Teorija Kombinatorike — IŠRM 2024/25

Anton Luka Šijanec

7. september 2025

Povzetek

Povzeto po zapiskih s predavanj profesorja Konvalinke.

Kazalo

1 Osnovni principi kombinatorike

Pri tem predmetu velja $\mathbb{N} \coloneqq \mathbb{N}_0$ ZDB $0 \in \mathbb{N}$.

1.1 Funkcija/preslikava

Definicija. $f : X \to Y$ je formalno množica parov $f \subseteq X \times Y$ s pogojem $\forall x \in X \exists! y \in Y \ni : (x, y) \in f$ ZDB za vsak $x \in X$ je $f(x)$ enolično definiran.

Funkcijo podamo tako, da:

1. naštejemo vse elemente f — vse pare (puščični diagram med množicama)
2. povemo predpis za preslikanje elementa — $f : \mathbb{N} \to \mathbb{N}; x \mapsto x^2$
3. z rekurzijo — $f : \mathbb{N} \to \mathbb{N}, f(0) = 1, f(1) = 1, f(n) = f(n-1) + f(n-2)$ za $n \geq 2$ (Fibonaccijevo zaporedje)

Definicija. Zaporedje je preslikava iz naravnih števil v katerokoli neprazno množico.

Definicija. Lastnosti preslikav. Naj bo $f : A \to B$ preslikava.

- f injektivna $\Leftrightarrow \forall a \in A, b \in B : f(a) = f(b) \Rightarrow a = b$
- f surjektivna $\Leftrightarrow \forall a \in A \exists b \in B \ni : f(b) = a$
- f bijektivna $\Leftrightarrow \forall a \in A \exists! b \in B \ni : f(b) = a$ ZDB f injektivna in f surjektivna hkrati

Kombinatorika je odkrivanje moči množic. Tu često želimo dokazati enakost moči dveh množic, najlepše to storimo s konstrukcijo bijekcije, saj velja:

Izrek. *Naj bo* $f : X \to Y$.

- f injektivna $\Rightarrow |X| \leq |Y|$
- f surjektivna $\Rightarrow |Y| \leq |X|$
- f bijektivna $\Rightarrow |X| = |Y|$

Imejmo n kroglic in k škatel. Vsako kroglico damo v eno od teh škatel. Postavitev kroglic v škatle je preslikava iz množice kroglic v množico škatel ($\{1..5\} \to \{a, b, c\}$). Injektivnost te preslikave pomeni, da ni praznih škatel, surjektivnost pa, da je v vsaki škatli vsaj ena kroglica.

Definicija. Nekaj oznak v kombinatoriki:

- $\mathbb{N} \coloneqq \{0, 1, 2, \dots\} \sim$ možne moči končnih množic
- $[n] \coloneqq \{1..n\}$, $[0] \coloneqq \emptyset$, $|[n]| = n$
- množica podmnožic A (potenčna množica A) $=: 2^A$, velja $\left|2^A\right| = 2^{|A|}$, odtod tudi ta oznaka
- množica preslikav $X \to Y =: Y^X$, saj $\left|Y^X\right| = |Y|^{|X|}$.
- $\sum_k \sim$ vsota po vseh $k \in \mathbb{N}$, $\sum_{k \geq a} \sim$ vsota po vseh $k \in \mathbb{N}, k \geq a$

Izrek. *Binomski izrek.*

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

1.2 Dirichletovo načelo (angl. Pigeonhole principle)

Če obstaja injekcija $X \to Y$, je $|X| \leq |Y|$. Če torej $|X| \geq |Y|$, ne obstaja injekcija $X \to Y$. Če imamo n kroglic v k škatlah in $n > k$, bosta gotovo vsaj v eni škatli vsaj dve kroglici.

Uporaba načela

- ob trinajstih ljudeh imata vsaj dva rojstni dan v istem mesecu. Kroglice so ljudje, škatle so meseci, preslikava je iz človeka v mesec rojstva.
- $X \subseteq \mathbb{N}$; $|X| = n+1$. $\exists x, y \in X \ni: n|\,(x-y) \wedge x \neq y$. Trditev je ekvivalentna temu, da sta v X dve števili z istim ostankom pri deljenju z n. Kroglice so števila, škatle so možni ostanki pri deljenju z n. Preslikava $x \mapsto x \mod n$. Kroglic je $n+1$, škatel je $n \Rightarrow$ po Dirichletu trditev velja.
- n ljudi. Trdimo, da $\exists 2$ človeka, ki poznata enako število ljudi. Imamo torej n kroglic — ljudi in n škatel — št. poznanstev ($\in \{0..(n-1)\}$). Preslikava preslika človeka v število njegovih znancev. Sicer velja $n = n$, toda ne moremo imeti hkrati nekoga, ki pozna 0 oseb in hkrati nekoga, ki pozna $n-1$ oseb, torej je število različnih poznanstev največ $n-1$. Dirichlet pove, da obstaja dve osebi, ki poznata enako število ljudi.
- $X \subseteq \{1..100\}$; $|X| = 10$. Trdimo, da obstajata dve disjunktni podmnožici X, ki imata enako vsoto. Kroglice so podmnožice X — $2^{10} = 1024$ jih je. Škatle so možne vsote elementov, torej $\in \{55..955\}$. Injekcije iz podmnožic X dolžine 10 v možne vsote po dirichletu ni, zato obstajata vsaj dve podmnožici, ki imata isto vsoto. Če sta nedisjunktni, jima odstranimo presek, pa dobimo disjunktni, ne da bi spremenili vsoto elementov.
- $X \subseteq \{1..2n\}$; $|X| = n+1$. Trdimo, da $\exists x, x' \in X \ni: x|x' \wedge x \neq x'$. Kroglice so X. Za katerokoli število velja $x = 2^a \cdot b$, kjer je b liho. Škatle so liha števila v $[2n]$. Preslikava slika $x \to b$ za b od prej. Ker je kroglic več kot škatel, velja $\exists x, x' \in X \ni: x = 2^a b \wedge x' = 2^{a'} b$. Če je $a < a'$, je $x'|x$, sicer je $x|x'$.

1.3 Načelo vsote in produkta

Izrek. *Načelo vsote. Naj bosta A, B množici. Če sta disjunktni, $|A \cup B| = |A| + |B|$. Če nista nujno disjunktni, velja $|A \cup B| = |A| + |B| - |A \cap B|$. Splošneje: $A_1, \ldots, A_n$ disjunktne $\Rightarrow |\bigcup_{k=1}^{n} A_k| = \sum_{k=1}^{n} |A_k|$.*

Interpretacija: Če so elementi množice bodisi tipa 1 bodisi tipa 2 (ne pa obeh hkrati), je skupno število vsota števila elementov tipa 1 in števila elementov tipa 2.

Izrek. *Načelo produkta. Naj bosta A, B množici. $|A \times B| = |A| \cdot |B|$. Splošneje: $A_1, \ldots, A_n$ množice $\Rightarrow |\Pi_{k=1}^{n} A_k| = \Pi_{k=1}^{n} |A_k|$.*

Izrek. *Interpretacija: Izberemo element iz A na toliko načinov, kolikor je elementov A, nato še neodvisno od prve izbire izberemo element iz B itd.*

Zgled. Primeri.

- oblačenje. Bodisi formalno bodisi neformalno (pravilo vsote). Formalna oprava sestoji iz ene izmed enajstih srajc in enih izmed petih hlač, neformalna pa iz ene izmed devetinpetdesetih majic in enih izmed štirih kavbojk (pravili produkta). Možnih oprav je torej $11 \cdot 5 + 59 \cdot 4 = 55 + 236 = 291$.
- $n-$mestna števila, ki vsebujejo štirico in same različne števke. Štirica je lahko na enem izmed n mest (pravilo vsote). Za preostale števke pa uporabimo varianto načela produkta, kjer število možnih izbir ni odvisno od prej izbranih elementov. Iskanih števil je $\frac{9!}{(10-n)!} + (n-1)\,\frac{8!\cdot 8}{(10-n)!}$ (levi člen za štirico na prvem mestu, desni člen za štirico na preostalih $n-1$ mestih).
- figure pri šahu razporedimo po 1. vrsti: 8 za tekača 1 in 7 za tekača 2 (skupaj 56/2 — tekačev medsebojno ne ločimo), 6 za konja 1 in 5 za konja 2 (skupaj 30/2), 4 za trdnjavo 1 in 3 za trdnjavo 2 (skupaj 12/2), 2 za kraljico in 1 za kralja (skupaj 2). Torej je možnih razporeditev $\frac{56}{2} \cdot \frac{30}{2} \cdot \frac{12}{2} \cdot 2 = 5040$.
- Fischerjev naključni šah (chess960). Figure so naključno razporejene po prvi vrsti z naslednjimi omejitvami: tekača sta na različnih barvah, kralj je med trdnjavama (da dopustimo rošadi). 4 za tekača 1 in 4 za tekača 2, 6 za konja 1 in 5 za konja 2 (skupaj $30/2 = 15$), 4 za kraljico in 1 za trdnjavi in kralja (preostanejo le še tri nedodeljena mesta). Torej je možnih razporeditev $= 4 \cdot 4 \cdot 15 \cdot 4 = 960$.
- dokaži $\left|2^A\right| = 2^{|A|}$ za končno množico $A \sim$ najdi bijekcijo Φ med $\{0,1\}^{|A|} \doteq \left\{0..\left(2^{|A|}\right) - 1\right\}$ in 2^A. $\Phi^{-1}(B) = \{a_i \in A; B_i = 1\}$, $\Phi(B) = (a_1 \in B, a_2 \in B, \ldots, a_n \in B)$. Velja $\Phi^{-1} \circ \Phi = id$ in $\Phi \circ \Phi^{-1} = id$. S kombinatoriko pa lahko to dokažemo malce bolj intuitivno. Za vsak element se odločimo, ali je v podmnožici ali ne. 2 izbiri za vsakega in izbire so neodvisne $\Rightarrow 2^{|A|}$.

Definicija. Permutacija X je bijekcija $X \to X$. Množica permutacij X je S_X ali $S(X)$. Množica permutacij $[n]$ je $S_{[n]}$ ali S_n. Permutacijo zapišemo z dvovrstično notacijo, primer: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix}$, ali pa z enovrstično, primer: $2 \quad 4 \quad 3 \quad 1 \quad 5$.

Definicija. $a_n \sim b_n$ ($(a_n)_{n\in\mathbb{N}}$ je asimptotsko enako $(b_n)_{n\in\mathbb{N}}$) $\Leftrightarrow \lim_{n\to\infty} \frac{a_n}{b_n} = 1$.

Definicija. $n! = n \cdot (n-1)!$ za $n \geq 1$, $0! = 1$

Izrek. *Velja* $|S_n| = n \cdot (n-1) \cdot \dots \cdot (n-(n-1)) = n!$

Dejstvo. *Stirlingova formula.* $n! \sim \left(\frac{n}{e}\right)^n \cdot \sqrt{2\pi n}$, *kjer* $\sim$ *predstavlja asimptotsko enakost.*

Permutacije lahko medsebojno komponiramo. Temu pravimo množenje.

Zgled. $4 \quad 1 \quad 3 \quad 2 \quad 5 \circ 1 \quad 4 \quad 3 \quad 5 \quad 2 = 4 \quad 2 \quad 3 \quad 5 \quad 1$

Izrek. *Za* A *množico vseh permutacij neke množice je* $(A, \circ)$ *grupa.*

Dokaz. Dokažimo le asociativnost, obstoj enote in inverz:

- $(\pi \circ \varphi) \circ \tau = \pi \circ (\varphi \circ \tau)$
- $\pi \circ id = id \circ \pi = \pi$
- $\forall \pi \in A \exists \tau \in A \ni: \pi \circ \tau = \tau \circ \pi = id$

□

Pripomba. Velja $|S_n| = n!$. Naj bo $\pi \in S_n$, $k \in [n]$. Oglejmo si zaporedje $k, \pi k, \pi^2 k, \dots$. Po Dirichletu $\exists i > j \ni: \pi^i(k) = \pi^j(k) \Rightarrow \pi^{j-i}(k) = k$ in imamo ciklično zaporedje $k, \pi k, \pi^2 k, \dots, k$. Cikel označimo z $\left(k, \pi k, \dots \pi^{j-i-1} k\right)$.

Posledica. *Vsaka permutacija je produkt disjunktnih ciklov.*

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 2 & 7 & 6 & 3 & 8 & 1 & 5 \end{pmatrix} = (1,4,6,8,5,3,7)(2) = (1,4,6,8,5,3,7)$$

Disjunktni cikli medsebojno komutirajo. Cikel je invarianten za ciklično shiftanje/zamikanje/vrtenje. Do vrstnega reda ciklov in znotrajciklične ureditve je zapis permutacije kot produkt disjunktnih ciklov enoličen.

Trditev. Naj bosta N, K množici, $|N| = n, |K| = k$.

1. Preslikav iz N v K je $\left|K^N\right| = |K|^{|N|} = k^n$.
2. Injektivnih preslikav iz N v K je $k(k-1)(k-2)\cdots(k-n+2)(k-n+1) = \frac{k!}{(k-n)!} =: k^{\underline{n}}$ (pravimo k na n padajoče)

Dokaz. Intuitiven dokaz. Naj bo $N = \{x_1, \dots, x_n\}$

1. Za vsak x_i imamo k izbir, kam se bo preslikal in izbire so neodvisne: $k \cdot \dots \cdot k = k^n$.
2. Za x_1 je k izbir, za x_2 je $k-1$ izbir itd. Če je $|K| > |N|$, bomo na neki točki vse skupaj množili z 0 in dobili 0, s čimer ustrezamo Dirichletu.

Formalnejši dokaz. Iščemo bijekcijo med K^N in $[k]^n$. $\Psi(f) = (j_1, \dots, j_n)$, kjer $f(x_i) = y_{j_i}$.

1. Formalno preštejemo urejene izbire n elementov iz množice $[k]$ s ponavljanjem — variacije s ponavljanjem.
2. Formalno preštejemo urejene izbire n elementov iz množice $[k]$ brez ponavljanja — variacije brez ponavljanja.

□

Pripomba. Za $k = n$ so injektivne preslikave s tudi surjektivne in s tem bijektivne: $n^{\underline{n}} = n!$.

Definicija. Oznaka $k^{\overline{n}} = k(k+1)(k+1)\cdots(k+n-2)(k+n-1)$ pomeni k na n naraščajoče.

2 Podmnožice in načrti

2.1 Binomski koeficienti

Definicija. Naj bo $k, n \in \mathbb{N}$, A množica. $\binom{A}{k} := \{B \subseteq A; |B| = k\}$ ZDB vse $k-$elementne podmnožice A.

Zgled. $\binom{[4]}{2} = \{\{1,2\}, \{1,3\}, \{1,4\}, \{2,3\}, \{2,4\}, \{3,4\}\}$, $\binom{[4]}{4} = \{\{1,2,3,4\}\}$, $\binom{[4]}{1} = \{\{1\}, \{2\}, \{3\}, \{4\}\}$, $\binom{[4]}{0} = \{\{\}\} = \{\emptyset\}$, $\binom{[4]}{-1} = \{\} = \emptyset$, $\bigcup_{k=0}^{|A|} \binom{A}{k} = 2^A$.

Definicija. Binomski koeficient/simbol. Naj bo $n, k \in \mathbb{N}$. $\binom{n}{k} := \left|\binom{[n]}{k}\right|$. Rečemo n nad k (angl. n choose k).

Zgled. $\binom{n}{0} = 1$, $\binom{n}{1} = n$, $\binom{n}{2} = \frac{n(n-1)}{2}$ (neurejeni pari)

Trditev.

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

Dokaz. Bijekcija $\Phi : \binom{[n]}{k} \to \binom{[n]}{n-k}$ s predpisom $\Phi(B) = B^{\mathcal{C}}$ in $\Phi^{-1}(B) = B^{\mathcal{C}}$. □

Trditev.

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

Dokaz. Dva načina.

1. Izberemo $1-$elementne podmnožice na n načinov, $2-$elementne na $n(n-1)$ načinov, ..., $k-$elementne na $n(n-1)\cdots(n-k+2)(n-k+1)$ načinov. Delimo s številom permutacij $[k]$, ker vrstni red elementov v množici ni pomemben. Podmnožic je torej $\frac{n^{\underline{k}}}{k!}$.

2. Preštejemo urejene izbire brez ponavljanja na dva načina:

   (a) $n^{\underline{k}}$: Izberemo k elementov, za prvega imamo n možnosti, za drugega $n-1$, ...

   (b) $k! \cdot \binom{n}{k}$: Izberemo $k-$elementno podmnožico in ji določimo vrstni red.

   $$\Rightarrow n^{\underline{k}} = k! \cdot \binom{n}{k}$$

   Če $k < 0$ ali $k > n$ je $\binom{n}{k} = 0$, sicer $\frac{n^{\underline{k}}}{k!} \cdot \frac{(n-k)!}{(n-k)!} = \frac{n!}{k!(n-k)!}$.

□

Zgled.

$$\binom{10}{7} =?= \binom{10}{3} = \frac{10 \cdot 9 \cdot 8}{6} = 120$$

Trditev. Rekurzivna zveza za binomske koeficiente:

$$\forall n, k \in \mathbb{N} : \binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}.$$

Dokaz. Dva načina:

1. Računsko.

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

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

2. Bijektivno z načelom vsote. Vzemimo poljubno $k-$podmnožico[1] $[n]$. Klasificirajmo jo glede na vsebnost n na dve očitno disjunktni podmnožici:

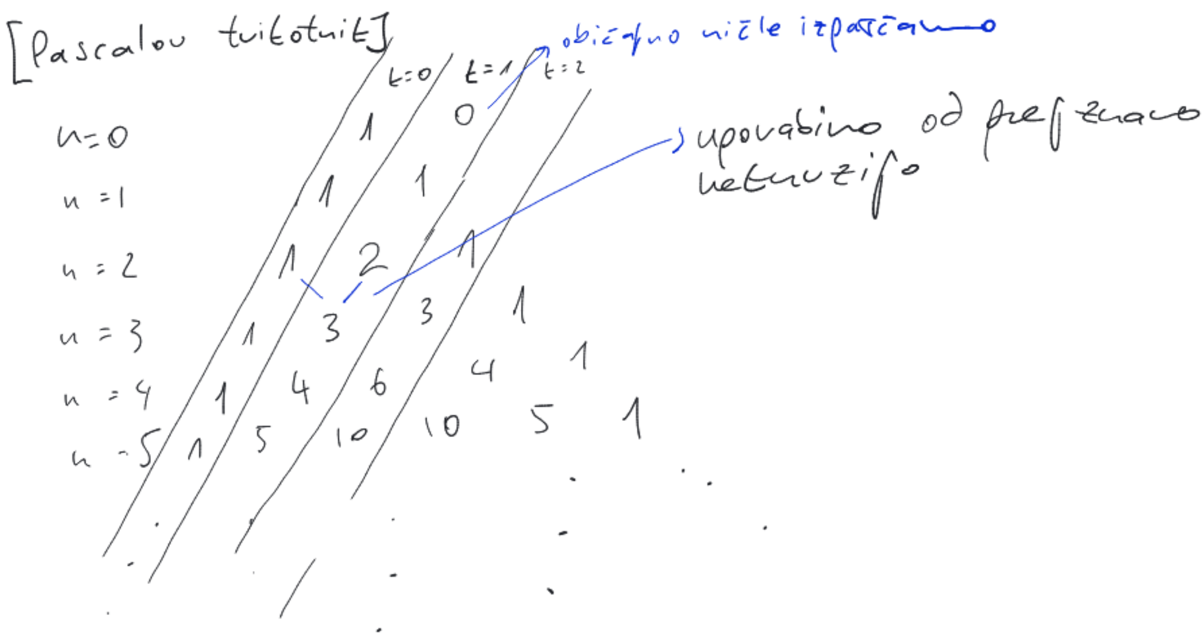
   (a) n je element te podmnožice. Takih je $\binom{n-1}{k-1}$.

[1] $k-$elementno podmnožico

(b) n ni element te podmnožice. Takih je $\binom{n-1}{k}$.

Formalno iščemo bijekcijo $\Phi : \binom{[n]}{k} \to \binom{[n-1]}{k-1} \cup \binom{[n-1]}{k}$. Predpis $\Phi(B) = B \backslash \{n\}$, $\Phi^{-1}(B) = \begin{cases} B \cup \{n\} & ; |B| = k-1 \\ B & ; |B| = k \end{cases}$

$\square$



Slika 1: Pascalov trikotnik

Pripomba.

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n \sim \bigcup_{k=0}^{n} \binom{[n]}{k} = 2^{[n]} \overset{\text{disjunktne}}{\Longrightarrow} \left| \bigcup_{k=0}^{n} \binom{[n]}{k} \right| = \left| 2^{[n]} \right|$$

Izrek. *Binomski izrek. Za a, b elementa komutativnega kolobarja (polja) in za $n \in \mathbb{N}$ velja*

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

Dokaz. Več načinov.

1. Induktivno. Baza $n = 0$: $1 = \binom{0}{0} a^0 b^0 = 1$. Korak $n-1 \to n$:

$$(a+b)^n = (a+b)^{n-1}(a+b) \overset{\text{I.P.}}{=} \left(\sum_{k=0}^{n-1} \binom{n-1}{k} a^{n-1-k} b^k \right)(a+b) = \sum_{k=0}^{n-1} \binom{n-1}{k} a^{n-k} b^k + \sum_{k=0}^{n-1} \binom{n-1}{k} a^{n-1-k} b^{k+1} =$$

... v desni vsoti naj bo $k' := k+1$ ...

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

... levo zgornjo mejo povečamo za 1, desno spodnjo zmanjšamo za 1, s čimer dodamo le dva ničelna člena. vezano spremenljivko k' preimenujemo v k ...

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

2. Enako kot prej, le da se ne utrujamo z mejami. Vse meje razširimo na vsa cela števila in s tem le dodamo neskončno ničelnih členov. Baza $n = 0$ velja kot prej. Korak $n-1 \to n$:

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

... zamaknemo $k \coloneqq k+1$ v desni vsoti ...

$$= \sum_k \binom{n-1}{k} a^{n-k} b^k + \sum_k \binom{n-1}{k-1} a^{n-k} b^k = \sum_k \left[\binom{n-1}{k} + \binom{n-1}{k-1} \right] a^{n-k} b^k = \sum_k \binom{n}{k} a^{n-k} b^k$$

3. Kombinatorično. $(a+b)^n = (a+b) \cdot \dots \cdot (a+b)$. Po distributivnosti je to vsota členov, ki so produkt enega člena iz prvega oklepaja, enega iz drugega, enega iz tretjega, itd. Če smo $k-$krat izbrali b, smo $n-k-$krat izbrali a (skupno imamo n izbir). Torej je vsak člen oblike $a^{n-k}b^k$, $0 \leq k \leq n$. Člen $a^{n-k}b^k$ dobimo na $\binom{n}{k}$ načinov, ker moramo izmed n oklepajev (faktorjev) izbrati tistih k, pri katerih vzamemo b.

$\square$

Posledica. $(1+x)^n = \sum_{k=0}^n \binom{n}{k} x^k$. *Za* $x = 1$*:* $2^n = \sum_{k=0}^n \binom{n}{k}$. *Za* $x = -1$*:* $0^n = \sum_{k=0}^n (-1)^k \binom{n}{k} = \delta_{n,0}$.

Definicija. Kronekerjeva delta. $\delta_{i,j} \coloneqq \begin{cases} 1 & ; i = j \\ 0 & ; i \neq j \end{cases}$

Trditev. $\forall n > 0 : \sum_{k \text{ sod}} \binom{n}{k} = \sum_{k \text{ lih}} \binom{n}{k}$ ZDB število lihih podmnožic neprazne končne množice A je enako številu sodih podmnožic A.

Dokaz. Izberemo in fiksiramo poljuben element $u \in A$. Bijekcija $\Phi(B) = \begin{cases} B \cup \{u\} & ; u \notin B \\ B \setminus \{u\} & ; u \in B \end{cases}$. $\square$

2.2 Izbori

Imamo n kroglic, k jih izberemo. Vprašamo se, ali je vrstni red pomemben in ali kroglice med izbirami vračamo v boben (nabor možnih kroglic za novo izbiro).

	s ponavljanjem	brez ponavljanja
vrstni red je pomemben — variacije	n^k	$n^{\underline{k}}$
vrstni red ni pomemben — kombinacije	$\binom{n+k-1}{k}$ — $1 \leq i_1 \leq i_2 \leq \dots \leq i_k \leq n$	$\binom{n}{k}$ — $1 \leq i_1 < i_2 < \dots < i_k \leq n$

Tabela 1: Izbori

Dokaz. Dokazujemo, da je kombinacij s ponavljanjem $\binom{n+k-1}{k}$. Iščemo število rešitev sistema $1 \leq i_1 \leq i_2 \leq \dots \leq i_k \leq n$. Naj bo $j_1 \coloneqq i_1$, $j_2 \coloneqq i_2 + 1$, $j_3 \coloneqq i_3 + 2$, $j_4 \coloneqq i_4 + 3$, ... $j_k \coloneqq i_k + k - 1$. Dobimo sistem $1 \leq j_1 < j_2 < \dots < j_k \leq n + k - 1$, ki ima enako rešitev kot prvotni sistem. Ta sistem pa ima $\binom{n+k-1}{k}$ rešitev (kombinacije brez ponavljanja). $\square$

Zgled. Primer za $n = 3$, $k = 3$: Kombinacije s ponavljanjem: 111, 112, 122, 123, 133, 222, 223, 233, 333. Kombinacije brez ponavljanja za $n \coloneqq n + k - 1 = 5$, $k \coloneqq k = 3$: 123, 124, 134, 135, 145, 234, 235, 245, 345.

2.3 Kompozicije

Definicija. Naj bo $n \in \mathbb{N}$. Pravimo, da je $(\lambda_1, \dots, \lambda_l) \in \mathbb{N}^l$ (vrstni red je pomemben), $\forall i \in [l] : \lambda_i \geq 1$, kjer $\sum_{i=1}^l \lambda_i = n$, kompozicija števila n. Pravimo, da je $(\lambda_1, \dots, \lambda_l) \in \mathbb{N}_0^l$ (vrstni red je pomemben), kjer $\sum_{i=1}^l \lambda_l = n$, šibka kompozicija števila n. $\lambda_1, \dots, \lambda_l$ so členi kompozicije, l je njena dolžina, n pa njena velikost.

Zgled. Vse kompozicije $n = 3$: $(3), (2,1), (1,2), (1,1,1)$, kajti $3 = 3 = 2+1 = 1+2 = 1+1+1$. Ena šibka kompozicija $n = 3$ (vseh je neskončno): $(2,0,0,0,1,0,0,0)$, kajti $3 = 2+0+0+0+1+0+0+0$.

Vprašanje. *Koliko je kompozicij za dan n?*

Izrek. *Število kompozicij* $n = 2^{n-1}$ *za* $n \geq 1$*. Število kompozicij* n *dolžine* $k = \binom{n-1}{k-1}$ *za* $n \geq 1, k \geq 1$*.*

Dokaz. Kompozicijo si predstavljajmo kot kroglice in pregrade: $4+2+2+3+1 \sim \circ\circ\circ\circ|\circ\circ|\circ\circ|\circ\circ\circ|\circ$. Kompozicija števila n: $n-1$ možnih pregrad $\simeq$ vsi dvojiški nizi dolžine $n-1 \Rightarrow 2^{n-1}$. Da bo k členov, moramo vstaviti (izbrati mesta za) $k-1$ pregrad: $\binom{n-1}{k-1}$ možnosti. $\square$

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

Dokaz. Več načinov.

1. Kroglice in pregrade. Ker so členi lahko ničelni, je lahko tudi več pregrad zapored brez kroglic vmes. Imamo torej $n+k-1$ „mest“. Na vsakem mestu je lahko bodisi kroglica bodisi pregrada. $k-1$ mest za pregrade izberemo na $\binom{n+k-1}{k-1}$ načinov. Kroglice so na preostalih mestih.

2. Iščemo število rešitev enačbe $x_1 + \cdots + x_k = n$ $(\forall i \in [k] : x_i \geq 0)$. Vzemimo $\forall i \in [k] : y_i := x_i + 1$. Sedaj je $y_i \geq 1$ in velja $y_1 + \cdots + y_k = n + k$. To pa so običajne kompozicije števila $n+k$ s k členi: $\binom{n+k-1}{k-1} = \binom{n+k-1}{n+k-1-(k-1)} = \binom{n+k-1}{n}$ rešitev.

3. Kombinatorično. Opazimo podobnost formule za število šibkih kompozicij in število kombinacij s ponavljanjem? x_i ponazarja, kolikokrat izberemo $i-$to kroglico: $x_i \in \{0..n\}$. k predstavlja število izbranih kroglic, n pa število različnih kroglic. Izmed k različnih kroglic izberemo n kroglic s ponavljanjem (vsako kroglico od 0 do $n-$krat).

□

2.4 Načelo vključitev in izključitev — NVI (angl. principle of inclusion and exclusion — PIE)

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

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

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

Izrek. *Naj bo $A_1, \ldots, A_n \subseteq A$ in $M = \{A_1, \ldots, A_n\}$. Za poljubno $I \subseteq [n]$ označimo $A_I := \bigcap_{i \in I} A_i$ (npr. $A_{\{2,4,8\}} = A_2 \cap A_4 \cap A_8$). Tedaj*

$$\left| \bigcup_{i=1}^{n} A_i \right| = |A_1| + \cdots |A_n| - |A_1 \cap A_2| - \cdots - |A_{n-1} \cap A_n| + |A_1 \cap A_2 \cap A_3| + \cdots$$

$$- |A_1 \cap A_2 \cap A_3 \cap A_4| + \cdots - \cdots + \cdots + (-1)^{n+1} |A_1 \cap \cdots \cap A_n| =$$

$$= \sum_{i=1}^{n} (-1)^{i-1} \sum_{1 \leq j_1 < \cdots < j_i \leq n} |A_{j_1} \cap A_{j_2} \cap \cdots \cap A_{j_i}| = \sum_{i=1}^{n} (-1)^{i-1} \sum_{X \in 2^M} \left| \begin{cases} \emptyset & ; |X| \neq i \\ \bigcap_{Y \in X} Y & ; \textit{sicer} \end{cases} \right| = \sum_{\emptyset \neq I \subseteq [n]} (-1)^{|I|-1} |A_I|$$

Dokaz. Naj bo $x \in \bigcup_{i=1}^{n} A_i$ poljuben. Denimo, da je x element natanko m (gotovo ≥ 1) množic izmed $A_1, \ldots, A_n$. Koliko je potem doprinos x k vsoti na desni?

$$m - \binom{m}{2} + \binom{m}{3} - \binom{m}{4} + \cdots = \binom{m}{1} - \binom{m}{2} + \binom{m}{3} - \binom{m}{4} + \cdots = -\binom{m}{0} + \left(\binom{m}{1} - \binom{m}{2} + \binom{m}{3} - \binom{m}{4} + \cdots \right) + \binom{m}{0} =$$

$$= -\binom{m}{0} - \left(-\binom{m}{1} + \binom{m}{2} - \binom{m}{3} + \binom{m}{4} - \cdots \right) + \binom{m}{0} = -\left(\binom{m}{0} - \binom{m}{1} + \binom{m}{2} - \binom{m}{3} + \binom{m}{4} - \cdots \right) + \binom{m}{0} =$$

Uporabimo dejstvo, da je število lihih podmnožic enako številu sodih.

$$= \cancel{-\left(\binom{m}{0} - \binom{m}{1} + \binom{m}{2} - \binom{m}{3} + \cdots \right)} + \overset{1}{\cancel{\binom{m}{0}}} = 1$$

Vsak element smo šteli natanko enkrat. □

Izrek. *NVI, druga verzija.*

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

Dokaz. Pri zadnjem enačaju uporabimo dejstvo, da je prazen presek univerzum ($A_\emptyset = A$).

