Kombinatorika 2 - zapiski s predavanj prof. Konvalinke

Tomaž Poljanšek

študijsko leto 2023/24

Kazalo

Seznam uporabljenih kratic

kratica	izraz
NSTE	naslednje trditve so ekvivalentne
orf	običajna rodovna funkcija
erf	eksponentna rodovna funkcija
fp	formalni polinom
fpv	formalna potenčna vrsta
dum	delno urejena množica

Poglavje 1

Osnove

1.1 Kako štejemo?

S končna množica, $|S| = ?$

Pogosto $S_n, n \in \mathbb{N}$.

Preštevalno zaporedje $|S_0|, |S_1|, |S_2| \dots$

Kaj je odgovor?

(1) Formula.

$[n] = \{1, 2 \dots n\}$.

$S_n = 2^{[n]} = P([n])$.

$|S_n| = 2^n$.

$S_n = \{\text{permutacije } n \text{ elementov}\}$.

$|S_n| = n! = 1 \cdot 2 \dots n$ „n fakulteta“, „n factorial“.

$S_n = \{\text{kompozicije } n \text{ s členi 1 ali 2}\}$, npr. $5 = 1+2+1$.

$|S_5| = 8$.

$1, 1, 2, 3, 5, 8 \dots$

$|S_n| = F_n$ - Fibonaccijevo zaporedje.

(2) Asimptotska formula.

$|S_n| \sim a_n$ (to pomeni $\lim_{n\to\infty} \frac{a_n}{|S_n|} = 1$).

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

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

(3) Z rekurzijo.

$S_n = 2^{[n]}$.

$a_n = |S_n|, a_n = 2a_{n-1};\ n \geq 1,\ a_0 = 1$.

$S_n = \{$kompozicije s členi 1 in 2$\}$.

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

F_{n-1} - kompozicije, ki se končajo z 1,

F_{n-2} - končajo z 2.

(4) Z rodovno funkcijo (generating function).

$(a_n)_{n\in\mathbb{N}}$ zaporedje.

$a_0 + a_1x + a_2x^2 + \cdots = \sum_{n=0}^{\infty} a_nx^n = \sum_n a_nx^n$ običajna (ordinary) rodovna funkcija - orf.

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

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

$\sum_n n!x^n$ //.

$\sum_n \frac{a_n}{n!}x^n$ eksponentna rodovna funkcija.

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

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

(4) je najboljši način, da poznamo zaporedje.

– Rodovna funkcija je velikokrat „lepa“, tudi če ni lepe formule za zaporedje.

  $i_n \ldots$ # involucij z n elementi ($\pi^2 = \mathrm{id}$).

  Ni enostavnejše formule za i_n.

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

– Do rodovne funkcije lahko pogosto pridemo neposredno s kombinatoričnim premislekom.

  Involucija = permutacija s cikli dolžine 1 ali 2.

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

x - cikli dolžine 1,

x^2 - cikli dolžine 2.

– V rodovni funkciji so „skrite“ (1)-(3).

1.2 Osnovne Kombinatorične strukture

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

$[n] = \{1, 2 \dots n\}$.

$2^A = P(A) = \{B \subseteq A\}$.

$\binom{A}{k} = \{B \subseteq A : |B| = k\}$ „A nad k“ (angl. „A choose k“).

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

$Y^X = \{f : X \to Y\}$.

Statistika na množici S je preslikava $S \to \mathbb{N}$.

$S = 2^A$.

Moč je statistika.

S končna množica, f statistika na S.

Pogosto gledamo polinom $\sum_{s \in S} x^{f(s)}$ (enumeration).

$|\cdot|$ na $2^{[3]} : 1 + 3x + 3x^2 + x^3 = (1 + x)^3$.

$S_n = \{\text{permutacije } [n]\} = \{f : [n] \to [n] \mid f \text{ bijektivna}\}$.

$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ - dvovrstična notacija.

2 1 3 - enovrstična notacija.

(1 2)~~(3)~~ - produkt disjunktnih ciklov.

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

Gotovo $\exists j_1 < j_2 : \pi^{j_1}(i) = \pi^{j_2}(i) \implies i = \pi^j(i);\ j > 0$.

$(i\ \pi(i) \dots \pi^{j-1}(i))$ cikel.

38241765 = (1 3 2 8 5)(4)(6 7) = (4)(2 8 5 1 3)(7 6).

Množenje permutacij: kompozicije.

Nekomutativno za $n > 2$.

Disjunktni cikli komutirajo.

Zapis: enoličen do vrstnega reda ciklov in ciklične ureditve ciklov.

Cikel dolžine 1 = negibna točka.

Cikel dolžine 2 = transpozicija.

$(S_n, \cdot)$ simetrična grupa.

$e = id = 1\ 2 \dots n$.

π^{-1} inverz (kot preslikava).

$3\ 8\ 2\ 4\ 1\ 7\ 6\ 5^{-1} = 5\ 3\ 1\ 4\ 8\ 7\ 6\ 2$.

$3\ 1\ 4\ 2 \cdot 4\ 2\ 3\ 1 = 2\ 1\ 4\ 3$ - množimo z desne.

Statistika: # ciklov = $c(\pi)$ (štejemo tudi cikle dolžine 1).

$n = 3 : x^3 + 3x^2 + 2x = x(x+1)(x+2)$.

$\sum_{\pi \in S_n} x^{c(\pi)} = \sum_k |\{\pi \in S_n : c(\pi) = n\}| x^k$.

$|\{\pi \in S_n : c(\pi) = n\}| =: c(n,k)$ - Stirlingovo število 1. vrste.

$\sum_{B \subseteq [n]} x^{|B|} = \sum_k \left|\binom{[n]}{k}\right| x^k$.

$\left|\binom{[n]}{k}\right| =: \binom{n}{k}$ - binomski koeficient.

Inverzija $\pi \in S_n$ je (i,j), da je za $i < j \quad \pi_i > \pi_j$.

$inv(\pi) = \#$ inverzij π.

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

$0 \leq inv(\pi) \leq \binom{n}{2}$.

Signatura permutacije: $(-1)^{inv(\pi)}$.

$sg\pi = 1$ - soda permutacija: produkt sodo mnogo transpozicij.

$sg\pi = -1$ - liha permutacija: produkt liho mnogo transpozicij.

$detA = \sum_{\pi \in S_n} (-1)^{inv(\pi)} a_{1,\pi(1)} \cdots a_{n,\pi(n)}$.

Izraz brez $(-1)^{inv(\pi)}$: permanenta.

$n = 3 :$

$1 + 2x + 2x^2 + x^3 = 1 + x^2 + x^3 + x + x^2 + x^3 = (1+x)(1+x^2)$.

$\sum_{\pi \in S_n} x^{inv(\pi)} = 1 \cdot (1+x)(1+x^2) \cdots (1+x^{n-1})$ - kasneje.

permutacij v S_n s k inverzijami: ni standardne oznake.

Spust/padec (descent) $i : \pi_i > \pi_{i+1}$.

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

$0 \leq des(\pi) \leq n - 1$.

permutacij v S_n s $k-1$ spusti = $A(n,k)$ - Eulersko število ($k-1$ iz zgodovinskih razlogov).

$\sum_k A(n,k)x^k = \sum_{\pi \in S_n} x^{1+des(\pi)} = A_n(x)$ - eulerski polinom.

$n = 3:$

$x + 4x^2 + x^3.$

Razdelitev/razbitje (angl. set partition) A je $\{B_1, B_2 \dots B_n\}$, da velja:

- $B_i \neq \emptyset$ za $i = 1 \dots k$,
- $B_i \cap B_j = \emptyset$ za $1 \leq i < j \leq k$,
- $\cup_{i=1}^k B_i = A$.

B_i: bloki razdelitve,

k # blokov,

razdelitev $[n]$ s k bloki $= S(n,k)$ - Stirlingovo število druge vrste.

$A = [3]: \quad \{\{1\},\{2\},\{3\}\}, \{\{1,2\},\{3\}\} \dots \{\{1,2,3\}\}.$

$x + 3x^2 + x^3.$

$S(4,2) = 4 + 3 = 7.$

Kompozicija # n je $\lambda = (\lambda_1 \dots \lambda_l), \lambda_i > 0$ člen kompozicije, $\lambda_i \in \mathbb{N}$,

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

$l(\lambda)$: # členov - dolžina.

$\lambda \models n$ - λ je kompozicija n.

Razčlenitev # n je $\lambda = (\lambda_1 \dots \lambda_l), \lambda_i > 0, \lambda_i \in \mathbb{N}$.

$\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_l, \sum_{i=1}^l \lambda_i = n$

(angl. integer partition).

$p(n)$ - # razčlenitev n.

$p_k(n)$ - # razčlenitev n s k členi.

$n = 4:$

$4, 31, 22, 13, 211, 121, 112, 1111$ - 8 kompozicij.

$4, 31, 22, 221, 1111$ - 5 razčlenitev.

$p(4) = 5, p_2(4) = 2.$

$B(n) = \sum_k S(n,k)$ - # razčlenitev $[n]$, Bellovo število.

$B(3) = 5.$

$L(n,k)$ - # razdelitev $[n]$ na k linearno urejenih blokov.

$L(4,2) = 4 \cdot 6 + 3 \cdot 2 \cdot 2 = 36$ - Lahovo število.

$E_n = \#$ alternirajočih permutacij v S_n - Eulerjevo število (Euler number).
$\pi_1 > \pi_2 < \pi_3 > \pi_4 \ldots$
Primerjaj: eulerska števila (eulerian number).
$1, 1, 1, 2, 5$.
Poti:
npr. poti od (0,0) do (n,m) s korakom (1,0) (vzhod) in (0,1) (sever);
npr. poti od (0,0) do (2n,0) s korakoma (1,1) in $(1, -1)$;
npr. poti od (0,0) do (2n,0) s korakoma (1,1) in $(1, -1)$, nikoli pod x osjo - Dyckove poti;
$c_n = \#$ Dyckovih poti dolžine n (konec v (2n,0)) - Catalanova števila.
1,1,2,5,14,42 . . .
Drevesa (povezani aciklični grafi).
\# označenih dreves na n vozliščih.
Cayleyev izrek: n^{n-2}.
Ravninska drevesa.
(Vrstni red pomemben).
Dvojiška drevesa: vsako vozlišče ima 2 ali 0 naslednikov.

1.3 Osnovna načela preštevanja

Načelo vsote: $A \cap B = \emptyset \implies |A \cap B| = |A| + |B|$.
$i \neq j : A_i \cap A_j = \emptyset \implies |\cup_{i=1}^n A_i| = \sum_{i=1}^n |A_i|$.
Načelo produkta: $|A \times B| = |A| \cdot |B|$, $|\prod_{i=1}^n A_i| = \prod_{i=1}^n |A_i|$.
Kombinatorično:

> 2 možnosti, izberemo eno ali drugo (ne pa obe) $\implies$ \# načinov je vsota \# načinov,
>
> dvakrat izbiramo, izbiri sta neodvisni $\implies$ \# načinov je produkt \# načinov.

Trditev 1.3.1. $|2^A| = 2^{|A|}$.

Dokaz 1.3.2. Za vsak element se odločimo, ali ga damo v podmnožico ali

ne. 2 izbiri, izbiramo $|A|$-krat, izbire so neodvisne $2 \cdot 2 \cdots 2 = 2^{|A|}$.
$\phi : 2^A \to \{0,1\}^{|A|}, A = \{a_1, a_2 \dots a_n\}$.
$\phi(B) = (\epsilon_1 \dots \epsilon_n), \epsilon_i = \begin{cases} 1 \; a_i \in B \\ 0 \text{ sicer} \end{cases}$
$\psi : \{0,1\}^{|A|} \to 2^A$.
$\psi(\epsilon_1 \dots \epsilon_n) = \{a_i : \epsilon_i = 1\}$.
$\psi \circ \phi, \phi \circ \psi$ identiteti.
$|\{0,1\}|^{|A|} = 2^{|A|}$. ■

Trditev 1.3.3.

1. $|K^N| = |K|^{|N|}$.
2. $|\{f \in K^n \text{ injektivna}\}| = |K|(|K|-1)\dots(|K|-|N|+1)$.
3. $|S_n| = n(n-1)\dots 1 = n!$.

Oznake:
$n^{\underline{k}} = n(n-1)\dots(n-k+1)$: n na k padajoče.
$n^{\overline{k}} = n(n+1)\dots(n+k-1)$: n na k naraščajoče.

Opomba. Pri 2. in 3. smo uporabili varianto načela produkta: izbire sicer niso neodvisne, je pa neodvisno število izbir.

Dirichletov princip (pigeon-hole principle):
$\phi : X \to Y$ injektivna $\implies |X| \le |Y|$.
Če damo n kroglic v k škatel, $n > k$, sta v vsaj eni škatli vsaj 2 kroglici.

Primer.

(1) n ljudi, med njimi sta dva, ki poznata enako mnogo ljudi.
$X =$ ljudje, $f = \#$ znanstev.
n kroglic, n škatel, ampak škatli 0 in $n-1$ ne moreta biti obe neprazni.

(2) $X \subseteq [2n], |X| = n+1$.
Obstajata $x,y \in X, x \neq y, x|y$.
$x = 2^k \cdot l, k \ge 0, k$ lih.

