3.1). Uporabi formulo  $p_k(n) = p_{k-1}(n-1) + p_k(n-k)$ .

Kaj pa rekurzija za  $p(n)$ ?

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

$$A_i = \{\text{razčlenitve } n, \text{ ki vsebujejo } i \text{ kot člen}\}$$

$$|A_i| = p(n-i)$$

$$|A_i \cap A_j| = p(n-i-j) \quad i \neq j$$

$$|A_I| = p(n - \sum_{i \in I} i)$$

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

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

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 lihomnogo 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 3.21.**

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

$$\frac{k(3k-1)}{2} : 1, 5, 12, 22, \dots$$

$$\frac{k(3k+1)}{2} : 2, 7, 15, 26, \dots$$

**Posledica 3.22** (Eulerjev petkotniški izrek).

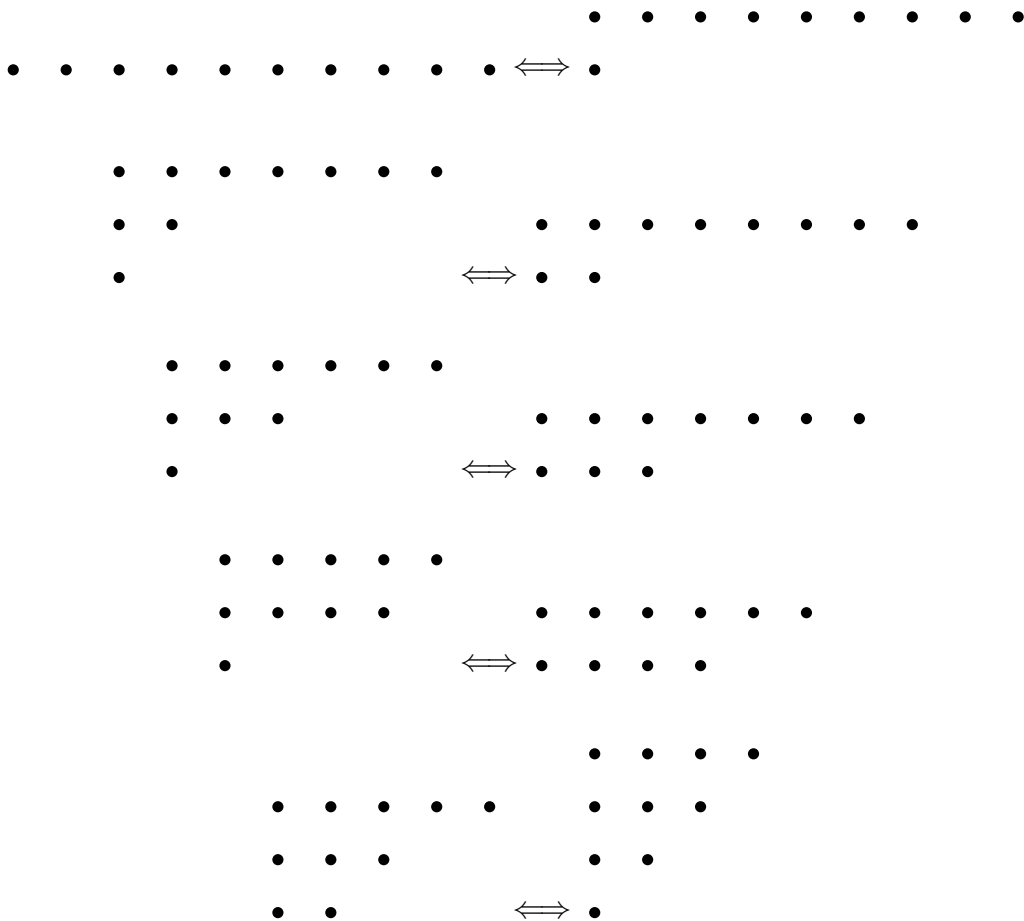
$$p(n) = p(n-1) + p(n-2) - p(n-5) - p(n-7) + p(n-12) + p(n-15) - p(n-22) - p(n-26) \dots$$

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

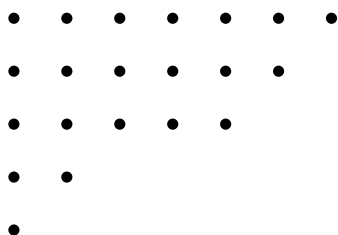
*Dokaz.* Iščemo "skoraj bijekcijo"