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

□

Zgled. Naloge.

1. Preštej permutacije brez negibnih točk v S_n. $a_0 = 1$, $a_1 = 0$, $a_2 = 1$, $a_3 = 2 = |\{(132), (123)\}|$, $a_4 = 6 = |\{(1234), (1243), (1324), (1342), (1423), (1432)\}|$, ...

   Naj bo $A \coloneqq S_n$, $A_i \coloneqq \{\pi \in S_n; \pi(i) = i\}$ ZDB vse permutacije, kjer je i negibna točka. Iščemo torej $\bigcap_{i=1}^n A_i^{\mathcal{C}} = \{\pi \in S_n; \pi \text{ nima negibne točke}\}$. Izračunajmo moči presekov:

   $|A_i| = (n-1)!$, $|A_i \cap A_j| = (n-2)!$, ..., splošno: $|A_I| = (n - |I|)!$

$$a_n = \sum_{I \subseteq [n]} (-1)^{|I|} |A_I| = \sum_{I \subseteq [n]} (-1)^{|I|} (n - |I|)! =$$

   ... imamo odvisnost le od moči I, ne pa tudi od vsebine I. Moč i se ponovi $\binom{n}{i}$−krat ...

$$= \sum_{i=0}^{n} (-1)^i (n-i)! \binom{n}{i} = \sum_{i=0}^{n} (-1)^i \cancel{(n-i)!} \frac{n!}{i! \cancel{(n-i)!}} = n! \sum_{i=0}^{n} \frac{(-1)^i}{i!}$$

2. Kakšna je verjetnost, da je naključno izbrana permutacija brez negibne točke?

$$\lim_{n \to \infty} \frac{\cancel{n!} \sum_{i=0}^{n} \frac{(-1)^i}{i!}}{\cancel{n!}} = \lim_{n \to \infty} \sum_{i=0}^{n} \frac{(-1)^i}{i!} = e^{-1}$$

   Velja namreč $e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!}$.

3. Preštej surjekcije $[n] \to [k]$.

$$A \coloneqq [k]^{[n]}$$
$$\forall i \in k : A_i \coloneqq \{f : [n] \to [k]; \forall i \in \{1..n\} : f(j) \neq i\} = \{f : [n] \to [k] \setminus \{i\}\}$$
$$|A_i| = (k-1)^n$$
$$A_i \cap A_j = \{f : [n] \to [k] \setminus \{i, j\}\}$$
$$|A_i \cap A_j| = (k-2)^n$$
$$A_I = \{f : [n] \to [k] \setminus I\}$$
$$|A_I| = (k - |I|)^n$$

$$|\{f : [n] \to [k]; f \text{ surjekcija}\}| = \left| \bigcap_{i=1}^{k} A_i^{\mathcal{C}} \right| = \sum_{I \subseteq [k]} (-1)^{|I|} (k - |I|)^n = \sum_{i=0}^{k} (-1)^i (k-i)^n \binom{k}{i} \overset{j := k-i}{=} \sum_{j=0}^{k} (-1)^{k-j} j^n \binom{k}{j}$$

4. Koliko je surjekcij v množico z 2 elementoma? $k = 2$. $\delta_{n,0} - 2 + 2^n$. S tremi? $k = 3$. $-\delta_{n,0} + 3 - 3 \cdot 2^n + 3^n$

Definicija. Eulerjeva funkcija ϕ (angl. totient function). $\phi(n) = |\{i \in [n]; \gcd(i, n) = 1\}|$ ZDB št. elementov, ki so manjši ali enaki n in tuji n.

n	1	2	3	4	5	6	7	8	9	10	11	12
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4

Tabela 2: Eulerjeva funkcija ϕ

Pripomba. Za praštevilo p velja $\phi(p) = p - 1$, $\phi(p^2) = p^2 - p$, $\phi(p^k) = p^k - p^{k-1} = p^k \left(1 - \frac{1}{p}\right)$.

Trditev. $\sum_{d|n} \phi(d) = n$ (vsota slik s ϕ deliteljev n je n).

Dokaz. Oglejmo si $\frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \ldots, \frac{n}{n}$ in okrajšajmo, kolikor se le da. Primer: $\frac{1}{12}, \frac{2}{12}, \frac{3}{12}, \frac{4}{12}, \frac{5}{12}, \frac{6}{12}, \frac{7}{12}, \frac{8}{12}, \frac{9}{12}, \frac{10}{12}, \frac{11}{12}, \frac{12}{12} \to \frac{1}{12}, \frac{1}{6}, \frac{1}{4}, \frac{1}{3}, \frac{5}{12}, \frac{1}{2}, \frac{7}{12}, \frac{2}{3}, \frac{3}{4}, \frac{5}{6}, \frac{11}{12}, \frac{1}{1}$. Možni imenovalci so delitelji n, možnih števcev z imenovalcem d pa je $\phi(d)$. Če torej grupiramo te ulomke (skupaj jih je n — desna stran enačbe) po imenovalcih (deliteljih), bo pri vsakem delitelju $\phi(d)$ ulomkov (leva stran enačbe). □

Izrazimo $\phi(n)$. Naj bo $n = p_1^{\alpha_1} \cdot \cdots \cdot p_k^{\alpha_k}$ in $\forall i \in [k] : \alpha_i \geq 1$. $A = [n]$; $\forall i \in \{1..k\} : A_i :=$ $\{$večkratniki p_i v $[n]\}$. Presek komplementov so števila, tuja n. $|A_i| = \left\lfloor \frac{n}{p_i} \right\rfloor = \frac{n}{p_i}$ (kajti $p_i | n$), $|A_i \cap A_j| = \frac{n}{p_i \cdot p_j}$, $|A_I| = \frac{n}{\prod_{i \in I} p_i}$.

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

Primer za $k = 2$ (število n je produkt dveh praštevil):

$$\phi(n) = n \sum_{I \subseteq \{1,2\}} (-1)^{|I|} \prod_{i \in I} p_i^{-1} = n\left(1 - p_1^{-1} - p_2^{-1} + p_1^{-1} p_2^{-1}\right) = n\left(1 - p_1^{-1}\right)\left(1 - p_2^{-1}\right)$$

Primer za splošen k (po distributivnosti):

$$\phi(n) = n\left(1 - p_1^{-1}\right)\left(1 - p_2^{-1}\right) \cdots \left(1 - p_k^{-1}\right) = n \prod_{p | n \text{ praštevilski delitelji}} \left(1 - p^{-1}\right)$$

2.5 Multinomski koeficient in multinomski izrek

Vprašanje. *Denimo, da imamo multimnožico (množico, v kateri dovolimo ponavljanje elementov)* $M := \{1^{a_1}, 2^{a_2}, \ldots, n^{a_n}\}$ *($i-$ti element se ponovi a_i-krat). Primer:* $M = \{1,1,1,2,3,3\} = \{1^3, 2^1, 3^2\}$. *Koliko je permutacij multimnožice?*

Naj bo $N = \sum_{i=1}^n a_i$. Enice razporedimo na $\binom{N}{a_1}$ načinov, dvojke na $\binom{N-a_1}{a_2}$, trojke na $\binom{N-a_1-a_2}{a_3}$, itd. Skupaj je permutacij torej

$$\binom{N}{a_1}\binom{N-a_1}{a_2}\binom{N-a_1-a_2}{a_3}\cdots\binom{N-a_1-\cdots-a_{n-2}=a_{n-1}+a_n}{a_{n-1}} \cdot \cancelto{1}{\binom{N-a_1-\cdots-a_{n-1}=a_n}{a_n}} =$$

$$= \frac{(a_1+\cdots+a_n)!}{a_1!\cancel{(a_2+\cdots+a_n)!}} \cdot \frac{\cancel{(a_2+\cdots+a_n)!}}{a_2!\,(a_3+\cdots+a_n)!} \cdot \cdots \cdot \frac{(a_{n-1}+a_n)!}{a_{n-1}!\cancel{(a_n)!}} \cdot \frac{\cancel{(a_n)!}}{a_n!\cancelto{1}{0!}} = \frac{N!}{a_1} \cdot \frac{1}{a_2} \cdot \frac{1}{a_3} \cdot \cdots \cdot \frac{1}{1} = \frac{(a_1+\cdots+a_n)!}{a_1! \cdot a_2! \cdot \cdots \cdot a_n!} =: \binom{N}{a_1, \ldots, a_n}$$

Drug način razmišljanja (intuitiven): Ponavljajoče elemente sprva tretiramo kot različne ($N!$ načinov), nato pa delimo s fakultetami frekvenc posameznih unikatnih elementov, saj teh elementov nočemo razlikovati.

Pripomba.

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

Izrek. *Multinomski izrek. Kako razpisati multinom na $n-$to potenco:*

$$(x_1 + \cdots + x_k)^n = \sum_{i_1+\cdots+i_k=n; i_1,\ldots,i_k \geq 0 \text{ (šibke kompozicije } n \text{ dolžine } k)} \binom{n}{i_1, \ldots, i_k} x_1^{i_1} \cdots x_k^{i_k}$$

2.6 Načrti in $t-$načrti

Definicija. $S \subseteq X \times Y$ je relacija. Za $x \in X$ in $y \in Y$ velja $xSy \Leftrightarrow (x,y) \in S$. Za $x \in X$ označimo $v_x(S) := |\{y \in Y; xSy\}|$ (število kljukic v vrstici x). Za $y \in Y$ označimo $s_y(S) := |\{x \in X; xSy\}|$ (število kljukic v stolpcu y).

Velja $|S| = \sum_{x \in X} v_x(S) = \sum_{y \in Y} s_y(S)$. Kdaj se zgodi, da je $\forall x, x' \in X : v_x(S) = v_{x'}(S)$; tedaj označimo kar $v(S)$ in analogno za $s(S)$ in tedaj velja $\sum_{x \in X} v_x(S) = v(S)|X|$. Če to velja za stolpce in vrstice, velja $v(S) \cdot |X| = s(S) \cdot |Y|$.

Zgled. Dva primera.

1. Trianguilacija ravninskega grafa je ravninski graf in zanjo velja, da so vsa lica $3-$cikli. Za vsak ravninski graf je moč najti triangulacijo ravninskega grafa. Naj bo G triangulacija ravninskega grafa. Za relacijo $S = EG \times FG$ s predpisom $eSf \Leftrightarrow e \in f$ velja $\forall e, e' \in EG : v_e(S) = v_{e'}(S) = 2$ in $\forall f, f' \in FG : s_f(S) = s_{f'}(S) = 3$. Torej $v(S) = 2$ in $s(S) = 3$, sledi $3|F| = 2|E|$.

2. Koliko deliteljev ima v povprečju število n? Naj bo $S = [n] \times [n]$ s predpisom $xSy \Leftrightarrow x|y$. Velja $s_y(S) =$ število deliteljev y in $v_x(S) = \left\lfloor \frac{n}{x} \right\rfloor$. $\sum_{i=1}^n \left\lfloor \frac{n}{i} \right\rfloor = \sum_{j=1}^n$št. del. j. Koliko je povprečje?

$$\frac{1}{n} \sum_{j=1}^n \#\text{del.} j \overset{\text{asimptotsko enako}}{\sim} \frac{1}{\cancel{n}} \sum_{i=1}^n \frac{\cancel{n}}{i} = \sum_{i=1}^n \frac{1}{i} = H_n = n - \text{to harmonično število}$$

$$\lim_{n \to \infty} H_n = \ln(n)$$

Motivacija za načrte Podjetje ima izdelek v več različicah in ga testira na več potrošnikih. Zahteve:

1. hočemo, da vsak potrošnik testira enako različic.
2. hočemo, da je vsaka različica enakokrat testirana.

Temu pravimo načrt. Sledi formalnejša definicija, kjer je število potrošnikov b, število različic v, k število različic na potrošnika, λ pa število potrošnikov na različico.

Definicija. $B = \{B_1, \ldots, B_b\}$ je načrt s parametri (v, k, λ), če velja $B_1, \ldots, B_b \subseteq [v]$, $\forall i \in [b] : |B_i| = k$, $\forall i \in [v] \, \exists$ natanko λ množic, v katerih je i vsebovan.

Če si predstavljamo relacijo $S \subseteq [v] \times B$ s predpisom $iSB_j \Leftrightarrow i \in B_j$, zanjo velja $v(S) = \lambda$ in $s(S) = k$, torej $v \cdot \lambda = k \cdot b$.

Pripomba. Potreben pogoj za načrt je, da je $v \cdot \lambda = k \cdot b$, da $k | v \cdot \lambda$ in da $b \leq \binom{v}{k} \implies \frac{v\lambda}{k} \leq \binom{v}{k} = \frac{v!}{k!(v-k)!} \Rightarrow \lambda \leq \frac{\cancel{k}\,\cancelto{(v-1)!}{v!}}{\cancelto{(k-1)!}{k!}\,\cancel{v}\,(v-k)!} = \binom{v-1}{k-1}$ (število $k-$elementnih podmnožic $[v]$, ki vsebujejo i)

Izrek. *Načrt s parametri* $(v, k, \lambda) \, \exists \Leftrightarrow \lambda \leq \binom{v-1}{k-1} \wedge k | v\lambda$.

Dokaz. Dokazujemo ekvivalenco.

($\Rightarrow$) Že dokazano v zgornji opombi (potreben pogoj).

($\Leftarrow$) Po predpostavki $\lambda \leq \binom{v-1}{k-1} \wedge k | v\lambda$. Npr. $v = 8, k = 4, \lambda = 3$ ustreza $4 | 8 \cdot 3$ in $3 \leq \binom{7}{3} = 35$.

Izberimo poljubnih b različnih $k-$podmnožic $[v]$. To lahko storimo, ker je $b = \frac{v\lambda}{k} \leq \frac{v}{k}\binom{v-1}{k-1} = \binom{v}{k}$.

Vzamemo npr. 1234, 1356, 1567, 1568, 2356, 3457. Z λ_i označimo, v koliko blokih je i. Tedaj $\lambda_1 = 4$, $\lambda_2 = 2$, $\lambda_3 = 4$, $\lambda_4 = 2$, $\lambda_5 = 5$, $\lambda_6 = 4$, $\lambda_7 = 2$, $\lambda_8 = 1$. To ni načrt.

k kljukic že je v vsakem stolpcu, a v vsaki vrstici ni enako kljukic (v $i-$ti jih je λ_i). Velja $\sum_{i=1}^{v} \lambda_i = k \cdot b = \lambda v \implies \frac{\sum_{i=1}^{v} \lambda_i}{v} = \overline{\lambda_i} = \lambda$. Če $\forall i \in [v] : \lambda_i = \lambda$, imamo načrt in smo končali, sicer vzamemo i in j, da $\lambda_i < \lambda < \lambda_j$ (gotovo $\exists$ zaradi razmisleka o povprečju).

Bloki so štirih disjunktnih tipov: $I : i, j \in B$, $II : i \notin B, j \in B$, $III : i \in B, j \notin B$, $IV : i \notin B, j \notin B$. Velja $\lambda_i = |I| + |III|$, $\lambda_j = |I| + |II|$. Vemo $\lambda_i < \lambda_j \Rightarrow |III| < |II| \Rightarrow$ gotovo $\exists$ vsak en blok tipa II.

Treba je še dokazati, da obstaja blok tipa II, kjer pri menjavi elementa j z elementom i dobimo blok, ki še ne obstaja. Vemo, da je blokov tipa II gotovo več od blokov tipa III. Po naši menjavi dobimo iz bloka II blok III. Ker je blokov tipa II več od blokov tipa III, $\exists$ blok tipa II, da ob menjavi dobimo nov blok tipa III, ki še ni med poprejšnjimi bloki — je nov.

Zakaj se algoritem ustavi? $\sum_{i=1}^{v} |\lambda_i - \lambda|$ je na vsakem koraku za 2 manjša. Ko je vsota enaka 1 (nedosegljivo stanje, kajti tedaj $\overline{\lambda_i} \neq \lambda$) ali 0, se ustavimo in imamo načrt.

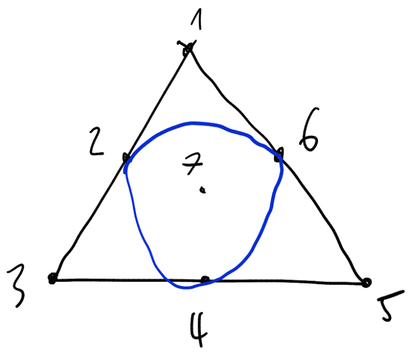
$\square$

Definicija. $t-$načrt. $B = \{B_1, \ldots, B_b\}$ je $t-$načrt s parametri (v, k, λ_t) ,če se ne le vsak element pojavi $t-$krat, temveč se celo vsaka $t-$elementna podmnožica $[v]$ pojavi natanko $t-$krat ZDB B je načrt in $\forall A \subseteq [v], |A| = t : A \subseteq B_j$ za natanko λ_t indeksov j.

Pripomba. Načrt je isto kot $1-$načrt. $t-$načrt je posplošitev načrta.

Zgled. Primeri.

1. Fanova ravnina.



Slika 2: Fanova ravnina za $v = 7$

Zapiši vse točke, ki ležijo na isti premici, kjer je moder krog tudi premica. 123, 156, 147, 257, 345, 362, 264. To je načrt in hkrati $2-$načrt s parametri $v = 7$, $k = 3$, $\lambda_1 = 3$, $\lambda_2 = 1$.

2. $3-$načrt s parametri $(8, 4, 1)$: 1235, 1248, 1267, 1346, 1378, 1457, 1568, 2347, 2368, 2456, 2578, 3458, 3567, 4678. To je tudi $2-$načrt s parametri $(8, 4, 3)$ in tudi načrt s parametri $(8, 4, 7)$. Ni pa $4-$načrt ($\{1, 2, 3, 4\}$ ni v nobenem bloku).

Izrek. *Če je B $t-$načrt s parametri (v, k, λ_t), je tudi $(t-1)-$načrt s paramatri (v, k, λ_{t-1}), kjer je $\lambda_{t-1} = \lambda_t \cdot \frac{v-(t-1)}{k-(t-1)}$.*

Dokaz. Naj bo $S \subseteq [v]$, $|S| = t-1$, $\lambda_S :=$ v koliko blokih je S vsebovana. Naj bo $R \subseteq [v] \times B$ relacija s predpisom $iRB_j \Leftrightarrow i \notin S \wedge S \cup \{i\} \subseteq B_j$. Razlaga: S je $t-1$ elementna množica, $S \cup \{i\}$ za $i \notin S$ je $t-$elementna množica. Zanjo po predpostavki vemo, da je v λ_t blokih.

V vrstici je za dani i 0 kljukic, če $i \in S$, sicer (če $i \notin S$) pa λ_t kljukic. Vrstic s kljukicami je $v - (t-1)$. Vseh vrstic je v, v $t-1$ vrsticah velja, da je $x \in S$. Torej je skupaj kljukic $\lambda_t (v - (t-1))$, če preštejemo po vrsticah.

V stolpcu je za dani B_j 0 kljukic, če $S \not\subseteq B_j$, sicer (če $S \subseteq B$), bo iRB_j, če je $i \notin S$ in $i \subseteq B_j$. V B_j je k elementov, v S jih je $t-1$, torej je v vsakem stolpcu $k - (t-1)$ kljukic. Stolpcev s kljukicami je λ_s $(S \subseteq B_j)$. Torej je skupaj kljukic $(k - (t-1)) \lambda_s$, če preštejemo po stolpcih.

$$\lambda_t (v - (t-1)) = (k - (t-1)) \lambda_s$$
$$\frac{\lambda_t (v - (t-1))}{(k - (t-1))} = \lambda_s$$
$$\lambda_{t-1} := \lambda_s$$

□

3 Permutacije, razdelitve, razčlenitve

3.1 Stirlingova števila 1. vrste

Definicija. $c(n, k) =$ število permutacij n elementov, ki imajo k ciklov.

Zgled. $c(3, 1) = 2$, $c(3, 2) = 3$, $c(3, 3) = 1$, $c(4, 2) = 4 \cdot 2 + 3 = 11$, $c(n, n) = 1$, $c(n, n-1) = \binom{n}{2}$, $c(n, 1) = (n-1)!$, $c(n, 0) = \delta_{0,n}$, $\sum_k c(n, k) = n!$ (vse permutacije n elementov).

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

Dokaz. Permutacije v S_n s k cikli ločimo na:

- take, ki vsebujejo cikel (n) (n je negibna točka): teh je $c(n-1, k-1)$
- take, ki ne vsebujejo cikla (n): teh je $c(n-1, k) \cdot (n-1)$. Če n odstranimo, se število ciklov ne spremeni, vendar ga ne moremo vstaviti nazaj enolično, temveč na $n-1$ načinov.

n\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	35	10	1

Tabela 3: Tabela Stirlingovih števil prve vrste.

□

Izrek. $\sum_{k=0}^{n} c(n, k) x^k = x^{\overline{n}}$

Zgled. $n = 3$: $2x^1 + 3x^2 + 1x^3 = x\left(x^2 + 3x + 2\right) = x(x+1)(x+2)$

Dokaz. Indukcija po $n \in \mathbb{N}_0$. Baza $n = 0$: $1 = 1$. Korak $n - 1 \to n$:

$$x^{\overline{n}} = x^{\overline{n-1}} (x + n - 1) \overset{\text{I. P.}}{=} \sum_{k=0}^{n-1} c(n-1,k)\, x^k (x+n-1) = \sum_k c(n-1,k)\, x^{k+1} + \sum_k (n-1)\, c(n-1,k)\, x^k =$$

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

□

Zgled. $x = 1$: število permutacij z vsemi števili ciklov $= \sum_k c(n,k) = x^{\overline{n}} = 1^{\overline{n}} = n! =$ vse permutacije.

3.2 Stirlingova števila 2. vrste in Bellova števila

Definicija. Razdelitev ali razbitje (ali particija) (angl. set partition) množice A je množica množic (pravimo jim bloki) $\{B_1, \ldots, B_k\}$, da velja:

- $\forall i \in [k] : B_i \neq \emptyset$
- $\forall i, k \in [k] : i \neq j \Rightarrow B_i \cap B_j = \emptyset$
- $\bigcup_{i=1}^{k} B_i = A$

Definicija. Stirlingovo število druge vrste $S(n,k)$ je število razdelitev množice $[n]$ s k bloki. Bellovo število $B(n)$ je število vseh razdelitev $[n]$.

Zgled. $S(4,2) = 7$; $\{1,2,3,4\}$ razdelimo na $\{\{\_\}, \{\_,\_,\_\}\}$ ×4, $\{\{\_,\_\}, \{\_,\_\}\}$ ×3 (fiksiramo enko v prvi blok, imamo še tri izbire za njeno sosedo, v drugem bloku so nato enolično določeni elementi)

n	$B(n)$
1	1
2	2
3	5
4	$S(4,1) + S(4,2) + S(4,3) + S(4,4) = 1 + 7 + 6 + 1 = 15$

Tabela 4: Bellova števila

Pripomba. $S(n,0) = \delta_{0,n}$, $S(n,n) = 1$, $B(n) = \sum_k S(n,k)$, $S(n,n-1) = \binom{n}{2}$

Trditev. Rekurzivna zveza. $S(n,k) = S(n-1,k-1) + k \cdot S(n-1,k)$, $B(n+1) = \sum_{k=0}^{n} \binom{n}{k} B(k)$

Zgled. $B(4) = \binom{3}{0} B(0) + \binom{3}{1} B(1) + \binom{3}{2} B(2) + \binom{3}{3} B(3) = 1 \cdot 1 + 3 \cdot 1 + 3 \cdot 2 + 1 \cdot 5 = 15$

Dokaz. Ločimo vse razdelitve $[n]$ s k bloki na dve disjunktni podmnožici:

- $\{n\}$ je blok: takih je $S(n-1,k-1)$
- $\{n\}$ ni blok: takih je $S(n-1,k) \cdot k$ — $\cdot k$ ker lahko v razdelitev $[n-1]$ na k blokov n vstavimo na k načinov (v enega izmed k blokov)

Vse razdelitve $[n+1]$ — Bellova števila: Naj bo $n+1$ v bloku s še k elementi, $0 \leq k \leq n$. Tedaj

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

... za rekurzijo si oglejmo razdelitve brez bloka z $n+1$. $\binom{n}{k}$ predstavlja izbiro elementov, ki so še skupaj z n ...

$$= \sum_{k=0}^{n} \binom{n}{k} B(n-k) \overset{\text{štejmo v drugo smer}}{=} \sum_{k=0}^{n} \binom{n}{n-k} B(k) = \sum_{k=0}^{n} \binom{n}{k} B(k)$$

$n\backslash k$	0	1	2	3	4	5	$B(n)$ (vsota po vrstici)
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

Tabela 5: Stirlingova števila druge vrste

□

To nas spomni na ekvivalenčne razrede.

Definicija. Ekvivalenčna relacija je refleksivna ($x \sim x$), simetrična ($x \sim y \Rightarrow y \sim x$) in tranzitivna ($x \sim y \wedge y \sim z \Rightarrow x \sim z$).

Pripomba. Množica razpade na ekvivalenčne razrede, ki tvorijo razdelitev. $S(n,k)$ je število ekvivalenčnih relacij na $[n]$ s k ekvivalenčnimi razredi. $B(n)$ je število ekvivalenčnih relacij na $[n]$.

Za surjekcijo $f : [n] \to [k]$ velja $\forall i \in [k] : f^{-1}(i) \neq \emptyset$ (praslika je neprazna množica). Ker je f funkcija, velja $\forall i, j \in [k] : i \neq j \Rightarrow f^{-1}(i) \cap f^{-1}(i) = \emptyset$ in $\bigcup_{i=1}^{k} f^{-1}(i) = [n]$. Surjekcija pa vseeno ni isto kot razdelitev — pomemben je vrstni red blokov.

Vprašanje. *Koliko surjekcij je iz $[n]$ v $[k]$? Odgovor: $S(n,k) \cdot k!$ — Surjekcija je razdelitev z vrstnim redom blokov. Koliko je $[4] \to [2]$ surjekcij? Odgovor: $S(4,2) \cdot 2! = 7 \cdot 2 = 14$*

Definicija. Premestitve so permutacije brez negibne točke.

Posledica. *Od prej se spomnimo, da je število surjekcij iz $[n]$ v $[k]$ enako $\sum_{j=0}^{k} (-1)^{k-j} \binom{k}{j} j^n$. Posledično je $S(n,k) = \sum_{j=0}^{k} \frac{(-1)^{k-j} j^n}{j!(k-j)!}$.*

Zgled.

$$S(n,2) = \frac{2^n}{2} - \frac{1}{1} + \frac{\delta_{0,n}}{2! \cdot 0!} = 2^{n-1} - 1 + \frac{\delta_{n,0}}{2}$$

Razdelimo n elementov v 2 bloka. Fiksirajmo 1 v prvi blok, za vsak preostali ($n-1$ jih ostane) element pa imamo dvojiški enum, ki pove, v katerem bloku je. -1 zato, ker mora biti drugi blok neprazen in izločimo opcijo, kjer so vsi dvojiški enumi enaki 0, $\delta_{n,0}$ zato, da popravimo primer, ko je $n = 0$.

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

Zgled. $n = 3$: $\sum_k S(3,k) x^{\underline{k}} = x + 3x(x-1) + x(x-1)(x-2) = x\left(1 \cancel{+3x} - 3 + x^2 \cancel{-3x} + 2\right) = x\left(\cancel{1-3} + x^2 \cancel{+2}\right) = x^3$

Dokaz. Več načinov.

- Indukcija

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

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

$$= \sum_k \left(S(n-1,k-1) + S(n-1,k) k\right) x^{\underline{k}} = \sum_k S(n,k) x^{\underline{k}}$$

- Kombinatorično: x^n: štetje
  - nizov dolžine n z elementi iz $[x]$
  - preslikav iz $[n]$ v $[x] = \left|[x]^{[n]}\right|$. Vsaka preslikava je surjekcija na svojo sliko. Oglejmo si vse slike $T \subseteq [x]$:

$$x^n = \left|[x]^{[n]}\right| = \sum_{T \subseteq [x]} |T|! \cdot S(n, |T|) \overset{\text{po močeh } |T|}{=} \sum_k k! \cdot S(n,k) \binom{x}{k} \overset{\binom{x}{k} = \frac{x^{\underline{k}}}{k!}}{=} \sum_k S(n,k) x^{\underline{k}}$$

Dokaz je veljaven za $x \in \mathbb{N}_0$. Da dokažemo, da sta dva polinoma stopnje $\leq n$ enaka, je dovolj preveriti ujemanje v $n+1$ različnih točkah, kajti razlika je polinom stopnje $\leq n$, če ni ničeln ima $\leq n$ ničel, kar je v neskladju s tem, da se polinoma ujemata v $n+1$ točkah (v ničlah se ne). Imamo polinoma stopnje n, ki se ujemata v ∞ točkah, torej sta enaka. Torej je dokaz veljaven tudi za realna števila.

□

3.3 Lahova števila

Imenujejo se po slovenskem aktuarju Ivu Lahu.

Definicija. $L(n,k)$ je število razdelitev $[n]$ na k linearno urejenih blokov. $\{152, 3674\} = \{3674, 152\}$, toda $\{152, 3674\} \neq \{125, 3764\}$. Vrstni red znotraj bloka je pomemben, ni pa pomemben vrstni red blokov.

Zgled. $L(4,2)$: $\{(\_), (\_, \_, \_)\}$ $\times 4 \cdot 3!$, $\{(\_, \_), (\_, \_)\}$ $\times 3 \cdot 2! \cdot 2!$ (enka v prvem bloku, vrstni red v 1. bloku, vrstni red v 2. bloku) $\Longrightarrow 24 + 12 = 36 = L(4,2)$.