$Y = \{i \in [2n] \text{ liho}\}$.
$x \mapsto l$.

1.4 Binomski koeficienti

$\binom{n}{k} = \left|\binom{[n]}{k}\right|$ = število k-elementnih podmnožic v $[n]$ = število izbir k elementov izmed n elementov.
$\binom{4}{2} = 6, \binom{5}{0} = 1, \binom{8}{-2} = 0, \binom{8}{9} = 0.$
$\binom{n}{0} = 1, \binom{n}{n} = 1, \binom{n}{1} = n.$
$\binom{n}{n-k} = \binom{n}{k}.$
$\phi : \binom{[n]}{n-k} \to \binom{[n]}{k}.$
$\phi(A) = A^c.$
$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}.$
$\binom{n-1}{k-1}$: izberemo n.
$\binom{n-1}{k}$: ne izberemo n-ja.
Pascalov trikotnik:

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

Trditev 1.4.1. $\binom{n}{k} = \frac{n^{\underline{k}}}{k!} = \begin{cases} \frac{n!}{n!(n-k)!} & 0 \le k \le 0 \\ 0 & k > n \end{cases}$

Dokaz 1.4.2.
Izberemo 1 element na n načinov, 2 na $n-1 \cdots \implies n^{\underline{k}}$ načinov, vsak izbor smo šteli $k!$-krat.
Ali: preštejemo urejene izbire k različnih elementov iz $[n]$;
$n^{\underline{k}} = \binom{n}{k} \cdot k!.$
$\binom{n}{k}$: najprej izberemo k elementov.

$k!$: nato jih uredimo. ■

Izrek 1.4.3 (Binomski izrek)**.** $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$;
$a,b \in K$ komutativni kolobar, $n \in \mathbb{N}$.

Dokaz 1.4.4.

D1. Indukcija po n:

$n = 0$: $1 = 1$

$n-1 \to n$:

$$\begin{aligned}(a+b)^n &= (a+b)^{n-1}(a+b) = \\ &\overset{\text{IP}}{=} \sum_{k=0}^{n-1} \binom{n-1}{k} a^k b^{n-1-k}(a+b) = \\ &= \sum_{k=0}^{n-1} \binom{n-1}{k} a^{k+1} b^{n-1-k} + \sum_{k=0}^{n-1} \binom{n-1}{k} a^k b^{n-k} = \\ &= \sum_{k=1}^{n-1} \binom{n-1}{k-1} a^k b^{n-k} + \sum_{k=1}^{n-1} \binom{n-1}{k} a^k b^{n-k} = \\ &= \sum_{k=0}^{n} \binom{n-1}{k-1} a^k b^{n-k} + \sum_{k}^{n} \binom{n-1}{k} a^k b^{n-k} = \\ &= \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.\end{aligned}$$

D2. $(a+b)^n = \sum_k \binom{n}{k} a^k b^{n-k}$ DN.

D3. $(a+b)\dots(a+b) = \sum_{\text{izbira } a \text{ ali } b}$ produkt izbranih $=$

$= \sum_k \binom{n}{k} a^k b^{n-k}$.

a izberemo k-krat.

Izberemo k oklepajev, pri katerih izberemo a.

■

$\binom{10}{3} = \frac{10\cdot 9\cdot 8}{3\cdot 2} = 120$.
$\binom{12}{10} = \binom{12}{2} = \frac{12\cdot 11}{2} = 66$.
Izbori: n kroglic, k izberemo.

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

$1 \leq i_1 \leq i_2 \leq \cdots \leq i_k \leq n.$

$j_1 = i_1, j_2 = i_2 + 1 \ldots j_k = i_k + k - 1.$

$1 \leq j_1 < j_2 < \cdots < j_k \leq n + k - 1.$

Trditev 1.4.5. Število kompozicij n je 2^{n-1} $(n \geq 1)$, število kompozicij s k členi je $\binom{n-1}{k-1}$ $(n \geq 1)$.

Dokaz 1.4.6.

n kroglic $\circ | \circ \circ \circ | \circ \circ : \; 6 = 1 + 3 + 2.$

$k - 1$ pregrad, $n - 1$ mest za pregrade. ■

Kompozicije: 2^{n-1}, $\binom{n-1}{k-1}$.

Šibka kompozicija: $(\lambda_1 \ldots \lambda_l)$; $\lambda_i \geq 0$, $\lambda_1 + \cdots + \lambda_l = n$.

$3 : 12, 3, 21, 102, 300, 0102 \ldots$

Število šibkih kompozicij n s k členi.

$n + k - 1$ objektov, premešamo na $\binom{n+k-1}{k-1}$ oz. $\binom{n+k-1}{n}$ načinov.

Še en dokaz:

$\lambda_1 + \cdots + \lambda_l = n, \; \lambda_i \geq 0.$

$\mu_i = \lambda_i + 1$ $\mu_i \geq 1$.

$\mu_1 + \cdots + \mu_l = n + k \implies \binom{n+k-1}{n-1}$.

Primerjaj z: kombinacije s ponavljanjem.

n kroglic, k-krat izbiram.

λ_i: kolikokrat izberemo i-to kroglico.

$\lambda_1 + \cdots + \lambda_n = k, \; \lambda_i \geq 0.$

Šibke kompozicije k z n členi: $\binom{k+n-1}{k}$.

Trditev 1.4.7.

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

Dokaz 1.4.8.

Koliko je urejenih razdelitev na linearno urejene bloke:

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

Tukaj predstavljajo

- $L(n,k)$: urejene bloke,
- $k!$: njihov vrstni red,
- $n!$: permutacije,
- $\binom{n-1}{k-1}$: šibke kompozicije.

■

Poti iz (0,0) v (n,m), premikamo se gor ali desno.
n-krat gor, m-krat desno: $\binom{n+m}{m}$ možnosti.
Poti iz (0,0) v $(2n,0)$, desno-gor ali desno-dol.
n-krat gor, n-krat dol: $\binom{2n}{n}$.
Dyckove poti: isto kot prej, se ne spustimo pod x-os.
Pot je slaba, če gre pod x-os:
Od tam naprej, kjer 1. doseže $y = -1$, prezrcalimo pot preko $y = -1$.
Konča se v $y = -2$.
Število slabih poti = število poti od (0,0) do $(2n, -2)$.
Teh je $\binom{2n}{n-1}$: $(n-1)$-krat gor, $(n+1)$-krat dol.

$$\begin{aligned}
c_n &= \text{število Dyckovih poti doižine } n \\
&= \binom{2n}{n} - \binom{2n}{n-1} \\
&= \frac{(2n!)}{n!\,n!} - \frac{(2n)!}{(n-1)!(n+1)!} \\
&= \binom{2n}{n}(1 - \frac{n}{n+1}) \\
&= \frac{1}{n+1}\binom{2n}{n}.
\end{aligned}$$

Multinomski koeficienti:

$\alpha_1 \times 1, \alpha_2 \times 2 \ldots \alpha_k \times k:\ 11..12..2..k$.

Na koliko načinov lahko premešamo:

$$\binom{\alpha_1+\cdots+\alpha_k}{\alpha_1}\binom{\alpha_2+\cdots+\alpha_k}{\alpha_2}\cdots\binom{\alpha_k}{\alpha_k}=\frac{(\alpha_1+\cdots+\alpha_k)!}{\alpha_1!\ldots\alpha_k!}.$$

Definiramo

$$\binom{\alpha_1+\cdots+\alpha_k}{\alpha_1,\alpha_2\ldots\alpha_k}:=\frac{(\alpha_1+\cdots+\alpha_k)!}{\alpha_1!\ldots\alpha_k!}. \tag{1.1}$$

Izrazu 1.1 pravimo multinomski simbol.

Figure v 1. vrsti pri šahu: $\frac{8!}{1!1!2!2!} = 7!$.

i-jem damo indekse $\alpha_1 \ldots \alpha_k:\ 1_1 \ldots 1_{\alpha_1} 2_1 \ldots k_{\alpha_k}$

Premešamo na $(\alpha_1+\cdots+\alpha_k)!$ načinov.

Eno permutacijo dobimo $(\alpha_1! \ldots \alpha_k!)$-krat.

Multimnožica M je množica, v kateri se elementi lahko ponavljajo.

$M = \{1,1,1,2,2,3,3,3,3\} = \{1^3, 2^2, 3^4\}$.

Število permutacij multimnožice je multinomski simbol.

Formalno je multimnožica (S,f), kjer je S množica, $f : S \to \mathbb{N}$ šteje kolikokrat se posamezen element ponovi.

1.5 Dvanajstera pot

n kroglic, k škatel; na koliko načinov lahko damo kroglice v škatle.

N: ne ločimo,

K: ločimo.

$N \setminus K$	vse	injekcije	surjekcije	
L L	k^n	$k^{\underline{n}}$	$k!S(n,k)$	
N L	$\binom{n+k-1}{k-1}$	$\binom{k}{n}$	$\binom{n-1}{k-1}$	
L N	$\sum_i S(n,i)$	$\begin{cases}1 & k \geq n\\ 0 & \text{sicer}\end{cases}$	$S(n,k)$	razdelitve
N N	$\overline{p_k(n)}$	$\begin{cases}1 & k \geq n\\ 0 & \text{sicer}\end{cases}$	$p_k(n)$	razčlenitve

$\binom{n+k-1}{k-1}$ - šibke kompozicije,
$\binom{k}{n}$ - neprazne škatle,
$\binom{n-1}{k-1}$ - kompozicije.
Vpeljemo ekvivalenčne relacije

- $f \sim_N g :\ \exists \pi \in S_n :\ f \circ \pi = g$
- $f \sim_K g :\ \exists \sigma \in S_k :\ \sigma \circ f = g$
- $f \sim_{N,K} g :\ \exists \pi \in S_n, \sigma \in S_k :\ \sigma \circ f \circ \pi = g.$

1.6 Rekurzije

$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$.
$c(n,k) = c(n-1,k-1) + (n-1)c(n-1,k)$;
$c(n-1,k-1)$: n negibna,
$(n-1)$: za kateri element vstavimo.
$S(n,k) = S(n-1,k-1) + kS(n-1,k)$;
$S(n-1,k-1)$: n v svojem bloku,
k: v kateri blok vstavimo.
$L(n,k) = L(n-1,k-1) + (n+k-1)L(n-1,k)$;
$L(n-1,k-1)$: n v svojem bloku,
$(n+k-1)$: kam vstavimo.
$B(n+1) = \sum_{k=0}^{n} \binom{n}{k} B(n-k) = \sum_{k=0}^{n} \binom{n}{k} B(k)$;
odstranimo blok, v katerem je $n+1$,
k: število elementov v bloku skupaj z $n+1$,
$\binom{n}{k}$: kateri elementi v bloku skupaj z $n+1$,
$B(n-k)$: razdelimo ostale.
$p_k(n) = p_{k-1}(n-1) + p_k(n-k)$;
$p_{k-1}(n-1)$: $\lambda_l = 1$,
$p_k(n-k)$: $\lambda_l \geq 2$ (odstranimo 1. stolpec v Ferrersovem diagramu).
$A(n,k) = (n+1-k)A(n-1,k-1) + kA(n-1,k)$;
ostranimo n,

k: n damo na konec ali za spust,
$(n+1-k)$: n damo na začetek ali za vzpon. V S_n velja še: števio spustov + število vzponov $= n-1$.
$2E_{n+1} = \sum_{k=0}^{n} \binom{n}{k} E_k E_{n-k}$ $n \geq 1$;
k: koliko elementov je pred $n+1$,
število obratno alternirajočih = število alternirajočih $(i \to n+1-i)$,
E_k: pred $n+1$, E_{n-k}: za $n+1$, štejemo in alternirajoče in obratno alternirajoče permutacije.
$c_{n+1} = \sum_{k=0}^{n} c_k c_{n-k}$;
k: ko 1. pridemo v $y=0$: pred in za tem sta Dyckovi poti.
$p(n) = p(n-1) + p(n-2) - p(n-5) - p(n-7) + p(n-12) + p(n-15) - \dots$
Eulerjev petkotniški izrek (dokaz kasneje) (pentagonal).

1.7 Načelo vklučitev in izključitev (NVI)

(Principle of inclusion and exclusion.)
$|A \cup B| = |A| + |B| - |A \cap B|$.
$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$.

Izrek 1.7.1 (NVI)**.**

$$\begin{aligned} |\cup_{i=1}^{n} A_i| &= |A_1| + |A_2| + \dots + |A_n| \\ &- |A_1 \cap A_2| - \dots - |A_{n-1} \cap A_n| \\ &+ |A_1 \cap A_2 \cap A_3| + \dots + |A_{n-2} \cap A_{n-1} \cap A_n| \\ &- \dots \\ &= \sum_{i=1}^{n} (-1)^{i-1} \sum_{1 \leq j_1 < \dots < j_k \leq n} |A_{j_1} \cap \dots \cap A_{j_k}| \\ &= \sum_{\emptyset \neq S \subseteq [n]} (-1)^{|S|-1} |A_S|, \end{aligned}$$

kjer je $A_S := \cap_{i \in S} A_i$.

Dokaz 1.7.2.
$x \in \cup_{i=1}^{n} A_i$.