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

$m = 10$ :



$s(\lambda) := \lambda_{l(\lambda)}$  najmanjši člen



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

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

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

Zakaj to ni vselej bijekcija? Prvo pravilo ne deluje, če

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

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

Drugo pravilo ne deluje, če

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

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

- če  $m \neq \frac{k \cdot (3k \pm 1)}{2}$ , smo našli bijekcijo,  $\alpha(m) - \beta(m) = 0$ .
  - če  $m = \frac{k \cdot (3k \pm 1)}{2}$ , 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	$k^n$	$k^n$	$k! \cdot s(n, k)$
Ne ločimo	Ločimo	$\binom{n+k-1}{k-1}$	$\binom{k}{n}$	$\binom{n-1}{k-1}$
Ločimo	Ne ločimo	$\sum_{i \leq k} s(n, i)$	$k \geq n ? 1 : 0$	$s(n, k)$
Ne ločimo	Ne ločimo	$\overline{p}_k(n)$	$k \geq n ? 1 : 0$	$p_k(n)$

## 4 Rodovne funkcije

### 4.1 Uvod

Na kakšne načine lahko predstavimo zaporedje?

1. Z eksplisitno formulo

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

2. Z rekurzivno zvezo

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

$$a_n = 2a_{n-1}, \quad a_0 = 1$$

$$b_n = nb_{n-1}, \quad n \geq 1, \quad b_0 = 1$$

$$F_n = F_{n-1} + F_{n-2}, \quad n \geq 2, \quad F_0 = 1, \quad F_1 = 1$$

3. Z asimptotsko formulo

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

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

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

*Opomba.*  $\sqrt{2\pi n} \left( \frac{n}{e} \right)^n$  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 približkom, ki ima splošni člen oblike  $a_n \sim An^B C^n$ .



#### 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  $\infty$ ) konvergenčni polmer. V  $x = \pm R$  ne moremo zagotovo trditi ničesar.

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

$$R = \frac{1}{\limsup_{n \rightarrow \infty} \sqrt[n]{|a_n|}} \in [0, \infty]$$

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

*Primer.*  $\sum_{n=0}^{\infty} 2^n x^n$ ,  $R = \lim_{n \rightarrow \infty} \left( \frac{2^n}{2^{n+1}} \right) = \frac{1}{2}$ ,  $\frac{1}{\limsup_{n \rightarrow \infty} \sqrt[n]{|2^n|}} = \frac{1}{2}$

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

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

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

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

Zaporedje lahko na ta način "zakodiramo" v funkcijo.

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

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).

$$\mathbb{R}[x] = \{a_0 + a_1x + a_2x^2 + \dots + a_nx^n : a_0, \dots, a_n \in \mathbb{R}\}$$

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).

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

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

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

$$\sum_k c(n, k) x^k = x^n \quad \sum_k S(n, k) x^{\bar{k}} = x^n$$

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

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

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

Koeficienti pri  $x^k$  so

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

$(\mathbb{R}[x], +, \cdot)$  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 formalnih potenčnih vrst).  $\mathbb{R}[[x]]$  je komutativna algebra zaporedij v  $\mathbb{R}$ .

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

Za operacije

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

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

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

Namesto  $(a_n)_n$  ali  $a_0, a_1, a_2, \dots$  pišemo  $\sum_{n=0}^{\infty} a_n x^n$  oziroma  $a_0 + a_1 x + a_2 x^2 + \dots$ . 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  $1 = 1 + 0x + 0x^2 + \dots$ . Velja tudi  $(1 + x + x^2 + \dots)(1 - x) = 1$ , torej je  $(1 - x)$  multiplikativni inverz za  $(1 + x + x^2 + \dots)$ . To poznamo kot formulo za potenčno vrsto.

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

**Trditev 4.6.**  $\sum_{n=0}^{\infty} a_n x^n$  ima inverz za množenje natanko tedaj, ko  $a_0 \neq 0$ .

*Dokaz.* ( $\Rightarrow$ )

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

$$a_0 b_0 = 1$$

$$a_0 b_1 + a_1 b_0 = 0$$

$$a_0 b_2 + a_1 b_1 + a_2 b_0 = 0$$

$$\dots = 0$$

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

$$\begin{aligned} b_0 &= \frac{1}{a_0} \\ b_1 &= -\frac{a_1 b_0}{a_0} \\ b_2 &= -\frac{a_1 b_1 + a_2 b_0}{a_0} \\ &\dots \end{aligned}$$

■

Vpeljimo nekaj oznak, ki jih bomo uporabljali v nadaljevanju.