Trditev. Rekurzivna zveza za Lahova števila: $L(n,k) = L(n-1,k-1) + L(n-1,k) \cdot (n-1+k)$

Dokaz. Ločimo razdelitve $[n]$ na k linearno urejenih blokov v dve disjunktni podmnožici:

- (n) je blok: takih je $L(n-1,k-1)$
- (n) ni blok: takih je $L(n-1,k) \cdot (n-1+k)$ — n lahko vstavimo nazaj bodisi za nek element ($n-1$ opcij) ali na začetek enega izmed blokov (k opcij)

□

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

Zgled. $L(4,2) = \frac{4!}{2!}\binom{3}{1} = 36$, $L(n,n) = 1$, $L(n,1) = n!$, $L(n,n-1) = n(n-1)$

Dokaz. Preštejmo urejene razdelitve na linearno urejene bloke na dva načina:
uredimo bloke in množimo z razdelitvami $= k! \cdot L(n,k) = n!\binom{n-1}{k-1}$ = permutacije množimo s kompozicijami (pregrade)

□

Izrek.

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

Dokaz. Induktivni. Baza $n = 0$. Korak $n-1 \to n$:

$$x^{\overline{n}} = x^{\overline{n-1}}(x+n-1) = \left(\sum_k L(n-1,k)\, x^{\underline{k}}\right) \cdot (x+n-1 = (x-k) + (n+k-1)) =$$

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

$$= \sum_k \left(L(n-1,k-1) + L(n-1,k)(n+k-1)\right) x^{\underline{k}} = \sum_k L(n,k)\, x^{\underline{k}}$$

□

Pripomba. Povzetek. Rekurzije:

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

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

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

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

Polinomske zveze:

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

Če namesto x vstavimo $-x$:

$$\sum_k c\left(n,k\right)\left(-x\right)^k = \sum_k c\left(n,k\right)\left(-1\right)^k x^k = \left(-x\right)^{\overline{n}} = \left(-x\right)\left(-x+1\right)\cdots\left(-x+n-1\right) \overset{\text{izpostavimo } -1}{=} \left(-1\right)^n x^{\underline{n}}$$

Če to zvezo pomnožimo z $\left(-1\right)^n$:

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

In podobno za Stirlingova števila druge vrste:

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

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

In Lahova:

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

$$\sum_k \left(-1\right)^{n-k} L\left(n,k\right) x^{\overline{k}} = x^{\underline{n}}$$

Velja neenakost — očitno zaradi (ne)upoštevanja vrstnega reda:

$$S\left(n,k\right) \leq c\left(n,k\right) \leq L\left(n,k\right)$$

Operacije v algebri seštevanje, množenje, množenje s skalarjem.

seštevanje+množenje nam dasta kolobar, seštevanje in množenje s skalarjem vektorski prostor, vse troje pa (komutativno) algebro.

Zgled. $m \times m$ matrike so nekomutativne algebre.

Zgled. $\mathbb{R}\left[x\right]$ je neskončnorazsežen vektorski prostor. Ena baza je $\left\{1, x, x^2, \dots\right\}$, spet druga je $\left\{1, x, x^{\underline{2}}, x^{\underline{3}}, \dots\right\}$, še ena je $\left\{1, x, x^{\overline{2}}, x^{\overline{3}}, \dots\right\}$.

Pripomba. Naših šest polinomskih zvez nam daje prehodne matrike med temi bazami.

Definicija. $\left(-1\right)^{n-k} c\left(n,k\right) =: s\left(n,k\right)$ (predznačeno Stirlingovo število prve vrste).

3.4 Razčlenitve in eulerjev petkotniški izrek

Definicija. Razčlenitev (angl. integer partition) $n \in \mathbb{N}_0$ je zaporedje $\lambda_1, \dots, \lambda_l$; $\forall i \in [l] : \lambda_l > 0$, $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_l$, $\lambda_1 + \cdots + \lambda_l = n$. Dodaten pogoj za razliko od kompozicij je linearna urejenost zaporedja (vrstni red ni pomemben). λ_i so členi razčlenitve, l je njena dolžina in n njena velikost. S $p_k\left(n\right)$ označimo število razčlenitev n dolžine k, s $\overline{p_k}\left(n\right)$ označimo število razčlenitev dolžine $\leq k$, s $p\left(n\right)$ pa število razčlenitev n (vseh dolžin).

Zgled. Razčlenitev števila $10 = 4+2+2+1+1$: $(4,2,2,1,1)$. Še ena: $(5,3,1,1)$.

Razčlenitve lahko predstavimo grafično z Youngovim ali Ferrersovim diagramom:

$$\begin{array}{ccccc}
 & 5 & 3 & 1 & 1 \\
4 & \circ & \circ & \circ & \circ \\
2 & \circ & \circ & & \\
2 & \circ & \circ & & \\
1 & \circ & & & \\
1 & \circ & & &
\end{array}$$

Slika 3: Ferrersov diagram ene razčlenitve števila 10.

Definicija. Če je λ razčlenitev, je λ' konjugirana razčlenitev. $(4,2,2,1,1)' = (5,3,1,1)$ ZDB pet členov je ≥ 1, trije členi so ≥ 2, en člen je ≥ 3 in en člen je ≥ 4 v originalni razčlenitvi. Predstavljamo si lahko kot transponiranje Ferrersovega diagrama.

Dejstvo. *Velja* $\lambda'' = \lambda$. *Velja* $\lambda'_i = |\{j; \lambda_j \geq i\}| = \max\{j : \lambda_j \geq i\}$. *Velja* $|\lambda'| = |\lambda|$ *(velikost se ohrani),* $l(\lambda') = \lambda_1$ *(velikost),* $\lambda'_1 = l(\lambda)$.

Trditev 1. $p_k(n) = \overline{p_k}(n-k)$ ZDB razčlenitev n s k členi je toliko, kolikor je razčlenitev $n-k$ z največ k členi.

Dokaz. V desno: Odstranimo prvi stolpec Ferrersovega diagrama in pregledamo preostale razčlenitve. Te imajo velikost $n-k$. Največ zato, ker je drugi stolpec lahko manjši od prvega. V levo: Dodamo en stolpec na levo s k kvadratki. □

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

Dokaz. Oglejmo si razčlenitve n dolžine k.

- Takih, kjer je zadnji člen $\lambda_l = 1$ (ZDB je drugi stolpec Ferrersovega diagrama manjši od prvega), je $p_{k-1}(n-1)$ — odstranimo zadnji člen.
- Takih, kjer je zadnji člen $\lambda_l \geq 2$ (ZDB je drugi stolpec Ferrersovega diagrama enako velik kot prvi), je $p_k(n-k)$ — od vseh členov odštejemo 1.

□

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

Dokaz. $\overline{p_k}(n) \overset{\text{očitno}}{=} p_k(n) + \overline{p_{k-1}}(n) \overset{\text{trditev 1}}{=} \overline{p_k}(n-k) + \overline{p_{k-1}}(n)$ □

Pripomba. Ti dve rekurziji sta precej drugačni kot za kombinacije, Stirlingova števila obeh vrst in Lahova števila. Tam smo namreč vselej argumente manjšali za največ 1, tu pa argument manjšamo za k.

Kaj pa rekurzija za $p(n)$? Uporabimo načelo vključitev in izključitev:

$$A = \{\text{razčlenitve števila } n\}$$

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

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

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

Opomba: $\forall a < 0 : p(a) = 0$

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

$$p_n = |A| = |\cup_{i=1}^n A_i| = \sum_{\emptyset \neq I \subseteq [n]} (-1)^{|I|+1} |A_I| =$$

$$= p(n-1) + p(n-2) \cancel{+p(n-3)} + \cdots + p(0) \cancel{-p(n-1-2)} - p(n-1-3) - \cdots +$$

$$+p(n-1-2-3) + p(n-1-2-4) + \cdots - \cdots + \cdots - \cdots =$$

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

Zaenkrat smo videli le koeficiente $\{-1, 0, 1\}$. A je to res? Izkazalo se bo, da ja. Oglejmo si en člen oziroma kako pridemo do koeficienta pred njim:

$$-p(n-7) = p(n-7) - p(n-1-6) - p(n-2-5) - p(n-3-4) + p(n-1-2-4)$$

Opazimo, da torej velja slednje. Označimo $\alpha(m) :=$ število razčlenitev m z liho mnogo **različnimi**[2] členi (v zgornjem primeru za $m = 7$ bodo to $\{\{7\}, \{1, 2, 4\}\}$) in $\beta(m) :=$ število razčlenitev m s sodo mnogo **različnimi** členi (v zgornjem primeru za $m = 7$ bodo to $\{\{1, 6\}, \{2, 5\}, \{3, 4\}\}$):

$$p(n) = \sum_{m=1}^{\infty} (\alpha(m) - \beta(m))\, p(n-m)$$

Sedaj vpeljimo tole lemo ...

Lema. $\alpha(m) - \beta(m) = \begin{cases} (-1)^{k-1} & ; m = \frac{k(3k \pm 1)}{2} \quad \text{za } k, m \in \mathbb{N} \\ 0 & ; \text{sicer} \end{cases}$.

[2] razčlenitev ima v splošnem lahko večkrat isti člen

... in nadaljujmo z izpeljavo rekurzije (spodnji izraz je Eulerjev petkoniški izrek):

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

Zgled. $p(8) = p(7) + p(6) - p(3) - p(1)$.

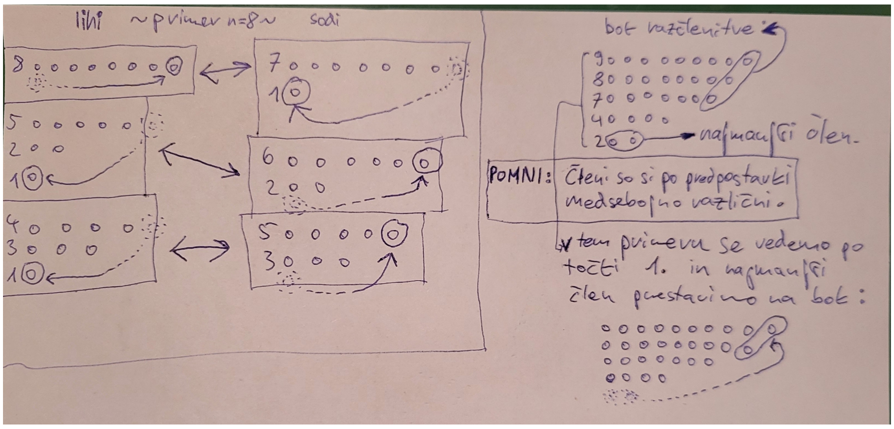
Dokaz. Dokaz leme. Iščemo „skoraj bijekcijo“ med množico razčlenitev m z liho različnimi členi in množico razčlenitev m s sodo različnimi členi. Zakaj „skoraj“? Ker seveda bijekcije ne pričakujemo za vse m, le za nekatere. Za nekatere m pričakujemo, da se bosta množici razlikovali po moči za 1.

Oglejmo si primer za $m = 8$. Razčlenitve 8 z liho mnogo različnimi členi so $8, 521, 431$, razčlenitve 8 s sodo mnogo različnimi členi so $71, 62, 53$ (enako jih je) (glej skico).

Definirajmo bok razčlenitve $b(\lambda) := \max\{i; \lambda_i = \lambda_1 - i + 1\}$ (ZDB število členov na začetku, ki se manjšajo za natanko 1[3]) in najmanjši člen razčlenitve $s(\lambda) := \lambda_{l(\lambda)}$.

Ločimo dve možnosti:

1. $s(\lambda) \leq b(\lambda)$. V tem primeru naša „skoraj bijekcija“ premakne najmanjši člen na bok.
2. $s(\lambda) > b(\lambda)$. V tem primeru bok postane najmanjši člen.



Slika 4: Skica „skoraj bijekcije“ in primera $m = 8$

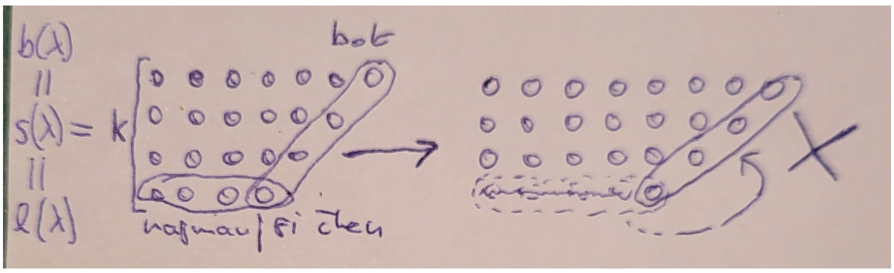
Ta naša „skoraj bijekcija“ na prvi pogled na primeru res ohranja zaprtost: slikamo razčlenitev z različnimi členi v razčlenitev z različnimi členi in iz take s sodimi členi napravimo tako z lihimi členi.

Toda najdena „skoraj bijekcija“ ne deluje, kadar:

1. $s(\lambda) = b(\lambda) = l(\lambda)$. Taka razčlenitev je oblike $k, k+1, k+2, \ldots, 2k-1$, torej

$$m = \frac{(2k-1)\cdot 2k}{2} - \frac{(k-1)k}{2} = \frac{k}{2}(4k - 2 - k + 1) = \frac{k(3k-1)}{2}.$$

Tu smo za seštevanje uporabili znano vrsto $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

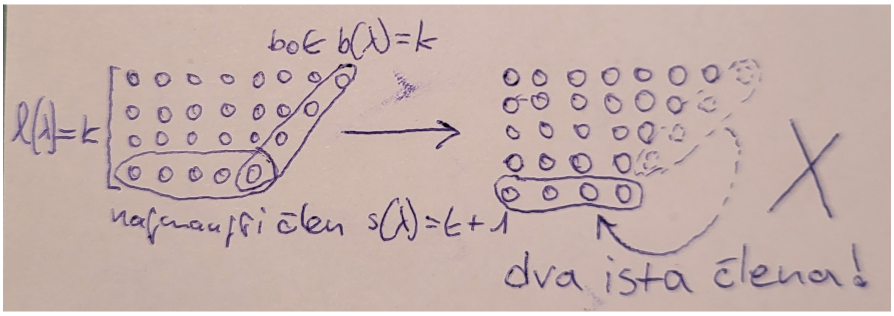


Slika 5: Skica tipa razčlenitve 1, kjer „skoraj bijekcija“ ne deluje.

[3] za 0 se ne morejo manjšati, ker so medsebojno različni, lahko pa je na neki točki med zaporednima členoma več kot 1 razlike

2. $b(\lambda) = l(\lambda) = s(\lambda) - 1$. Taka razčlenitev je oblike $k+1, k+2, k+3, \ldots, 2k$, torej

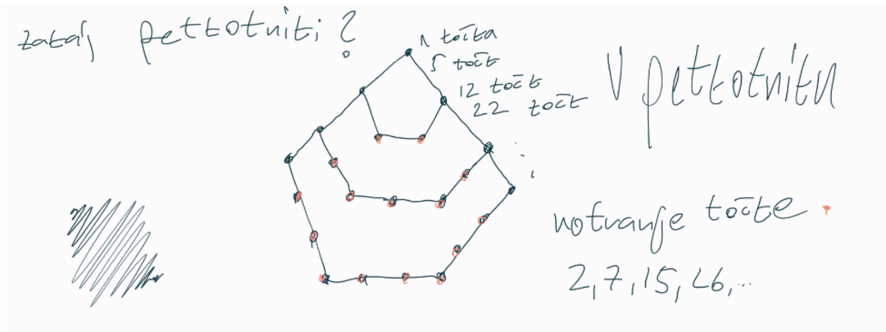
$$m = \frac{2k(2k+1)}{2} - \frac{k(k+1)}{2} = \frac{k}{2}(4k+2-k-1) = \frac{k(3k+1)}{2}.$$



Slika 6: Skica tipa razčlenitve 2, kjer „skoraj bijekcija“ ne deluje.

Torej, če $m \neq \frac{k(3k\pm1)}{2}$, imamo bijekcijo in $\alpha(m) - \beta(m) = 0$. Če $m = \frac{k(3k\pm1)}{2}$ dobimo bijekcijo, če odstranimo to posebno obliko, ki povzroča napako. Ta posebna oblika ima k členov. Če je v takem primeru k lih, imamo $\alpha(m) - \beta(m) = 1$, če je k sod, imamo $\alpha(m) - \beta(m) = -1$.

Zakaj se to imenuje petkotniški izrek?



Slika 7: Zakaj **petkotniški** izrek?

In ravno

$$\left(\frac{k(3k+1)}{2}\right)_{k\in\mathbb{N}} = 2, 7, 15, 26, \ldots \text{ nam da notranje točke petkotnikov}$$

$$\left(\frac{k(3k-1)}{2}\right)_{k\in\mathbb{N}} = 1, 5, 12, 22, \ldots \text{ nam da robne točke petkotnikov}$$

□

3.5 Dvanajstera pot (angl. twelvefold way)

Vprašanje. *Na koliko načinov lahko razporedimo n kroglic v k škatel?*

- *Ali kroglice ločimo ali ne?*
- *Ali škatle ločimo ali ne?*
- *Ali iščemo vse možnosti ali le injektivne preslikave ali le surjektivne?*

Zgled. Imejmo $N = \{1,2,3,4,5\}$ kroglice in $K = \{a,b,c,d\}$ škatle. Definirajmo preslikave $N \to K$:

- $f(1) = a$, $f(2) = a$, $f(3) = b$
- $g(1) = a$, $g(2) = b$, $g(3) = a$
- $h(1) = b$, $h(2) = b$, $h(3) = d$

Če nanje gledamo kot na preslikave, so vse medsebojno paroma različne. Toda

- Če ne ločimo kroglic med sabo, velja $f = g$ (a pri obeh dobi dve kroglici, b pri obeh dobi eno), $g \neq h$ ($|g^*(a)| = 2 \neq 0 = |h^*(a)|$) in posledično $h \neq f$.
- Če ne ločimo škatel med sabo, velja $f = h$ (pri obeh sta skupaj $1, 2$ in 3 je ločena), $h \neq g$ ($g(1) \neq g(2)$, toda $h(1) = h(2)$) in posledično $f \neq g$.
- Če ne ločimo niti kroglic niti škatel, pa $f = g = h$, kajti vse slikajo dve kroglici v isto škatlo in tretjo kroglico posebej.

N kroglice	K škatle	vse	injektivne	surjektivne
Ločimo	Ločimo	k^n	$k^{\underline{n}}$	$S(n,k) \cdot k!$
Ne ločimo	Ločimo	$\binom{n+k-1}{k-1}$ šibke kompozicije	$\binom{n}{k}$	$\binom{n-1}{k-1}$ kompozicije št. n dolž. k
Ločimo	Ne ločimo	$\sum_{i=0}^{k} S(n,i)$	`(int)` $(n \leq k)$ torej $\in \{0,1\}$	$S(n,k)$
Ne ločimo	Ne ločimo	$\overline{p_k}(n)$	`(int)` $(n \leq k)$	$p_k(n)$ razčlenitve

Tabela 6: Dvanajstera pot

V resnici preštevamo ekvivalenčne razrede za določene ekvivalenčne relacije:

- $f \overset{\text{kroglic ne ločimo}}{\sim_N} g \Leftrightarrow \exists$ permutacija $\pi \in S_n \ni: f \circ \pi = g$
- $f \overset{\text{škatel ne ločimo}}{\sim_K} g \Leftrightarrow \exists$ permutacija $\sigma \in S_k \ni: \sigma \circ f = g$
- $f \overset{\text{niti kroglic niti škatel ne ločimo}}{\sim_{N,K}} g \Leftrightarrow \exists$ permutaciji $\pi \in S_n, \sigma \in S_k \ni: \sigma \circ f \circ \pi = g$

4 Rodovne funkcije (angl. generating function)

4.1 Uvod

Definicija. Zaporedje $(a_n)_{n \in \mathbb{N}}$ je preslikava $\mathbb{N} \to K$. Naj bo K polje — komutativen obseg (npr. $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$ (p praštevilo)).

Polje je $(K, +, \cdot)$ za komutativni $+, \cdot$, kjer je $(K, +)$ Abelova grupa in $(K \setminus \{0\}, \cdot)$ prav tako Abelova grupa ter velja distributivnost.

Za K obseg velja $\forall n \in \mathbb{N} : 1 \overset{n-\text{krat}}{+ \cdots +} 1 \in K$. Najmanjše število $p \ni: 1 \overset{p-\text{krat}}{+ \cdots +} 1 = 0$, je karakteristika K, pišemo $\operatorname{char} K$. Če tak $p \nexists$, pravimo $\operatorname{char} K = 0$.

Zgled. $\operatorname{char} \mathbb{Z}_p = p$ za p praštevilo.

Naša predpostavka v tem poglavju je, da za naše polje K velja $\operatorname{char} K = 0$ (npr. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$). Torej v tem poglavju velja

Definicija. Zaporedje je preslikava $\mathbb{N} \to K$, kjer je K polje s karakteristiko 0.

Kdaj rečemo, da poznamo zaporedje?

- Eksplicitna formula: $a_n = a^n$; $b_n = n!$
- Rekurzivna formula: $a_n = 2a_{n-1}$ z $a_0 = 1$; $b_n = nb_{n-1}$ z $b_0 = 1$; $F_n = F_{n-1} + F_{n-2}$ z $F_0 = F_1 = 1$
- Asimptotska formula: $a_n \sim b_n$ (asimptotska enakost: $\lim_{n\to\infty} \frac{a_n}{b_n} = 1$), kjer je b_n neko znano preprosto zaporedje. Recimo Stirlingova formula: $n! \sim \sqrt{2\pi n} \left(\frac{n}{e}\right)^n$.
- Rodovna funkcija: $\sum_{n=0}^{\infty} 2^n x^n = 1 + 2x + 4x^2 + 8x^3 + \cdots = \frac{1}{1-2x}$ (uporabimo obrazec za geometrijsko vrsto $\sum_{k=0}^{n} q^k = \frac{1-q^{n+1}}{1-q}$ oziroma $\sum_{n=0}^{\infty} q^n = \frac{1}{1-q}$ za konvergenčni radij $x \in \left(\frac{-1}{2}, \frac{1}{2}\right)$). Torej rodovna funkcija zaporedja $(2^n)_{n \in \mathbb{N}}$ je $\frac{1}{1-2x}$.

Vrstam oblike $\sum_{n=0}^{\infty} a_n x^n$ pravimo potenčne vrste. Iz analize vemo, da $\sum_{n=0}^{\infty} a_n x^n$ konvergira za $|x| < R$, kjer R imenujemo konvergenčni polmer in ga izračunamo z $R = \frac{1}{\limsup_{n\to\infty} \sqrt[n]{|a_n|}} \in [0, \infty]$. Velja $R = \lim_{n\to\infty} \left|\frac{a_n}{a_{n+1}}\right|$, če limita obstaja.

Zgled. Izračunajmo nekaj konvergenčnih radijev.

- $\sum_{n=0}^{\infty} 2^n x^n$:

$$R = \frac{1}{\limsup_{n\to\infty} \sqrt[n]{|2^n|}} = \frac{1}{2} = \lim_{n\to\infty} \left| \frac{a_n}{a_{n+1}} \right| = \lim_{n\to\infty} \left| \frac{2^{\cancel{n}}}{2^{\cancel{n}+1}} \right| = \frac{1}{2}$$

- $\sum_{n=0}^{\infty} \frac{x^n}{n!} = e^x$:

$$R = \lim_{n\to\infty} \left| \frac{\frac{1}{n!}}{\frac{1}{(n+1)!}} \right| = \lim_{n\to\infty} \frac{(n+1)!}{n!} = \lim_{n\to\infty} (n+1) = \infty$$

- $\sum_{n=0}^{\infty} n! x^n$:

$$R = \lim_{n\to\infty} \left| \frac{a_n}{a_{n+1}} \right| = \lim_{n\to\infty} \frac{n!}{(n+1)!} = 0$$

  Preverimo še ročno za $x = 0$: $\sum_{n=0}^{\infty} n! 0^n = 1$. Torej velja, da sta naslednji vrsti enaki, ker sta definirani le v $x = 0$, kjer sta enaki: $\sum_{n=0}^{\infty} n! x^n = \sum_{n=0}^{\infty} (n!)^2 x^n$.

Torej zaporedja lahko podamo tudi kot rodovne funkcije.

V kombinatorki namesto običajnih potenčnih vrst študiramo formalne potenčne vrste.

4.2 Formalne potenčne vrste (FPV)

Definicija. Naj bo K polje in $\operatorname{char} K = 0$. $K[x]$ je množica polinomov s koeficienti v K, torej

$$K[x] \coloneqq \left\{ a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n ; n \in \mathbb{N}, a_i \in K \right\}.$$

Polinom $p \in K[x]$ je preslikava $p : K \to K$. Definiramo seštevanje polinomov

$$\sum_{n=0}^{n_1} a_n x^n + \sum_{n=0}^{n_2} b_n x^n = \sum_{n=0}^{\max\{n_1, n_2\}} (a_n + b_n) x^n,$$

množenje s skalarjem

$$\alpha \sum_{n=0}^{n_1} a_n x^n = \sum_{n=0}^{n_1} \alpha a_n x^n,$$

množenje polinomov (konvolucijsko)

$$\left(\sum_{n=0}^{n_1} a_n x^n \right) \cdot \left(\sum_{n=0}^{n_2} b_n x^n \right) = a_0 b_0 + (a_0 b_1 + a_1 b_0) x + (a_0 b_2 + a_1 b_1 + a_2 b_0) x^2 + \cdots + a_{n_1} b_{n_2} x^{n_1 + n_2} =$$

$$= \sum_{n=0}^{n_1+n_2} x^n \sum_{k=0}^{n} a_k b_{n-k} = \sum_{n=0}^{n_1+n_2} x^n \sum_{i,j\geq 0, j+j=n} a_i b_j.$$

Toda $K[x]$ lahko definiramo tudi drugače — kot končno zaporedje koeficientov:

$$K[x] = \left\{ (a_n \in K)_{n\in\mathbb{N}} ; \exists n_0 \in \mathbb{N} \forall n > n_0 : a_n = 0 \right\}.$$

In analogno predstavimo operacije seštevanja $(a_n)_{n\in\mathbb{N}} + (b_n)_{n\in\mathbb{N}} = (a_n + b_n)_{n\in\mathbb{N}}$, množenja s skalarjem $\lambda (a_n)_{n\in\mathbb{N}} = (\lambda a_n)_{n\in\mathbb{N}}$ in konvolucijskega množenja polinomov $(a_n)_{n\in\mathbb{N}} (b_n)_{n\in\mathbb{N}} = \left(\sum_{k=0}^{n} a_k a_{n-k}\right)_{n\in\mathbb{N}}$.

Velja, da je $K[x]$ komutativna algebra.

Definicija. $K[[x]] \coloneqq \left\{ (a_n \in K)_{n\in\mathbb{N}} \right\}$ je množica formalnih potenčnih vrst oziroma množica zaporedij. Namesto $(a_n)_{n\in\mathbb{N}}$ ali $a_0, a_1, a_2, \ldots$ pišemo $\sum_{n=0}^{\infty} a_n x^n$ ali $a_0 + a_1 x + a_2 x^2 + \cdots$. Toda pozor: x tukaj ni spremenljivka. Nikoli ničesar ne vstavimo v x. Poleg tega K nima nujno metrike: ne potrebujemo limite za $\sum_{n=0}^{\infty}$ in ne definiramo konvergenčnega polmera, a kljub temu lahko definiramo naslednje operacije:

$$\sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} b_n x^n = \sum_{n=0}^{\infty} (a_n + b_n) x^n$$

$$\lambda \sum_{n=0}^{\infty} a_n x^n = \sum_{n=0}^{\infty} \lambda a_n x^n$$

$$\left(\sum_{n=0}^{\infty} a_n x^n \right) \cdot \left(\sum_{n=0}^{\infty} b_n x^n \right) = \sum_{n=0}^{\infty} c_n x^n,$$

kjer je $c = \sum_{k=0}^{n} a_k b_{n-k} = \sum_{i,j\geq 0, ij\in n} a_i b_j = a_0 b_n + a_1 b_{n-1} + \cdots + \cdots + \cdots + a_n b_0$ in to je končna vrsta, ki obstaja v vsakem polju, zato je definicija dobra.

Trditev. S temi operacijami je $K\left[[x]\right]$ komutativna algebra.

Dokaz. Dokažimo le komutativnost množenja

$$\left(\sum_{n=0}^{\infty} a_n x^n\right) \cdot \left(\sum_{n=0}^{\infty} b_n x^n\right) = \sum_{n=0}^{\infty} x^n \sum_{k=0}^{\infty} a_k b_{n-k} \overset{K \text{ komutativen obseg}}{=} \sum_{n=0}^{\infty} x^n \sum_{k=0}^{\infty} b_k a_{n-k} = \left(\sum_{n=0}^{\infty} b_n x^n\right) \cdot \left(\sum_{n=0}^{\infty} a_n x^n\right)$$

in obstoj enote za množenje

$$\sum_{n=0}^{\infty} \delta_{n,0} x^n = 1 + 0x + 0x^2 + \cdots =: \underline{1}$$

$$\sum_{n=0}^{\infty} a_n x^n \cdot \underline{1} = \sum_{n=0}^{\infty} x^n \sum_{k=0}^{n} \left(a_k \delta_{n-k,0}\right) = \sum_{n=0}^{\infty} 1 \cdot a_n x^n = \sum_{n=0}^{\infty} a_n x^n$$

□

Definicija. Kolobar K ima delitelje niča, če $\exists a, b \in K \ni: a \neq 0 \wedge b \neq 0 \wedge a \cdot b = 0$.

Zgled. 2 je v $\mathbb{Z}_6$ delitelj niča, kajti $2 \cdot 3 = 0$, in $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ je v $M_2(\mathbb{R})$ delitelj niča, kajti $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$.

Dejstvo. *Obseg nima deliteljev niča, kajti če $a \cdot b = 0$ in $a \neq 0$, je $a^{-1}ab = b = 0$.*

Trditev. V $K\left[[x]\right]$ ni deliteljev niča.

Dokaz. Naj bo

$$\sum_{n=0}^{\infty} a_n x^n = \overset{\neq 0 \text{ t. j. najmanjši, različen od } 0}{a_{n_0}} x^{n_0} + a_{n_0+1} x^{n_0+1} + \cdots$$

$$\sum_{n=0}^{\infty} b_n x^n = \overset{\neq 0 \text{ t. j. najmanjši, različen od } 0}{b_{m_0}} x^{m_0} + a_{m_0+1} x^{m_0+1} + \cdots$$

Tedaj

$$\left(\sum_{n=0}^{\infty} a_n x^n\right) \cdot \left(\sum_{n=0}^{\infty} b_n x^n\right) = \overset{\neq 0, \text{ ker } K \text{ obseg}}{a_{n_0} b_{m_0}} x^{n_0+m_0} + \cdots$$

Kateri elementi imajo inverz za množenje? □

Trditev. $\sum_{n=0}^{\infty}$ ima inverz za množenje $\Leftrightarrow a_0 \neq 0$.