Trdimo, da x prispeva 1 k vsoti na desni.

Recimo, da je x v natanko m množicah A_i $(1 \leq m \leq n)$:

$$\begin{aligned} & m - \binom{m}{2} + \binom{m}{3} - \cdots + (-1)^m \binom{m}{m} \\ & = 1 - \left(\binom{m}{0} - \binom{m}{1} + \binom{m}{2} - \cdots + (-1)^{m-1} \binom{m}{m} \right) \\ & = 1 - (1-1)^m = 1. \end{aligned}$$

■

Trditev 1.7.3 (NVI, 2. verzija)**.**

$$\left| \cap_{i=1}^n A_i^C \right| = \sum_{S \subseteq [n]} |A_S|.$$

Dokaz 1.7.4.

$$\begin{aligned} \left| \cap_{i=1}^n A_i^C \right| &= \left| (\cup_{i=1}^n A_i)^C \right| \\ &= |A| - | \cup_{i=1}^n A_i| \\ &= |A| + \sum_{\emptyset \neq S \subseteq [n]} (-1)^{|S|} |A_S| \\ &= \sum_{S \subseteq [n]} |A_S|, \end{aligned}$$

kjer velja še $A_\emptyset = A$. ■

Primer.

(1) Koliko je k-elementnih antiverig v B_n?
$B_n = (2^{[n]}, \subseteq)$ Boolova algebra, antiveriga - množica neprimerljivih elementov.

k=1: 2^n (vsi elementi).

k=2:

$$\begin{aligned}
&S = \{(A,B) : A, B \subseteq [n]\}\\
&S_1 = \{(A,B) : A \subseteq B\}\\
&S_2 = \{(A,B) : B \subseteq A\}\\
&|S_1^C \cap S_2^C| = |S| - |S_1| - |S_2| + |S_1 \cap S_2| = 4^n - 2 \cdot 3^n + 2^n;
\end{aligned}$$

4^n: vse možnosti $x \in, \notin A,B$, 3^n: vse razen $x \in A, \notin B \dots$
$\implies \frac{1}{2}(4^n - 2 \cdot 3^n + 2^n)$.

k=3:

$$\begin{aligned}
&S = \{(A,B,C) : A,B,C \in 2^{[n]}\}\\
&S_1 : A \subseteq B, S_2 : B \subseteq A, S_3 : A \subseteq C, S_4 : C \subseteq A\\
&S_5 : B \subseteq C, S_6 : C \subseteq B.\\
&|\cap_{i=1}^6 S_i^C| = 8^n - 6 \cdot 6^n + 3 \cdot 4^n + 6 \cdot 5^n - 6 \cdot 4^n - \overset{\text{DN}}{\dots}
\end{aligned}$$

$6^n : S_i$, 4^n : npr. $S_1 \cap S_2$, 5^n: npr. $S_1 \cap S_3$, 4^n : npr. $S_1 \cap S_4$.

(2) i_n: število premestitev v S_n = število permutacij v S_n brez negibne točke (dearangement).

$$\begin{aligned}
A &= S_n\\
A_i &= \{\pi \in S_n : \pi_i = i\}\\
|A_I| &= (n - |I|)!\\
i_n &= \sum_{I \subseteq [n]} (-1)^{|I|}(n - |I|)!\\
&= \sum_{k=0}^{n} \binom{n}{k} (-1)^k (n-k)!\\
&= n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}.
\end{aligned}$$

$P(\pi \text{ premestitev}) = \sum_{k=0}^n \frac{(-1)^k}{k!} \xrightarrow{n\to\infty} e^{-1}$.

(3) Število surjekcij iz $[n]$ v $[k]$.

$$\begin{aligned}
A &= [k]^{[n]} \\
A_i &= ([k] \setminus \{i\})^{[n]} \\
\left|\cap_{i=1}^{n} A_i^C\right| &= \sum_{I \subseteq [n]} (-1)^{|I|}(k - |I|)^n \\
&= \sum_{k=1}^{n} \binom{k}{i} (-1)^i (k-i)^n \\
&\overset{i=k-i}{=} \sum_{j=1}^{k} (-1)^{k-j} \binom{k}{j} j^n \\
&= k! S(n,k);
\end{aligned}$$

surjekcija je urejena razdelitev;

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

(4) Eulerjev petkotniški izrek:

$$p(n) = p(n-1) + p(n-2) - p(n-5) - \dots$$

$$\begin{aligned}
&A = \{\text{razčlenitve } n\} \\
&A_i = \{\text{razčlenitve } n, \text{ ki vsebujejo } i \text{ za člen}\},\ i = 1,2\dots n \\
&|A_i| = p(n-i) \\
&|A_i \cap A_j| = p(n-k-j) \\
&|A_I| = p(n - \sum_{i \in I} i)
\end{aligned}$$

$$\begin{aligned}
p(n) &= p(n-1) + p(n-2) + p(n-3) + \dots \\
&- p(n-1-2) - p(n-1-3) - p(n-2-3) - \dots \\
&+ p(n-1-2-3) - \dots \\
&= p(n-1) + p(n-2) - p(n-5) - p(n-7) + \dots
\end{aligned}$$

Franklinova bijekcija:

$p(n) = \sum_{m=1}^{\infty} (\alpha(m) - \beta(m)) p(n-m)$; m - razčlenitve z različnimi členi,

$\alpha(m) =$ število razčlenitev m z liho mnogo različnimi členi,
$\beta(m) =$ število razčlenitev m z sodo mnogo različnimi členi.
Bijekcija

$$\begin{aligned}\Phi :&\{\text{razčlenitev } m \text{ z liho mnogo različnimi členi}\}(\backslash\{\dots\})\\ &\to \{\text{razčlenitev } m \text{ z sodo mnogo različnimi členi}\}(\backslash\{\dots\}).\end{aligned}$$

$f(\lambda) = \max\{i : \lambda_i = \lambda_1 - i + 1\}$ - bok,
$g(\lambda) = \lambda_{l(\lambda)}$ - najmanjši člen,

a) $f(\lambda) \geq g(\lambda)$: min $\to$ bok,

b) $f(\lambda) < g(\lambda)$: bok $\to$ min,

a) ne dela (število členov se ohrani),
b) ne dela (2 člena enako dolga),
a) ne dela, ko:
$f(\lambda) = g(\lambda) = l(\lambda)$
$m = k + (k+1) + \dots + (2k-1) = \frac{2k(2k-1)}{2} - \frac{k(k-1)}{2} = \frac{k(3k-1)}{2}$
$(\alpha(m) - \beta(m)) = (-1)^{k-1}$ (k lih ali sod).
b) ne dela, ko:
$f(\lambda) = g(\lambda) - 1 = l(\lambda)$
$m = (k+1) + (k+2) + \dots + (2k) = \dots = \frac{k(3k+1)}{2}$
$(\alpha(m) - \beta(m)) = (-1)^{k-1}$.
Eulerjev petkotniški izrek:

$$\begin{aligned}p(n) &= \sum_{k=1}^{\infty}(-1)^{k-1}\left(p\left(n - \frac{k(3k-1)}{2}\right) + p\left(n - \frac{k(3k+1)}{2}\right)\right)\\ \text{oz.} &\sum_{k\in\mathbb{Z}}(-1)^k p\left(n - \frac{k(3k+1)}{2}\right) = 0.\end{aligned}$$

Tukaj smo upoštevali ko vstavimo $-k$: $\frac{-k(-3k-1)}{2} = \frac{k(3k+1)}{2}$ in $p(0) = 0$.

Izrek 1.7.5 („NVI“)**.**
$f, g : B_n \to K$, K komutativni kolobar.

$$f(T) = \sum_{S\subseteq T} g(S)(\forall T \in B_n) \iff g(T) = \sum_{S\subseteq T}(-1)^{|T\backslash S|} f(S)(\forall T \in B_n).$$

Zgled.

$des(\pi) = |\{i : \pi(i) > \pi(i+1)\}|$

$D(\pi) = \{i : \pi(i) > \pi(i+1)\}$

$D(1\ 4\ 2\ 6\ 5\ 3) = \{2{,}4{,}5\}$

$f_n(T) = |\{\pi \in S_n : D(\pi) = T\}|$

npr. $n = 8, T = \{1{,}5\}$

$g_n(T) = |\{\pi \in S_n : D(\pi) \subseteq T\}|$

$T = \{t_1, t_2 \dots t_k\}$

$g_n(T) = \binom{n}{t_1}\binom{n-t_1}{t_2-t_1}\binom{n-t_1-\dots-t_{k-1}}{t_k} = \binom{n}{t_1, t_2-t_1 \dots t_k - t_{k-1}, n-t_k}$

$\_ < \_ < \_ < \underline{t_i} \lesseqgtr \_$: zaradi $\subseteq$: tam lahko spust ali pa ne.

// če lastnosti točno določene: težko ($f_n(T)$), če „vsebovano" ($g_n(T)$): lažje $g_n(T) = \sum_{S \subseteq T} f_n(S)$.

$$\begin{aligned} f_n(T) &= \sum_{S\subseteq T} (-1)^{|T\setminus S|} g_n(S) \\ &= \sum_{S\subseteq T} (-1)^{|T\setminus S|} \binom{n}{s_1, s_2 - s_1 \dots n - s_k} \\ &\overset{\text{vaje}}{=} det\left[\binom{n-t_i}{t_{j+1}-t_j}\right]_{i,j=0}^{|T|}. \end{aligned}$$

Npr. $n = 8$, $T = \{1{,}5\}, t_0 = 0, t_{|T|} = n + 1 = 9$.

$$f_8(\{1{,}5\}) = \begin{vmatrix} \binom{8}{1} & \binom{8}{5} & \binom{8}{8} \\ \binom{7}{0} & \binom{7}{1} & \binom{7}{7} \\ \binom{3}{-4} & \binom{3}{0} & \binom{3}{3} \end{vmatrix} = 217.$$

Dokaz 1.7.6.

$(\implies)$:

$$\begin{aligned}
\sum_{S\subseteq T}(-1)^{|T\setminus S|}f(S) &= \sum_{S\subseteq T}(-1)^{|T\setminus S|}f(S)\sum_{U\subseteq S}g(U)\\
&= \sum_{U\subseteq T}\left(\sum_{U\subseteq S\subseteq T}(-1)^{|T\setminus S|}\right)g(U)\\
&\overset{k=|S\subseteq U|}{=} \sum_{U\subseteq T}\sum_{k=0}^{|U|}\binom{|T\setminus U|}{k}(-1)^{|T\setminus U|-k}g(U)\\
&= g(T).
\end{aligned}$$

Na notranji vsoti uporabimo binomski izrek za -1 in 1 :

$$(1-1)^{|T\setminus S|} = \begin{cases} 1 : U = T\\ 0 : U \subset T\end{cases}$$

■

1.8 Polinomske enkosti

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

Izrek 1.8.1.

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

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

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

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

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

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

Opomba. $K[x] = \{\text{polinomi v } x\}$ vektorski prostor (celo algebra), K komutativen obseg.
$\{x^n\}, \{x^{\underline{n}}\}, \{x^{\overline{n}}\}$ naravne baze.

Dokaz 1.8.2.

(a) Indukcija (na vajah drugače):

$n = 0$: 1=1

$n - 1 \to n$:

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

(b) $x \to -x$ v (a).

(c) Preslikava = razdelitev + injekcija,

število preslikav iz $[n]$ v $[k] = \sum_k S(n,k)x^{\underline{k}}$, kjer predstavljajo

- k: število blokov,
- $S(n,k)$: razdelimo $[n]$ na k blokov,
- $x^{\underline{k}}$: injekcija $[k] \to [x]$.

Dokazali smo za $x \in \mathbb{N} \implies$ polinoma sta enaka (ujemanje v ∞ točkah).

(e) Z indukcijo (DN).

■

$\pi = 4\ 2\ 5\ 1\ 6\ 3$

$inv(\pi) = 7$

$I(\pi) = \{(1,2), (1,4), (1,6) \ldots\}$

$TI(\pi) = (a_1 \ldots a_n)$; $a_k = \{(i,j) : \pi_i > \pi_j = k\}$ („desna stran“) - tabela inverzij.

$TI(\pi) = (3,1,3,0,0,0)$

$0 \leq a_i \leq n - i$, a_i: koliko levo od i večjih od i.

Trditev 1.8.3.

$TI : S_n \to [0,n-1] \times [0,n-2] \times \cdots \times [0,0]$ je bijekcija.

Posledica 1.8.4.

$$\sum_{\pi \in S_n} q^{inv(\pi)} = \underline{n!} = (1+q)(1+q+q^2)\dots(1+q+\cdots+q^{n-1}).$$

$\pi = 4\ 1\ 7\ 3\ 9\ 6\ 2\ 8\ 5$,

$TI(\pi) = (1,5,2,0,4,2,0,1,0)$,

inverz: $9 \to 9\ 8 \to 7\ 9\ 8 \to 7\ 9\ 6\ 8 \to 7\ 9\ 6\ 8\ 5 \to 4\ 7\ 9\ 6\ 8\ 5$

$\to 4\ 7\ 3\ 9\ 6\ 8\ 5 \to 4\ 7\ 3\ 9\ 6\ 2\ 8\ 5 \to 4\ 1\ 7\ 3\ 9\ 6\ 2\ 8\ 5$.