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

$$[x^n]F(x) := a_n \text{ (} n\text{-ti člen zaporedja)}$$

$$F(0) := [x^0]F(x)$$

$$(F \cdot G)(0) := F(0) \cdot G(0)$$

**Definicija 4.7** (Odvod formalne potenčne vrste). Definiramo po zgledu odvajanja polinomov pri analizi.

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

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

**Trditev 4.8** (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

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

Na desni pa

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

kar lahko zapišemo kot

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

Od tod neposredno sledi naša formula.

■

**Definicija 4.9.**

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

**Trditev 4.10.** 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 4.11.** 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 4.12** (Karakteristika). Je najmanjše tako število  $k$ , da velja  $\underbrace{1 + 1 + \dots}_{k\text{-krat}} = id$ .

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

*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  $5! = 6! = \dots = 0$ . 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.

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

Pri kombinatoriki jo bomo nekoliko obrnili.

$$c + bx + ax^2 = c(1 - y_1x)(1 - y_2x)$$

$\frac{1}{y_1}$  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 4.13.**

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

*Dokaz.*

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

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  $1, 1, 2, 3, 5, 8, \dots$ . Uporabili bomo oznaki  $F_n = n$ -ti člen Fibonaccijevega zaporedja in  $F(x) = \sum_{n=0}^{\infty} F_n \cdot x^n$ , t.j. Fibonaccijeva formalna potenčna vrsta.

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

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

$$\begin{aligned} F(x)(1 - x - x^2) &= 1 \\ F(x) &= \frac{1}{1 - x - x^2} \end{aligned}$$

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 eksplisitno 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 4.14** (Recept za reševanje homogene linearne rekurzivne enačbe s konstantnimi koeficienti).

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

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  $\lambda_1, \dots, \lambda_k$  ničle z večkratnostmi  $\alpha_1, \dots, \alpha_k$ .

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

*Dokaz.* Pomnožimo vrsto z  $x^n$  in seštejmo od  $d$  do  $\infty$ .

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



$$\begin{aligned}
0 &= c_d(F(x) - a_0 - a_1x - \dots - a_{d-3}x^{d-3} - a_{d-2}x^{d-2} - a_{d-1}x^{d-1}) \\
&+ c_{d-1}x(F(x) - a_0 - a_1x - \dots - a_{d-3}x^{d-3} - a_{d-2}x^{d-2}) \\
&+ c_{d-2}x^2(F(x) - a_0 - a_1x - \dots - a_{d-3}x^{d-3}) \\
&+ \dots \\
&+ c_1x^{d-1}(F(x) - a_0) \\
&+ c_0x^dF(x)
\end{aligned}$$

$F(x)(c_d + c_{d-1}x + c_{d-2}x^2 + \dots + c_1x^{d-1} + c_0x^d) = P(x)$  polinom stopnje  $< d$

$$F(x) = \frac{P(x)}{c_d + c_{d-1}x + c_{d-2}x^2 + \dots + c_1x^{d-1} + c_0x^d}$$

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

$$\begin{aligned}
F(x) &= \frac{P(x)}{c_d \prod_{i=1}^k (1 - \lambda_i x)^{\alpha_i}} = \\
&= \sum_{i=1}^k \sum_{j=1}^{\alpha_i} \frac{A_{i,j}}{(1 - \lambda_i x)^j} = \\
&= \sum_{i=1}^k \sum_{j=1}^{\alpha_i} A_{i,j} \sum_{n=0}^{\infty} \binom{n+j-1}{j-1} \lambda_i^n x^n \\
a_n &= \sum_{i=1}^k \left( \sum_{j=1}^{\alpha_i} A_{i,j} \binom{n+j-1}{j-1} \right) \lambda_i^n = \sum_{i=1}^k p_i(n) \lambda_i^n \\
\binom{n+j-1}{j-1} &= \frac{(n+j-1)(n+j-2)\dots(n+1)}{(j-1)!} \\
\text{polinom stopnje } (j-1) &\implies \deg(p_i) < \alpha_i
\end{aligned}$$

■

**Izrek 4.15** (Reševanje nekaterih nehomogenih rekurzivnih enačb).

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

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

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

$\deg(r(n)) \leq \deg(q)$ ,  $\alpha$ -kratnost  $\lambda$  v karakterističnem polinomu,

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

*Dokaz.* Prepuščen bralcu.