Dokaz. Dokazujemo ekvivalenco:

($\Rightarrow$) $\left(\sum_{n=0}^{\infty} a_n x^n\right)\left(\sum_{n=0}^{\infty} b_n x^n\right) = \underline{1} \Rightarrow a_0 \cdot b_0 = 1 \Rightarrow a_0 \neq 0$

($\Leftarrow$) Po predpostavki $a_0 \neq 0$. Skonstruirajmo inverz.

- Veljati mora $a_0 b_0 = 1$. Tak $b_0 \exists : b_0 = a_0^{-1}$.
- Veljati mora $a_0 b_1 + a_1 b_0 = 0 \Rightarrow b_1 = \frac{-a_1 b_0}{a_0}$ in to $\exists$, ker $a_0 \neq 0$.
- Veljati mora $a_0 b_2 + a_1 b_1 + a_2 b_0 = 0 \Rightarrow b_2 = \frac{-a_1 b_1 - a_2 b_0}{a_0}$ in to $\exists$, ker $a_0 \neq 0$.
- ...
- Vedno obstaja vsak člen iskanega inverza, torej smo našli inverz $\sum_{n=0}^{\infty} b_n x^n$ za

$$b_n = \frac{-\sum_{i,j \geq 0, i+j=n, i \neq 0} a_i b_j}{a_0}.$$

□

Zgled.

$$\left(1 + 2x + 4x^2 + 8x^3 + \cdots\right)(1 - 2x) = 1 + \cancel{(-2+2)\, x} + \cancel{(0-4+4)\, x^2} + \cdots + \cancel{\left(1 \cdot 0 + 2 \cdot 0 + \cdots + 2^{n-1}(-2) + 2^n\right) x^n} = 0$$

in velja

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

Definicija. Naj bo $F(x) = \sum_n a_n x^n \in K[[x]]$. Ime potenčne vrste je $F(x)$ (to ni funkcija). $[x^n] F(x)$ je $n-$ti člen zaporedja/FPV. $\left[x^0\right] F(x) =: F(0)$ je oznaka za $0-$ti koeficient in ne pomeni vstavljanja 0 za x, saj $F(x)$ ni funkcija. To so vse samo oznake.

Dejstvo. $(F \cdot G)(0) = F(0) \cdot G(0)$. *Velja $F(x)$ je obrnljiva $\Leftrightarrow F(0) \neq 0$.*

Odvajanje FPV: Iz analize vemo

$$f'(x) = \lim_{n \to 0} \frac{f(x) - f(x-h)}{n}$$

in za $|x| < R$

$$\left(\sum_{n=0}^{\infty} a_n x^n \right)' := \sum_{n=0}^{\infty} a_n n x^{n-1}.$$

Toda v FPV nimamo limit in metrik, zato odvajanje definiramo.

Definicija.

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

Zgled. $\left(\frac{1}{1-x} = \sum_{n=0}^{\infty} x^n \right)' = \sum_{n=0}^{\infty} (n+1) x^n$

Zgled. $\left(\frac{1}{1-2x} = \sum_{n=0}^{\infty} 2^n x^n \right)' = \sum_{n=0}^{\infty} 2^{n+1} (n+1) x^n$

Vprašanje. *Ali obstaja $F(x)$, da velja $F'(x) = F(x)$ (diferencialne enačbe). Tedaj $\forall n \in \mathbb{N} : (n+1) a_{n+1} = a_n$: $a_1 = a_0$, $2a_2 = a_1$, $3a_3 = a_2$, ... in $a_2 = \frac{a_0}{2}$, $a_3 = \frac{a_2}{3} = \frac{a_0}{2 \cdot 3 = 6}$ in ti ulomki vselej obstajajo, ker* $\operatorname{char} K = 0$*, zato $2 \neq 0 \wedge 6 \neq 0 \wedge \cdots$. Sledi $a_n = \frac{a_0}{n!}$.*

Dobljena potenčna vrsta $\sum_{n=0}^{\infty} \frac{x^n}{n!}$ predstavlja zaporedje obratnih vrednosti od $n!$. To vrsto poimenujemo

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

Lahko definiramo še splošneje

$$e^{ax} := \sum_{n=0}^{\infty} \frac{a^n}{n!} x^n$$

Trditev.

$$e^{ax} + e^{bx} = e^{(a+b)x}$$

Dokaz.

$$L = \sum_n \frac{a^n}{n!} x^n \cdot \sum_n \frac{b^n}{n!} x^n = \sum_n x^n \sum_{k=0}^{n} \frac{a^k}{k!} \frac{b^{n-k}}{(n-k)!}$$

$$D = \sum \frac{(a+b)^n}{n!} x^n \overset{\text{binomski izrek}}{=} \sum_n \frac{\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}}{n!} x^n = \sum_n \frac{\sum_{k=0}^{n} \cancel{n!} a^k b^{n-k}}{k!(n-k)! \cancel{n!}} x^n$$

$$L = D$$

□

Dejstvo. $(e^{ax})' = \sum_n \cancel{(n+1)} \frac{a^{n+1}}{\cancel{(n+1)!}} x^n_{n!} = a \sum_n \frac{a^n}{n!} x^n = a e^{ax}$

Dejstvo. $(F(x) \cdot G(x))' = F'(x) G(x) + F(x) G'(x)$

Dejstvo.

$$\left(\frac{F(x)}{G(x)} \right)' = \frac{F'(x) G(x) - F(x) G'(x)}{G^2(x)}, \text{ kadar } G(0) \neq 0$$

Kompozicija FPV Iz analize vemo, da je kompozicija za funkcije (ob upoštevanju definicijskega območja) definirana

$$(f \circ g)(x) = f(g(x)).$$

Pri FPV je taka definicija neuporabna, ker ne moremo vstavljati argumenta.

Imejmo $F(x) = \sum_n a_n x^n$ in $G(x) = \sum_n b_n x^n$. Da bi kompozicijo definirali kot nekaj algebraično podobnega analizni kompoziciji, si oglejmo najprej

$$a_0 + a_1 G(x) + a_2 G^2(x) + \cdots + a_n G^n(x).$$

Slednje je dobro definiran izraz v $K[[x]]$. Toda kako definirati kompozicijo? Radi bi imeli nekaj takega:

$$(F \circ G)(x) = \lim_{N \to \infty} \sum_{n=0}^{N} a_n G^n(x) = a_0 + a_1 \left(b_0 + b_1 x + b_2 x^2 + \cdots\right) + a_2 (b_0 + \cdots)^2 + \cdots$$

Limito imamo le, če imamo metriko oz. razdaljo. Pri predmetu Kombinatorika 2 definiramo metriko na $F[[x]]$ v stilu „F in G sta blizu, če se nizki koeficienti ujemajo“. Takrat je smiselno govoriti o limiti. Več o tem torej pri KOMB2.

Zaenkrat intuitivno razmislimo o obstoju $F \circ G$. Oglejmo si koeficient pri x^0:

$$\left[x^0\right](F \circ G) = a_0 + a_1 b_0 + a_2 b_0^2 + a_3 b_0^3$$

To je element K. Toda K ni nujno metrični prostor. Edine smiselne vsote v K so torej končne. Ta vsota bo končna, če je $F(x)$ je polinom („končna FPV“) ali $b_0 = 0$ (tedaj je $\left[x^0\right](F \circ G) = a_0$).

Izkaže se: $(F \circ G)(x)$ je definiram $\Leftrightarrow F(x)$ je polinom ali $b_0 = 0$.

Dokaz. „dokazujemo“ ekvivalenca:

($\Rightarrow$) zgornji razmislek

($\Leftarrow$) Če je $F(x)$ polinom $\Rightarrow a_0 + a_1 G(x) + \cdots$ je končna vsota. Če je $b_0 = 0$, je $(F \circ G)(x) = a_0 + a_1\left(b_1 x + b_2 x^2 + \cdots\right) + a_2\left(b_1 x + b_2 x^2 + \cdots\right)^2 + \cdots$ in velja $\left[x^0\right] = a_0$, $\left[x^1\right] = a_1 b_2$, $\left[x^2\right] = a_1 b_2 + a_2 b_1^2$, $\left[x^3\right] = a_1 b_3 + 2 a_2 b_1 b_2 + a_3 b_1^3$,... Torej koeficient pri x^n je neka končna vsota, ker prispevajo k vsoti samo členi do $a_n\left(b_1 x + b_2 x^2 + \cdots\right)^n$.

Torej za izračun $[x^n](F \circ G)(x)$ je potrebno upoštevati le $a_0 + a_1 G(x) + \cdots + a_n G^n(x)$, se pravi le končno vsoto. Ta koeficient lahko izračunamo s končno mnogo operacijami. ☐

Povzetek. Torej $\exists (F \circ G)(x) \Leftrightarrow F(x)$ polinom ali $G(0) = 0$.

Zgled. Nekaj primerov:

- $5(e^x)^3 - 2(e^x)^2 + 1$ obstaja.
- e^{e^x} ne obstaja.
- $e^{e^x - 1}$ obstaja, saj $G(0) = 0$.
- $\cos \sin x$ obstaja, ker $\sin 0 = 0$. Velja $\cos x = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \cdots$ in $\sin x = x - \frac{x^3}{3!} + \frac{x^5}{5!}$.
- $\sin \cos x$ ne obstaja, ker $\cos 0 \neq 0$ niti sin ni polinom.

Dejstvo. *Izkaže se, da je $x = 0 + 1 \cdot x + 0 \cdot x^2 + \cdots$ enota za komponiranje. Če je $a_0 = 0$ in $a_1 \neq 0$, ima $\sum_n a_n x^n$ inverz za kompozicijo. A to pomeni, da ima inverz? Ne. $F(x) = x^2$ nima inverza, ker $a_0 = 0$.*

4.3 Uporaba rodovnih funkcij pri reševanju rekurzivnih enačb

Zgled. Fibonaccijevo zaporedje. $F_n = F_{n-1} + F_{n-2}$ z $F_0 = F_1 = 1$. Naj bo $F(x)$ FPV za Fibonaccijevo zaporedje. $F(x) = 1, 1, 2, 3, 5, 8, 13, \ldots$. Tedaj velja $x \cdot F(x) = 0, 1, 1, 2, 3, 5, 8, 13, \ldots$ in $x^2 \cdot F(x) = 0, 0, 1, 1, 2, 3, 5, 8, 13, \ldots$ in velja

$$F(x) = 1 + x \cdot F(x) + x^2 \cdot F(x)$$

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

$$F(x) \cdot \left(1 - x - x^2\right) = 1$$

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

Zgled. $a_n = 2a_{n-1}$ za $n \geq 1$ in $a_0 = 1$. Množimo $a_n = 2a_{n-1}$ z x^n in dodajmo $\sum_{n=1}^{\infty}$.

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

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

$$F(x) - a_0 = \sum_{n=1}^{\infty} a_n x^n = \sum_{n=1}^{\infty} 2a_{n-1} x^n = 2\sum_{n=1}^{\infty} a_{n-1} x^n = 2x \sum_{n=1}^{\infty} a_{n-1} x^{n-1} = 2x \sum_{n=0}^{\infty} a_n x^n = 2xF(x)$$

$$F(x) - a_0 = 2xF(x) \Longrightarrow F(x) - 2xF(x) = a_0 \Longrightarrow F(x)(1-2x) = a_0 \Longrightarrow F(x) = \frac{a_0}{1-2x}$$

Vstavimo $a_0 = 1$ in dobimo geometrijsko vrsto:

$$\frac{1}{1-2x} = \sum_{n=0}^{\infty} 2^n x^n \Rightarrow a_n = 2^n$$

Torej iz rekurzivnega zapisa zaporedja smo dobili eksplicitno formulo za člen zaporedja.

Zgled. $a_n = 3a_{n-1} - 2a_{n-2}$ za $n \geq 2$ in $a_0 = 1$ in $a_1 = 4$. Spet množimo $a_n = 3a_{n-1} - 2a_{n-2}$ z x^n in dodajmo $\sum_{n=2}^{\infty}$:

$$\sum_{n=2}^{\infty} a_n x^n = \sum_{n=2}^{\infty} 3a_{n-1} x^n - \sum_{n=2}^{\infty} 2a_{n-2} x^n = 3x \sum_{n=2}^{\infty} a_{n-1} x^{n-1} - 2x^2 \sum_{n=2}^{\infty} a_{n-2} x^{n-2} = 3x \sum_{n=1}^{\infty} a_n x^n - 2x^2 \sum_{n=0}^{\infty} a_n x^n =$$

$$= 3x \left(\sum_{n=0}^{\infty} a_n x^n - a_0 \right) - 2x^2 \sum_{n=0}^{\infty} a_n x^n = 3x(F(x) - a_0) - 2x^2 F(x)$$

$$\sum_{n=2}^{\infty} a_n x^n = \sum_{n=0}^{\infty} a_n x^n - a_1 x - a_0 = 3x(F(x) - a_0) - 2x^2 F(x)$$

$$F(x) - a_1 x - a_0 = 3x(F(x) - a_0) - 2x^2 F(x)$$

$$F(x) - 4x - 1 = 3x(F(x) - 1) - 2x^2 F(x)$$

$$F(x) - 3xF(x) + 2x^2 F(x) = 4x + 1 - 3x = 1 + x \Longrightarrow F(x)\left(1 - 3x + 2x^2\right) = 1 + x \Longrightarrow F(x) = \frac{1+x}{1-3x+2x^2}$$

Pri analizi bi razcepili in pretvorili $\frac{1+x}{1-3x+2x^2} = \frac{x+1}{(2x-1)(x-1)} = \frac{A}{2x-1} + \frac{B}{x-1}$. Torej izraze pri analizi pretvarjamo v ničelno obliko takole: $ax^2 + bx + c = a(x - x_1)(x - x_2)$. Uporabimo lahko obrazec za ničle: $x_{1,2} = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$.

Pri kombinatoriki pa rajši izraze preoblikujemo drugače, takole: $c + bx + ax^2 = c(1 - y_1 x)(1 - y_2 x)$. To pa zato, ker ima $\frac{1}{1-\alpha x}$ lep razvoj — geometrijska vrsta.

Opazimo $y_{1,2} = \frac{1}{x_{1,2}}$ — vidimo, da če za x vstavimo y_1^{-1} ali y_2^{-1}, bo vrednost izraza nič.

$$y_{1,2} = \frac{1}{x_{1,2}} = \frac{2a}{-b \pm \sqrt{b^2-4ac}} = \frac{2a}{-b \pm \sqrt{b^2-4ac}} \cdot \frac{-b \mp \sqrt{b^2-4ac}}{-b \mp \sqrt{b^2-4ac}} = \frac{2a\left(-b \mp \sqrt{b^2-4ac}\right)}{\cancel{b^2} - \left(\cancel{b^2} - 4ac\right)} = \frac{\cancel{2a}\left(-b \mp \sqrt{b^2-4ac}\right)}{\cancel{4a}^{2}c} =$$

$$= \frac{-b \mp \sqrt{b^2-4ac}}{2c} = y_{1,2}$$

Torej $y_{1,2}$ sta ničli, od kvadratne funkcije $cy_2 + by + a$. Pri kombinatoriki nas zanimata ničli obrnjenega polinoma. Vrnimo se spet k

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

"Kombinatoriško" ob upoštevanju $(a, b, c) = (2, -3, 1)$ razcepimo imenovalec $y_{1,2} = \frac{-b \pm \sqrt{b^2-4ac}}{2c} = \frac{3 \pm \sqrt{9-2\cdot 4}}{2\cdot 1} = \left\{\frac{3+1}{2}, \frac{3-1}{2}\right\} = \{2, 1\}$ in dobimo

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

Sedaj najdimo A in B:

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

$$1+x=A\left(1-2x\right)+B\left(1-x\right)$$

$$1+x=A-2Ax+B-Bx$$

In primerjamo koeficiente pri 1 in koeficiente pri x da dobimo sistem enačb:

$$1=A+B\Longrightarrow B=1-A$$

$$1=-2A-B\Longrightarrow B=-1-2A$$

$$1-A=-1-2A\Longrightarrow A=-2\Longrightarrow B=1+2=3$$

Pripomba. A in B lahko najdemo tudi z metodo prekrivanja, ko nimamo večkratnih ničel:

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

Obe strani množimo z $(1-x)$ in vstavimo $x=\frac{1}{1}=1$:

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

$$\frac{1+1}{\left(1-2\right)}=A+\cancel{\frac{B\left(1-1\right)}{1-2}}\Longrightarrow A=\frac{2}{-1}=-2$$

Obe strani množimo z $(1-2x)$ in vstavimo $x=\frac{1}{2}$:

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

$$\frac{1+\frac{1}{2}}{\left(1-\frac{1}{2}\right)}=\cancel{\frac{A\left(1-2\frac{1}{2}\right)}{1-\frac{1}{2}}}+B\Longrightarrow B=\frac{\frac{3}{2}}{\frac{1}{2}}=\frac{3\cdot 2}{2}=\frac{6}{2}=3$$

Torej: Prekrijemo v levi strani enačbe imenovalec pod A in v levo strani vstavimo $x=y_1^{-1}$ in vrednost leve strani je enaka vrednosti A.

Nadaljujmo z

$$F\left(x\right)=\frac{A=-2}{1-x}+\frac{B=3}{1-2x}=\frac{3}{1-2x}-\frac{2}{1-x}=3\sum_{n=0}^{\infty}2^nx^n-2\sum_{n=0}^{\infty}x^n=\sum_{n=0}^{\infty}3\cdot 2^nx^n-\sum_{n=0}^{\infty}2\cdot x^n$$

Kar nam da eksplicitno enačbo za člen zaporedja $a_n=3\cdot 2^n-2$.

Zgled. $F_n=F_{n-1}+F_{n-2}$ za $n\geq 2$ in $F_0=F_1=1$. Zopet množimo z x^n in seštejemo z $\sum_{n=2}^{\infty}$.

$$\sum_{n=2}^{\infty}F_nx^n=\sum_{n=2}^{\infty}F_{n-1}x^n+\sum_{n=2}^{\infty}F_{n-2}x^n$$

$$\sum_{n=0}^{\infty}F_nx^n-F_0-F_1x=x\sum_{n=2}^{\infty}F_{n-1}x^{n-1}+x^2\sum_{n=2}^{\infty}F_{n-2}x^{n-2}$$

$$F\left(x\right)-F_0-F_1x=x\sum_{n=1}^{\infty}F_nx^n+x^2\sum_{n=0}^{\infty}F_nx^n$$

$$F\left(x\right)-F_0-F_1x=x\left(F\left(x\right)-F_0\right)+x^2F\left(x\right)$$

$$F\left(x\right)-xF\left(x\right)-x^2F\left(x\right)=F_0+F_1x-xF_0$$

$$F\left(x\right)\left(1-x-x^2\right)=F_0+F_1x-F_0x$$

$$F\left(x\right)=\frac{F_0+F_1x-F_0x}{1-x-x^2}=\frac{1\cancel{+x-x}}{1-x-x^2}$$

$$y_{1,2}=\frac{-b\pm\sqrt{b^2-4ac}}{2c}=\frac{1\pm\sqrt{1+4}}{2}=\left\{\frac{1+\sqrt{5}}{2},\frac{1-\sqrt{5}}{2}\right\}$$

$$F\left(x\right)=\frac{1}{\left(1-\frac{1+\sqrt{5}}{2}x\right)\left(1-\frac{1-\sqrt{5}}{2}x\right)}=\frac{A}{1-\frac{1+\sqrt{5}}{2}x}+\frac{B}{1-\frac{1-\sqrt{5}}{2}x}=\frac{A\left(1-\frac{1-\sqrt{5}}{2}x\right)}{\left(1-\frac{1+\sqrt{5}}{2}x\right)\left(1-\frac{1-\sqrt{5}}{2}x\right)}+\frac{B\left(1-\frac{1+\sqrt{5}}{2}x\right)}{\left(1-\frac{1-\sqrt{5}}{2}x\right)\left(1-\frac{1+\sqrt{5}}{2}x\right)}$$

$$1=A\left(1-\frac{1-\sqrt{5}}{2}x\right)+B\left(1-\frac{1+\sqrt{5}}{2}x\right)$$

$$0=-\frac{1-\sqrt{5}}{2}A-\frac{1+\sqrt{5}}{2}B\Longrightarrow\frac{1+\sqrt{5}}{2}B=-\frac{1-\sqrt{5}}{2}A\Longrightarrow B=-\frac{\left(1-\sqrt{5}\right)\cancel{2}}{\cancel{2}\left(1+\sqrt{5}\right)}A=-\frac{\left(1-\sqrt{5}\right)^2}{1-5=-4}A=\frac{1-2\sqrt{5}+5}{4}A$$

$$1=A+B\Longrightarrow B=1-A$$

$$1-A=\frac{6-2\sqrt{5}}{4}A\Longrightarrow 1=A+\frac{3-\sqrt{5}}{2}A=\left(1+\frac{3-\sqrt{5}}{2}\right)A\Rightarrow\frac{1}{\frac{2+3-\sqrt{5}}{2}}=A=\frac{2}{5-\sqrt{5}}=\frac{10+2\sqrt{5}}{25-5=20}=\frac{5+\sqrt{5}}{10}$$

$$B=\frac{3-\sqrt{5}}{2}A=\frac{3-\sqrt{5}}{\cancel{2}}\cdot\frac{\cancel{2}}{5-\sqrt{5}}=\frac{\left(3-\sqrt{5}\right)\left(5+\sqrt{5}\right)}{\left(5-\sqrt{5}\right)\left(5+\sqrt{5}\right)}=\frac{15+3\sqrt{5}-5\sqrt{5}-5}{25-5}=\frac{10-2\sqrt{5}}{20}=\frac{5-\sqrt{5}}{10}$$

Pripomba. Tole bi bilo mnogo lažje rešiti z metodo prekrivanja.

$$F\left(x\right)=\frac{\frac{5+\sqrt{5}}{10}}{1-\frac{1+\sqrt{5}}{2}x}+\frac{\frac{5-\sqrt{5}}{10}}{1-\frac{1-\sqrt{5}}{2}x}=\frac{5+\sqrt{5}}{10}\left(\frac{1}{1-\frac{1+\sqrt{5}}{2}x}\right)+\frac{5-\sqrt{5}}{10}\left(\frac{1}{1-\frac{1-\sqrt{5}}{2}x}\right)=$$
$$=\frac{5+\sqrt{5}}{10}\sum_{n=0}^{\infty}\left(\frac{1+\sqrt{5}}{2}\right)^n x^n+\frac{5-\sqrt{5}}{10}\sum_{n=0}^{\infty}\left(\frac{1-\sqrt{5}}{2}\right)^n x^n$$

S tem smo dobili eksplicitno enačbo za $n-$ti člen Fibonaccijevega zaporedja:

$$a_n=\frac{5+\sqrt{5}}{10}\cdot\left(\frac{1+\sqrt{5}}{2}\right)^n+\frac{5-\sqrt{5}}{10}\cdot\left(\frac{1-\sqrt{5}}{2}\right)^n$$

Preverimo $a_6=\frac{5+\sqrt{5}}{10}\cdot\left(\frac{1+\sqrt{5}}{2}\right)^6+\frac{5-\sqrt{5}}{10}\cdot\left(\frac{1-\sqrt{5}}{2}\right)^6\overset{\text{kalkulator}}{=}13$

Seveda to lahko zapišemo lepše in bolj standardno:

$$a_n=\frac{5+\sqrt{5}}{10}\cdot\frac{2}{1+\sqrt{5}}\cdot\left(\frac{1+\sqrt{5}}{2}\right)^{n+1}+\frac{5-\sqrt{5}}{10}\cdot\frac{2}{1-\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{n+1}=$$

$$=\frac{5+\sqrt{5}}{5\left(1+\sqrt{5}\right)}\cdot\left(\frac{1+\sqrt{5}}{2}\right)^{n+1}+\frac{5-\sqrt{5}}{5\left(1-\sqrt{5}\right)}\left(\frac{1-\sqrt{5}}{2}\right)^{n+1}=$$

$$=\frac{\sqrt{5}\left(\frac{5}{\sqrt{5}}+1\right)}{5\left(1+\sqrt{5}\right)}\cdot\left(\frac{1+\sqrt{5}}{2}\right)^{n+1}+\frac{\sqrt{5}\left(\frac{5}{\sqrt{5}}-1\right)}{5\left(1-\sqrt{5}\right)}\left(\frac{1-\sqrt{5}}{2}\right)^{n+1}=$$

$$=\frac{\sqrt{5}\left(\frac{5\sqrt{5}}{5}+1\right)}{5\left(1+\sqrt{5}\right)}\cdot\left(\frac{1+\sqrt{5}}{2}\right)^{n+1}+\frac{\sqrt{5}\left(\frac{5\sqrt{5}}{5}-1\right)}{5\left(1-\sqrt{5}\right)}\left(\frac{1-\sqrt{5}}{2}\right)^{n+1}=$$

$$=\frac{\sqrt{5}\cancel{(\sqrt{5}+1)}}{5\cancel{(1+\sqrt{5})}}\cdot\left(\frac{1+\sqrt{5}}{2}\right)^{n+1}+\frac{-\sqrt{5}\cancel{(1-\sqrt{5})}}{5\cancel{(1-\sqrt{5})}}\left(\frac{1-\sqrt{5}}{2}\right)^{n+1}=$$

$$=\frac{5}{5\sqrt{5}}\cdot\left(\frac{1+\sqrt{5}}{2}\right)^{n+1}+\frac{-5}{5\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{n+1}=$$

$$=\frac{1}{\sqrt{5}}\cdot\left(\frac{1+\sqrt{5}}{2}\right)^{n+1}-\frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{n+1}=$$

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

Zgled. $a_n = -2a_{n-1} - 2a_{n-2}$ za $n \geq 2$ in $a_0 = 1$ in $a_1 = -1$. Zopet množimo z x^n in seštejemo z $\sum_{n=0}^{\infty}$.

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

$$\sum_{n=0}^{\infty} a_n x^n - a_0 - a_1 x = -2x \sum_{n=2}^{\infty} a_{n-1} x^{n-1} - 2x^2 \sum_{n=2}^{\infty} a_{n-2} x^{n-2}$$

$$F(x) - a_0 - a_1 x = -2x \left(\sum_{n=0}^{\infty} a_n x^n - a_0 \right) - 2x^2 \sum_{n=0}^{\infty} a_n x^n$$

$$F(x) - a_0 - a_1 x = -2x \left(F(x) - a_0 \right) - 2x^2 F(x)$$

$$F(x) + 2xF(x) + 2x^2 F(x) = a_0 + a_1 x + 2x a_0$$

$$F(x) \left(1 + 2x + 2x^2 \right) = 1 - 1x + 2x$$

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

$$y_{1,2} = \frac{-b \pm \sqrt{b^2-4ac}}{2c} = \frac{-2 \pm \sqrt{4-8}}{2} = \frac{-2 \pm \sqrt{-4}}{2} = -1 \pm i$$

$$F(x) = \frac{1+x}{\left(1-(-1+i)x\right)\left(1-(-1-i)x\right)} = \frac{A}{1-(-1+i)x} + \frac{B}{1-(-1-i)x}$$

Rešimo tokrat z metodo prekrivanja:

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

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

in vstavimo v enačbo

$$F(x) = \frac{\frac{1}{2}}{1-(-1+i)x} + \frac{\frac{1}{2}}{1-(-1-i)x} = \frac{1}{2}\left(\sum_{n=0}^{\infty} (-1+i)^n x^n + \sum_{n=0}^{\infty} (-1-i)^n x^n \right)$$

Torej eksplicitna formula za člen zaporedja se glasi

$$a_n = \frac{(-1+i)^n + (-1-i)^n}{2}$$

Toda naše zaporedje je očitno realno. Radi bi se znebili kompleksnih števil. Uporabimo polarne koordinate in de Moirrejev obrazec $z = x + iy = re^{i\varphi} = r(\cos\varphi + i\sin\varphi)$; $z^n = (x+iy)^n = r^n e^{in\varphi} = r^n(\cos n\varphi + \sin n\varphi)$.

$$(-1+i)^n = \left(\sqrt{2}\left(\cos\frac{3\pi}{4} + i \sin\frac{3\pi}{4} \right) \right)^n = 2^{n/2}\left(\cos\frac{3\pi n}{4} + i\sin\frac{3\pi n}{4} \right)$$

$$(-1-i)^n = 2^{n/2}\left(\cos\frac{3\pi n}{4} - i\sin\frac{3\pi n}{4} \right)$$

Vstavimo:

$$a_n = \frac{(-1+i)^n + (-1-i)^n}{2} = \frac{2^{n/2}\left(\cos\frac{3\pi n}{4} \cancel{+ i\sin\frac{3\pi n}{4}}\right) + 2^{n/2}\left(\cos\frac{3\pi n}{4} \cancel{- i\sin\frac{3\pi n}{4}}\right)}{2} = \frac{2^{n/2}\cos\frac{3\pi n}{4}}{2}$$

Zgled. $a_n = 6a_{n-1} - 9a_{n-2}$ za $n \geq 2$ in $a_0 = 1$ in $a_1 = 5$. Kot prej množimo z x^n in seštejemo z $\sum_{n=2}^{\infty}$:

$$\sum_{n=2}^{\infty} a_n x^n = 6 \sum_{n=2}^{\infty} a_{n-1} x^n - 9 \sum_{n=2}^{\infty} a_{n-2} x^n$$

$$F(x) - a_0 - a_1 x = 6x\left(F(x) - a_0\right) - 9x^2 F(x)$$

$$F(x)\left(1 - 6x + 9x^2\right) = a_0 + a_1 x - 6a_0 x$$

$$F(x) = \frac{1+5x-6x=1-x}{1-6x+9x^2}$$

$$y_{1,2} = \frac{6 \pm \sqrt{36-36}}{2} = \frac{6}{2} = 3$$

$$F(x) = \frac{1-x}{(1-3x)^2} = \frac{A}{1-3x} + \frac{B}{(1-3x)^2}$$

Metoda prekrivana tu deluje le za B (množimo z $(1-3x)^2$ in vstavimo $x = \frac{1}{3}$). Če množimo z $(1-3x)$ in vstavimo $x = \frac{1}{3}$, delimo z nič v desnem členu. Torej

$$B = 1 - \frac{1}{3} = \frac{2}{3}$$

$$\frac{1-x}{(1-3x)^2} = \frac{A}{1-3x} + \frac{B}{(1-3x)^2} \overset{\text{na skupni imenovalec}}{=} \frac{1(1-3x)+\frac{2}{3}}{(1-3x)^2}$$

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

$$A + \frac{2}{3} = 1 \Rightarrow A = 1 - \frac{2}{3} = \frac{1}{3}$$

Nadaljujmo

$$F(x) = \frac{\frac{1}{3}}{1-3x} + \frac{\frac{2}{3}}{(1-3x)^2}$$

Levi člen znamo razviti v potenčno vrsto. Kako pa desni člen razvijemo?

$$\frac{1}{(1-3x)^2} = \sum_{n=0}^{\infty} ?x^n$$

Več načinov:

1. Konvolucija: Vemo (geometrijska vrsta)

$$\frac{1}{1-3x} = \sum_{n=0}^{\infty} 3^n x^n$$

Kvadrirajmo:

$$\frac{1}{1-3x} \cdot \frac{1}{1-3x} = \sum_{n=0}^{\infty} x^n \sum_{k=0}^{n} 3^k 3^{n-k} = \sum_{n=0}^{\infty} x^n \sum_{k=0}^{n} 3^n = \sum_{n=0}^{\infty} x^n 3^n \sum_{k=0}^{n} 1 = \sum_{n=0}^{\infty} x^n 3^n (n+1)$$

2. Odvajanje: Odvajajmo izraz

$$\frac{1}{1-3x} = \sum_{n=0}^{\infty} 3^n x^n \qquad /'$$

$$\frac{0 \cdot (1-3x) - 1 \cdot (-3)}{(1-3x)^2} = \frac{3}{(1-3x)^2} = \sum_n 3^n n x^{n-1} = \sum_n 3^{n+1}(n+1)x^n = 3\sum_n 3^n (n+1) x^n$$

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

3.