Dokaz 1.8.5. trditve.

Skonstruiramo inverz:

$(a_1 \dots a_n),\ 0 \leq a_i \leq n-i$.

Vpisujemo $n, n-1 \dots 1$: i pišemo za a_i elementi. ■

Dokaz 1.8.6. posledice.

$\sum_{\pi \in S_n} q^{inv(\pi)} = n!_q = \underline{n!} = \underline{n}\underline{(n-1)}\dots 1$ - q fakulteta, $\underline{i} = 1 + q + \cdots + q^{i-1}$ - polinom, q-naravno število (q-integer).

$$\begin{aligned} D &= (1+q+\cdots+q^{n-1})(1+q+\cdots+q^{n-2})\dots 1 \\ &= \sum_{0 \leq a_i \leq n-i} q^{a_1} q^{a_2} \dots q^{a_n} \\ &\overset{\text{trditev}}{=} \sum_{\pi \in S_n} q^{inv(\pi)}. \end{aligned}$$

■

Opomba.

$maj(\pi) = \sum_{i \text{ spust } \pi} i$ oz. $\sum_{i \in D(\pi)} i$ - majorski indeks

$maj(4\ 2\ 5\ 1\ 3) = 1 + 3 = 4$

$\sum_{\pi \in S_n} q^{maj(\pi)} = \sum_{\pi \in S_n} q^{inv(\pi)} = \underline{n!}$.

Definicija 1.8.7 (q-binomski koeficient)**.**

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

$\binom{n}{\underline{0}} = \binom{n}{\underline{n}} = 1$
$\binom{n}{\underline{1}} = \underline{n}$ $\binom{4}{\underline{2}} = \frac{(1+q+q^2+q^3)(1+q+q^2)(1+q)}{(1+q)(1+q)} = (1+q^2)(1+q+q^2)$ $q = 1 : \binom{n}{\underline{k}} = \binom{n}{k}$.

Trditev 1.8.8.

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

Dokaz 1.8.9.

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

kjer je

$$q^{n-k}\underline{k!} + \underline{n-k} = q^{n-k} + \cdots + q^n + 1 + \cdots + q^{n-k-1} = 1 + q + \cdots + q^n = \underline{n}.$$

■

Posledica 1.8.10. $\binom{n}{\underline{k}}$ je polinom v q.

Trditev 1.8.11.

$$\prod_{i=1}^{n}(1+q^{i-1}x) = \sum_{k=0}^{n}\binom{n}{\underline{k}}x^k.$$

Dokaz 1.8.12. Indukcija:

$n = 0 : 1 = 1$

$n - 1 \to n$:

$$\begin{aligned} \prod_{i=1}^{n}(1+q^{i-1}x) &= \left(\sum_{k=0}^{n}\binom{n-1}{\underline{k}}x^k\right)\cdot(1+q^{n-1}x) \\ &= \sum_k q^{\binom{k}{2}}\binom{\text{n-1}}{\underline{k}}x^k + \sum_k q^{\binom{k-1}{2}+n-1}\binom{n-1}{\underline{k-1}}x^k \\ &= \sum_k q^{\binom{k}{2}}\left(\binom{n-1}{k} + q^{\binom{k-1}{2}+n-1-\binom{k}{2}}\binom{n-1}{\underline{k-1}}\right)x^k. \end{aligned}$$

Upoštevali smo $\binom{k-1}{2} - \binom{k}{2} = -\binom{k-1}{1}$. ■

$\mathbb{Z}_p$, p praštevilo - končen obseg.

Izrek 1.8.13.
Obseg moči $n \in \mathbb{N}$ obstaja $\iff$ $n = p^k$; p praštevilo. Obseg je do izomorfizma natančno določen.
$\mathbb{F}_q$ - oznaka.

Izrek 1.8.14.
V $\mathbb{F}_q^n$ je $\binom{\underline{n}}{\underline{k}}$ k-dimenzionalnih podprostorov.

Primer. $q = 4, n = 4, k = 2:\ (1 + 4^2) + (1 + 4 + 4^2) = 38.$

Dokaz 1.8.15. Spomnimo se: $[n]$ ima $\binom{n}{k}$ k-podmnožic, štejemo urejene k-terice različnih števil: $k!\binom{n}{k} = n^{\underline{k}}$.
Štejemo k-terice linearno neodvisnih vektorjev v $\mathbb{F}_q^n$:

$$(q^k - 1)(q^k - q) \dots (q^k - q^{k-1})X = (q^n - 1)(q^n - q) \dots (q^n - q^{n-1});$$

$q^k - q^i$: vsi v podprostoru brez linearnih kombinacij že vzetih,
$q^n - q^i$: vsi brez linearnih kombinacij že vzetih.
X: število izbir podprostora.

$$X = \frac{q^{\binom{k}{2}}(q-1)^k \underline{n}\underline{(n-1)} \dots \underline{(n-k+1)}}{q^{\binom{k}{2}}(q-1)^k \underline{k!}} = \binom{\underline{n}}{\underline{k}}.$$

■

Definicija 1.8.16 (q-multinomski koeficient)**.**

$$\begin{aligned}\binom{\underline{a_1 + \dots + a_k}}{\underline{a_1}, \underline{a_2} \dots \underline{a_k}} &= \frac{\underline{(a_1 + \dots + a_k)!}}{\underline{a_1!} \dots \underline{a_k!}} \\ &= \binom{\underline{a_1 + \dots + a_k}}{\underline{a_1}}\binom{\underline{a_2 + \dots + a_k}}{\underline{a_2}} \dots \binom{\underline{a_k}}{\underline{a_k}}.\end{aligned}$$

$\implies$ je polinom (produkt polinomov).

$x_1 \dots x_n$ permutacija multimnožice $\{1^{a_1}, 2^{a_2} \dots n^{a_n}\}$.
Inverzija: $(i,j) : i < j, x_i > x_j$.

inv: število inverzij,
$inv(1\ 2\ 1\ 1\ 2\ 3) = 2$.

Izrek 1.8.17. $M = \{1^{a_1}, 2^{a_2} \dots n^{a_n}\}$

$$\sum_{\pi \in S(M)} q^{inv(\pi)} = \binom{a_1 + \cdots + a_n}{\underline{a_1} \dots \underline{a_n}}.$$

Primer.
$q = 1 : |S(M)| = \binom{a_1+\cdots+a_n}{a_1 \dots a_n}$
$a_1 = \cdots = a_n = 1 : \sum_{\pi \in S_n} q^{inv(\pi)} = n!$ - posplošitev formul za multinomske koeficiente in Stirlingova števila 1. vrste.

Dokaz 1.8.18.

$$\sum_{\pi \in S(M)} q^{inv(\pi)} \underline{a_1}! \dots \underline{a_n}! = \underline{(a_1 + \cdots + a_n)!}$$
$$\sum_{\pi_0 \in S(M)} q^{inv(\pi_0)} \cdot \sum_{\pi_1 \in S_{a_1}} q^{inv(\pi_1)} \cdots \sum_{\pi_n \in S_{a_n}} q^{inv(\pi_n)} = \sum_{\pi \in S_{a_1+\cdots+a_n}} q^{inv(\pi)}.$$

Iščemo bijekcijo

$$\begin{aligned} \Phi : &(\pi_0 \pi_1 \dots \pi_n) \to \pi \\ &S(M) S_{a_1} \dots S_{a_n} \mapsto S_{a_1+\cdots+a_n}. \end{aligned}$$

$M = \{1^4, 2^2, 3^3\}$
$(1\ 2\ 2\ 1\ 3\ 1\ 3\ 3\ 1, 2\ 4\ 1\ 3, 2\ 1, 1\ 3\ 2) \mapsto 2\ 6\ 5\ 4\ 7\ 1\ 9\ 8\ 3$.
V π_0 enke spremenimo v $1 \dots a_1$ v vrstnem redu, ki ga določa π_1, v π_0 dvojke spremenimo v $a_1 + 1 \dots a_2$ v vrstnem redu, ki ga določa π_2, itn.
$inv(\pi_0) + \cdots + inv(\pi_n) = inv(\Phi(\pi_0 \dots \pi_n))$.
Vsaka inverzija $\Phi(\pi_0 \dots \pi_n)$ prihaja bodisi od inverzije π_i bodisi od inverzije π_0 (glede na „indeks“ v π_0) $\implies$ vsota enaka. ∎

Poglavje 2

Formalne potenčne vrste

2.1 Uvod

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

$\sum_n S(n,k)x^n$ neskončna vsota.

V analizi: potenčne vrste:

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

Konvergira za $|x| < R$ - konvergenčni polmer:

$$R = \frac{1}{\limsup_{n\to\infty} \sqrt[n]{|a_n|}} \overset{\text{če obstaja}}{=} \lim_{n\to\infty} \left|\frac{a_n}{a_{n+1}}\right| \in [0, \infty].$$

Primer. $\sum_{n=0}^{\infty} x^n : R = 1$

$\sum_{n=0}^{\infty} \frac{x^n}{n!} : R = \lim_{n\to\infty} \frac{\frac{1}{n!}}{\frac{1}{(n+1)!}} = \frac{(n+1)!}{n!} = \infty$

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

$\sum_{n=0}^{\infty} n!^2 x^n = \sum_{n=0}^{\infty} n!x^n$ - definirana samo v 0, obe z vrednostjo 1 tam.

$F(x) = \begin{cases} e^{-\frac{1}{x^2}};\ x \neq 0 \\ 0;\ x = 0 \end{cases} : \mathbb{R} \to \mathbb{R}.$

$F^{(n)}(0) = 0\ \forall n \geq 0 \implies F(x) = 0 + 0x + 0x^2 + \dots$

Potenčne vrste niso „najboljše“ za študij zaporedij.

2.2 Formalne potenčne vrste

K komutativni obseg s karakteristiko $0 : 1 + 1 + \cdots + 1 \neq 0 \; \forall n \geq 1$.
$\mathbb{Q}, \mathbb{R}, \mathbb{C}$
$\frac{1}{n!}$ je definirano
$K[[x]] = \{(a_n)_n : a_n \in K\} = K^{\mathbb{N}}$ - množica formalnih potenčnih vrst (FPV) = zaporedje
$K[x] = \{(a_n)_n : a_n \in K, a_n = 0 \; \forall n \geq n_0\}$ - množica polinomov.
V $K[[x]]$ vpeljemo operacije:

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

$$\lambda(a_n)_n = (\lambda a_n)_n,$$

$((a_n)_n \cdot (b_n)_n) = (c_n)_n;\; c_n = \sum_{k=0}^{n} a_k b_{n-k}$ - konvolucijsko množenje.

$K[[x]]$ algebra formalnih potenčnih vrst: komutativna, (1,0,0,0 . . .) enota za množenje: $\sum_{k=0}^{n} a_k \cdot \delta_{n-k,0} = a_n$.
Oznake:

$(a_n)_n \leftrightarrow \sum_n a_n x^n$: ni vsota (samo oznaka), x je ločilo (ni spremenljivka, ne „vstavljamo“),

$$(a_0 + a_1 x + \dots)(b_0 + b_1 x + \dots) = a_0 b_0 + (a_1 b_0 + a_0 b_1)x + \dots,$$

$$1 + 0x + 0x^2 + \cdots = 1,$$

$[x^n]F(x) := a_n$ - „koeficient pred x^n“,

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

Trditev 2.2.1. $F(x)$ ima inverz $\iff F(0) \neq 0$.

Dokaz 2.2.2.
$(\Longrightarrow)$:

$$F(x)G(x) = 1$$
$$F(0)G(0) = 1 \implies F(0) \neq 0$$

$(\Longleftarrow)$:

$$
\begin{aligned}
&F(x) = a_0 + a_1x + a_2x^2 + \ldots, a_0 \neq 0 \\
&G(x) = b_0 + b_1x + b_2x^2 + \ldots \\
&F(x)G(x) = 1 \\
&a_0b_0 = 1 \implies b_0 = \frac{1}{a_0} \\
&a_0b_1 + a_1b_0 = 0 \implies b_1 = \frac{-a_1b_0}{a_0} \\
&a_0b_2 + a_1b_1 + a_2b_0 = 0 \implies b_2 = \frac{-a_1b_1 - a_2b_0}{a_0} \\
&\vdots
\end{aligned}
$$

■

Opomba. K komutativen kolobar s karakteristiko 0.
$F(x)$ ima inverz $\iff$ $F(0)$ ima inverz v K.

$v(F(x)) = \begin{cases} \min n : [x^n]F(x) \neq 0 & F(x) \neq 0 \\ \infty & F(x) = 0 \end{cases}$ - valuacija.
$v(F(x)G(x)) = v(F(x)) + v(G(x))$ ($\implies$ ni deliteljev niča)
$v(F(X) + G(x)) \geq \min\{v(F(x)), v(G(x))\}$
$v(\lambda F(x)) = \begin{cases} v(F(x));\ \lambda \neq 0 \\ \infty;\ \lambda = 0 \end{cases}$
$d(F(x), G(x)) = 2^{-v(F(x)-G(x))}$ - metrika
$d(F(x), G(x)) = 2^{-k} \iff [x^n]F(x) = [x^n]G(x)\ \forall n \leq k.$

Trditev 2.2.3. $(K[[x]], d)$ je poln metrični prostor.