■

## 4.4 Binomska vrsta

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

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

**Definicija 4.16** (Posplošeni binomski koeficient). Zahtevamo samo  $n \in \mathbb{N}$ .

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

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

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

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

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

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

$$\begin{aligned} \binom{-k}{n} &= \frac{-k(-k-1)\dots(-k-n+1)}{n!} = \frac{(-1)^n(n+k-1)\dots(k+1)k}{n!} \cdot \frac{(k-1)!}{(k-1)!} = \\ &= \frac{(-1)^n(n+k-1)!}{n!(k-1)!} = (-1)^n \binom{n+k-1}{k-1} \end{aligned}$$

*Primer.*

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

Uporabimo simbol  $!!$ . Velja  $7!! = 1 \cdot 3 \cdot 5 \cdot 7$  oziroma za soda števila:  $6!! = 2 \cdot 4 \cdot 6$ . 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  $n \geq 1$ , sicer je  $\binom{\frac{1}{2}}{n} = 0$ .

**Definicija 4.17** (Binomska vrsta). Naj bo  $K$  obseg in  $\lambda \in K$ .

$$\begin{aligned} B_\lambda(x) &= \sum_{n=0}^{\infty} \binom{\lambda}{n} x^n \\ &= 1 + \lambda x + \frac{\lambda(\lambda-1)}{2} x^2 + \frac{\lambda(\lambda-1)(\lambda-2)}{6} x^3 + \dots \end{aligned}$$

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

*Primer.* Če za  $\lambda$  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  $\lambda$  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 4.13).

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 4.18** (Binomski izrek s črtico).

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

*Dokaz.* Z indukcijo.

Baza indukcije:  $n = 0$ ,  $1 = 1 \checkmark$

Indukcijski korak:  $n - 1 \implies n$

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

Dokaz za naraščajoče potence prepustimo bralcu. ■

#### 4.4.1 Catalanova števila

**Definicija 4.19** (Catalanovo število).  $C_n$  je število pravih postavitev oklepajev na nizu  $n + 1$  števil  $(t_0 \ t_1 \ t_2 \ \dots \ t_n)$ .

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

$$\begin{aligned}
 n = 0 & \quad (t_0) \\
 n = 1 & \quad (t_0 t_1) \\
 n = 2 & \quad (t_0 t_1) t_2 \quad t_0 (t_1 t_2) \\
 n = 3 & \quad ((t_0 t_1) t_2) t_3 \quad (t_0 t_1) (t_2 t_3) \quad t_0 (t_1 (t_2 t_3)) \quad (t_0 (t_1 t_2)) t_3 \quad t_0 ((t_1 t_2) t_3)
 \end{aligned}$$

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

*Primer.* Pri  $((t_0 t_1) t_2) t_3$  je “zadnje množenje” med  $((t_0 t_1) t_2)$  in  $t_3$ , pri  $(t_0 t_1) (t_2 t_3)$  pa med  $(t_0 t_1)$  in  $(t_2 t_3)$ .

V splošnem,  $(t_0 t_1 \dots t_k) \cdot (t_{k+1} \dots t_{n+1})$ , kjer velja  $0 \leq k \leq n$ . Ostane nam še izbira oklepajev med  $k$  členi in  $(n + 1) - (k + 1) = n - k$  členi.

**Izrek 4.20** (Rekurzivna zveza za  $C_n$ ).

$$C_{n+1} = \sum_{k=0}^n C_k C_{n-k} \quad n \geq 0$$

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

**Izrek 4.21** (Eksplisitna 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.

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

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.

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

Nadaljujemo tako, da izračunano vstavimo v prvotno ničlo.

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

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.

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

Zato je to naša rešitev.

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

■

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

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

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 zelenimi konstrukcijami in postavljanjem oklepajev, bodisi pokažete, da ima konstrukcija isto rekurzivno zvezo.