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

Oglejmo si primer za $k=3$:

$$\frac{1}{(1-x)^3} = \frac{1}{1-x} \cdot \frac{1}{1-x} \cdot \frac{1}{1-x} = \left(1+x+x^2+\cdots\right)\left(1+x+x^2+\cdots\right)\left(1+x+x^2+\cdots\right)$$

Zanima nas na primer koeficient pri x^5. Lahko vzamemo recimo 1 iz prvega, 1 iz drugega in x^5 iz tretjega faktorja $(x^0 \cdot x^0 \cdot x^5)$. Ali pa $x^2 \cdot x \cdot x^2$ ali pa $x^4 \cdot x \cdot 1$, ... In koliko je takih načinov? Toliko, kolikor je šibkih kompozicij števila 5 s tremi členi.

$$[x^n]\,\frac{1}{(1-x)^k} = \#\text{ šibkih kompozicij } n \text{ s } k \text{ členi} = \binom{n+k-1}{k-1}$$

To vidimo tudi iz dejstva, da velja $F(x) \cdot G(x) = \sum_n x^n \sum_{i,j \geq 0, i+j=n} a_i b_j$ in $i, j \geq 0, i+j=n$ so ravno šibke kompozicije števila n z dvema členoma. Enako velja za

$$F(x) \cdot G(x) \cdot H(x) = \sum_n x^n \sum_{i,j,k \geq 0, i+j+k=n} a_i b_j c_k.$$

To pomeni, da

$$F(x)^k = \sum_n x^n \sum_{i_1,\ldots,i_k \geq 0 \wedge i_1+\cdots+i_k=n} a_{i_1} a_{i_2} \cdots a_{i_k}$$

oziroma za naš specifičen primer

$$\frac{1}{(1-x)^k} = \sum_n (\#\text{ šibkih kompozicij } n \text{ s } k \text{ členi})\, x^n = \sum_n \binom{n+k-1}{k-1}.$$

Logično torej velja

$$\frac{1}{(1-cx)^k} = \sum_n \binom{n+k-1}{k-1} c^n x^n$$

oziroma za naš specifičen primer

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

Ali pa za nek tretji primer:

$$\frac{1}{(1+4x)^3} = \sum_n \binom{n+3-1}{3-1} (-4)^n x^n = \sum_n \binom{n+2}{2} (-4)^n x^n$$

Torej eksplicitna formula splošnega člena zaporedja se glasi

$$a_n = \frac{3^n}{3} + \frac{2}{3} \cdot 3^n (n+1) = 3^{n-1} + 2(n+1)\, 3^{n-1} = 3^{n-1} (1 + 2(n+1)) = 3^{n-1} (2n+3)$$

Definicija. Homogena linearna rekurzivna zveza s konstantnimi koeficienti (HLRZSKK) je predpis za zaporedje oblike

$$c_d a_n + c_{d-1} a_{n-1} + \cdots + c_0 a_{n-d} = 0 \quad \wedge \quad c_d \neq 0, c_0 \neq 0, \forall i \in \{0..d\} : c_i \in \mathbb{C} \text{ za } n \geq 0 \text{ in } a_0, \ldots, a_{d-1} \text{ podani.}$$

Take HLRZSKK smo reševali (izrazili a_0 eksplicitno) v primerih zgoraj. Vselej tako, da smo jih enačbo pomnožili z x^n in sešteli z $\sum_{n=d}^{\infty}$ in nato izrazili v obliki $F(x) = \sum_{n=0}^{\infty} a_n x^n$. Če torej zgornjo enačbo pomnožimo z x^n in seštejemo z $\sum_{n=d}^{\infty}$, dobimo takle izraz:

$$\left(\sum_{n=d}^{\infty} c_d a_n x^n = c_d \sum_{n=d}^{\infty} a_n x^n = c_d \left(\overbrace{\sum_{n=0}^{\infty} a_n x^n}^{=F(x)} - a_0 - a_1 x - a_2 x^2 - \cdots - a_{d-1} x^{d-1} \right) \right) + \qquad \text{iz prvega člena}$$

$$+ c_{d-1} x \left(F(x) - a_0 - a_1 x - a_2 x^2 - \cdots - a_{d-2} x^{d-2} \right) + \qquad \text{iz drugega člena}$$

$$+ c_{d-2} x^2 \left(F(x) - a_0 - a_1 x - a_2 x^2 - \cdots - a_{d-3} x^{d-3} \right) + \qquad \text{iz tretjega člena}$$

$$\vdots$$

$$c_0 x^d F(x) = 0$$

Nato smo izrazili

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

Velja $\deg p(x) \leq d-1$, ker so vsi polinomi, ki jih seštevamo, stopnje manjše od $d-1$. Ni pa nujno točno $d-1$, ker nikjer nismo predpostavili, da koeficienti pred x^{d-1} niso vsi ničelni oziroma se ne seštejejo v nič. Torej $\deg p < d$.

Toda imenovalec je gotovo stopnje d, ker smo predpostavili $c_0 \neq 0$.

Dobimo racionalno rodovno funkcijo zaporedja s stopnjo števca manjšo od stopnje imenovalca.

Sedaj bi radi razcepili imenovalec:

$$c_d + c_{d-1}x + \cdots + c_0 x^d \underset{\text{vsak } p\in\mathbb{C} \text{ ima razcep na linearne faktorje}}{\overset{\text{osnovni izrek algebre}}{=}} c_d \prod_{i=1}^{k} (1 - y_i x)^{\alpha_i}$$

Za $y_1, \ldots, y_k$ velja, da je $\frac{1}{y_i}$ ničla polinoma na levi stopnje α_i. Oziroma če v polinom na levi vstavimo $\frac{1}{y}$ namesto x:

$$c_d + c_{d-1}\frac{1}{y} + \cdots + c_0 \frac{1}{y^d}$$

in izpostavimo $\frac{1}{y^d}$, dobimo

$$\frac{1}{y^d}\left(c_d y^d + c_{d-1}y^{d-1} + \cdots + c_0\right)$$

in $y_1, \ldots y_k$ so ničle tega obrnjenega polinoma stopenj $\alpha_1, \ldots, \alpha_k$.

Torej sedaj imamo

$$\frac{p(x)}{c_d \prod_{i=1}^{k}(1-y_i x)^{\alpha_i}} \overset{\text{parcialni ulomki}}{=} \sum_{i=1}^{k}\sum_{j=1}^{\alpha_i} \frac{A_{ij}}{(1-y_i x)^j} = \sum_{i=1}^{k}\sum_{j=1}^{\alpha_i} A_{ij}\frac{1}{(1-y_i x)^j} = \sum_{i=1}^{k}\sum_{j=1}^{\alpha_i} A_{ij} \sum_{n=0}^{\infty}\binom{n+j-1}{j-1} y_i^n x^n$$

s tem pa dobimo eksplicitno formulo za a_n:

$$a_n = \sum_{i=1}^{k}\left(\sum_{j=1}^{\alpha_i} A_{ij}\binom{n+j-1}{j-1}\right) y_i^n = \sum_{i=1}^{k}\left(\sum_{j=1}^{\alpha_i} A_{ij}\frac{(n+j-1)^{\underline{j-1}}}{(j-1)!}\right) y_i^n$$

Opazimo, da je $\sum_{j=1}^{\alpha_i} A_{ij}\frac{(n+j-1)^{\underline{j-1}}}{(j-1)!}$ polinom v spremenljivki n stopnje $\leq \alpha_i - 1$ (za polinom gledamo $(n+j-1)^{\underline{j-1}}$ in opazimo, da je stopnja/potenca največja, ko $j = \alpha_i$). Toda zakaj $\leq \alpha_i - 1$ in ne $= \alpha_i - 1$? Ker nimamo zagotovila za to, ali je A_{ij} neničeln, niti ga nismo izrazili. A vseeno gotovo velja, da je to polinom stopnje $< \alpha_i$.

Povzetek. Imamo torej $c_d a_n + c_{d-1}a_{n-1} + \cdots + c_0 a_{n-d} = 0$ za $n \geq d$ ob predpostavki $c_d \neq 0, c_0 \neq 0, \forall i \in \{0..d\} : c_d \in \mathbb{C}$. Poiščemo ničle karakterističnega polinoma (tistega obrnjenega)

$$c_d \lambda^d + c_{d-1}\lambda^{d-1} + \cdots + c_0$$

in to so $\lambda_1, \ldots, \lambda_k$ s kratnostmi $\alpha_1, \ldots, \alpha_k$. Nato za neke polinome p_i, za katere velja $\deg p_i < \alpha_i$, velja:

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

Izrek. *Rešitev HLRESKK je $a_n = \sum_{i=1}^{k} p_i(n)\lambda_i^n$, kjer so $\lambda_1, \ldots \lambda_k$ ničle karakterističnega polinoma mnogokratnosti $\alpha_1, \ldots \alpha_k$, p_i pa so polinomi stopnje $< \alpha_i$.*

Dokaz. Dokazano zgoraj v razmisleku. □

Ta izrek nam služi kot nastavek za hitrejše reševanje HLRESKK.

Zgled. $a_n = 2a_{n-1}$ za $n \geq 1$ in $a_0 = 1$. Torej karakteristični polinom je $\lambda - 2$. Edina ničla je $\lambda_1 = 2$ (torej $k = 1$) in njena kratnost je $\alpha_1 = 1$. Za p_1 vemo, da je stopnje manjše od 1, torej je to konstantni polinom. Izrazimo lahko

$$a_n = C\lambda_1^n = C \cdot 2^n$$

C dobimo tako, da vstavimo $n = 0$: $a_0 = 1 = C \cdot 2^0 = C \Rightarrow C = 1$ in s tem $a_n = 2^n$.

Zgled. $a_n - 3a_{n-1} + 2a_{n-2} = 0$ za $n \geq 0$ in $a_0 = 1$ in $a_1 = 4$. Karakteristični polinom je $\lambda^2 - 3\lambda + 2 = (\lambda - 2)(\lambda - 1)$. Imamo torej $k = 2$ ničli $\lambda_1 = 2$ in $\lambda_2 = 1$, obe s kratnostjo $\alpha_{1,2} = 1$, zatorej sta p_1 in p_2 oba konstantna.

$$a_n = A2^n + B1^n = A2^n + B$$

Vstavimo $n = 0$: $1 = A + B \Rightarrow B = 1 - A$ in $n = 4$: $4 = A2 + B \Rightarrow B = 4 - 2A$. Naposled $4 - 2A = 1 - A \Rightarrow 3 = A$ in $B = -2$. Potemtakem $a_n = 3 \cdot 2^n - 2$

Zgled. $F_n - F_{n-1} - F_{n-2} = 0$ za $n \geq 2$ in $F_0 = F_1 = 1$. Karakteristični polinom je $\lambda^2 - \lambda - 1 = 0$, torej $\lambda_{1,2} = \frac{1 \pm \sqrt{1+4=5}}{2}$, obe kratnosti $\alpha_{1,2} = 1$. Torej

$$F_n = A\left(\frac{1+\sqrt{5}}{2}\right)^n + B\left(\frac{1-\sqrt{5}}{2}\right)^n$$

Vstavimo $n = 0$: $1 = A + B \Rightarrow B = 1 - A$ in $n = 1$: $1 = A\frac{1+\sqrt{5}}{2} + B\frac{1-\sqrt{5}}{2}$ ... dobimo $A = \frac{1}{\sqrt{5}}$ in $B = \frac{-1}{\sqrt{5}}$, torej

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

Zgled. $a_n - 6a_{n-1} + 9a_{n-2} = 0$ za $n \leq 2$ in $a_0 = 1$ in $a_1 = 5$. Dobimo karakteristični polinom $0 = \lambda^2 - 6\lambda + 9 = (\lambda - 3)^2$. Dobimo $k = 1$ ničlo $\lambda_1 = 3$ kratnosti $\alpha_1 = 2$. Torej bo polinom $p_1(n)$ stopnje manjše od 2, torej oblike $p(n) = An + B$.

$$a_n = (An + B)\, 3^n$$

Vstavimo $n = 0$: $1 = B$ in $n = 1$: $5 = (A + 1)\, 3 \Rightarrow 5 = 3A + 3 \Rightarrow 2 = 3A \Rightarrow A = \frac{2}{3}$ in zategadelj

$$a_n = \left(\frac{2n}{3} + 1\right) 3^n$$

Iskanje rešitev nekaterih nehomogenih linearnih rekurzivnih enačb s konstantnimi koeficienti (NLRESKK) NLRESKK je oblike $c_d a_n + c_{d-1}a_{n-1} + \cdots + c_0 a_{n-d} = q(n)\lambda^n$ Torej desna stran ni 0, temveč je polinom, pomnožen z $n-$to potenco nekega koeficienta, denimo $\left(n^2 + 3n + 1\right) 5^n$ ali pa $n(-5)^n$ ali pa 3^n ali pa $n^3 - 3n + 1$.

Metoda:

1. Rešimo homogeno enačbo (desno stran nadomestimo z ničlo).
2. Poiščemo partikularno rešitev z nastavkom

   $$r(n) \cdot n^a \cdot \lambda^n,$$

   kjer je r polinom stopnje, manjše ali enake stopnji polinoma q ZDB $\deg r \leq \deg q$. Če je q stopnje 2, bo r oblike $An^2 + Bn + C$. Če je q konstanta, bo tudi r konstanta. a je stopnja λ v karakterističnem polinomu. Torej pogledamo, kolikokratna ničla karakterističnega polinoma iz reševanja homogene enačbe je λ (da, to je tista λ, ki je na desni strani dana na $n-$to potenco). Lahko tudi ni ničla, v tem primeru je $a = 0$. Torej $a \geq 0$.

Zgled. $a_n - 4a_{n-1} + 5a_{n-2} - 2a_{n-3} = n - 2$ za $n \geq 3$. Karakteristični polinom $0 = \lambda^3 - 4\lambda^2 + 5\lambda - 2 = (\lambda - 1)^2(\lambda - 2)$. Torej rešitev homogenega dela je $a_n = (An + B) + C \cdot 2^n$. TODO XXX FIXME najdemo A, B, C.

Sedaj pa najdimo še partikularno rešitev z nastavkom upoštevaje $\lambda = 1, \alpha_1 = 2$, torej $a = 2$, in $q(n) = n - 2 \Rightarrow \deg q = 2$, torej $\deg r \leq 2$:

$$a_n = (Dn + E)\, n^2 1^n = Dn^3 + En^2$$

Vstavimo to partikularno rešitev v nalogo:

$$Dn^3 + En^2 - 4\left(D(n-1)^3 + E(n-1)^2\right) + 5\left(D(n-2)^3 + E(n-2)^2\right) - 2\left(D(n-3)^3 + E(n-3)^2\right) = n - 2$$

Oglejmo si koeficiente pri n^1 in pri n^0 (ostali se morajo pokrajšati):

$$\left[n^1\right]: \quad -4(D3 - 2E) + 5(E3 \cdot 4 - 4E) - 2\left(D3 \cdot 3^2 - 6E\right) = 1$$

$$\left[n^0\right]: \quad -4(-D + E) + 5(-8D + 4E) - 2(-27D + 9E) = -2$$

In dobimo D in E. TODO XXX FIXME NE RAZUMEM Nikomur se ni dalo izračunati rešitve, ampak mogoče je $D = \frac{-1}{2}$ in $E = \frac{-1}{6}$. Se pa niti približno nikomur ni dalo izračunati A, B, C. Ampak dalo bi se jih. Potemtakem bi bila končna rešitev vsota partikularne rešitve in rešitve homogeniziranega problema

$$a_n = Dn^3 + En^2 + (An + B) + C \cdot 2^n \overset{\text{mogoče}}{=} \frac{-1}{2}n^3 + \frac{-1}{6}n^2 + (An + B) + C \cdot 2^n$$

4.4 Binomska vrsta in Catalanova števila

Opomba. Od prej vemo $(1+x)^n = \sum_{k=0}^{n}\binom{n}{k}x^k$ in $\frac{1}{(1+x)^k} = \sum_{n=0}^{\infty}\binom{n+k-1}{k-1}x^n$. Kaj pa $(1+x)^{\frac{1}{2}}$ oziroma $\sqrt{1+x}$? Želimo, da velja $\sqrt{1+x}^2 = 1+x$.

Definicija. Posplošeni binomski koeficient. Naj bo $\lambda \in K$ za K poljuben komutativen obseg (polje) s char $K = 0$ in naj bo $n \in \mathbb{N}$ Tedaj

$$\binom{\lambda}{n} = \frac{\lambda^{\underline{n}}}{n!} = \frac{\lambda(\lambda-1)(\lambda-2)\cdots(\lambda-n+1)}{n!}$$

Zgled.

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

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

Definicija. Naj bo $n \in \mathbb{N}$. Soda fakulteta $(2n)!! \coloneqq (2n)(2n-2)(2n-4)\cdots(2)$, liha fakulteta $(2n-1)!! \coloneqq (2n-1)(2n-3)(2n-5)\cdots(1)$.

Zgled. $7!! = 1\cdot 3\cdot 5\cdot 7 = 105$, $6!! = 2\cdot 4\cdot 6 = 48$.

Zgled. Naj bo $n \geq 1$:

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

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

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

Zgled. $\binom{\lambda}{0} = \frac{1}{1} = 1$, $\binom{\lambda}{1} = \frac{\lambda}{1} = \lambda$, $\binom{\lambda}{2} = \frac{\lambda(\lambda-1)}{2}$, $\binom{-1}{n} = \frac{(-1)(-1-1)(-1-2)\cdots(-1-n+1)}{n!} = (-1)^n\frac{1\cdot 2\cdot 3\cdots n}{n!} = (-1)^n$

Definicija. Binomska vrsta. Za $\lambda \in K$ (K komutativni obseg = polje s karakteristiko 0):

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

Zgled. Naj bo $\lambda \in \mathbb{N}$. Pišimo $n = \lambda$

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

Zgled. Kaj pa če $\lambda \in -\mathbb{N}$? Pišimo $\lambda = -k$ (glej primer zgoraj za $\binom{-k}{n}$)

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

Radi bi pisali $B_\lambda(x) = (1+x)^\lambda$. Zaenkrat smo to dokazali z zgornjima zgledoma za $\lambda \in \mathbb{Z}$. A velja za vsako polje s karakteristiko 0?

Pričakovali bi $\left(B_{\frac{1}{2}}(x)\right)^2 = 1+x$. Preverimo, kaj je $B_{\frac{1}{2}}(x)$ (glej primer zgoraj za $\binom{\frac{1}{2}}{n}$)

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

Pričakovali bi še celo $B_\lambda(x)\cdot B_\mu(x) = B_{\lambda+\mu}(x)$. Če to drži, dokažemo tudi prejšnje pričakovanje ($B_{\frac{1}{2}}(x)\cdot B_{\frac{1}{2}}(x) = B_1(x)$).

Pričakovali bi tudi $B'_\lambda(x) = \lambda B_{\lambda-1}(x)$.

Lema.

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

Dokaz. Indukcija.

- Baza: $n = 0$: $1 = 1$
- Korak:

$$(a+b)^{\underline{n}} = (a+b-n+1)\,(a+b)^{\underline{n-1}} \overset{\text{I. P.}}{=} ((a-(n-1-k))+(b-k)) \sum_{k} \binom{n-1}{k} a^{\underline{n-1-k}} b^{\underline{k}} =$$

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

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

$$= \sum_{k} \left[\binom{n-1}{k} + \binom{n-1}{k-1} \right] a^{\underline{n-k}} b^{\underline{k}} = \sum_{k} \binom{n}{k} a^{\underline{n-k}} b^{\underline{k}}$$

Lema dokazana.

□

Izrek. $B_\lambda(x) \cdot B_\mu(x) = B_{\lambda+\mu}(x)$

Dokaz.

$$B_\lambda(x) \cdot B_\mu(x) = \sum_{n} \binom{\lambda}{n} x^n \cdot \sum_{n} \binom{\mu}{n} x^n \overset{\text{konvolucija}}{=} \sum_{n} x^n \sum_{k=0}^{n} \frac{\lambda^{\underline{k}}}{k!} \cdot \frac{\mu^{\underline{n-k}}}{(n-k)!} = \sum_{n} \frac{1}{n!} x^n \sum_{k=0}^{n} \frac{n!\lambda^{\underline{k}}\mu^{\underline{n-k}}}{k!\,(n-k)!} =$$

$$= \sum_{n} \frac{1}{n!} x^n \sum_{k=0}^{n} \binom{n}{k} \lambda^{\underline{k}} \mu^{\underline{n-k}} = \sum_{n} \frac{(\lambda+\mu)^{\underline{n}}}{n!} x^n = \sum_{n} \binom{\lambda+\mu}{n} x^n = B_{\lambda+\mu}(x)$$

□

Trditev. $B'_\lambda(x) = \lambda B_{\lambda-1}(x)$

Dokaz. Spomnimo se definicije odvoda FPV: $[x^n]\, F'(x) \coloneqq (n+1)\, a_{n+1}$

$$[x^n]\, B'_\lambda(x) = (n+1) \cdot \binom{\lambda}{n+1} = (n+1)\, \frac{\lambda^{\underline{n+1}}}{(n+1)!} = \frac{\lambda^{\underline{n+1}}}{n!}$$

$$[x^n]\, \lambda B_{\lambda-1}(x) = \lambda \binom{\lambda-1}{n} = \lambda \frac{(\lambda-1)^{\underline{n}}}{n!} = \frac{\lambda^{\underline{n+1}}}{n!}$$

□

Sedaj lahko označimo (glej primer zgoraj)

Definicija.

$$\sqrt{1+x} \coloneqq (1+x)^{\frac{1}{2}} = B_{\frac{1}{2}}(x) = 1 + \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{2^{2n-1} n} \binom{2n-2}{n-1} x^n = 1 + \frac{1}{2}x - \frac{1}{8}x^2 + \frac{1}{16}x^3 + \cdots$$

To lahko uporabimo recimo za iterativni izračun $\sqrt{\frac{1}{2}}$ — $\sqrt{\frac{1}{2}} = B_{\frac{1}{2}}\left(-\frac{1}{2}\right) = \cdots$ ali pa recimo $1,4142135 \approx \sqrt{2} \approx 1 + \frac{1}{2} - \frac{1}{8} + \frac{1}{16} = 1,4375$. FPV uporabljamo analitično (to je snov Analitične kombinatorike).

Definicija. Catalanovo število C_n je število pravilnih postavitev oklepajev na nizu $t_0 t_1 \cdots t_n$, ob upoštevanju, da oklepaj zajame par (bodisi dva atoma bodisi atom in oklepajski izraz bodisi oklepajski izraz in atom bodisi dva oklepajska izraza) in da mora končni niz imeti par izrazov (bodisi dva atoma bodisi atom in oklepajski izraz bodisi oklepajski izraz in atom bodisi dva oklepajska izraza). $C_1 \coloneqq 1 \eqqcolon C_0$.

Zgled. $C_2 = 2$: $(t_0 t_1)\, t_2$ in $t_0\,(t_1 t_2)$, $C_3 = 5$: $t_0\,((t_1 t_2)\, t_3)$ in $((t_0 t_1)\, t_2)\, t_3$ in $(t_0 t_1)\,(t_2 t_3)$ in $(t_0\,(t_1 t_2))\, t_3$ in $t_0\,(t_1\,(t_2 t_3))$.

Dejstvo. *Velja* $C_0 = 1$, $C_1 = 1$, $C_2 = 2$, $C_3 = 5$, $C_4 = 14$, $C_5 = 42$, $C_6 = 132$, ...

Dejstvo. *Rekurzivna zveza:* $C_{n+1} = \sum_{k=1}^{n} C_{n-k} \cdot C_k$. *Razlaga: Vsota predstavlja izbiro zadnje operacije,* C_{n-k} *predstavlja možne postavitve oklepajev desnega argumenta operacije in* C_k *predstavlja možne postavitve oklepajev levega argumenta operacije:*

$$\left(\overset{\text{možnosti za postavitev oklepajev tu je } C_k}{t_1 t_2 \cdots t_k}\right) \overset{\text{zadnja operacija — } n \text{ izbir}}{\cdot} \left(\overset{\text{tu pa } C_{n-k}}{t_{k+1} t_{k+2} \cdots t_{n+1}}\right)$$

Definirajmo rodovno funkcijo za Catalanova števila in najdimo ekspliciten izraz $n-$tega Catalanovega števila iz rekurzivne zveze.

$$F(x) = \sum_{n=0}^{\infty} C_n x^n = 1 + x + 2x^2 + 5x^3 + 14x^4 + 42x^5 + \cdots$$

Opazimo, da rekurzivna zveza ni linearna.

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

Množimo enačbo z x^{n+1} in seštejmo s $\sum_{n=0}^{\infty}$:

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

Opazimo, da je $\sum_{k=0}^{n} C_k C_{n-k}$ ravno konvolucija, torej $F(x) \cdot F(x)$:

$$F(x) - C_0 = F(x) - 1 = xF^2(x)$$

$$xF^2(x) - F(x) + 1 = 0$$

Ne dobimo linearne enačbe, temveč kvadratno. A jo lahko rešimo?

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

Dobimo nek čuden izraz. Poskusimo z obrazcem za ničle kvadratne enačbe:

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

To si moramo malce bolj razložiti. Prej smo izračunali

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

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

Torej

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

To ni formalna potenčna vrsta, po deljenju števca z imenovalcem dobimo $\frac{1}{x} + \cdots$. Poskusimo še drugo rešitev obrazca za ničle:

$$\frac{1-\sqrt{1-4x}}{2x} = \frac{1 - 1 + 2\sum_{n=1}^{\infty} \frac{1}{n}\binom{2n-2}{n-1} x^n}{2x} = \frac{\sum_{n=1}^{\infty} \frac{1}{n}\binom{2n-2}{n-1} x^n}{x} = \sum_{n=1}^{\infty} \frac{1}{n}\binom{2n-2}{n-1} x^{n-1} = \sum_{n=0}^{\infty} \frac{1}{n+1}\binom{2n}{n} x^n$$

To pa je formalna potenčna vrsta. Ta vrsta res reši kvadratno enačbo. Vstavimo, da preverimo (čeprav že vemo):

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

$$= \frac{2 - 2\sqrt{1-4x} - 4x}{4x} - \frac{1-\sqrt{1-4x}}{2x} + 1 = \frac{1 - 1\sqrt{1-4x} - 2x}{2x} - \frac{1-\sqrt{1-4x}}{2x} + 1 = \frac{-2x}{2x} + 1 = 0$$

Povzetek. $C_n = \frac{1}{n+1}\binom{2n}{n}$. Recimo: $C_4 = \frac{1}{5}\binom{8}{4} = \frac{1}{\cancel{5}} \cdot \frac{\cancel{8}^{2}\cdot 7\cdot \cancel{6}\cdot \cancel{5}}{\cancel{4}\cdot \cancel{3\cdot 2}} = 14$.

Pripomba. Catalanova števila preštevajo veliko različnih struktur. Recimo:

- dvojiških dreves s štirimi listi je C_3. To je očitno, saj dvojiška drevesa ponazarjajo ravno abstraktna skladenjska drevesa, ki jih ustvari razčlenjevalnik po razčlenjanju oklepajskega izraza (Principi programskih jezikov in Algoritmi in podatkovne strukture 2).
- Dyckeove poti: Začnemo na višini 0. Na vsakem koraku se lahko pomaknemo bodisi gor bodisi dol, na koncu se moramo vrniti nazaj na višino 0, nikoli se ne pomaknemo pod višino 0. To je zopet očitno, saj je ekvivalentno zapisu oklepajskega izraza v „reverse polish notation“: Višina predstavlja višino sklada, atom predstavlja operacijo push, torej višanje sklada, operacija predstavlja dva popa in en push, torej nižanje sklada. Na koncu zahtevamo samoten element na skladu. Operacija (nižanje) na višini bi pomenilo napako „pop from empty stack“, zato je prepovedana.
- Triangulacija $(n+2)-$kotnika. Za $n = 1$ imamo samo en trikotnik, za $n = 2$ imamo kvadrat, ki mu vrišemo diagonalo na dva načina, za $n = 3$ imamo petkotnik, ki mu, da dobimo triangulacijo, vrišemo dve diagonali, kar lahko storimo na 5 načinov.
- V knjigi Enumerative Combinatorics vol. 2 je 66 matematičnih struktur, ki jih preštevajo C_n. Na spletni strani avtorja je še > 100 dodatnih.

4.5 Rodovne funkcije razčlenitev

Spomnimo se:

- $p(n) =$ število razčlenitev števila n
- $p_k(n) =$ število razčlenitev števila n s k členi
- $\overline{p_k}(n) =$ število razčlenitev števila n z največ k členi

In veljajo naslednje rekurzivne zveze

- $p_k(n) = p_{k-1}(n-1) + p_k(n-k)$
- $\overline{p_k}(n) = \overline{p_k}(n-k) + p_{k-1}(n)$
- $p(n) = p(n-1) + p(n-2) - p(n-5) - p(n-7) + p(n-12) + \cdots = \sum_{k=1}^{\infty} (-1)^{k+1}\left(p\left(n - \frac{k(3k-1)}{2}\right) + p\left(n - \frac{k(3k+1)}{2}\right)\right)$

Sedaj nas zanimajo rodovne funkcije za ta zaporedja.

Spomnimo se najprej

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

in velja

$$[x^n]\,G(x) = \text{ \#šibkih kompozicij št. } n \text{ s tremi členi.}$$

Sedaj si oglejmo

$$H(x) = \frac{1}{1-x}\cdot\frac{1}{1-x^2}\cdot\frac{1}{1-x^3} = \left(1+x+x^2+\cdots\right)\cdot\left(1+x^2+x^4+\cdots\right)\cdot\left(1+x^3+x^6+\cdots\right)$$

tu lahko recimo x^5 dobimo kot $x^{5\cdot 1}\cdot x^{0\cdot 2}\cdot x^{0\cdot 3}$ ali kot $x^{3\cdot 1}\cdot x^{1\cdot 2}\cdot x^{0\cdot 3}$ ali kot $x^{2\cdot 1}\cdot x^{0\cdot 2}\cdot x^{1\cdot 3}$ ali kot $x^{1\cdot 1}\cdot x^{2\cdot 2}\cdot x^{0\cdot 3}$ ali pa kot $x^{0\cdot 1}\cdot x^{1\cdot 2}\cdot x^{1\cdot 3}$. Torej koeficient pri x^5 je 5. Drugače povedano, lahko 5 zapišemo kot $1+1+1+1+1 = 1+1+1+2 = 1+1+3 = 1+2+2 = 2+3$.