Dokaz 2.2.4.

$$
\begin{aligned}
d \geq 0, d = 0 &\iff F = G \\
d(F(x), G(x)) &= d(G(x), F(x)) \\
d(F(x), H(x)) &= 2^{-v(F(x)-H(x))} \\
&= 2^{-v(F(x)-G(x)+G(x)-H(x))} \\
&\leq \max\{2^{-v(F(x)-G(x))}, 2^{-v(G(x)-H(x))}\} \\
&= \max\{d(F(x), G(x)), d(G(x), H(x))\} \\
&\leq d(F(x), G(x)) + d(G(x), H(x)).
\end{aligned}
$$

■

$F_m(x) = \sum_n a_n^{(m)} x^n$ Cauchyjevo zaporedje
$\forall k \exists M: \; M_1, M_2 \geq M \implies d(F_{M_1}(x), F_{M_2}(x)) < 2^{-k}$
oz. $[x^n]F_{M_1}(x) = [x^n]F_{M_2}(x) \; \forall n \leq k$.
Torej za vsak $[x^n]F_n(x)$ konstantni od nekod naprej in enaki npr. a_n.
$F(x) = \sum_n a_n x^n$ je limita $(F_n(x))_m$.

Primer.
$\left(\sum_n x^n\right)(1-x) = 1$
$c_n = 1 \cdot (-1) + 1 \cdot 1 = 0 \; \forall n \geq 1$
$c_0 = 1$.
Torej $\sum_n x^n = \frac{1}{1-x} \implies 1-x$ inverz od $\sum_n x^n$.
$\lim_{N\to\infty} \sum_{n=0}^{N} x^n = \frac{1}{1-x}$.

Opomba. $(F_m(x))_m$ konvergira v $K[[x]]$, če je $([x^n]F_m(x))_m$ od nekod naprej konstantno, npr a_n; v tem primeru je $\lim_{m\to\infty} F_m(x) = \sum_n a_n x^n$.

Odvajanje:
$F'(x) = \lim_{h\to 0} \frac{F(x+h)-F(x)}{h}$.
Za $K[[x]]$:
$[x^n]F'(x) := (n+1)[x^{n+1}]F(x)$
$\left(\sum_n a_n x^n\right)' = F(x)'G(x) + F(x)G(x)'$.

Dokaz: DN.
$\left(\frac{F(x)}{G(x)}\right)' = \frac{F(x)'G(x)-F(x)G(x)'}{G(x)^2}$; $G(0) \neq 0$

Primer.

$F'(x) = F(x)$

$(n+1)a_{n+1} = a_n$

$na_n = a_{n-1}$

a_0 poljubno

$a_n = \frac{a_0}{n!}$.

$e^{\lambda x} := \sum_n \frac{\lambda^n}{n!} x^n$
$e^{\lambda x} \cdot e^{\mu x} = e^{(\lambda+\mu)x}$
$L = \sum_{k=0}^{n} \frac{\lambda^k}{k!} \frac{\mu^{n-k}}{(n-k)!} \stackrel{?}{=} \frac{(\lambda+\mu)^n}{n!} = D.$
Binomski izrek v K: enakost velja.
$F'(x) = \frac{1}{1-x},\ F(0) = 0$
$(n+1)a_{n+1} = 1$
$a_n = \frac{1}{n}$
$\log \frac{1}{1-x} := \sum_{n=1}^{\infty} \frac{x^n}{n!}$
$e^{\log \frac{1}{1-x}} \stackrel{?}{=} \frac{1}{1-x}.$
Najprej definicija kompozituma, dokaz enakosti kasneje.
Bolj splošno:
$F(0) = 1$
$\log(F(x)G(x)) = \log F(x) + \log G(x)$: DN.
Binomska vrsta:
$\lambda \in K, n \in \mathbb{N}$, $\binom{\lambda}{n} := \frac{\lambda^{\underline{n}}}{n!}$ posplošen binomski koeficient.
$B_\lambda(x) = \sum_{n=0}^{\infty} \binom{\lambda}{n} x^n$
$n \in \mathbb{N}:\ B_n(x) = \sum_{k=0}^{\infty} \binom{n}{k} x^n = (1+x)^n.$

Trditev 2.2.5.

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

Dokaz 2.2.6.

$D = \frac{(\lambda+\mu)^{\underline{n}}}{n!} = \sum_{k=0}^{n} \frac{\lambda^{\underline{k}}}{k!} \frac{\mu^{\underline{n-k}}}{(n-k)!} = L$
$\sum_{k=0}^{n} \binom{n}{k} \lambda^{\underline{k}} \mu^{\underline{n-k}} = (\lambda+\mu)^{\underline{n}}.$

Indukcija: DN. ■

$B_\lambda(x) := (1+x)^\lambda$

$n \in \mathbb{N}: \ B_n(x) \cdot B_{-n}(x) = 1$

$(1+x)^{-n} = \frac{1}{(1+x)^n}$

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

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

$$\begin{aligned}(1-x)^{-k} &= \frac{1}{1-x} \cdots \frac{1}{1-x} \\ &= \sum_{n=0}^{\infty} \left(\sum_{n_i \geq 0, \sum_{i=1}^{k} n_i = n} 1 \right) x^n \\ &= \sum_n (\text{število šibkih kompozicij } n \text{ s } k \text{ členi}) x^n \\ &= \sum_n \binom{n+k-1}{k-1} x^n\end{aligned}$$

$F(x)G(x)H(x) = \sum_{n=0}^{\infty} \left(\sum_{n_1,n_2,n_3 \geq 0, n_1+n_2+n_3=n} a_{n_1} b_{n_2} c_{n_3} \right) x^n$

$\binom{-1}{n} = (-1)^n \binom{n}{0} = (-1)^n$

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

$$\begin{aligned}\binom{\frac{1}{2}}{n} &= \frac{\frac{1}{2}\left(-\frac{1}{2}\right)\dots\left(\frac{1}{2}-n+1\right)}{n!} \\ &= \frac{(-1)^{n-1}(2n-3)!!}{2^n \cdot n!} \cdot \frac{(2n-2)!!}{(2n-2)!!} \\ &= \frac{(-1)^{n-1}(2n-2)!}{2^n \cdot n! \cdot 2^{n-1} \cdot (n-1)!} \\ &= \frac{(-1)^{n-1}}{2^{2n-1} \cdot n} \binom{2n-2}{n-1}; \ n \geq 1.\end{aligned}$$

2.3 Kompozitum

$F(x) = \sum_n a_n x^n$
$G(x) = \sum_n b_n x^n$
$F \circ G(x) = F(G(x)) = ?$
$(F \circ G)(x) = a_0 + a_1 G(x) + a_2 G^2(x) + \cdots = \lim_{N\to\infty} \sum_{n=0}^{N} a_n G^n(x)$.
Kdaj ta limita obstaja?

Trditev 2.3.1. $(F_n(x))_n$.
$\lim_{N\to\infty} F_n(x)$ obstaja $\iff$ $\lim_{n\to\infty} v(F_n(x)) = \infty$.

Dokaz 2.3.2.
$(\Longrightarrow)$:

$$\left(\sum_{n=0}^{N} F_n(x)\right)_N \text{ je Cauchyjevo :}$$
$$\forall x\ \exists N_0\ \forall N, M \geq N_0 : d\left(\sum_{n=0}^{N} F_n(x), \sum_{m=0}^{M} F_m(x)\right) \leq 2^{-k}$$
$$M = N - 1 :\ v(F_N(x)) \geq k.$$

$(\Longleftarrow)$:

$$\forall k \exists N_0\ \forall N \geq N_0 : v(F_n(x)) \geq k \text{ (predpostavka)}$$
$$\begin{aligned} N > M \geq N_0 : d\left(\sum_{n=0}^{N} F_n(x), \sum_{m=0}^{M} F_m(x)\right) &\\ = 2^{-v(F_{M+1}(x)+\cdots+F_N(x))} &\\ \leq \max\{2^{-v(F_{M+1}(x))} \ldots 2^{-v(F_N(x))}\} &\\ \leq 2^{-k}. & \end{aligned}$$

∎

$$\begin{aligned} F \circ G(x) \text{ obstaja} &\iff \lim_{n\to\infty} v(a_n G^n(x)) = \infty \\ &\iff v(G(x)) > 0 \text{ ali } a_n = 0 \text{ od nekod naprej} \\ &\iff F \text{ polinom ali } G(0) = 0. \end{aligned}$$

Velja $v\left(a_n G^n(x)\right) = \begin{cases} n \cdot v(G(x));\ a_n \neq 0 \\ \infty;\ a_n = 0 \end{cases}$

Primer.

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

$G(x) = e^x$

$(F \circ G)(x) = e^{2x} - 3e^x + 1$ - ok

$F(x) = G(x) = e^x$ - ni ok

$F(x) = e^x$

$G(x) = e^x - 1$

$e^{e^x - 1}$ - ok.

Opomba.

$F(x) = \sum_n a_n x^n$

$G(x) = \sum_n b_n x^n,\ b_0 = 0$

$a_0 + a_1(b_1 x + b_2 x^2 + \dots) + a_2(b_1 x + b_2 x^2 + \dots)^2 + \dots$

Za izračun koeficienta pri x^5 izračunamo končno vsoto.

Enota za kompozitum: $x = 0 + 1 \cdot x + 0 \cdot x^2 + \dots$

$F \circ x = a_0 + a_1 x + a_2 x^2 + \dots = F = x \circ F = 1 \cdot (a_0 + a_1 x + \dots)$

Izrek 2.3.3.

$F \in K[[x]]$ ima inverz za kompozitum $\iff$ $F(x) = a_0 + a_1 x;\ a_1 \neq 0$ ali $v(F(x)) = 1$.

Primer.

$x - x^2$ ima inverz,

$e^x - 1$ ima inverz,

x^2 nima inverza.

$F^{<-1>}$ - inverz za kompozitum.

Dokaz 2.3.4.

$(\Longrightarrow)$:

$$F(x) = \sum_n a_n x^n$$

$$G(x) = \sum_n b_n x^n \text{ inverz od } F$$

$$a_0 = 0 \overset{?}{\iff} b_0 = 0$$

$$(\Longleftarrow) : F \circ G = a_0 + a_1(b_1 x + \dots) + a_2(\dots)^2 + \dots$$

$$[x^0]F(G(x)) = a_0 = [x^0]x = 0$$

$(\Longrightarrow)$: isto?

$$1. a_0 \neq 0, b_0 \neq 0$$

$$\Longrightarrow F{,}G \text{ polinoma, } deg(F \circ g) = deg(F) \cdot deg(G) = 1$$

$$\Longrightarrow deg(F) = deg(G) = 1$$

$$2. a_0 = b_0 = 0$$

$$v(F \circ G) = v(F) \cdot v(G) = 1$$

$$\Longrightarrow v(F) = v(G) = 1$$

$$\Longrightarrow F(x) = a_1 x + a_2 x^2 + \dots;\ a_1 \neq 0.$$

($\Longleftarrow$):

$$F(x) = a_0 + a_1 x;\ a_1 \neq 0$$
$$a_0 + a_1 y = x \implies y = \dots$$
$$F^{<-1>}(x) = -\frac{a_0}{a_1} + \frac{x}{a_1}$$
$$F(x) = a_1 x + a_2 x^2 + \dots; a_1 \neq 0.$$

Levi inverz: $G_1(x) = b_0 + b_1 x + \dots$

$$G_1 \circ F = x$$
$$b_0 + b_1(a_1 x + \dots) + b_2(a_1 x + \dots)^2 + \dots = x$$
$$[x^0] : b_0 = 0$$
$$[x^1] : a_1 b_1 = 0 \implies b_1 = \frac{1}{a_1}$$
$$[x^2] : b_1 a_2 + b_1 a_1^2 = 0 \implies b_2 = -\frac{b_1 a_2}{a_1^2}$$
$$[x^3] : b_1 a_3 + 2b_2 a_1 a_2 + b_3 a_1^3 = 0 \implies b_3 = \dots \frac{\because}{a_1^3}$$
$$[x^n] : \dots + b_n a_1^n = 0;\ n \geq 1.$$
$$b_n = \dots \text{ rekurzivno.}$$

Desni inverz: $G_2(x) = c_0 + c_1 x + \dots,\ c_0 = 0$

$$F \circ G_2 = x$$
$$a_1(c_1 x + \dots) + a_2(c_1 x + \dots)^2 + \dots = x$$
$$[x^0] : 0 = 0$$
$$[x^1] : a_1 c_1 = 1 \implies c_1 = \frac{1}{a_1}$$
$$[x^2] : a_1 c_2 + a_2 c_1^2 = 0 \implies c_2 = -\frac{a_2 c_1^2}{a_1}$$
$$[x^3] : a_1 c_3 + 2a_2 c_1 c_2 + a_3 c_1^3 = 0 \implies c_3 = \frac{\because}{a_1}$$
$$[x^n] : a_1 c_n + \dots = 0 \implies c_n = \frac{\because}{a_1}.$$

■

$(G_1 \circ F) \circ G_2 = G_2$
$G_1 \circ (F \circ G_2) = G_1$.
Iz asociativnosti (ki je nismo dokazali) sledi $G_1 = G_2 = F^{<-1>}$.