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

## 4.5 Rodovne funkcije razčlenitev

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

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

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

$$(1+x+x^2+\dots)(1+x^2+x^4+\dots)(1+x^3+x^6+\dots) \quad [x^5]$$

Izberemo nekaj iz prvega oklepaja, prištejemo  $2 \cdot$  nekaj iz drugega in  $3 \cdot$  nekaj iz tretjega.

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

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 4.22.**

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

*Dokaz.* Koeficient na obeh straneh je število rešitev enačbe

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

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

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

**Trditev 4.23.**

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

**Trditev 4.24.**

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

Pri  $[x^n] : (1+x+x^2+\dots)(1+x^2+x^4+\dots)\dots(1+x^n+x^{2n}+\dots)(1+x^{n+1}+x^{2n+2}+\dots)\dots$   
ignoriramo

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

*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

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

## 4.6 Uporaba rodovnih funkcij

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

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

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

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

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

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

(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 ekvivalentnih razredov barvanj.

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

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

*Primer* (Ciklična grupa).  $C_n = \{(1\ 2\ 3\ \dots\ n)^i : 0 \leq i \leq n\} \leq S_n$

$$C_n \cong \mathbb{Z}_n$$

$$\phi : \mathbb{Z}_n \rightarrow C_n := i \rightarrow (1\ 2\ \dots\ n)^i$$

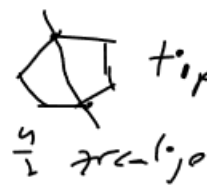
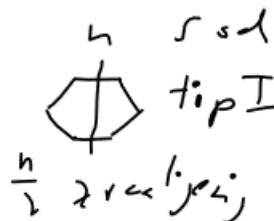
*Primer* (Diedrska grupa).  $D_n = \{\text{rotacije} + \text{zrcaljenja}\} \leq S_n$

$$|D_n| = 2n \text{ (} n \text{ zrcaljenj in } n \text{ rotacij)}$$

$n$  lih



$n$  zrcaljenj



**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.* 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.*

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

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

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 5.1 pri definiciji orbite).

**Definicija 5.6** (Stabilizator).

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

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

**Definicija 5.7** (Negibna točka).

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

Elemente  $X_g$  imenujemo negibne točke  $g$ -ja.

**Izrek 5.8.**

$$G_x \leq G$$

*Dokaz.*

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

■

*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 5.9.**

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

*Dokaz.* Spomnimo se levih odsekov ...

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

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

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

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

$\phi$  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  $\phi$  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.

$$|G| = |G_x| |G_x| = 3 \cdot 4 = 12$$

id + rotacije za  $120^\circ$  + rotacije za  $180^\circ$

$$1 + 4 \cdot 2 + 3 = 12$$

*Primer.* Preštej simetrije kocke.

$$|G| = |G_x| |G_x| = 3 \cdot 8 = 24$$

## 5.2 Burnsidova lema

**Lema 5.10** (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  $\sum_{g \in G} |X_g|$ .

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

Analizirajmo pomen faktorja  $\sum_{x \in X} \frac{1}{|G_x|}$ . 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

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

oziroma računsko (oznaka  $\sigma$  = 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 simetrane stranic (0 negibnih točk) in  $\frac{n}{2}$  zrcaljenj preko diagonale (2 negibni točki).

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

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

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

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

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

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

*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.*  $3 \times 3$  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  $90^\circ$  vedno 0, pri rotacijah za  $180^\circ$  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  $G \leq S_n$  permutacijska grupa,  $n = |X|$ .  $g \in G$  je permutacija elementov iz  $X$ , ki jo seveda lahko enolično zapišemo  $g$  kot produkt disjunktnih ciklov.

**Definicija 5.11** (Ciklični indeks). Označimo z  $\alpha_i(g)$  število ciklov dolžine  $i$ . Ciklični indeks  $Z_G(t_1, \dots, t_n)$  definiramo kot

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

*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  $180^\circ$  ima 2 cikla dolžine 2 ( $(1\ 2\ 3\ 4)$  in  $(1\ 4\ 3\ 2)$ ), torej  $(t_2)^2$ , vsaka od dveh rotacij za  $90^\circ$  pa je cikel dolžine 4, torej  $2 \cdot (t_4)^1$ .

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