V splošnem: koeficient pri x^n je število razčlenitev števila n s členi $1, 2, 3$.

Splošneje:

Vprašanje. *Kolikšen je v*

$$\prod_{i=1}^{k}\frac{1}{1-x^i} = \left(1+x+x^2+\cdots\right)\left(1+x^2+x^4+\cdots\right)\cdots\left(1+x^k+x^{2k}+\cdots\right)$$

koeficient pri x^n? ZDB Koliko je rešitev enačbe $n = a_1\cdot 1 + a_2\cdot 2 + \cdots + a_n\cdot k$ za $a_i \in \mathbb{N}_0$?

Odgovor:

$$[x^n]\prod_{i=1}^{k}\frac{1}{1-x^i} = \textit{ število razčlenitev } n \textit{ s členi } \leq k$$

Kako se to odraža v Ferrersovim diagramu? Ima največ k stolpcev. Za konjugiranko te razčlenitve torej velja, da ima največ k vrstic oziroma ima največ k členov.

Z drugimi besedami, konjugiranje je bijekcija med razčlenitvami n s členi $\leq k$ in razčlenitvami n z največ k členi. Nadaljujmo:

$$[x^n]\prod_{i=1}^{k}\frac{1}{1-x^i} = \text{ število razčlenitev } n \text{ s členi } \leq k = \overline{p_k}\,(n)$$

S tem razmislekom smo dokazali trditev:

Trditev.

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

Kaj pa rodovna funkcija za $\sum_n p_k\,(n)\,x^n$? Torej zanimajo nas razčlenitve n z natanko k členi. V Ferrersovem diagramu bi se to odražalo kot natanko k vrstic. Če te razčlenitve konjugiramo, dobimo razčlenitve s Ferrersovimi diagrami z natanko k stolpci, to pa so razčlenitve n s členi, ki so vsi $\leq k$, vsaj eden pa je enak k. Zapišimo si kot enačbo:

$$\sum_n p_k\,(n)\,x^n = \overbrace{\left(1+x+x^2+\cdots\right)}^{\text{poljubno število enk}}\overbrace{\left(1+x^2+x^4+\cdots\right)}^{\text{poljubno število dvojk}}\cdots\overbrace{\left(x^k+x^{2k}+\cdots\right)}^{\text{vsak en člen } k} = \frac{1}{1-x}\cdot\frac{1}{1-x^2}\cdots\frac{1}{1-x^{k-1}}\cdot\frac{x^k}{1-x^k}$$

Torej smo dokazali naslednjo trditev:

Trditev.

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

Oglejmo si spet prvo trditev:

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

Kaj se dogaja s $\overline{p_k}\,(n)$, ko $k\to\infty$? $\overline{p_k}\,(n)$ gre z rastočim k proti $p\,(n)$. Velja namreč $\overline{p_k}\,(x) = p\,(n)$ za $k \geq n$ (očitno; razčlenitev n nikdar nima več kot n členov). S tem dobimo še zadnjo trditev:

Trditev.

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

Dokaz. Intuitiven dokaz. Ta dokaz ni povsem pravilen, ker nismo definirali metrike, brez nje pa ni moč definirati neskončnega produkta.

Kaj je koeficient pri x^n v $\frac{1}{1-x^1}\cdot\frac{1}{1-x^2}\cdots\frac{1}{1-x^n}\cdot\frac{1}{1-x^{n+1}}\cdots$ Čim iz faktorjev od $\frac{1}{1-x^{n+1}} = 1+x^{n+1}+x^{2(n+1)}+\cdots$ naprej (vključno z njim) vzamemo člen, ki ni 1, ta faktor ne vpliva na koeficient pri x^n, kar bo dobljen produkt gotovo imel potenco višjo od n.

Torej koeficient pri x^n je koeficient pri x^n v končnem produktu

$$\frac{1}{1-x^1}\cdot\frac{1}{1-x^2}\cdots\frac{1}{1-x^n} = \left(1+x+x^2+\cdots\right)\left(1+x^2+x^4+\cdots\right)\cdots\left(1+x^n+x^{2n}+\cdots\right).$$

Torej koeficient pri x^n je število rešitev enačbe $n = a_1\cdot 1 + a_2\cdot 2+\cdots+a_n\cdot n$, to pa je ravno $p\,(n)$ — število število razčlenitev n. □

Definicija. Naj bo (distinct) $d\,(n) :=$ število razčlenitev s samimi različnimi členi.

Iščemo rodovno funkcijo za $d\,(n)$:

$$\sum_n d\,(n)\,x^n = \prod_{i=1}^{\infty}\overbrace{\left(1+x^i\right)}^{\text{lahko nimamo člena } i \text{ ali pa imamo enega}} = (1+x)\left(1+x^2\right)\left(1+x^3\right)\cdots$$

Definicija. Naj bo (odd) $o\,(n) :=$ število razčlenitev s samimi lihimi členi.

Zgled. $5 = 5 = 3+1+1 = 1+1+1+1+1$; $o\,(5) = 3$.

Iščemo rodovno funkcijo za $d\,(n)$:

$$\sum_n o\,(n)\,x^n = \prod_{i \text{ lih}}\left(x+i^i\right)$$

Trditev. $\forall n\in\mathbb{N} : d\,(n) = o\,(n)$

Dokaz.

$$\sum_n d(n)\,x^n = \prod_{i=1}^{\infty}\left(1+x^i\right) = \prod_{i=1}^{\infty}\left(1+x^i\right)\frac{\prod_{i=1}^{\infty}\left(1+x^i\right)}{\prod_{i=1}^{\infty}\left(1+x^i\right)} = \frac{\prod_{i=1}^{\infty}\left(1+x^{2i}\right)}{\prod_{i=1}^{\infty}\left(1+x^i\right)} = \prod_{i\ \text{lih}}^{\infty}\left(1+x^i\right) = \sum_n o(n)\,x^n$$

□

4.6 Uporaba rodovnih funkcij (zgolj zanimivost)

Vprašanje. *Zakaj so rodovne funkcije tako uporabne?*

1. Rodovna funkcija je „pogosto“ „lepa“, tudi če za zaporedje „ni“ „lepe“ forumule:

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

$$\sum_n S(n,k)\,x^n = \frac{x^k}{(1-x)(1-2x)\cdots(1-kx)}$$

$$\sum_n S(n,k)\,\frac{x^n}{n!} = \frac{1}{k!}\left(e^x-1\right)^k$$

Naj bo i_n št. involucij (permutacija, ki je sama sebi inverz: $\pi^2 = id$ oz $\pi^{-1} = \pi$ — to so permutacije, ki ima v zapisu z disjunktnimi cikli samo cikle dolžine 1 in 2) v S_n.

$$\sum_n i_n\frac{x^n}{n!} = e^{x+\frac{x^2}{2}}$$

2. Rodovna funkcija daje vse ostale načine podajanja zaporedja. Vsi ostali zapisi zaporedja so skriti v rodovni funkciji. Dva primera:

$$\sum_n F_n x^n = \frac{1}{1-x-x^2}$$

preko zapisa na parcialne ulomke dobimo eksplicitno formulo. Prav tako dobimo rekurzivni zapis:

$$\left(1-x-x^2\right)\sum_n F_n x^n = 1$$

na levi je koeficient pri x^n kar $F_n - F_{n-1} - F_{n-2}$, na desni pa 0 za $n \geq 2$. Odkrili smo še skrito rekruzivno zvezo.

$$\sum_n p_k(n)\,x^n = \frac{x^k}{(1-x)\left(1-x^2\right)\cdots\left(1-x^k\right)} = \left(\sum_n p_{k-1}(n)\,x^n\right)\cdot\frac{x}{1-x^k}$$

Torej $\left(1-x^k\right)\sum_n p_k(n)\,x^n = x\sum_n p_{k-1}(n)\,x^n$ in torej koeficient pri členu x^n je $p_k(n) - p_k(n-k) = p_{k-1}(n-1)$. Dobili smo še rekurzivno zvezo za p_k, skrito v rodovni funkciji.

3. Rodovno funkcijo se da pogosto dobiti neposredno iz kombinatoričnega opisa zaporedja

   (a) Kompozicije s členi 1 in 2: $2 = 2 = 1+1$, $3 = 1+1+1 = 2+1 = 1+2$, $4 = 1+1+1+1 = 2+1+1 = 1+2+1 = 1+1+2 = 2+2$, ... dobimo zaporedje $2, 3, 5, \ldots$ (Fibbonacijeva števila).
   Ena možnost je, da je zadnji člen kompozicije 1. Tisto pred njim podaja ravno eno kompozicijo števila $n-1$.
   Sicer je zadnji člen kompozicije 2 in tisto pred njim podaja ravno eno kompozicijo števila $n-2$.
   Torej je kompozicij števila n s členi 1 in 2 ravno $F_n = F_{n-1} + F_{n-2}$ in $F_0 = F_1 = 1$.
   Rodovna funkcija bo torej oblike

$$F(x) = \frac{1}{1-\underline{\qquad}},$$

   ker gre za zaporedje (zaporedja so rodovne funkcije take oblike).

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

   manjkajoči člen je $x+x^2$, ker so členi zaporedja lahko bodisi 1 bodisi 2.
   Torej kompozicije s členi 1 in 3:

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

(b) Involucije: permutacije, kjer velja $\pi^2 = id$, in nato še permutacije, kjer velja $\pi^3 = id$, in nato še permutacije, kjer velja $\pi^6 = id$:

$$e^{x+\frac{x^2}{2}}$$

beremo kot: „permutacija je sestavljena iz — e“ „ciklov dolžine —□□“ „ena — x“ „in — +“ „dve — $\frac{x^2}{2}$“.

$$e^{x+\frac{x^3}{3}}$$

beremo kot: „permutacija je sestavljena iz — e“ „ciklov dolžine —□□“ „ena — x“ „in — +“ „tri — $\frac{x^3}{3}$“.

$$e^{x+\frac{x^2}{2}+\frac{x^3}{3}+\frac{x^6}{6}}$$

beremo kot: „permutacija je sestavljena iz — e“ „ciklov dolžine —□□“ „ena — x“ „in — +“ „dve — $\frac{x^2}{2}$“ „in — +“ „tri — $\frac{x^3}{3}$“ „in — +“ „šest — $\frac{x^6}{6}$“.

4. Asimptotika je prav tako skrita v rodovni funkciji. Imamo rodovno funkcijo, potenčno vrsto okoli izhodišča. Glejmo nanjo kot na dejansko funkcijo (izposojamo si iz Kombinatorike 2). Ta funkcija ima singularosti — točke nedefiniranosti. Študiramo singularnosti in asimptotiko določa singularnost, ki je najbližje izhodišču.

   Primer za Fibonaccijeva števila:

$$\sum F_n x^n = \frac{1}{1-x-x^2}$$

   Singularnosti so ničle $1-x-x^2=0$, $x=\frac{-1\pm\sqrt{5}}{2}$, $x_0=\frac{-1+\sqrt{5}}{2}$ je od obeh bližje izhodišču. To pomeni, da je asimptotika od $F_n \sim A \cdot \frac{1}{x_0^n} = \cdots$, kjer je A nekaj izračunljivega.

5. Iz rodovne funkcije lahko izračunamo povprečja itd.

   (a) Koliko elementov imajo podmnožice $[n]$ v povprečju? $\frac{n}{2}$. Kako to izračunamo preko rodovne funkcije?

$$\overset{\text{delimo s št. podmnožic}}{\frac{1}{2^n}} \quad \overset{\text{seštevamo po možnih velikostih podmnožic}}{\sum_{k=0}^{n}} \quad \overset{\text{pojavnost velikosti}}{\binom{n}{k}} \cdot \overset{\text{število elementov}}{k} = ?$$

   Po binomskem izreku vemo $\sum_k \binom{n}{k} x^k = (1+x)^n$. Odvajamo to in dobimo $\sum_k \binom{n}{k} k x^{k-1} = n(1+x)^{n-1}$. Vstavimo $x=1$ in dobimo $\sum_k \binom{n}{k} k = n \cdot 2^{n-1} = \frac{n}{2}$.

   (b) Koliko imajo permutacije v S_n v povprečju ciklov? To pa ni več tako očitno. Poskusimo preko rodovne funkcije:

$$\overset{\text{delimo s številom vseh permutacij}}{\frac{1}{n!}} \quad \overset{\text{po vsej številčnostih ciklov}}{\sum_k} \quad \overset{\text{koliko jih je s } k \text{ cikli}}{c(n,k)} \quad k = ?$$

$$\sum_k c(n,k)\, x^k = x^{\overline{n}} = x(x+1)(x+2)\cdots(x+n-1)$$

   Zopet odvajajmo (produkt več faktorjev):

$$\sum_k c(n,k)\, k x^{k-1} = x'(x+1)(x+2)\cdots(x+n-1) +$$

$$+x(x+1)'(x+2)\cdots(x+n-1)+x(x+1)(x+2)'\cdots(x+n-1)+\cdots+x(x+1)(x+2)\cdots(x+n-1)' =$$
$$= 1(x+1)(x+2)\cdots(x+n-1)+x1(x+2)\cdots(x+n-1)+x(x+1)1\cdots(x+n-1)+\cdots+x(x+1)(x+2)\cdots 1$$

   Vstavimo $x=1$ in dobimo

$$\sum_k c(n,k)\, k = 2\cdot 3\cdots n + 1\cdot 3\cdot 4\cdots n + \cdots + 1\cdot 2\cdots(n-1) = n!\left(1+\frac{1}{2}+\cdots+\frac{1}{n}\right) = n! H_n$$

   Dobili smo, kar smo hoteli.

$$\frac{1}{n!}\sum_k c(n,k)\, k = \frac{1}{\cancel{n!}}\cancel{n!} H_n = H_n \sim \log n$$

   Iskanje povprečja v splošnem:

$$\frac{F'(1)}{F(1) \text{ skupno št. objektov}} = \log' F(x)\,|_{x=1}$$

5 Pólyeva teorija ([pójeva] teorija)

Madžarski matematik Pólya György (1887–1985).

Vprašanje. *Koliko je ogrlic z n koraldami in r barvami, če sta dve ogrlici enaki, če eno iz druge dobimo z rotacijo. Za $n = 4$, $r = 2$: $\circ\circ\circ\circ$, $\bullet\circ\circ\circ$, $\bullet\bullet\circ\circ$, $\bullet\bullet\bullet\circ$, $\bullet\circ\bullet\circ$, $\bullet\bullet\bullet\bullet$ (6)*

Vprašanje. *Koliko je zapestnic z n koraldami in r barvami, če sta dve zapestnici enaki, če eno iz druge dobimo z rotacijo ali zrcaljenjem? Za $n = 4$, $r = 2$: $\circ\circ\circ\circ$, $\bullet\circ\circ\circ$, $\bullet\bullet\circ\circ$, $\bullet\bullet\bullet\circ$, $\bullet\circ\bullet\circ$, $\bullet\bullet\bullet\bullet$ (6) v tem primeru enako.*

Če $n = 6$, $r = 2$ sta $\circ\circ\bullet\bullet\circ\bullet$ in $\bullet\circ\bullet\bullet\circ\circ$ različni ogrlici (z vrtenjem oziroma v tej 1D predstavitvi shiftom ne moremo iz ene v drugo), toda sta pa isti zapestnici (z zrcaljenjem oziroma v tej 1D predstavitvi reverseom iz leve dobimo desno).

Še krajši primer dveh istih zapestnic, ki nista isti ogrlici: $\circ\oplus\bullet$, $\circ\bullet\oplus$

Torej nekateri objekti so ekvivalentni, zanima nas število ekvivalenčnih razredov barvanj.

5.1 Permutacijska grupa

Množico korald bomo označevali z X, $|X| =: n \in \mathbb{N}$.

Grupa $(G, \cdot)$ je neprazna množica z asociativno operacijo, enoto in inverzi.

Zgled. S_n je nekomutativna grupa permutacij z operacijo $\circ$.

Definicija. Permutacijska grupa je podgrupa S_n, označimo $G \leq S_n$.

Izrek. *Cayley. Vsaka končna grupa je izomorfna neki permutacijski grupi. Ne bomo dokazali.*

Definicija. Ciklična grupa — grupa rotacij pravilnega $n-$kotnika: $C_n = \left\{(123\cdots n)^i; 0 \leq i < n\right\}$ je ciklična grupa in velja $(C_n, \circ) \underset{\text{izomorfna}}{\simeq} (\mathbb{Z}_n, +)$ z izomorfizmom $\varphi : \mathbb{Z}_n \to C_n; i \mapsto (123\cdots n)^i$.

Definicija. Diedrska grupa —Grupa vseh simetrij pravilnega $n-$kotnika: $D_n = \{\text{rotacije in zrcaljenja}\} \leq S_n$, specifično.

Dejstvo. *Velja $|D_n| = 2n$. Predstavljajmo si zrcaljanja/simetrije $n-$kotnika. Če je n lih, bo simetrala potekala skozi eno vozlišče in skozi eno stranico. Takih simetral je n. Če je n sod, bo simetrala potekala bodisi skozi dve stranici (tip I) bodisi skozi dve vozlišči (tip II). Takih je $\frac{n}{2} + \frac{n}{2} = n$.*

Upoštevamo še n rotacij in dobimo $2n$.

Zgled. Prav pride skica: $D_4 = \{id, (1234), (13)(24), (1432), (12)(34), (14)(23), (13), (24)\}$

Pripomba. Tudi S_n je permutacijska grupa.

Oglejmo si sedaj $G \leq S_X$, kjer je S_X množica korald, npr. $X = [n]$.

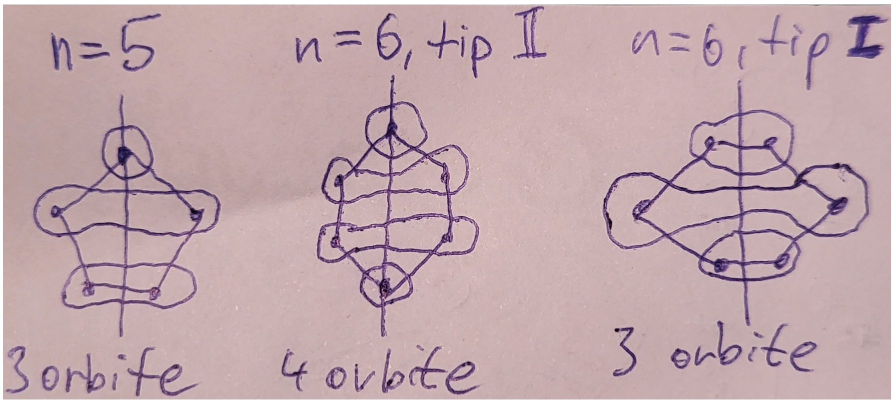
Definicija. Definiramo relacijo $x, y \in X$ s predpisom $x \sim y \Leftrightarrow \exists g \in G \ni: g \cdot x = y$. Trdimo, da je to ekvivalenčna relacija:

- Refleksivnost: $x \sim x$ $(g = id)$
- Simetričnost: $x \sim y \Rightarrow \exists g \in G \ni: g \cdot x = y \Rightarrow g^{-1} \cdot g \cdot x = g^{-1}y \Rightarrow g^{-1}y = x \wedge g^{-1} \in G \Rightarrow \exists g^{-1} \in G \ni: g^{-1}y = x \Rightarrow y \sim x$
- Tranzitivnost: $x \sim y \wedge y \sim z \Rightarrow \exists g, h \in G \ni: g \cdot x = y \wedge h \cdot y = z \Rightarrow g \cdot h \cdot x = h \cdot y = z \Rightarrow \exists g \cdot h \in G \ni: g \cdot h \cdot x = z \Rightarrow x \sim z$

X razpade na ekvivalenčne razrede, ki jih imenujemo orbite, ki jih označimo z $Gx := \{g \cdot x; g \in G\}$.

Zgled. $G = C_n \Longrightarrow Gx = X$ (samo ena orbita), $G = D_n \Longrightarrow Gx = X$, $G = S_n \Longrightarrow Gx = X$,

$$G = \{id, \text{zrcaljenje}\} \Longrightarrow \text{število orbit} = \begin{cases} \frac{n+1}{2} & ; n \text{ lih} \\ \frac{n}{2} & ; n \text{ sod in zrcaljenje je tipa I} \\ \frac{n}{2} + 1 & ; n \text{ sod in zrcaljenje je tipa II} \end{cases}.$$



Slika 8: Primer orbit za $n = 5$ in $n = 6$ za tip I in II.

Definicija. Z X/G označimo množico orbit, z $|X/G|$ število orbit, z $G_x \coloneqq \{g \in G; g \cdot x = x\}$ stabilizator $x-$a, z $X_g \coloneqq \{x \in X; g \cdot x = x\}$ množico negibnih točk $g-$ja.

Trditev. $G_x \leq G$ (stabilizator $x-$a je podgrupa G)

Dokaz. $id \in G_x$ velja. Zaprtost: $g, h \in G_x \Rightarrow g \cdot x = x, h \cdot x = x \Rightarrow (g \cdot h) \cdot x = g \cdot (h \cdot x) = g \cdot x = x \Rightarrow g \cdot h \in G_x$. Inverz: $g \in G_x \Rightarrow g \cdot x = x \Rightarrow g^{-1} \cdot x = g^{-1} \cdot g \cdot x = x \Rightarrow g^{-1} \in G_x$. □

Zgled. $G = C_n$, $G_x = \{id\}$, $X_g = \begin{cases} X & ; g = id \\ \emptyset & ; \text{sicer} \end{cases}$

Zgled. $G = D_n$, $G_x = \{id, \text{eno izmed zrcaljenj}\}$, $|X_g| = \begin{cases} n & ; g = id \\ 0 & ; g \in C_n \\ 1 & ; g \text{ zrcaljenje}, n \text{ lih} \\ 0 & ; g \text{ zrcaljenje tipa I}, n \text{ sod} \\ 2 & ; g \text{ zrcaljenje tipa II}, n \text{ sod} \end{cases}$

Zgled. $G = S_n$, $|X/G| = 1$, $Gx = X$, $G_x = (n-1)!$, $|X^g|$ = število negibnih točk permutacije g.

5.2 Burnsidova lema

Trditev. Naj bo $x \in X$ poljuben. Velja $|G| = |G_x| \cdot |Gx|$ (to še ni Burnsidova lema)

Zgled. Za $G = C_n$: $n = 1 \cdot n$. Za $G = D_n$: $2n = 2 \cdot n$. Za $G = S_n$: $n! = (n-1)! \cdot n$.

Dokaz. Naj bo G poljubna grupa in $H \leq G$ njej poljubna podgrupa. Spomnimo se nekaj stvari od lani:

- $g \cdot H \coloneqq \{g \cdot h; h \in H\}$ je levi odsek. Npr. za $g = e$ je $e \cdot H = H$. Izkaže se, da za $g, g' \in G$ velja bodisi $g \cdot H = g' \cdot H$ bodisi $g \cdot H \cap g' \cdot H = \emptyset$. Odseki torej tvorijo razdelitev G.
- Velja še, da imajo odseki enako moč, ker lahko tvorimo bijekcijo $H \to gH$, ki slika $h \mapsto gh$ z inverzom $h \mapsto g^{-1}h$.
- Vpeljemo lahko torej množico vseh levih odsekov — kvocientno množico, oznaka $G/H \coloneqq \{gH; g \in G\}$.
- Ker so vsi odseki enako veliki, lahko njihovo število dobimo takole: $|G/H| = \frac{|G|}{|H|}$. Posledično moč podgrupe vselej deli moč grupe. $[G : H]$ je indeks podgrupe H.

Sedaj vse to uporabimo za podgrupo stabilizator: $H = G_x$. Dobimo $|G/G_x| = \frac{|G|}{|G_x|}$. Iščemo torej bijekcijo $Gx \to G/Gx$. Preslikajmo nek element iz Gx takole $\varphi : g \cdot x \mapsto g \cdot G_x$ v levi odsek.

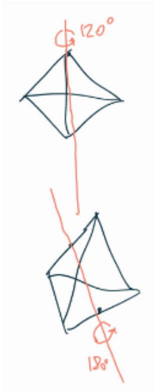
Preveriti moramo dobro definiranost. X razpade na orbite. Resda vsak element x v orbiti lahko izrazimo kot $g \cdot x$ za nek g, toda ta g ni enolično določen. Preveriti moramo, da za dva g, h, za katera velja $g \cdot x = h \cdot x$, velja tudi $g \cdot G_x = h \cdot G_x$. Po predpostavki velja $g \cdot x = h \cdot x \Leftrightarrow h^{-1} \cdot g \cdot x = x \Leftrightarrow h^{-1} \cdot g \in G_x \Leftrightarrow h^{-1} \cdot g \cdot G_x = G_x \overset{h\cdot\backslash}{\Leftrightarrow} g \cdot G_x = h \cdot G_x$.

Z najdeno celo ekvivalenco $g \cdot x = h \cdot x \Leftrightarrow g \cdot G_x = h \cdot G_x$. Torej smo dokazali še, da če je $g \cdot G_x = h \cdot G_x$, potem je $g \cdot x = h \cdot x$. To je injektivnost. Dokazati moramo le še surjektivnost.

Surjektivnost: Poljuben $g \cdot G_x$ je res slika nekega elementa iz orbite, specifično elementa $g \cdot x$.

Dokazali smo, da je φ bijekcija, torej je $|Gx| = \frac{|G|}{|G_x|}$ oziroma $|Gx| \cdot |G_x| = |G|$. □

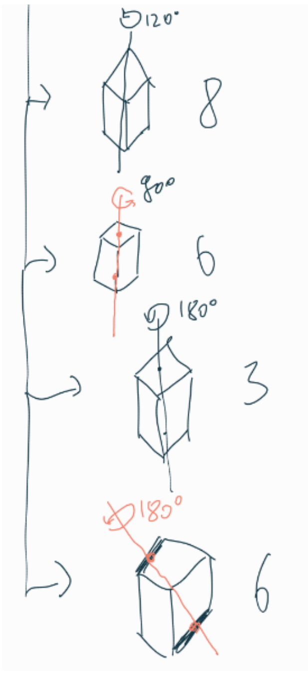
Zgled. Preštejmo simetrije tetraedra. $|G| = |G_x|\,|Gx|$. Vzemimo eno oglišče. Moč orbite tega oglišča je 4 (do vseh oglišč lahko pridemo z D_n). Kolikšna je moč stabilizatorja? Katere simetrije fiksirajo x? Tri. Torej je vseh simetrij 12. To so: identiteta, rotacija v eno in drugo smer skozi vsako izmed štirih oglišč, rotacija za 180 stopinj skozi središči dveh nasprotiležnih stranic za tri take pare nasprotiležnih stranic: $1 + 2 \cdot 4 + 3 = 12$.



Slika 9: Simetrije tetraedra, razen identitete.

Zgled. Preštejmo simetrije kocke. $|G| = |G_x|\,|Gx|$. $G_x = X$, $|G_x| = 8$, $|G_x| = 3$ (identiteta in rotaciji za 120° v obe smeri okoli telesne diagonale). Potemtakem $|G| = 3 \cdot 8 = 24$.

Te simetrije so: identiteta, dve rotaciji za 120° za obe smeri okoli štirih telesnih diagonal, rotaciji za 90° v levo in desno okoli premice skozi težišči dveh nasprotnih ploskev (taki pari so trije), tri rotacije za 180° (po ravninah $x = 0$, $y = 0$ in $z = 0$ — težišče kocke je v $0, 0, 0$), rotacija za 180° okoli telesne zveznice, ki povezuje dve medsebojno najbolj oddaljeni in vzporedni stranici (takih parov je 6). Skupaj torej $1 + 2 \cdot 4 + 2 \cdot 3 + 3 + 6 = 24$.



Slika 10: Simetrije kocke, razen identitete.

In velja $G \cong S_4$.

Povzetek. Naj bo G permutacijska grupa, X množica točk. Tedaj $Gx \coloneqq \{gx; \forall g \in G\}$ orbita, $G_x = \{g \in G; gx = x\} \leq G$ stabilizator, $X/G = \{Gx; \forall x \in X\}$ množica orbit, $X_g = \{x \in X; gx = x\}$ negibne točke. $\forall x \in X : |G| = |Gx|\,|G_x|$.

Lema. *Burnsidova lema. Število orbit je enako povprečnemu številu negibnih točk ZDB*

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

Dokaz. Pretvorimo

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

Orbite (ekvivalenčni razredi) so lahko različnih velikosti. Recimo, da se X deli na štiri orbite velikosti 1, 2, 4, 6. Tedaj bo izraz

$$\sum_{x\in X}\frac{1}{|Gx|} = \left(\frac{1}{1}\right)+\left(\frac{1}{2=\text{ velikost orbite}}+\frac{1}{2}\right)+\left(\overbrace{\frac{1}{4}+\frac{1}{4}+\frac{1}{4}+\frac{1}{4}}^{\text{elementi orbite moči 4}}\right)+\left(\frac{1}{6}+\frac{1}{6}+\frac{1}{6}+\frac{1}{6}+\frac{1}{6}+\frac{1}{6}\right) = 1+1+1+1 =$$

$$= 4 = \text{število orbit} = \sum_{\sigma\in X/G}\sum_{x\in\sigma}\frac{1}{|\sigma|} = \sum_{\sigma\in|X/G|}1 = |X/G|$$

Torej

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

□

Zgled. Imejmo $G = C_n$ in $X = [n]$. Velja $1 = |X/G| = \frac{1}{n}\left(\overset{\text{identiteta}}{n} + \overset{\text{pravih rotacij}}{(n-1)}\cdot 0\right) = \frac{n}{n} = 1$.