Trditev 2.3.5.
$F_n(0) = 0$
$\lim_{N\to\infty} \prod_{n=1}^{N}(1 + F_n(x))$ obstaja $\iff$ $\lim_{n\to\infty} v(F_n(x)) = \infty$.
Dokaz DN.

Primer.
$(1 + x)(1 + x)(1 + x)\dots$ - ni ok,
$(1 + x)(1 + x^2)(1 + x^3)\dots$ - ok.

Opomba.
$K[[x]]$
$K[[x,y]] = K^{\mathbb{N}\times\mathbb{N}}$
$\sum a_{n,m}x^n y^m$ bivariantna potenčna vrsta.
$\sum_{k,m} \binom{n}{k} x^k y^m = \sum_m (1 + x)^n y^n = \frac{1}{1-(1+x)y}$.
$K[[x_1, x_2 \dots]]$
$x_1x_2^2x_3 + x_2x_3 + \dots$ - ok
$x_1x_2x_3x_4 \cdots$ - ni ok.

2.4 Reševanje linearnih rekurzivnih enačb s konstantnimi koeficienti

Primer.

(1) $a_n = 2a_{n-1} + 1$ $n \geq 1, a_0 = 1$
$1, 3, 7, 15 \dots$
$F(x) = \sum_n a_n x^n$ rodovna funkcija (angl. generating function) zapo-

redja.

$$\begin{aligned}
F(x) - 1 &= \sum_{n=1}^{\infty} a_n x^n = \sum_{n=1}^{\infty} (2a_{n-1} + 1)x^n = 2xF(x) + \frac{x}{1-x} \\
F(x)(1-2x) &= 1 + \frac{x}{1-x} = \frac{1}{1-x} \\
F(x) &= \frac{1}{(1-x)(1-2x)}.
\end{aligned}$$

Ekvivalentno:

$$\begin{aligned}
&a_n = 2a_{n-1} + 1 \quad / \cdot x^n \sum_{n=1}^{\infty} \\
&F(x) - 1 = \frac{x}{1-x} + 2xF(x) \\
&F(x) = \frac{1}{(1-x)(1-2x)} = \frac{A}{1-x} + \frac{B}{1-2x} = \frac{A(1-2x) + B(1-x)}{(1-x)(1-2x)} \\
&/ \cdot (1-x), x = 1 \\
&\frac{1}{-1} = A \implies A = -1 \\
&/ \cdot (1-2x), x = \frac{1}{2} \\
&B = 2
\end{aligned}$$

$a_n = -1 + 2^{n+1}$.

(2) $F_n = F_{n-1} + F_{n-2}\ n \geq 2, F_0 = F_1 = 1 \quad / \cdot x^n \sum_{n=2}^{\infty}$

$$\begin{aligned}
&F(x) = \sum_n F_n x^n \\
&F(x) - 1 - x = x(F(x) - 1) + x^2 F(x) \\
&F(x) = \frac{1}{1-x-x^2} = \frac{1}{(1-y_1x)(1-y_2x)}.
\end{aligned}$$

Ničli $1 - x - x^2$ sta $\frac{1}{y_1}, \frac{1}{y_2}$

y_1, y_2 sta ničli $y^2 - y - 1$ (obrnjen polinom), torej $x_1,x_2 = \frac{-1 \pm \sqrt{5}}{2}$.

V splošnem:

$p(x) = c_0 + c_1x + \cdots + c_dx^d;\ c_d \neq 0$

ima ničle $\lambda_1 \dots \lambda_d$, ima
$p^{\text{obr}}(x) = c_0 x^d + c_1 x^{d-1} + \dots + x_d$ (obrnjeni polinom) ničle $\frac{1}{\lambda_1} \dots \frac{1}{\lambda_d}$:

$$\begin{aligned} p^{\text{obr}}\left(\frac{1}{\lambda_i}\right) &= c_0 \cdot \frac{1}{\lambda_i^d} + c_1 \cdot \frac{1}{\lambda_i^{d-1}} + \dots + c_d \\ &= \frac{c_0 + c_1\lambda_i + \dots + c_d\lambda_i^d}{\lambda_i^d} = 0 \end{aligned}$$

$$\begin{aligned} F(x) &= \frac{1}{1 - x - x^2} \\ &= \frac{1}{(1-y_1x)(1-y_2x)} \\ &= \frac{\frac{1}{1-\frac{y_2}{y_1}}}{1-y_1x} + \frac{\frac{1}{1-\frac{y_1}{y_2}}}{1-y_2x} \\ &= \frac{1}{y_1-y_2}\left(\frac{y_1}{1-y_1x} - \frac{y_2}{1-y_2x}\right) \\ & y_1 - y_2 = 5 \\ \implies F_n &= \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+1}\right). \end{aligned}$$

Izrek 2.4.1. NSTE (naslednje trditve so ekvivalentne) za $(a_n)_n, a_n \in \mathbb{C}$:

(1) $c_d a_n + c_{d-1}a_{n-1} + \dots + c_n a_{n-d} = 0, \quad n \geq d,\ c_0, c_d \neq 0,$

(2) $F(x) = \sum_n a_n x^n = \frac{P(x)}{c_d + \dots + c_0 x^d},\ deg\ P < d,$

(3) $a_n = \sum_{i=1}^k p_i(n)\lambda_i^n,\ \lambda_1 \dots \lambda_k$ ničle $c_d y^d + \dots + c_0$ (karakteristični polinom) s kratnostmi $\alpha_1 \dots \alpha_k$, $deg\ p_i < \alpha_i$.

Dokaz 2.4.2.

(1) $\Longrightarrow$ (2):

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

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

$$F(x) = (c_d + c_{d-1}x + c_{d-2}x^2 + \cdots + c_0 x^d) = P(x) \quad degP < d.$$

(2) $\Longrightarrow$ (1):

$$(c_d + c_{d-1}x + \cdots + c_0 x^d) \cdot \sum_n a_n x^n = P(x)$$

$$n \geq d: \ [x^n]: \ c_d a_n + \cdots + c_0 a_{n-d} = 0.$$

(2) $\Longrightarrow$ (3):

$$\begin{aligned} \sum_n a_n x^n &= \frac{P(x)}{c_d(1-\lambda_1 x)^{\alpha_1} \ldots (1-\lambda_m x)^{\lambda_m}} \\ &\stackrel{\text{parc}}{=} \sum_{i=1}^{k} \sum_{j=1}^{\alpha_i} \frac{A_{ij}}{(1-\lambda_i x)^j} \\ \frac{1}{(1-x)^d} &= \sum_n \binom{n+d-1}{d-1} x^n \\ a_n &= \sum_{i=1}^{k} \left(\sum_{j=1}^{\alpha_i} A_{ij} \cdot \binom{n+j-1}{j-1} \right) \lambda_i^n, \end{aligned}$$

$$\binom{n+j-1}{j-1} \text{ polinom v } n \text{ stopnje } j-1 < \alpha_i.$$

(3) $\Longrightarrow$ (2): podobno: $p_i(n)$ zapišemo v bazi $\binom{n+j-1}{j-1}$. ■

Primer.

$a_n - 7a_{n-1} + 18a_{n-2} - 12a_{n-3} = 0$, a_0, a_1, a_2 dani.

$y^3 - 7y^2 + 18y - 12 = (y-2)^2(y-3)$

$\Longrightarrow$ $a_n = 2^n(An + B) + 3^n \cdot C$.

A,B,C dobimo iz a_0, a_1, a_2 (vstavimo, dobimo sistem).

Opomba.
$\sum_n a_n x^n = \frac{P(x)}{Q(x)},\ degP \geq degQ \iff c_d a_n + \cdots + c_n a_{n-d} = 0$ za $n \geq N$ (dovolj velik).

Opomba.
$c_d a_n + \cdots + c_0 a_{n-d} = r(n) \cdot \lambda^n,\ deg\ r = \alpha.$
Homogena + partikularna
$\sum_n r(n)\lambda^n x^n = \frac{R(x)}{(1-\lambda x)^\alpha}.$
Če λ α_i-kratna ničla karakterističnega polinoma: $\sum_{j=1}^{\alpha+\alpha_i} \ldots$
Nastavek: $n^{\alpha_i} q(n)\lambda^n,\ deg\ q = \alpha_i - 1.$

Primer.
$a_n - 4a_{n-1} + 4a_{n-2} = n \cdot 2^n,\ n \geq 2.$
Partikularna: $n^2 \cdot (An + B)2^n$.

2.5 Nadaljevanje uporabe običajnih rodovnih funkcij

$F(x) = \sum_n a_n x^n$
$F(x) \overset{\text{orf}}{\longleftrightarrow} (a_n)_n$
$F^{'}(x) \overset{\text{orf}}{\longleftrightarrow} ((n+1)a_{n+1})_n$
$xF^{'}(x) \overset{\text{orf}}{\longleftrightarrow} (na_n)_n$
$DF(x) := F^{'}(x)$, D: operator odvajanja.
$(xD)^2 F(x) \overset{\text{orf}}{\longleftrightarrow} (n^2 a_n)_n$
$p(xD)F(x) \overset{\text{orf}}{\longleftrightarrow} (p(n)a_n)_n, \quad p$ polinom.

Primer.
$\sum_{j=0}^n j^2$
$\frac{1}{1-x} \overset{\text{orf}}{\longleftrightarrow} (1)_n$
$(xD)^2 \frac{1}{1-x} \overset{\text{orf}}{\longleftrightarrow} (n^2)_n$
$x \cdot \left(\frac{x}{(1-x)^2}\right)^{'} = \cdots = \frac{x(1+x)}{(1-x)^3} = F(x)$ - samo členi.
$F(x) \overset{\text{orf}}{\longleftrightarrow} (a_n)_n$

$F(x) \cdot \frac{1}{1-x} \xleftrightarrow{\text{orf}} \left(\sum_{j=0}^{n} a_j\right)_n$ - vsota je konvolucija z $(1)_n$.

$$\begin{aligned}[x^n]\left(F(x) \cdot \frac{1}{1-x}\right) &= [x^n]\left(\frac{x}{(1-x)^4} + \frac{x^2}{(1-x)^4}\right) \\ &= \binom{n+2}{3} + \binom{n+1}{3} \\ &= \frac{n(n+1)(2n+1)}{6}.\end{aligned}$$

$F(x) \cdot G(x) = \sum_n a_n x^n \cdot \sum_n b_n x^n = \sum_n \left(\sum_{k=0}^{n} a_k b_{n-k}\right) x^n$.
Naj bo 1. del struktura A ($(a_n)_n$ preštevalno zaporedje),
naj bo 2. del struktura B ($(b_n)_n$ preštevalno zaporedje):
$\sum_{k=0}^{n} a_k b_{n-k}$.

Primer.

(1) m kroglic, rdeče, črne, zelene, zelenih kroglic sodo in so na koncu.
$1, 2, 5, 10 \ldots$
A: rdeče / črne kroglice: $2^n \to \frac{1}{1-2x}$
B: sodo mnogo zelenih kroglic: $1, 0, 1, 0, 1 \cdots \to \frac{1}{1-x^2}$
$\frac{1}{1-2x} \cdot \frac{1}{1-x^2} = \frac{\frac{4}{3}}{1-2x} + \frac{-\frac{1}{2}}{1-x} + \frac{\frac{1}{6}}{1+x}$
$a_n = \frac{4}{3} \cdot 2^n - \frac{1}{2} + \frac{1}{6}(-1)^n$.

(2) Kompozicije s k členi
A: neničelno število: $0, 1, 1, 1, 1 \cdots \to \frac{x}{1-x}$
$\left(\frac{x}{1-x}\right)^k = \sum_n \binom{n+k-1}{k-1} x^{n+k} = \sum_n \binom{n-1}{k-1} x^n$,
šibke kompozicije:
$\left(\frac{1}{1-x}\right)^k$,
kompozicije z lihimi členi: $0, 1, 0, 1, 0, 1 \cdots \to \frac{x}{1-x^2}$
$\left(\frac{x}{1-x^2}\right)^k$.