Zgled. Imejmo $G = D_n$ in $X = [n]$. Velja $1 = |X/G|$. Za n lih:

$$\frac{1}{2n}\left(\overset{\text{identiteta}}{n} + \overset{\text{pravih rotacij}}{(n-1)}\cdot 0 + \overset{\text{zrcaljenja}}{n}\cdot\overset{\text{negibna točka}}{1}\right) = \frac{2n}{2n} = 1$$

Za n sod:

$$\frac{1}{2n}\left(\overset{\text{identiteta}}{n} + \overset{\text{pravih rotacij}}{(n-1)}\cdot 0 + \overset{\text{zrcaljenja tipa I}}{\frac{n}{2}}\cdot\overset{\text{negibna točka}}{0} + \overset{\text{zrcaljenja tipa II}}{\frac{n}{2}}\cdot\overset{\text{negibna točka}}{2}\right) = \frac{2n}{2n} = 1$$

Zgled. $G = \{id, \text{eno zrcaljenje}\}$ in $X = [n]$. Za n lih:

$$\frac{n+1}{2} = |X/G| = \frac{1}{|G|=2}\left(\overset{\text{identiteta}}{n} + \overset{\text{zrcaljenje}}{1}\right) = \frac{n+1}{2}$$

Za n sod in zrcaljenje je tipa I:

$$\frac{n}{2} = |X/G| = \frac{1}{2}\left(\overset{\text{identiteta}}{n} + \overset{\text{zrcaljenje}}{0}\right) = \frac{n}{2}$$

Za n sod in zrcaljenje tipa II:

$$\frac{n}{2}+1 = |X/G| = \frac{1}{2}\left(\overset{\text{identiteta}}{n} + \overset{\text{zrcaljenje}}{2}\right) = \frac{n+2}{2} = \frac{n}{2}+1$$

Zgled. $G = S_n$ in $X = [n]$. Velja

$$1 = |X/G| = \frac{1}{n!}\sum_{\pi\in S_n}\text{št. negibnih točk permutacije } \pi$$

To ni tako očitno brez Burnsidove leme.

Zgled. Imejmo 3x3 papirnato mrežo in dve različni celici preluknjajmo. Koliko je različnih konfiguracij, če lahko eno iz druge dobimo z zrcaljenjem in rotacijami (torej grupa D_4)?

Uporabimo Burnsidovo lemo. Izračunajmo št. negibnih točk za vsako permutacijo.

- id ima $|X|$ negibnih točk in velja $|X| = \binom{9}{2} = 36$: $1\cdot 36 = 36$
- rotaciji za 90 stopinj nimata negibnih točk: $2\cdot 0 = 0$

- rotacija za 180 stopinj ima štiri negibne točke: $1 \cdot 4 = 4$

$$\begin{matrix} \circ & \circ & \circ \\ \bullet & \circ & \bullet \\ \circ & \circ & \circ \end{matrix}, \quad \begin{matrix} \circ & \bullet & \circ \\ \circ & \circ & \circ \\ \circ & \bullet & \circ \end{matrix}, \quad \begin{matrix} \circ & \circ & \bullet \\ \circ & \circ & \circ \\ \bullet & \circ & \circ \end{matrix}, \quad \begin{matrix} \bullet & \circ & \circ \\ \circ & \circ & \circ \\ \circ & \circ & \bullet \end{matrix}$$

- zrcaljenja: $4 \cdot 6 = 24$
  - $\updownarrow$: 6

$$\begin{matrix} \circ & \circ & \circ \\ \bullet & \bullet & \circ \\ \circ & \circ & \circ \end{matrix}, \quad \begin{matrix} \circ & \circ & \circ \\ \circ & \bullet & \bullet \\ \circ & \circ & \circ \end{matrix}, \quad \begin{matrix} \circ & \circ & \circ \\ \bullet & \circ & \bullet \\ \circ & \circ & \circ \end{matrix}, \quad \begin{matrix} \circ & \bullet & \circ \\ \circ & \circ & \circ \\ \circ & \bullet & \circ \end{matrix}, \quad \begin{matrix} \bullet & \circ & \circ \\ \circ & \circ & \circ \\ \bullet & \circ & \circ \end{matrix}, \quad \begin{matrix} \circ & \circ & \bullet \\ \circ & \circ & \circ \\ \circ & \circ & \bullet \end{matrix}$$

  - $\leftrightarrow$ enako, le da si predstavljamo papirčke rotirane za 90 stopinj: 6
  - pozitivna diagonala: 6

$$\begin{matrix} \bullet & \circ & \circ \\ \circ & \bullet & \circ \\ \circ & \circ & \circ \end{matrix}, \quad \begin{matrix} \circ & \circ & \circ \\ \circ & \bullet & \circ \\ \circ & \circ & \bullet \end{matrix}, \quad \begin{matrix} \bullet & \circ & \circ \\ \circ & \circ & \circ \\ \circ & \circ & \bullet \end{matrix}, \quad \begin{matrix} \circ & \bullet & \circ \\ \bullet & \circ & \circ \\ \circ & \circ & \circ \end{matrix}, \quad \begin{matrix} \circ & \circ & \bullet \\ \circ & \circ & \circ \\ \bullet & \circ & \circ \end{matrix}, \quad \begin{matrix} \circ & \circ & \circ \\ \circ & \circ & \bullet \\ \circ & \bullet & \circ \end{matrix}$$

  - negativna diagonala: enako, le da si predstavljamo papirčke rotirane za 90 stopinj — 6

Skupaj torej 64 negibnih točk. Elementov diedrske grupe D_4 je 8, torej je število orbit $\frac{1}{8} \cdot 64 = 8$. Predstavniki orbit so

$$\begin{matrix} \bullet & \bullet & \circ \\ \circ & \circ & \circ \\ \circ & \circ & \circ \end{matrix}, \quad \begin{matrix} \bullet & \circ & \bullet \\ \circ & \circ & \circ \\ \circ & \circ & \circ \end{matrix}, \quad \begin{matrix} \bullet & \circ & \circ \\ \circ & \bullet & \circ \\ \circ & \circ & \circ \end{matrix}, \quad \begin{matrix} \bullet & \circ & \circ \\ \circ & \circ & \bullet \\ \circ & \circ & \circ \end{matrix}, \quad \begin{matrix} \bullet & \circ & \circ \\ \circ & \circ & \circ \\ \circ & \circ & \bullet \end{matrix}, \quad \begin{matrix} \circ & \bullet & \circ \\ \bullet & \circ & \circ \\ \circ & \circ & \circ \end{matrix}, \quad \begin{matrix} \circ & \bullet & \circ \\ \circ & \circ & \circ \\ \circ & \bullet & \circ \end{matrix}, \quad \begin{matrix} \circ & \bullet & \circ \\ \circ & \bullet & \circ \\ \circ & \circ & \circ \end{matrix}$$

Vsi elementi po orbitah so:

- $$\begin{matrix} \bullet & \bullet & \circ \\ \circ & \circ & \circ \\ \circ & \circ & \circ \end{matrix} = \begin{matrix} \bullet & \circ & \circ \\ \bullet & \circ & \circ \\ \circ & \circ & \circ \end{matrix} = \begin{matrix} \circ & \circ & \circ \\ \bullet & \circ & \circ \\ \bullet & \circ & \circ \end{matrix} = \begin{matrix} \circ & \circ & \circ \\ \circ & \circ & \circ \\ \bullet & \bullet & \circ \end{matrix} = \begin{matrix} \circ & \circ & \circ \\ \circ & \circ & \circ \\ \circ & \bullet & \bullet \end{matrix} = \begin{matrix} \circ & \circ & \circ \\ \circ & \circ & \bullet \\ \circ & \circ & \bullet \end{matrix} = \begin{matrix} \circ & \circ & \bullet \\ \circ & \circ & \bullet \\ \circ & \circ & \circ \end{matrix} = \begin{matrix} \circ & \bullet & \bullet \\ \circ & \circ & \circ \\ \circ & \circ & \circ \end{matrix}$$
- $$\begin{matrix} \bullet & \circ & \bullet \\ \circ & \circ & \circ \\ \circ & \circ & \circ \end{matrix} = \begin{matrix} \bullet & \circ & \circ \\ \circ & \circ & \circ \\ \bullet & \circ & \circ \end{matrix} = \begin{matrix} \circ & \circ & \circ \\ \circ & \circ & \circ \\ \bullet & \circ & \bullet \end{matrix} = \begin{matrix} \circ & \circ & \bullet \\ \circ & \circ & \circ \\ \circ & \circ & \bullet \end{matrix}$$
- $$\begin{matrix} \bullet & \circ & \circ \\ \circ & \bullet & \circ \\ \circ & \circ & \circ \end{matrix} = \begin{matrix} \circ & \circ & \circ \\ \circ & \bullet & \circ \\ \bullet & \circ & \circ \end{matrix} = \begin{matrix} \circ & \circ & \circ \\ \circ & \bullet & \circ \\ \circ & \circ & \bullet \end{matrix} = \begin{matrix} \circ & \circ & \bullet \\ \circ & \bullet & \circ \\ \circ & \circ & \circ \end{matrix}$$
- $$\begin{matrix} \bullet & \circ & \circ \\ \circ & \circ & \bullet \\ \circ & \circ & \circ \end{matrix} = \begin{matrix} \circ & \circ & \bullet \\ \bullet & \circ & \circ \\ \circ & \circ & \circ \end{matrix} = \begin{matrix} \circ & \circ & \circ \\ \circ & \circ & \bullet \\ \bullet & \circ & \circ \end{matrix} = \begin{matrix} \circ & \circ & \circ \\ \bullet & \circ & \circ \\ \circ & \circ & \bullet \end{matrix} = \begin{matrix} \bullet & \circ & \circ \\ \circ & \circ & \circ \\ \circ & \bullet & \circ \end{matrix} = \begin{matrix} \circ & \bullet & \circ \\ \circ & \circ & \circ \\ \bullet & \circ & \circ \end{matrix} = \begin{matrix} \circ & \bullet & \circ \\ \circ & \circ & \circ \\ \circ & \circ & \bullet \end{matrix} = \begin{matrix} \circ & \circ & \bullet \\ \circ & \circ & \circ \\ \circ & \bullet & \circ \end{matrix}$$
- $$\begin{matrix} \bullet & \circ & \circ \\ \circ & \circ & \circ \\ \circ & \circ & \bullet \end{matrix} = \begin{matrix} \circ & \circ & \bullet \\ \circ & \circ & \circ \\ \bullet & \circ & \circ \end{matrix}$$
- $$\begin{matrix} \circ & \bullet & \circ \\ \bullet & \circ & \circ \\ \circ & \circ & \circ \end{matrix} = \begin{matrix} \circ & \circ & \circ \\ \bullet & \circ & \circ \\ \circ & \bullet & \circ \end{matrix} = \begin{matrix} \circ & \circ & \circ \\ \circ & \circ & \bullet \\ \circ & \bullet & \circ \end{matrix} = \begin{matrix} \circ & \bullet & \circ \\ \circ & \circ & \bullet \\ \circ & \circ & \circ \end{matrix}$$
- $$\begin{matrix} \circ & \bullet & \circ \\ \circ & \circ & \circ \\ \circ & \bullet & \circ \end{matrix} = \begin{matrix} \circ & \circ & \circ \\ \bullet & \circ & \bullet \\ \circ & \circ & \circ \end{matrix}$$

- $$\begin{array}{ccc}\circ & \bullet & \circ\\ \circ & \bullet & \circ\\ \circ & \circ & \circ\end{array} = \begin{array}{ccc}\circ & \circ & \circ\\ \bullet & \bullet & \circ\\ \circ & \circ & \circ\end{array} = \begin{array}{ccc}\circ & \circ & \circ\\ \circ & \bullet & \circ\\ \circ & \bullet & \circ\end{array} = \begin{array}{ccc}\circ & \circ & \circ\\ \circ & \bullet & \bullet\\ \circ & \circ & \circ\end{array}$$

Če bi torej take preluknjane papirčke uporabljali kot recimo nek identifikacijski dokument, bi lahko identificirali osem različnih osebkov.

5.3 Ciklični indeks in Pólyjev izrek

Definicija. Imamo elemente X, $|X| = n$, permutacijsko grupo $G \leq S_X$ in $g \in G$ je permutacija elementov iz X. Zapišimo g kot produkt disjunktnih ciklov in zapišimo g kot produkt disjunktnih ciklov, z $\alpha_i(g)$ označimo število ciklov dolžine i. Ciklični indeks je polinom

$$z_G(t_1, \dots, t_n) \coloneqq \frac{1}{|G|} \sum_{g \in G} t_1^{\alpha_i(g)} t_2^{\alpha_2(g)} t_3^{\alpha_3(g)} \cdots t_n^{\alpha_n(g)}.$$

Zgled. $G = C_4$, $X = [4]$. Ogrlica s štirimi koraldami.

$$z_G(t_1, t_2, t_3, t_4) = \frac{1}{4}\left(\overset{\text{identiteta: 4 cikle dolžine 1}}{t_1^4} + \overset{\text{rotacija 180: 2 cikla dolžine 2}}{t_2^2} + \overset{\text{dve rotaciji 90: 1 cikel dolžine 4}}{2t_4}\right)$$

Ciklični indeks nam pove povprečno ciklično strukturo elementov G.

Zgled. $G = D_4$, $X = [4]$. Zapestnica s štirimi koraldami.

$$z_G(t_1, t_2, t_3, t_4) = \frac{1}{8}\left(\overset{id}{t_1^4} + \overset{\text{rotacije}}{t_2^2 + 2t_4} + \overset{\text{horizontalno in vertikalno zrcaljenje}}{2t_2^2} + \overset{\text{diagonalni zrcaljenji}}{2t_1^2 t_2}\right)$$

Zgled. Simetrije tetraedra (štiri oglišča), ki delujejo na ogliščih. Dvanajst jih je: orbita je velikosti 4, tri simetrije fiksirajo vozlišče: id, dve rotaciji za 120 za vsako izmed štirih vozlišč ($4 \cdot 2 = 8$ in imajo isto ciklično strukturo), tri rotacije za 180 stopinj prek nasprotnih vzporednih stranic.

$$z_G(t_1, t_2, t_3, t_4) = \frac{1}{12}\left(\overset{id}{t_1^4} + \overset{120^\circ}{8t_1 t_3} + \overset{180^\circ}{3t_2^2}\right)$$

Zgled. Simetrije tetraedra, ki delujejo na stranicah (6 stranic). Grupa simetrij je ista, spremeni pa se X in s tem ciklična struktura.

$$z_G(t_1, t_2, t_3, t_4, t_5, t_6) = \frac{1}{12}\left(\overset{id}{t_1^6} + \overset{120^\circ}{8t_3^2} + \overset{180^\circ}{3t_1^2 t_2^2}\right)$$

Zgled. Simetrije tetraedra, ki delujejo na ploskvah (4 ploskve). Grupa simetrij je ista, spremeni pa se X in s tem ciklična struktura.

$$z_G(t_1, t_2, t_3, t_4) = \frac{1}{12}\left(\overset{id}{t_1^4} + \overset{120^\circ}{8t_1 t_3} + \overset{180^\circ}{t_2^2}\right)$$

Zgled. G so simetrije kocke, X so oglišča kocke. 24 jih je (ena orbita z osmimi elementi, tri simetrije oglišča ne premaknejo), ker $3 \cdot 8 = 24$. To so identiteta, rotaciji 90 po eni izmed treh osi, rotacija 180 po eni izmed treh osi, rotaciji 120 okoli telesne diagonale za štiri take diagonale, rotacija 180 po telesni diagonali, ki jo tvorita središči dveh nasprotnih stranic (takih parov je 6).

Opazimo lahko $G \hat{=} S_4$. Imamo štiri glavne telesne diagonale in natanko vse naštete permutacije so permutacije teh diagonal.

$$z_G(t_1, t_2, t_3, t_4, t_5, t_6, t_7, t_8) = \frac{1}{24}\left(t_1^8, 3 \cdot 2 \cdot t_4^2 + 3t_2^4 + 4 \cdot 2 \cdot t_3^2 t_1^2 + 6t_2^4\right)$$

Izrek.

$$z_{C_n}(t_1, \dots, t_n) = \frac{1}{n} \sum_{d \mid n} \varphi(d)\, t_d^{\frac{n}{d}}$$

Dokaz. $C_n = \left\{(1,2,\ldots,n)^i\,; 0 \le i \le n-1\right\}$. Npr. $(123456)^2 = (135)\,(246)$, $(123456)^3 = (14)\,(25)\,(36)$, $(123456)^4 = (153)\,(264)$.

Razmislimo, kaj se zgodi, če damo cikel $(12\cdots n)$ na potenco, ki je delitelj n? $d|n$ in

$$(12\cdots n)^d = (1 \quad d+1 \quad 2d+1 \quad 3d+1 \quad \cdots)\,(2 \quad d+2 \quad 2d+2 \quad 3d+2 \quad \cdots)\,;$$

dobimo produkt d ciklov dolžin $\frac{n}{d}$.

Kaj pa, če ga damo na potenco, ki ni delitelj n? $(123456)^5 = (165432)$. Če sta si potenca in dolžina tuji $\gcd(n,d) = 1$, dobimo en cikel ZDB $(1\cdots n)^i$ je $n-$cikel, če sta si i in n tuji števili.

Sedaj označimo $d = D\,(n,i)$, torej $n = d\cdot n'$ in $i = d\cdot i'$. To pomeni, da

$$(123\cdots n)^i = \left(\overbrace{(123\cdots n)^d}^{\text{produkt } d \text{ ciklov dolžine } \frac{n}{d}=n'}\right)^{i'} =$$

po konstrukciji sta n' in i' tuji, po prejšnjem razmisleku torej te $n'-$cikli na $i'-$to potenco ostanejo n' cikli

$$= \text{produkt } d \text{ ciklov dolžin } \left(n' = \frac{n}{d}\right)$$

Torej od te potence i dobimo $t_{\frac{n}{d}}^d$ doprinos k cikličnemu indeksu. Kolikokrat dobimo ta rezultat? Koliko je $i-$jev, da je $D\,(n,i) = d$? Torej $i = d\cdot i'$ pri pogojih $1 \le i' \le \frac{n}{3}$ in $D\left(i', \frac{n}{d}\right)$. Pozitivnih števil, manjših od $\frac{n}{d}$, ki so tuja z $\frac{n}{d}$, je $\varphi\left(\frac{n}{d}\right)$.

Potemtakem $z_{C_n}\,(t_1,\ldots,t_n) = \frac{1}{n}\sum_{d|n}\varphi\left(\frac{n}{d}\right)t_{\frac{n}{d}}^d = \frac{1}{n}\sum_{d|n}\varphi\,(d)\,t_d^{\frac{n}{d}}$. Opomba: $\varphi\,(n) = n\prod_{p|n, p \text{ praštevilo}}\left(1-\frac{1}{p}\right)$ □

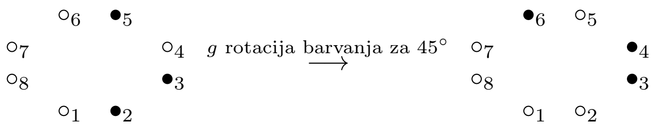
Izrek.

$$z_{D_n}\,(t_1,\ldots,t_n) = \frac{1}{2}z_{C_n}\,(t_1,\ldots,t_n) + \begin{cases} \frac{1}{2}t_1 t_2^{\frac{n-1}{2}} & ; n \text{ lih} \\ \frac{1}{4}t_2^{\frac{n}{2}} + \frac{1}{4}t_1^2 t_2^{\frac{n}{2}-1} & ; n \text{ sod} \end{cases}$$

Dokaz. Prvi člen: seveda je $C_n \subseteq D_n$. Izračunajmo še doprinos zrcaljenja. Za lih n imamo po en cikel (negibna točka) in $\frac{n-2}{2}$ dvaciklov, za n sod pa imamo pol zrcaljenj tipa I in pol zrcaljenj tipa II. □

5.4 Neekvivalentna barvanja

Definicija. X je množica korald, $|X| = n$, $G \le S_X$ permutacijska grupa, R množica barv, $|R| = r$. Barvanje je funkcija $b : X \to R$, R^X je množica barvanj. Velja $\left|R^X\right| = r^n$. Če G deluje na X, se nam implicitno porodi tudi delovanje na R^X. Oglejmo si primer $n = 8$, $r = 2$:

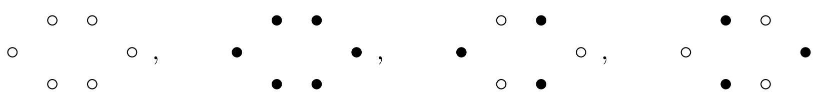


Definiramo preslikavo barvanja takole: $\hat{g}\cdot b\,(x) = b\left(g^{-1}\cdot x\right)$. Če je $r > 1$, dobimo delovanje grupe, izomorfni G, na R^X (podrobnosti na KOMB2).

Sedaj nas zanimajo orbite barvanj — zanima nas, katera barvanja so ekvivalentna do permutacije za dano permutacijsko grupo.

Da dobimo število orbit tega delovanja, moramo po Burnsidovi lemi izračunati povprečno število negibnih točk.

Zgled. $n = 6$, $r = 2$, g rotacija za 120 stopinj. Negibne točke so štiri:



Pri rotaciji za 90 stopinj sta negibni točki samo barvanji vseh točk z isto barvo (2), pri rotaciji za 180 stopinj je negibnih barvanj 8 (3^2 — trem zaporednim vozliščem lahko izberemo poljubno barvo, ostala tri imajo nato določeno barvo).

Dejstvo. *Splošneje: Naj bo $g \in G$ neka permutacija X. Barvanje b je negibna točka za g $(g\cdot b = b) \Leftrightarrow$ vse koralde v enem ciklu $g-$ja so iste barve.*

Dokaz. $g \cdot b = b \sim \forall x \in X : gb(x) = b(x) \sim b\left(g^{-1}x\right) = b(x) \sim g^{-1}x$ in x sta iste barve $\sim x$ in gx sta iste barve $\sim x$ in g^2x sta iste barve $\sim \forall i : b(x) = b\left(g^i x\right)$. Torej $x, g \cdot x, g^2 x, \cdots$ so vsi iste barve ZDB cel cikel je iste barve. $\square$

Torej je $r^{c(g)}$ število negibnih barvanj g, kjer je $c(g) = \sum_i \alpha_i(g)$, kjer je $\alpha_i(g)$ je število ciklov v g dolžine i.

Izrek. *Pólyjev izrek. Število neekvivalentnih barvanj je*

$$\frac{1}{|G|}\sum_{g\in G} r^{c(g)} = z_G(r,\ldots,r) \overset{\text{definicija } z_G}{=} \sum_{g\in G} r^{\alpha_1(g)} r^{\alpha_2(g)} \cdots r^{\alpha_n(g)} = \sum_{g\in G} r^{\sum_i \alpha_i(g)}$$

Dokaz. Zgornji razmislek. $\square$

Zgled. Ogrlic z n koraldami in r barvami je

$$\frac{1}{n}\sum_{g\in C_n} r^{c(g)} = z_{C_n}(r,\cdots,r) = \frac{1}{n}\sum_{d|n}\varphi(d)\, r^{\frac{n}{d}}$$

Npr. za $n = 4$: $\frac{1}{4}\left(r^4 + r^2 + 2r\right)$, torej za $r = 2$ je $\frac{1}{4}(16+4+4) = 6$.

Zgled. Zapestnic z n koraldami in r barvami je

$$\frac{1}{2n}\sum_{g\in D_n} r^{c(g)} = z_{D_n}(r,\cdots,r) = \frac{1}{2n}\sum_{d|n}\varphi(d)\, r^{\frac{n}{d}} + \begin{cases} \frac{1}{2} r r^{\frac{n-1}{2}} = \frac{1}{2} r^{\frac{n+1}{2}} & ; n \text{ lih} \\ \frac{1}{4} r^{\frac{n}{2}} + \frac{1}{4} r^2 r^{\frac{n}{2}-1} = \frac{1}{4} r^{\frac{n}{2}} + \frac{1}{4} r^{\frac{n}{2}+1} & ; n \text{ sod} \end{cases}.$$

Zgled. Naj bo $G = S_n$, $X = [n]$ in $|R| = r$. Dve barvanji sta očitno v tem primeru ekvivalentni takrat, ko za vsako barvo velja, da je v obeh barvanjih uporabljena enakokrat. Očitno je torej neekvivalentnih barvanj toliko, kolikor je šibkih kompozicij n z r členi $= \binom{n+r-1}{r-1}$. Po drugi strani je to po Pólyjevem izreku enako

$$\frac{(n+r-1)!}{(r-1)!n!} = \binom{n+r-1}{r-1} = \frac{1}{|G|}\sum_{\pi\in S_n} r^{c(\pi)} = \frac{1}{n!}\sum_{\pi\in S_n} r^{c(\pi)} = \frac{1}{n!}\sum_{k \text{ št. ciklov}} \overset{\text{stirling1: št permutacij } [n] \text{ s } k \text{ cikli}}{c(n,k)}\, r^k$$

$$\frac{(n+r-1)!}{(r-1)!\cancel{n!}} = \frac{\cancel{1}}{\cancel{n!}}\sum_k c(n,k)\, r^k$$

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

Prišli smo do prehodne matrike med dvema bazama polinomov (najdene na začetku tečaja).

Sedaj pa recimo, da nas zanima število neekvivalentnih barvanj, pri čemer zahtevamo, da je β_i korald barve 1, β_2 korald barve 2, ...

Izrek. *Posplošeni Pólyjev izrek. Imejmo X množico korald ($|X| = n$), G permutacijsko grupo, R množico barvanj, $|R| = r$. Število neekvivalentnih barvanj z β_i koraldami barve i je enako koeficientu pri $u_1^{\beta_1} u_2^{\beta_2} \cdots u_r^{\beta_r}$ v*

$$z_G\left(u_1 + \cdots + u_r, u_1^2 + \cdots + u_r^2, \ldots u_1^n + \cdots + u_r^n\right).$$

Zgled. Vzemimo $G = C_4$, $n = 4$, $r = 2$ (ogrlice).

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

Po posplošenem Pólyevem izreku

$$z_{C_4}\left(u_1+u_2, u_1^2+u_2^2, u_1^3+u_2^3, u_1^4+u_2^4\right) = \frac{1}{4}\left((u_1+u_2)^4 + \left(u_1^2+u_2^2\right)^2 + 2\left(u_1^4+u_2^4\right)\right) =$$

$$= \frac{1}{4}\left(u_1^4 + 4u_1^3u_2 + 6u_1^2u_2^2 + 4u_1u_2^3 + u_2^4 + u_1^4 + 2u_1^2u_2^2 + u_2^4 + 2u_1^4 + 2u_2^4\right) =$$

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

Torej obstajata dve neekvivalentni barvanji ogrlic z dvema črnima in dvema belima koraldama, ker je 2 koeficient pri $u_1^2u_2^2$.

Zgled. Vzemimo $G = D_6$, $n = 6$, $r = 3$. Koliko je zapestnic z eno črno, tremi belimi in dvema rdečima koraldama?

$$\begin{aligned} z_{D_6}(t_1, \ldots, t_6) &= \overbrace{\frac{1}{12}\left(t_1^6 + \varphi(2)\, t_2^3 + \varphi(3)\, t_3^2 + \varphi(6)\, t_6\right)}^{\text{rotacije}} + \frac{1}{4} t_2^3 + \frac{1}{4} t_1^2 t_2^2 = \\ &= \frac{1}{12}\left(t_1^6 + t_2^3 + 2t_3^2 + 2t_6\right) + \frac{1}{4} t_2^3 + \frac{1}{4} t_1^2 t_2^2 \end{aligned}$$

Zanima nas

$$\left[u_1 u_2^3 u_3^2\right] \frac{1}{12}\left((u_1+u_2+u_3)^6 + \left(u_1^2+u_2^2+u_3^2\right)^3 + 2\left(u_1^3+u_2^3+u_3^3\right)^2 + 2\left(u_1^6+u_2^6+u_3^6\right)\right) +$$

$$+\frac{1}{4}\left(u_1^2+u_2^2+u_3^2\right)^3 + \frac{1}{4}(u_1+u_2+u_3)^2\left(u_1^2+u_2^2+u_3^2\right)^2 =$$

... kjer imamo same kvadrate, kube ali potence 6, gotovo ne bomo dobili potrebnega u_1 ...

$$= \left[u_1 u_2^3 u_3^2\right]\left(\frac{1}{12}(u_1+u_2+u_3)^6 + \frac{1}{4}(u_1+u_2+u_3)^2\left(u_1^2+u_2^2+u_3^2\right)^2\right) =$$

$$= \frac{1}{12}\binom{6}{1,3,2} + \left[u_1 u_2^3 u_3^2\right]\left(\frac{1}{4}(u_1+u_2+u_3)^2\left(u_1^2+u_2^2+u_3^2\right)^2\right) = \cdots$$

... razmislimo: Da dobimo $u_1 u_2^3 u_3^2$ iz $(u_1+u_2+u_3)^2\left(u_1^2+u_2^2+u_3^2\right)^2$, moramo v prvem faktorju vzeti $u_1 u_2$ (koeficient $\binom{2}{1,1} = \frac{(1+1)!}{1!1!} = 2$) ali $u_1 u_3$ (koeficient $\binom{2}{1,1} = 2$). Če vzamemo $u_1 u_2$, moramo v drugem faktorju vzeti $u_2^2 u_3^2$ (koeficient $\binom{2}{1,1} = 2$). Če vzamemo $u_1 u_3$, moramo v drugem faktorju vzeti $u_2^3 u_3^2$, kar pa se ne zgodi (koeficient 0). Torej je $\left[u_1 u_2^3 u_3^2\right]\left((u_1+u_2+u_3)^2\left(u_1^2+u_2^2+u_3^2\right)^2\right) = 2 \cdot 2 = 4$ ...

$$= \frac{1}{12}\frac{6!}{1!3!2!} + \frac{4}{4} = \frac{\cancel{2}\cdot\cancel{3}\cdot\cancel{4}\cdot 5\cdot\cancel{6}}{\cancel{3}\cdot\cancel{2}\cdot\cancel{2}\cdot\cancel{12}} + 1 = 5 + 1 = 6$$

Torej je neekvivalentnih barvanj z zahtevanimi lastnosti šest.

Dokaz. Zgolj skica dokaza. Uporabimo Burnsidovo lemo, ko naša grupa deluje na barvanjih z β_i koraldami barve i. Še vedno velja, da je barvanje negibna točka za permutacijo $\Leftrightarrow$ vsi elementi v ciklu so iste barve.

Dokaz s primerom: C_4, $n = 4$, $r = 2$, $\beta_1 = 2$, $\beta_2 = 2$. Vsa barvanja so (brez izločanja ekvivalentnih)

$$\begin{matrix}\bullet & \circ \\ \bullet & \circ\end{matrix}, \quad \begin{matrix}\circ & \circ \\ \bullet & \bullet\end{matrix}, \quad \begin{matrix}\circ & \bullet \\ \circ & \bullet\end{matrix}, \quad \begin{matrix}\bullet & \bullet \\ \circ & \circ\end{matrix}, \quad \begin{matrix}\bullet & \circ \\ \circ & \bullet\end{matrix}, \quad \begin{matrix}\circ & \bullet \\ \bullet & \circ\end{matrix}.$$

Po Burnsidovi lemi je dovolj za vsako permutacijo pogledati, koliko negibnih točk (barvanj) ima.

- identiteta: 6
- rotacija 90: 0
- rotacija 180: 2

Število negibnih točk pa ravno ustreza koeficientom v $(u_1+u_2)^4 + \left(u_1^2+u_2^2\right)^2 + 2\left(u_1^4+u_2^4\right)$. V prvem členu 6, v drugem členu 2, v tretjem členu 0. To pojasnimo tako: če imamo cikel dolžine i, je vseh i korald iste barve.

Oglejmo si recimo $\left(u_1^2+u_2^2\right)^2 = \left(u_1^2+u_2^2\right)\left(u_1^2+u_2^2\right)$. To pripada rotaciji za 90 stopinj, ki ima dva cikla ((13) (24)). Torej ko izbiramo iz prvega faktorja, izberemo bodisi u_1^2, kar pomeni „obe koraldi v ciklu z barvo 1“, bodisi u_2^2, kar pomeni „obe koraldi v ciklu z barvo 2“

To je ideja dokaza. Cel dokaz smo izpustili. Ne bo na ustnem. □

Pripomba. Polinom $z_G(u_1 + \cdots + u_r, \ldots u_1^n + u_r^n)$ je homogen stopnje n (vsak monom je stopnje n) in simetričen (menjava u_i z u_j) ne spremeni koeficientov — vseeno je namreč, kako rečemo $i-$ti barvi, rdeča ali črna.

6 Trije klasični izreki iz teorije delno urejenih množic

6.1 Delno urejene množice — DUM (angl. partially ordered set — poset)

Definicija. Naj bo P množica in $\leq : P \times P \to \{0,1\}$ relacija. $(P, \leq)$ je delno urejena množica, če velja

1. refleksivnost: $\forall x \in P : x \leq x$
2. antisimetričnost: $\forall x, y \in P : x \leq y \wedge y \leq x \Rightarrow x = y$
3. tranzitivnost: $\forall x, y, z \in P : x \leq y \wedge y \leq z \Rightarrow x \leq z$

Zgled. $\underline{n} := ([n], \leq) =: \mathbf{n}$, $(\mathbb{N}, \leq)$, $(\mathbb{Q}, \leq)$, $(\mathbb{R}, \leq)$, $\left(\mathbb{N} \leq \{0\}, \overset{\text{deli}}{|}\right)$, $\left(\overset{\text{delitelji } n}{D_n}, |\right)$, $B_n := \left(2^{[n]}, \subseteq\right)$ (Boolova algebra).

Definicija. Naj bo $(P, \leq)$ DUM, $x, y \in P$:

- x in y sta neprimerljiva, če $x \not\leq y \wedge y \not\leq x$, sicer sta primerljiva
- $x < y :\Leftrightarrow x \leq y \wedge x \neq y$
- $x \lessdot y :\Leftrightarrow x < y \wedge \nexists z \ni : x < z < y$. Pravimo, da je x predhodnik y oziroma da y pokriva x
- x je maksimalen element P, če $\nexists z \in P \ni : x < z$. (lahko jih je več)
- x je minimalen element P, če $\nexists z \in P \ni : z < x$. (lahko jih je več)
- x je največji element P, če $\forall z \in P : z \leq x$ (opazimo, da je največji element lahko le en). Največji je, če obstaja, gotovo maksimalen.
- x je najmanjši element P, če $\forall z \in P : x \leq z$ (lahko je le en). Najmanjši je, če obstaja, gotovo minimalen.

Zgled. Nekaj primerov:

- V $\underline{n}$ za $i < n$ velja $i \lessdot i + 1$.
- V $(\mathbb{R}, \leq)$ $\nexists x, y \ni : x \lessdot y$.
- V B_n za $A \neq [n]$ in $i \in [n], i \notin A$ velja $A \lessdot A \cup \{i\}$.
- V D_n za $d \neq n$ in p praštevilo in $p \not| d$ velja $d \lessdot d \cdot p$.

Definicija. Hassejev diagram[4] je graf z vozlišči elementi P in povezavami med $x, y \in P \Leftrightarrow x \lessdot y \vee y \lessdot x$. Rišemo tako, da če $x < y$, rišemo y nad x.

Pripomba. Hassejev diagram B_n je izomorfen grafu Q_n ($n-$dimenzionalni hiperkocki).

Trditev. Končna neprazna DUM vsebuje maksimalen element.

Dokaz. Vzemimo poljuben $x_1 \in P$. Če je maksimalen, smo ga našli, če ni, obstaja večji. Ponavljamo postopek in v končno korakih najdemo maksimalnega. $\square$

Zgled. $(\mathbb{N}, \leq)$ nima maksimalnega elementa.

Definicija. Naj bo $(P, \leq)$ DUM. $A \subseteq P$ je antiveriga, če $\forall x, y \in A, x \neq y : x, y$ neprimerljiva.

Zgled. Primeri antiverig:

- Singleton je vselej antiveriga. Prazna množica je vselej antiveriga.
- A antiveriga v $\underline{n} \Longrightarrow |A| \leq 1$
- A antiveriga v $B_n \Longrightarrow \exists k \in \mathbb{N} \ni : \forall M \in A : |M| = k$ ZDB antiverige v B_n so množice, ki vsebujejo natanko enakomočne množice.

Definicija. Naj bo $(P, \leq)$ DUM. $C \subseteq P$ je veriga, če $\forall x, y \in C : x, y$ primerljiva.

Zgled. Primeri verig:

- Singletoni je vselej veriga. Prazna množica je vselej veriga.

[4] Risbe prepuščene bralcu.

- Vsaka podmnožica v $\underline{n}$ je veriga.
- $\{1, 2, 12\}$ je veriga v D_{12}
- $\{\{1\}, \{1, 2\}, \{1, 2, 3\}\}$ je veriga v B_n
- množica maksimalnih elementov je antiveriga

Definicija. Širina DUM je velikost največje največje antiverige v njej. Višina DUM je velikost največje verige v njej.

DUM	širina	višina
$\underline{n}$	1	n
B_3	3	4
B_n	$\binom{n}{\lfloor \frac{n}{2} \rfloor}$ ni očitno, dokaže Spernerjev izrek	$n+1$

Tabela 7: Primeri višin in širin DUM

Zgled.

6.2 Dilworthov izrek

Izrek. *Mirsky. Naj bo P končna DUM. Naj bo m minimalno število antiverig, s katerimi lahko pokrijemo P. Naj bo M višina P ZDB velikost največje verige v P. Tedaj $m = M$.*

Dokaz. Naj bo C poljubna veriga v P, pokrita z antiverigami $A_1, \ldots, A_l$. Očitno gotovo velja, da sta poljubna dva elementa v C elementa različnih antiverig. Se pravi $|C| \leq l \Rightarrow M \leq m$.

$m \leq M$ dokažimo z indukcijo po moči DUM P.

- baza: $|P| = 1$. Tedaj $1 = m = M = 1$
- korak: $|P| > 1$. Po I. P. $m \leq M$ za vsako strogo podmnožico P.
  - Velja $A = \{\text{maksimalni elementi } P\}$ je neprazna antiveriga.
  - $P \setminus A$ je manjša DUM z višino $M - 1$.
    - Zakaj? Vsaka najdaljša veriga ima en maksimalen element.
    - Maksimalen element namreč v končni DUM vedno obstaja in če veriga ne vsebuje kakega maksimalnega elementa, ga lahko verigi dodamo in dobimo večjo verigo.
  - $P \setminus A$ po I. P. lahko pokrijemo z $M - 1$ antiverigami, torej lahko P pokrijemo z M antivegirami (elementi, ki smo jih odstranili P, da smo dobili $P \setminus A$, so natanko antiveriga)

□

Pripomba. Dokaz je konstruktiven — daje nam algoritem, kako najti pokritje z najmanj antiverigami:

- $A_1 =$ maksimalni elementi v P
- $A_2 =$ maksimalni elementi v $P \setminus A_1$
- $A_3 =$ maksimalni elementi v $P \setminus A_1 \setminus A_2$
- ...

Izrek. *Dilworth. Naj bo P končna DUM in naj bo m minimalno število verig, s katerimi lahko pokrijemo P in naj bo M velikost največje antiverige (širina DUM P). Tedaj velja $m = M$.*

Dokaz. Naj bo A poljubna antiveriga in imejmo pokritje P z verigami $C_1, \ldots, C_l$. Tedaj velja, da sta poljubna dva elementa antiverige A pokrita z dvema različnima verigama (sicer bi bila primerljiva), torej velja $|A| \leq l \Rightarrow M \leq m$.

Dokažimo $m \leq M$ z indukcijo na $|P|$:

- Baza: $|P| = 1$. velja $1 = m = M = 1$
- Korak: $|P| > 1$. Po I. P. za vse manjše podmnožice velja $m \leq M$.

- Vzemimo C poljubno najdaljšo verigo v P. Tedaj je $P \setminus C$ manjša DUM. Širina (velikost največje antiverige) se odstranitvi C bodisi zmanjša bodisi ne spremeni.
  * Če se zmanjša:
    - $P \setminus C$ po I. P. lahko pokrijemo z $\leq M-1$ verigami. Torej lahko P pokrijemo z $\leq M$ verigami (dodamo C).
  * Širina ostane enaka. Izberemo antiverigo $A = \{a_1, \ldots, a_M\}$ v $P \setminus C$. Definirajmo:
    - $S^+ := \{x \in P; \exists a \in A \ni : a \leq x\}$ ZDB elementi P (in ne $P \setminus C$), ki so večji od kakega elementa antiverige A, unija elementi A.
    - $S^- := \{x \in P; \exists a \in A \ni : x \leq a\}$ ZDB elementi P, ki so manjši od kakega elementa antiverige A, unija elementi A.
    - Velja $S^+ \cap S^- = A$. Očitno $A \subseteq S^+$ in $A \subseteq S^-$, torej $A \subseteq S^+ \cap S^-$. Nadalje za poljuben $x \in S^+ \cap S^-$ velja $a_i \leq x \leq a_j$ za neka a_i, a_j. Po tranzitivnosti torej $a_i \leq a_j$ in ker sta to elementa antiverige $a_i = a_j$ in posledično še $a_i = x = a_j$, torej $x \in A$, kar pomeni $S^+ \cap S^- \subseteq A$.
    - Velja $S^+ \cup S^- = P$. Očitno $S^+ \cup S^- \subseteq P$. Dokažimo še $P \subseteq S^+ \cup S^- \Leftrightarrow \forall x \in P : x \in S^+ \vee x \in S^-$. PDDRAA $x \notin S^+ \wedge x \notin S^-$, kar bi pomenilo $x \notin A \wedge \forall a \in A : x \not\leq a \wedge x \not\geq a \Rightarrow x$ neprimerljiv z vsemi $a \in A \Rightarrow A \cup \{x\}$ antiveriga v P, daljša od A, toda A je dolžine M in M je po predpostavki dolžine največje antiverige v P $\rightarrow\leftarrow$.
    - Velja $S^+ \neq P$. Dokažimo, da najmanjši element C, recimo mu x, ni v S^+. PDDRAA $x \in S^+ \Rightarrow \exists a \in A \ni : a \leq x$. Ker je A antiveriga v $P \setminus C$, $x \neq a$. Potemtakem $a < x$. To pa bi pomenilo, da je $C \cup \{a\}$ daljša veriga od C, toda C je po izbiri najdaljša veriga $\rightarrow\leftarrow$.
    - Velja $S^- \neq P$. Analogno: največji elementi C naj bo x. $x \notin S^-$, sicer $\exists a \in A \ni : x \leq a$ in ker $x \neq a$, saj je A antiveriga v $P \setminus C$, $x < a$, kar bi pomenilo, da je $C \cup \{a\}$ daljša veriga od C, slednja pa je po izbiri najdaljša $\rightarrow\leftarrow$.
    - S^+ ima širino M in je strogo manjša DUM od P, torej ga po I. P. lahko pokrijemo z M verigami $C_1^+, \ldots, C_M^+$.
    - S^- ima širino M in je strogo manjša DUM od P, torej ga po I. P. lahko pokrijemo z M verigami $C_1^-, \ldots, C_m^-$.
    - Elementov A je M mnogo in po prejšnjem razmisleku morajo biti v različnih verigah. BSŠ $a_i \in C_i^+$ in $a_i \in C_i^-$.
    - Po konstrukciji S^+ in S^- in zato C_i^+ in C_i^- velja $\forall i \in [M] : \forall c \in C_i^+ : a_i \leq c$ in $\forall i \in [M] : \forall c \in C_i^- : c \leq a_i$. Torej $C_i^+ \cap C_i^- = \{a_i\}$. Potemtakem je $\forall i \in [M] : C_i := C_i^+ \cup C_i^+$ veriga v P in verige $C_i, \ldots, C_M$ pokrijejo P.
    - S tem smo našli M (širina DUM P) verig v P, ki pokrijejo P in dokazali izrek.

□

Pripomba. V Dilworthovem izreku bi lahko predpostavili, da so verige, s katerimi pokrivamo, disjunktne. Naj bo $C_1, \ldots, C_m$ pokritje z verigami. Tedaj je $C_1, C_2 \setminus C_1, C_3 \setminus C_2 \setminus C_1, \ldots, C_m \setminus \cdots \setminus C_2 \setminus C_1$ spet pokritje, tokrat z disjunktnimi verigami.

Povzetek. Dilworthov izrek pravi, da je širina delno urejene množice enaka minimalnemu številu disjunktnih verig, s katerimi lahko pokrijemo to delno urejeno množico.

Definicija. Naj bo G graf. $M \subseteq E(G)$ je prirejanje (angl. matching), če velja $\forall e, f \in M : e \neq f \Rightarrow e \cap f = \emptyset$.

Pripomba. Pri Optimizacijskih metodah omenimo učinkovit algoritem, ki najde največje prirejanje v dvodelnem grafu.

Naj bo P DUM. Skonstruirajmo dvodelen graf. Za vozlišča vzemimo dve kopiji P, $V = P \times \{0, 1\}$. Povezave definiramo tako: $x < y \in P \Rightarrow x' \in P_0$ in $y'' \in P_1$ povezana v dvodelnem grafu. Izkaže se, da je največje prirejanje ravno najmanjše pokritje z verigami.

6.3 Spernerjev izrek

Lema. *Srednji koeficient v vrstici Pascalovega trikotnika največji izmed vseh v isti vrstici ZDB*

$$\forall n, k : \binom{n}{k} \leq \binom{n}{\lfloor \frac{n}{2} \rfloor}$$

Dokaz.

$$\binom{n}{k} \leq \binom{n}{k+1} \Leftrightarrow \frac{\binom{n}{k}}{\binom{n}{k+1}} \leq 1 \Leftrightarrow \frac{\cancel{n!}\,(k+1)\cancel{!}\,\cancel{(n-k-1)!}}{\cancel{k!}\,(n-k)\cancel{!}\,\cancel{n!}} \leq 1 \Leftrightarrow \frac{k+1}{n-k} \leq 1 \Leftrightarrow k+1 \leq n-k \Leftrightarrow 2k+1 \leq n \Leftrightarrow k \leq \frac{n-1}{2}$$

Se pravi za $k \leq \frac{n-1}{2}$ bionmski koeficienti naraščajo, nato pa začno padati. Torej:

- za n sod velja $k < \frac{n}{2} \Rightarrow \binom{n}{k} \leq \binom{n}{k+1}$ in $k \geq \frac{n}{2} \Rightarrow \binom{n}{k} \geq \binom{n}{k+1}$
- za n lih velja $k \leq \frac{n-1}{2} \Rightarrow \binom{n}{k} \leq \binom{n}{k+1}$ in $k \geq \frac{n+1}{2} \Rightarrow \binom{n}{k} \geq \binom{n}{k+1}$

□

Definicija. Tako zaporedje, ki najprej narašča in nato pada ZDB $a_0 \leq a_1 \leq \cdots \leq a_k \geq a_{k+1} \geq \cdots$ kličemo „unimodalno".

Zgled. $\left(\binom{n}{k}\right)_{k=0}^{n}$ je unimodalno zaporedje.

Izrek. *Sperner. Širina Boolove algebre (B_n) je $\binom{n}{\lfloor \frac{n}{2} \rfloor}$.*

Dokaz. Dokazujemo enakost.

($\geq$) Dokazujemo, da je širina $\geq \binom{n}{\lfloor \frac{n}{2} \rfloor} \sim$ najdaljša antiveriga je dolga $\binom{n}{\lfloor \frac{n}{2} \rfloor}$. Dovolj je najti eno take dolžine. Ta antiveriga je $\binom{[n]}{\lfloor \frac{n}{2} \rfloor}$. Spomnimo se, da so antiverige v B_n natanko množice enakomočnih množic.

($\leq$) Naj bo A poljubna antiveriga.

- Koliko je maksimalnih verig v B_n? Verige v B_n so oblike $\emptyset \lessdot \{i_1\} \lessdot \{i_1, i_2\} \lessdot \cdots \lessdot \{i_1, \ldots, i_n\}$. Začnimo z $\emptyset$. Dodamo en element na n možnosti, drugi element na $n-1$ možnosti, ... $n-$ti element je enolično določen. Se pravi je v B_n $n!$ maksimalnih verig.
- Koliko je maksimalnih verig v B_n, ki vsebujejo dano množico $T \subseteq [n]$? $(n - |T|)! \cdot |T|!$. Prvi faktor predstavlja izbiro elementov, ki jih bomo dajali v množico (in se s tem vzpenjali po verigi), vendar je že določeno, bomo dodali elemente iz T. Pomnožimo z možnimi permutacijami elementov iz T, ker je zaporedje dodajanja v množico za vzpenjanje po verigi poljubno.
- Koliko je maksimalnih verig v B_n, ki vsebujejo kakšno (torej natanko eno — več jih ne more, ker je A antiveriga) množico iz A? Odvisno od tega, kako velika je ta množica iz A. Za vsak element antiverige $T \in A$ torej $(n - |T|)! \cdot |T|!$ (prejšnja točka). Potemtakem je skupaj takih verig, ki vsebujejo kakšno množico A, vsota tega izraza po vseh elementih A:

$$\sum_{T \in A} (n - |T|)! \cdot |T|! \leq n! \qquad / : n!$$

$$\sum_{T \in A} \frac{(n - |T|)! \cdot |T|!}{n!} \leq 1$$

$$\sum_{T \in A} \frac{1}{\binom{n}{|T|}} \leq 1$$

$$\sum_{T \in A} \frac{1}{\binom{n}{\lfloor \frac{n}{2} \rfloor}} \overset{\text{lema}}{\leq} \sum_{T \in A} \frac{1}{\binom{n}{|T|}} \leq 1$$

$$\frac{|A|}{\binom{n}{\lfloor \frac{n}{2} \rfloor}} = \sum_{T \in A} \frac{1}{\binom{n}{\lfloor \frac{n}{2} \rfloor}} \overset{\text{lema}}{\leq} \sum_{T \in A} \frac{1}{\binom{n}{|T|}} \leq 1$$

$$\frac{|A|}{\binom{n}{\lfloor \frac{n}{2} \rfloor}} \leq 1$$

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

□

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

Definicija. Pravimo, da je DUM P stopničasta (angl. ranked), če obstaja predlikava rang : $P \to \mathbb{N}$ s predpisom $\operatorname{rang} x = 0 \Leftrightarrow x$ je minimalen element in $x \lessdot y \Rightarrow \operatorname{rang} y = \operatorname{rang} x + 1$.

6.4 Hallov izrek

Definicija. Prirejanje M je popolno, če $\forall v \in V \exists e \in M \ni: v \in e$.

Pripomba. Za popolno prirejanje velja $|M| = \frac{|V|}{2}$. Popolno prirejanje ne obstaja v vsakem grafu.

Definicija. Naj bo $G = X \cup Y$ dvodelen graf in M prirejanje. M je popolno prirejanje iz X v Y, če $\forall x \in X \exists e \in M \ni: x \in e$ ZDB vsa vozlišča iz X so pokrita.

Dejstvo. *Če obstaja popolno prirejanje iz X v Y, velja $|M| = |X| \leq |Y|$. To popolno prirejanje namreč definira injekcijo iz X v Y.*

Velja celo več $\forall A \subseteq X : |A| \leq |N(A)|$, kjer je $N(A)$ unija soseščin vozlišč iz A ZDB

$$N(A) \coloneqq \{y \in Y; \exists x \in A \ni: \{x, y\} \in E\}.$$

To je očitno. Če bi ne veljalo za nek A, bi ne mogli konstruirati iz A injekcije v Y z uporabo le povezav iz E.

Izrek. *Hall. Naj bo G dvodelen graf. $\exists$ popolno prirejanje iz X v Y $\Leftrightarrow \forall A \subseteq X : |A| \leq |N(A)|$.*

Dokaz. Dokazujemo ekvivalenco.

($\Rightarrow$) Očitno, dokazano v zgornjem dejstvu.

($\Leftarrow$) Po predpostavki velja $\forall A \subseteq X : |A| \leq |N(A)|$. Uporabili bomo Dilworthov izrek.

- Skonstruirajmo DUM $P = X \cup Y$ s predpisom $\forall a \in P : a \leq a$ in $\forall x \in X, y \in Y : x \leq y :\Leftrightarrow xy \in E$.
- Naj bo $\{x_1, \ldots, x_k, y_1, \ldots, y_l\}$ najdaljša antiveriga v P.
- Če je $A = \{x_1, \ldots, x_k\}$, velja $N(A) \subseteq Y \setminus \{y_1, \ldots, y_l\}$; po konstrukciji (najdaljše antiverige) med $x_1, \ldots, x_k$ in $y_1, \ldots, y_l$ ni povezav. Velja

$$k = |A| \leq |N(A)| \leq |Y| - l$$

$$k \leq |Y| - l$$

$$k + l \leq |Y|$$

  Označimo $M = k + l \leq |Y|$ (dolžina najdaljše antiverige v P). Po Dilworthovem izreku lahko cel P pokrijemo z M disjunktnimi verigami.
- V naši P so verige prazne množice, singletoni ali dvoelementne množice. Označimo z a število dvoelementnih verig izmed teh M verig, s katerimi lahko pokrijemo P.
- Dokažimo $a = |X|$.
  - Gotovo je očitno $a \leq |X|$. Vsaka dvoelementna veriga vsebuje vozlišče iz X in vozlišče iz Y in ker so disjunktne, jih je kvečjemu toliko, kot elementov X.
  - Sedaj še $a \geq |X|$. Velja $M = a + \underbrace{|X| - a}_{\text{singletoni v } X} + \underbrace{|Y| - a}_{\text{singletoni v } Y}$. Torej:

$$\cancel{a} + |X| \cancel{- a} + \cancel{|Y|} - a = \underbrace{M \leq \cancel{|Y|}}_{\text{dokazali prej}}$$

$$|X| - a \leq 0$$

$$|X| \leq a$$

  - Torej $|x| = a$, torej nam dvoelementne verige dajejo popolno prirejanje iz X v Y.

$\square$

Pripomba. Torej iz Dilwortha „sledi“ Hall. Lahko pa bi tudi dokazali Dilwortha s Hallom.

Posledica. *Naj bo $G = X \cup Y$ neprazen dvodelni graf in naj velja $\forall x \in X, y \in Y : \deg x \geq \deg y$. Potem obstaja popolno prirejanje iz X v Y.*

Dokaz. Naj bo $A \subseteq X$ poljubna in $B \coloneqq N(A)$. Dokazati hočemo $|A| \leq |B|$. Naj bo $e(A,B)$ število povezav med A in B.

Po predpostavki $\exists d \in \mathbb{N} \forall x \in X, y \in Y : \deg(x) \geq d \geq \deg(y)$. Recimo $d \coloneqq \min_{x \in X} \deg x$.

$$d \cdot |B| \geq \sum_{y \in B} \deg(y) \overset{\text{XX}}{\geq} e(A,B) = \sum_{x \in A} \deg x \geq d\,|A|$$

Razlaga XX: seveda lahko iz B poteka povezava v kako vozlišče iz $X \setminus A$. Seveda velja $A \subseteq N(N(A))$, očitno pa ne velja vedno $A = N(N(A))$.

$$d\,|B| \geq d\,|A|$$

Ker G ni prazen, je d neničeln in lahko krajšamo:

$$|B| \geq |A|$$

$\square$

Posledica. *$G = X \cup Y$ je biregularen dvodelni graf (vsa vozlišča iz X so iste stopnje in vsa vozlišča iz Y so iste stopnje) in $EG \neq \emptyset$. Tedaj obstaja vsaj eno od tega:*

- *popolno prirejanje iz X v Y*
- *popolno prirejanje iz Y v X*

Dokaz. Naj bo r tak, da $\forall x \in X : r = \deg x$, in s tak, da $\forall y \in Y : s = \deg y$. Velja

$$|EG| = r\,|X| = s\,|Y|$$

$$r \geq s \Leftrightarrow |X| \leq |Y|$$

Ločimo dve možnosti:

- $|X| \leq |Y| \Rightarrow r \geq s$ in posledično obstaja popolno prirejanje iz X v Y po zgornji posledici
- $|Y| \leq |X| \Rightarrow s \geq r$ in posledično obstaja popolno prirejanje iz Y v X po zgornji posledici

$\square$

Zgled. N kart. Izberemo pet naključnih kart, izbrane štiri od njih damo v izbranem vrstnem redu prijatelju, ki je s trikom seznanjen. Ta mora ugotoviti, katera je peta.

Neurejenih peteric kart je $\binom{N}{5}$, urejenih četveric kart pa je $N^{\underline{4}}$. Definirajmo dvodelni graf, $VG = X \cup Y$, kjer so X vse neurejene peterice kart, Y pa vse urejene četverice kart. V grafu sta vozlišči A in B povezani, če $A \subseteq B$.

Iščemo popolno prirejanje iz X v Y, torej iz neurejenih peteric v urejene četverice. Potreben pogoj je, da je $\binom{N}{5} \leq N^{\underline{4}}$.

$$\frac{\cancel{N(N-1)(N-2)(N-3)}(N-4)}{120} \leq 1 \cdot \cancel{N(N-1)(N-2)(N-3)}$$

$$N - 4 \leq 120$$

$$N \leq 124$$

Primer za $N = 52$ (standardne karte). Med temi petimi kartami sta dve enake barve. Odstranimo tisto, ki je podvojene barve, tisto drugo damo na vrh kupčka štirih, ki ga podamo partnerju. Tako partner izve barvo karte, ki nam ostane v rokah.

Karte so oštevilčene s številkami A,2,3,4,5,6,7,8,9,10,J,Q,K (13 številk). Številke si predstavljajmo kot kolobar $\mathbb{Z}_{12}$, kjer velja $\forall a, b \in \mathbb{Z}_{12} : a - b \leq 6 \vee b - a \leq 6$. Torej za vsak par kart si lahko izberemo eno iz para kart, da bomo, ko prištejemo največ 6 (dovolimo wrap), dobili drugo izmed para.

To storimo za dve naši karti, ki sta iste barve. Prijatelju na vrh kupčka torej damo tisto karto, da ji bo lahko prištel število kvečjemu 6, da bo dobil karto, ki je ostala nam v rokah.

Število, ki ga mora prišteti, mu sporočimo s permutacijo preostalih treh kart, ki mu jih damo na dno kupčka na nek dogovorjen način. Permutacij treh kart je ravno šest. Recimo: Vse karte so med seboj različne, torej jih lahko na dogovorjen način uredimo leksikografsko s ključem (barva, številka) in te tri karte tretiramo kot številke 1 (najmanjša karta), 2 (vmesna karta), 3 (največja karta). Permutacij $\{1, 2, 3\}$ je šest.

Dejstvo. *Še en življenjski trik, ki nam ga je povedal profesor. Conwayev trik. Če vemo, kateri je zadnji dan februarja (za 2025 je petek), je petek tudi 4. 4., 6. 6., 8. 8., 10. 10., 12. 12. (sodi meseci od februarja dalje) in 9. 5., 5. 9., 7. 11., 11. 7. (profesor pove nekaj podobnega kot to, da si Američani to lahko zapomnijo lažje, ker mnogi od devete ure zjutraj do pete popoldne delajo v trgovini 7eleven)*

7 Končni avtomati

Definicija. Naj bo $G = (V, E)$ usmerjen utežen graf z utežmi $w : E \to K$ za K kolobar. $V = \{v_1, \ldots, v_p\}$. Matrika sosednosti je

$$A_{ij} = \begin{cases} w(v_i v_j) & ; v_i v_j \in E \\ 0 & ; v_i v_j \notin E \end{cases}$$

Sprehod v grafu je pot, le da zahtevamo, da se vozlišča ne ponavljajo. Sprehod dolžine n je $\Gamma : x_0, x_1, \ldots x_n$, kjer $\forall i \in [n] : x_{i-1}x_i : x_{i-1}x \in E$. Teža sprehoda je $w(\Gamma) = w(x_0 x_1) \cdot w(x_1 x_2) \cdots w(x_{n-1}, x_n)$. Za $1 \leq i, j \leq p$ in $n \in \mathbb{N}$ definirajmo

$$A_{ij}(n) := \sum_{\Gamma \text{ sprehod dolžine } n \text{ od } v_i \text{ do } v_j} w(\Gamma)$$

Pripomba. V posebnem, če je utež vselej enaka 1, je $A_{ij}(n)$ število sprehodov dolžine n med v_i in v_j. Velja

$$A_{ij}(1) = A_{ij} = \begin{cases} w(v_i v_j) & ; v_i v_j \in E \\ 0 & ; \text{sicer} \end{cases}.$$

Velja $A(n) \in K^{P \times P}$, $A(A) = A$.

Trditev. $A_{ij}(n) = (A^n)_{ij}$.

Dokaz. Induktivni dokaz.

- baza
  - $n = 0$: $A(0) = I = A^0$
  - $n = 1$: $A(1) = A^1$
- korak: $A_{ij}(n) = \sum_{k=1}^{p} A_{ik}(n-1)\, w(v_k v_j) \overset{\text{I. P.}}{=} \sum_{k=1}^{p} A_{ik}^{n-1} A_{kj} = \left(A^{n-1}A\right)_{ij} = A_{ij}^n$

□

Definicija. Definirajmo

$$F_{ij}(x) = \underbrace{\sum_{n=0}^{\infty}}_{\text{dolžina sprehoda}} A_{ij}(n)\, x^n = \sum_{n=0}^{\infty} A_{ij}^n x^n = \left(\underbrace{\sum_{n=0}^{\infty} A^n x^n}_{\text{geometrijska vrsta}} \right)_{ij} = \left(\frac{1}{I - xA} \right)_{ij} =$$

$$= \left((I - xA)^{-1} \right)_{ij} \overset{\text{Cramerjevo pravilo}}{=} \frac{(-1)^{i+j}}{\det(I - xA)} (I - xA) \overbrace{ji}^{\text{brez } i\text{-tega stolpca in } j\text{-te vrstice}} = (-1)^{i+j} \frac{\det(I - xA)^{ji}}{\det(I - xA)}$$

OK to poglavje je useless tko nč nismo povedal pametnega najbrž ne bo spraševal ... Je blo pa omenjeno Conwayevo „look and say“ zaporedje 1, 11, 21, 1211, 111221, 312211, 13112221, 1113213211, ... Če vas res zanima, kaj smo počeli na zadnjem predavanju, prenesite moj neberljivi rokopis.