(3) $S(n,k)$
$n = 7, k = 3 : \{\{1, 4, 5\}, \{2, 7\}, \{3, 6\}\}$
$\sum_n S(n,k) x^n = ?$

Vrstni red določimo: 1 v 1. bloku, v 2. bloku najmanjše število, ki ni v 1. bloku ...
$\to$ 1 2 3 1 1 3 2 (primer od prej).
Dobimo: zaporedje n števil v $[k]$, vsa od 1 do k se pojavijo, 1. pojavitev i je pred 1. pojavitvijo $i+1$
$1\ (1\dots 1)2(1/2\dots 1/2)3(\dots)\dots$
$x\cdot\frac{1}{1-x}\cdot x\cdot\frac{1}{1-2x}\dots$
$\sum_n S(n,k)x^n=\frac{x^k}{(1-x)(1-2x)\dots(1-kx)}$.
Ekvivalentno: $(1-kx)\sum_n S(n,k)x^n=\sum_n S(n-1,k-1)x^n$
$[x^n]: S(n,k)-kS(n-1,k)=S(n-1,k-1)$
$\frac{x^k}{(1-x)\dots(1-kx)}=\frac{(-1)^k}{k!}+\sum_{j=1}^k\frac{A_j}{1-jx}\overset{DN}{=}\dots$

(4) Razčlenitve
$\overline{p_k}(n)\overset{\text{konjugiranje}}{=}$ število razčlenitev n s členi $\leq k$

$$\frac{1}{1-x}\cdot\frac{1}{1-x^2}\cdots\frac{1}{1-x^k}$$
$$=\sum_n\overline{p_k}(n)x^n$$
$$=(1+x+x^2+\dots)(1+x^2+x^4+\dots)(1+x^3+\dots)\dots(1+x^k+\dots)$$

$[x^n]: x^n=x^{m_1}\cdot x^{2m_2}\dots x^{km_k}$
$n=m_1+2m_2+\dots+km_k$
$k\dots k\dots 32\dots 21\dots 1$

$$\begin{aligned}\sum_n p_n(n)x^n&=\lim_{k\to\infty}\sum_n\overline{p_k}(n)\\&=\lim_{n\to\infty}\frac{1}{\prod_{j=1}^n(1-x^i)}\\&=\prod_{i=1}^\infty\frac{1}{1-x^i}.\end{aligned}$$

$d(n)$: število razčlenitev n z različnimi členi
$\sum_n d(n)x^n=\prod_{i=1}^\infty(1+x^i)$ (0 ali 1-krat vedno)
$o(n)=$ število razčlenitev n z lihimi členi

$\sum_n o(n)x^n = \prod_{i=0}^{\infty} \frac{1}{1-x^{2i+1}}$
$\prod_i (1+x^i) \cdot \frac{1-x^i}{1+x^i} = \prod_i \frac{1-1^{2i}}{1-x} = \prod_i \frac{1}{1-x^{2i+1}}$
$\implies o(n) = d(n)$.

DN: bijekcija.

(5) c_n: Dyckove poti dolžine n.
$c_{n+1} = \prod_{k=0}^{n} c_k \cdot c_{n-k} \qquad / \cdot x^{n+1} \sum_n$
$F(x) - 1 = x \cdot \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} c_k c_{n-k}\right) x^n = x \cdot F^2(x)$
$F(x) = 1 + xF^2(x)$:
1: prazna, $xF^2(x)$: dolžine n, $2n$ korakov
Motzkinova pot: v smeri $(1{,}1), (1, -1), (1{,}0)$
$M(x) = 1 + xM(x) + x^2M^2(x)$:
1: prazna, $xM(x)$: naravnost, $x^2M^2(x)$: desno-gor
$xF^2 - F + 1 = 0$
$F = \frac{-1 \pm \sqrt{1-4x}}{2x}$
$\sqrt{1-4x} = 1 - \sum_{n=1}^{\infty} \frac{1}{n}\binom{2n-2}{n-1} \cdot \frac{(-1)^n}{2^{2n-1}}(-4x)^n = 1 - \sum_{n=1}^{\infty} \frac{2}{n}\binom{2n-2}{n-1} x^n$
$\frac{1+\sqrt{1-4x}}{2x}$ - ne, ker $\frac{2+\dots}{2x}$
$\frac{1-\sqrt{1-4x}}{2x} = \sum_{n=0}^{\infty} \frac{1}{n+1}\binom{2n}{n} x^n$.
Druga utemeljitev:
$4x^2F^2 - 4xF + 4x = 0$
$\left(2xF - \left(1 - \sqrt{1-4x}\right)\right)\left(2xF - \left(1 + \sqrt{1-4x}\right)\right) = 0$ v $K[[x]]$.
$2xF - \left(1 + \sqrt{1-4x}\right) \neq 0$ (konstantni koeficient nima 0)
$\implies 2xF = 1 - \sqrt{1-4x}$.

$F^k(x)$: razdelimo na k delov, vsakemu damo strukturo F.
$\sum_{k=0}^{\infty} F^k(x) = \frac{1}{1-F(x)}$: razdelimo na poljubno mnogo delov, vsakemu F.

Primer.

(1) Kompozicije n.
$$\frac{1}{1-\frac{x}{1-x}} = \frac{1-x}{1-2x} = \begin{cases} 2^{n-1};\ n > 0 \\ 0;\ n = 0 \end{cases}$$
kompozicije s členi 1 in 2

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

(2) $2 \times n$ plošča, domine 2×1.

Primitivni tlakovanji

$\frac{1}{1-x-x^2}$

Domini 1×1 in 2×1.

$n = 1$: 1 možnost,

$n = 2$: 3,

$n = 3$: 2,

$n = 4$: 2,

$\vdots$

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

(3) Primitivna Dyckova pot: se ne dotakne x osi.

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

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

Levi faktor Dyckove poti: $L(x) = \frac{F(x^2)}{1-x-x^2F(x)} = \cdots = \frac{2}{1-2x+\sqrt{1-4x^2}}$

$F(x^2)$: Dyckova pot (na začetku), $xF(x^2)$: korak + Dyckova pot.

DN: $L_n = \binom{n}{\lfloor \frac{n}{2} \rfloor}$, namig: $\frac{1}{\sqrt{1-4x}} =?$

$(F \circ G)(x) = a_0 + a_1 G(x) + a_2 G^2(x) + \dots$: razdelimo na poljubno delov, vsakemu delu damo strukturo G, delom da strukturo F.

Primer.

Število kompozicij s sodo mnogo lihimi členi.

$n = 0 : 1$

$n = 1 : 0$

$n = 2 : 1$

$n = 3 : 0$

$n = 4 : 3$

$n = 5 : 0$

$n = 6 : 8$

$n = 7 : 0$

$n = 8 : 21$

$G(x) = \frac{x}{1-x^2}$ - lihi
$F(x) = \frac{1}{1-x^2}$ - sodo mnogo.

$$\begin{aligned}(F \circ G)(x) &= \frac{1}{1 - \left(\frac{x}{1-x^2}\right)^2} \\ &= \frac{(1-x^2)^2}{(1-x-x^2)(1+x-x^2)} \\ &= \dots \\ &= 1 + \frac{x}{2}\left(\frac{1}{1-x-x^2} - \frac{1}{1+x-x^2}\right) \\ &= \sum_{n \text{ lih}} F_n x^n\end{aligned}$$

kjer se, ko razpišemo $\left(\frac{1}{1-x-x^2} - \frac{1}{1+x-x^2}\right)$ sodi odštejejo, lihi štejejo 2-krat, to delimo z 2.

Primer (Dobri Will Hunting).

(1) Matrika sosednosti: $A = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 2 & 1 \\ 0 & 2 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix}$.

(2) Matrika, ki opisuje sprehode dolžine $3 : A^3 = \begin{bmatrix} 2 & 7 & 2 & 3 \\ 7 & 2 & 12 & 7 \\ 2 & 12 & 0 & 2 \\ 3 & 7 & 2 & 2 \end{bmatrix}$.

(3) Poišči rodovno funkcijo za sprehode $i \to j$

$$\sum_{k=0}^{\infty} A^k x^k = (I - Ax)^{-1} = \frac{1}{det(I - Ax)} \left[\dots\right]$$

(4) $1 \to 3$:
$\frac{2x^2+2x^3}{1-7x^2-2x^3+4x^4}$.

2.6 Uporaba eksponentnih rodovnih funkcij

$F(x) = \sum_n \frac{a_n}{n!} x^n$
$F(x) \xleftrightarrow{\text{erf}} (a_n)_n$
$\left[\frac{x^n}{n!}\right] F(x) = a_n$
$\left[\frac{x^n}{n!}\right] F(x) = n![x^n]F(x)$
$F'(x) \xleftrightarrow{\text{erf}} (a_{n+1})_n$
$xF'(x) \xleftrightarrow{\text{erf}} (n \cdot a_n)_n$
$p(xD)F(x) \xleftrightarrow{\text{erf}} (p(n)a_n)_n.$

Primer.

(1) $F_{n+2} = F_{n+1} + F_n;\ n \geq 0$
$F(x) = \sum_n \frac{F_n}{n!} x^n$
$F''(x) - F'(x) - F(x) = 0$
$\lambda^2 - \lambda - 1 = 0 \implies \lambda_{1,2} = \frac{1 \pm \sqrt{5}}{2}$
$F(x) = Ae^{\frac{1+\sqrt{5}}{2}x} + Be^{\frac{1-\sqrt{5}}{2}x}$
$F_n = \left[\frac{x^n}{n!}\right] F(x) = A\left(\frac{1+\sqrt{5}}{2}\right)^n + B\left(\frac{1-\sqrt{5}}{2}\right)^n.$

(2) i_n: število involucij v S_n ($\pi^2 = id$).
$i_n = i_{n-1} + (n-1)i_{n-2};\ n \geq 2$:
i_{n-1}: n fiksna točka
i_{n-2}: n v transpoziciji z enim od $n-1$ ostalih.
$I(x) = \sum_n \frac{i_n}{n!} x^n$
$I'' - I' - (xI' + I) = 0$
$I'' - (x+1)I' - I = 0$
$(I' - (x+1)I)' = 0$
$I' - (x+1)I = c$
$x = 0:\ 1 - 1 = 0 = c$
$I' = (x+1)I$
$\int \frac{dI}{I} = \int (x+1)dx$
$\ln I = \frac{x^2}{2} + x + \log D$

$I = De^{x+\frac{x^2}{2}} \xRightarrow{x=0} D = 1$
$I(x) = e^{x+\frac{x^2}{2}}$.

$F(x) = \sum_n \frac{a_n}{n!} x^n$
$G(x) = \sum_n \frac{b_n}{n!} x^n$
$F(x)G(x) = \sum_n \left(\sum_{k=0}^n \frac{a_k}{k!} \frac{b_{n-k}}{(n-k)!} \right) x^n = \sum_n \left(\sum_{k=0}^n \binom{n}{k} a_k b_{n-k} \right) \frac{x^n}{n!}$
$\sum_{k=0}^n \binom{n}{k} a_k b_{n-k}$: binomska konvolucija.
orf: neoznačene strukture,
erf: označene strukture.

Primer.
d_n: premestitve v S_n (dearangement) - permutacije brez negibne točke.
$D(x) = \sum_n \frac{d_n}{n!} x^n$.
Permutacija = premestitev + množica negibnih točk.
(1 5 2) (3) (4 8 7) (6)
$\frac{1}{1-x} = D(x) \cdot e^x$
$D(x) = \frac{e^{-x}}{1-x}$
$e^{-x} = \sum_n \frac{(-1)^n}{n!} x^n$
$\frac{e^{-x}}{1-x} = \sum_n \left(\sum_{k=0}^n \frac{(-1)^k}{k!} \right) x^n$
$d_n = n! \sum_{k=0}^n \frac{(-1)^k}{k!}$.

$$\begin{aligned} F(x)G(x) &= \sum_n \left(\sum_{k=0}^n \binom{n}{k} a_k b_{n-k} \right) \frac{x^n}{n!} \\ &= \sum_n \left(\sum_{(S_1,S_2), S_1 \cap S_2 = \emptyset, S_1 \cup S_2 = [n]} a_{|S_1|} b_{|S_2|} \right) \frac{x^n}{n!} \end{aligned}$$

$$F^k(x) = \sum_n \left(\sum_{(i_1 \dots i_k), i_j \geq 0, i_1 + \dots + i_k = n} \binom{n}{i_1 \dots i_k} a_{i_1} \dots a_{i_k} \right) \frac{x^n}{n!}.$$

Predpostavimo $F(0) = 0$!!

$$\begin{aligned} F^k(x) &= \sum_n \left(\sum_{(S_1 \ldots S_k), S_i \neq \emptyset, S_i \cap S_j = \emptyset, S_1 \cup \cdots \cup S_k = n} a_{|S_1|} \ldots a_{|S_k|} \right) \frac{x^n}{n!} \\ &= k! \sum_n \left(\sum_{(B_1 \ldots B_k) \text{razdelitev } [n]} a_{|B_1|} \ldots a_{|B_k|} \right) \frac{x^n}{n!}. \end{aligned}$$

Izrek 2.6.1.
$F(0) = 0$.
$\frac{1}{k!} F^k(x)$ je erf za strukturo: izberemo razdelitev na k blokov in vsakemu bloku damo strukturo F.

Primer.
$\sum_n S(n,k) \frac{x^n}{n!} = \frac{1}{k!}(e^k - 1)^k$
F: neprazna množica: $0,1,1 \ldots \overset{\text{erf}}{\Longrightarrow} e^x - 1$.
Binomski izrek $(e^x - 1)k = e^{-kx} - \ldots$ nam da formulo za $S(n,k)$.
$\sum_n c(n,k) \frac{x^n}{n!} = \frac{1}{k!} \left(\log \frac{1}{1-x} \right)^k$
F: cikel: $a_n = (n-1)!$ za $n \geq 1 \overset{\text{erf}}{\Longrightarrow} \log \frac{1}{1-x}$
$\sum_n L(n,k) \frac{x^n}{n!} = \frac{1}{k!} \left(\frac{x}{1-x} \right)^k$
F: neprazna linearno urejena množica: $a_n = (n)!$ za $n \geq 1 \overset{\text{erf}}{\Longrightarrow} \log \frac{1}{1-x}$.

Izrek 2.6.2 (Eksponentna formula)**.**
$F(0) = 0$.
$e^{F(x)}$ je erf za strukturo: izberemo razdelitev, vsakemu bloku damo strukturo F.

Dokaz 2.6.3. $\sum_{k=0}^{\infty} \frac{1}{k!} F^k(x) = e^{F(x)}$. ■

Primer.

(1) Permutacija = množica disjunktnih ciklov.
$\frac{1}{1-x} = e^{\log \frac{1}{1-x}}$.
DN: direktno.

(2) Involucija = množica ciklov dolžine 1 in 2: (0,1,1,0,0 . . .)
$\sum_n \frac{i_n}{n!} = e^{x+\frac{x^2}{2}}$
$a_n = |\{\pi \in S_n : \pi^6 = id\}|$
$\sum_n \frac{a_n}{n!} x^n = e^{x+\frac{x^2}{2}+\frac{x^3}{3}+\frac{x^6}{6}}$
$\sum_n \frac{d_n}{n!} x^n = e^{\sum_{n\geq 2}\frac{x^n}{n}} = e^{\log\frac{1}{1-x}-x} = \frac{e^{-x}}{1-x}$.

(3) $\sum_n \frac{B(n)}{n!} x^n = e^{e^x-1}$.

(4) a_n: število 2-regularnih grafov ($deg\, v = 2\ \forall v \in V(G)$),
F : moč množice neusmerjenih ciklov dolžime ≥ 3: $a_n = \frac{(n-1)!}{2}$; $n \geq 3$
$\sum_n \frac{a_n}{n!} x^n = e^{\sum_{n\geq 3}\frac{(n-1)!}{2}\frac{x^n}{n}} = e^{\frac{1}{2}\left(\log\frac{1}{1-x}-x-\frac{x^2}{2}\right)} = \frac{e^{-\frac{x}{2}-\frac{x^2}{4}}}{\sqrt{1-x}}$.

Kompozitum:
$(F \circ G)(x) = \sum_k \frac{a_k}{k!} G^k(x)$.

Izrek 2.6.4 (O kompoziciji)**.**
$F(x), G(x), F(0) = 0$.
Potem je $(F \circ G)(x)$ erf za strukturo: množico razdelimo na bloke, vsakemu bloku damo strukturo G, množici blokov damo strukturo F.

Primer.

(1) $\widetilde{B(n)}$: urejena Bellova števila = število urejenih razdelitev množice $[n]$.
$\widetilde{B(2)} = 3$: {1,2}; {1},{2}; {2},{1}
$\widetilde{B(n)} = \sum_k S(n,k)k!$.
$\widetilde{B(n)}$: število vseh surjekcij iz $[n]$.
$\sum_n \frac{\widetilde{B(n)}}{n!} x^n = \frac{1}{1-(e^x-1)} = \frac{1}{2-e^x}$
$G(x) = e^x - 1$
$F(x) = \frac{1}{1-x}$.

(2) Permutacije z lihim številom ciklov
$\sum_n a_n \frac{x^n}{n!} = \frac{e^{\log\frac{1}{1-x}} - e^{-\log\frac{1}{1-x}}}{2} = \frac{1}{2}\left(\frac{1}{1-x} - (1-x)\right)$.
$G(x) = \log\frac{1}{1-x}$
$F(x) = \frac{e^x - e^{-x}}{2}$ $\qquad (F(x) - F(-x)$: lihi)

$$a_n = \begin{cases} 0;\ n = 0 \\ 1;\ n = 1 \\ \frac{n}{2};\ n \geq 2 \end{cases}$$

orf	erf
$F(x)G(x)$	$F(x)G(x)$
$F^k(x)$	$\frac{1}{k!}F^k(x)$
$\frac{1}{1-F(x)},\ F(0) = 0$	$e^{F(x)}$
$F \circ G$	$F \circ G$

2.7 Algebraične rodovne funkcije

$K[x]$ polinomi,

$K[[x]]$ formalni polimon (fp?),

$K(x)$ racionalne funkcije (polje ulomkov za $K[x]$),

$\frac{1}{x} \in K(x),\ \frac{1}{x} \notin K[[x]]$,

$K(x) \cap K[[x]]$ racionalna rodovna funkcija.

Za taka zaporedja imamo linearne rekurzije.

$F(x) = \sum_n a_n x^n$

$xF^2 - F + 1 = 0$

$c_{n+1} = \sum_{k=0}^{n} c_k c_{n-k}$ kvadratična rekurzija.

Ali je $F(x) \in K(x)$?

$F(x) = \frac{P(x)}{Q(x)}$

$xP^2 = PQ - Q^2 = Q(P - Q)$

$L :$ deg $P \cdot 2 + 1$ - liha stopnja,

$$D : \begin{cases} \text{deg } P < \text{deg } Q \implies Q(P-Q) \text{ sode stopnje} \\ \text{deg } P \geq \text{deg } Q \implies \text{deg } Q(P-Q) \leq 2 \cdot \text{ deg } P \end{cases}$$

Definicija 2.7.1.

$F(x) \in K[[x]]$ je algebraična reda d, če

$Q_d(x)F^d(x) + Q_{d-1}(x)F^{d-1}(x) + \cdots + Q_0(x) = 0$ za $Q_0, Q_d \in K[X]$, $Q_0, Q_0 \neq 0$, ne obstaja taka enačba stopnje $< d$.

Algebraična reda d = racionalna fpv (formalna potenčna vrsta).

$F(x) = \sum_n F_n x^n,\ M(x) = \sum_n M_n x^n$ algebraični reda 2.

$Q_d(x)F^d(x) + \cdots + Q_0(x) = 0$ za $Q_0, Q_d \neq 0$

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

$M_n : x^2F(x)^2 + xF(x) + 1 = 0.$

S-drevo:

$S \subseteq \{1, 2, 3 \ldots\}.$

Drevo s korenom, vsak element je list ali pa je število naslednikov v S.

{2,3}-drevo

a_n: število S-dreves z n vozlišči,

b_n: število S-dreves z n listi.

$U(x) = \sum_n a_n x^n$

$V(t) = \sum_n b_n t^n.$

$S = \{2{,}3\}$

$U(x) = x + xU^2(x) + xU^3(x)$:

x: 1 vozlišče.

$V(t) = t + v^2(t) + v^3(t)$:

koren ne prispeva k številu listov.

$U(x) = x + \sum_{k\in S} xU^k(x)$

$V(t) = t + \sum_{k\in S} V^k(t)$, $1 \notin S$.

S končna $\implies$ S algebraična.

Če S neskončna, sta U in V vseeno lahko algebraični.

Primer.

- $S = \{2\}$ - dvojiška drevesa.
  $v = t + v^2$
  $v^2 - v + t = 0 \implies v = \frac{1-\sqrt{1-4t}}{2} = \sum_{n=1}^{\infty} c_{n-1}t^n$
  c_n: število dvojiških dreves z $n + 1$ listi.

- $S = \{k\}$
  $v = t + v^k$ - Lagrangeeva inverzija (kasneje).

- $S = \{1, 2, 3, 4 \dots\}$
  $U = x + x\sum_{k=1}^{\infty} U^k = x + x\frac{U}{1-U}$
  $U - U^2 = x - xU + xU = x$
  $U^2 - U + x = 0 \implies U = \frac{1-\sqrt{1-4x}}{2} = \sum_{n=1}^{\infty} c_{n-1}x^n$
  c_n: število ravninskih dreves z $n + 1$ vozlišči.

Izkaže se: U,V algebraični $\iff$ S se za končno množico razlikuje od končne unije aritmetičnih zaporedij.

Trditev 2.7.2.
$K_{alg}[[x]] = \{F[x] \in K[[x]] \text{ algebraična}\}$ je podalgebra $K[[x]]$.

$xF^2 - F + 1 = 0$
$F^2 + 2xFF' = 0$
$F' = \frac{F^2}{1-2xF} \stackrel{?}{=} a + bF;\ a, b \in K(x)$
$F^2 = a + bF - 2axF - 2bxF^2$
$(1 - 2bx)F^2 + (2ax - b)F - ax = 0$
$(1 - 2bx + (2ab - x))F - 1 - 2bx - ax = 0$
$\rightarrow$: 2 enačbi (pri $[F]$ in $[F^0]$), 2 neznanki (a, b).
$a = \frac{1}{x(1-4x)}$
$b = \frac{2x-1}{x(1-4x)}$
$F' - \frac{1}{x(1-4x)} - \frac{2x-1}{x(1-4x)}F = 0$
$x(1 - 4x)F' - 1 - (2x - 1)F = 0$
$F' = \sum_n nc_nx^{n+1}$
$[x^n] : nc_n - 4(n - 1)c_{n-1} + 2c_{n-1} + c_n$ za $n > 1$
$c_n = \frac{2(n-1)}{n+1}c_{n-1} \implies \dots c_n = \frac{1}{n+1}\binom{2n}{n}$.

Definicija 2.7.3.
$F(x) \in K[[x]]$ je D-končna, če je

$R_n(x)F^{(d)}(x) + \cdots + R_1 F'(x) + R_0 = 0$ za $R_i(x) \in K[x]$.
Ekvivalentno: vektorski prostor nad $K(x)$, generiran z $F, F', F'' \ldots$ je končno razsežen.

Definicija 2.7.4.
$(a_n)_n$ je P-rekurzivna, če je $p_d(n)a_n + \cdots + p_0(n)a_{n-d} = 0$ za $n \geq d$.

Trditev 2.7.5.
$F(x) = \sum_n a_n x^n$ je D-končna $\iff$ $(a_n)_n$ je P-rekurzivna.

Torej: za P-rekurzivno zaporedje lahko člene hitro izračunamo.

Zgled.
$F(x) = \sum_n C_n x^n$ je D-končna,
e^x je D-končna: $F' - F = 0$,
e^x ni algebraična.

Izrek 2.7.6.
$F(x)$ algebraična $\implies$ D-končna.

Dokaz 2.7.7. (skica):
$Q_d(x)F^d(x) + \cdots + Q_0(x) = 0 \quad /'$
$Q_d(x)' F^d(x) + dQ_d(x)F^{d-1}(x)F'(x) + \cdots + Q_0'(x) = 0$
$F'(x) \in K(x, F(x))$
Iz algebre:
K obseg, u v večjem obsegu;

(i) v algebraičnem: $K[u] = K(u)$ končno razsežen VP,

(ii) v transcendentnem: $K[u] \subseteq K[x]$ („u spremenljivka“).

$K = K[x]$
$u = F(x)$
$K[u] = K(x, F(x))$.
Torej: $K(x, F(x))$ je končno razsežen VP nad $K(x)$, torej so $1, F, F' \ldots$ linearno neodvisni $\implies$ F je D-končna. ∎

2.8 Eulerjeva in eulerska števila

E_n: število alternirajočih permutacij v S_n.

$E_3 = 2$ $(231), (132)$

$2E_{n+1} = \sum_{k=0}^{n} \binom{n}{k} E_k E_{n-k} + \delta_{n0}$

$E(x) = \sum_n \frac{E_n}{n!} x^n$

$2F' = F^2 + 1$

$\int \frac{2dF}{F^2+1} = \int dx$

$2 \arctan F = x + 2c$

$F = \tan\left(\frac{x}{2} + c\right)$

$F(0) = 1 = \tan c \implies c = \frac{\pi}{4}$

$\tan\left(\frac{x}{2} + \frac{\pi}{4}\right) = \frac{\tan\frac{x}{2}+1}{1-\tan\frac{x}{2}} = \frac{\sin\frac{x}{2}+\cos\frac{x}{2}}{\cos\frac{x}{2}-\sin\frac{x}{2}} = \frac{1+\sin x}{\cos x}$.

Izrek 2.8.1.

$\sum_n \frac{E_n}{n!} x^n = \frac{1+\sin x}{\cos x}$ oz.

$\frac{1}{\cos x} = \sum_{n \text{ sod}} \frac{E_n}{n!} x^n$

$\frac{1}{\sin x} = \sum_{n \text{ lih}} \frac{E_n}{n!} x^n$

Opomba.

Bernoullijeva števila.

$$B_n = \begin{cases} 1; \ n = 0 \\ \frac{1}{2}; \ n = 1 \\ 0; \ n > 1, n \text{ lih} \\ \frac{(-1)^{\frac{n}{2}+1} E_{n-1}}{2^n(2^n-1)}; \ n > 0, n \text{ sod} \end{cases}$$

$\sum_n B_n \frac{x^n}{n!} = \frac{xe^x}{e^x-1}$

$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$

$\sum_{n=1}^{\infty} \frac{1}{n^4} = \frac{\pi^4}{90}$

$\sum_{n=1}^{\infty} \frac{1}{n^{2k}} = \frac{2^{2n}(-1)^{k+1}\pi^{2k}}{2\cdot(2k)!} = \frac{E_{2k-1}\pi^{2k}}{2(2k-1)!(2^{2k}-1)} = \zeta(2k)$

Riemmanova funkcija ζ:

$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ za $Re\ s > 1$.

Z analitičnim nadaljevanjem lahko ζ definiramo na $\mathbb{C} \setminus \{1\}$.

$\zeta(-n) = \frac{B_{n+1}}{n+1}$ - (soda?) negativna števila so ničle - trivialne ničle.

Riemmanova hipoteza:

$Re\ z = \frac{1}{2}$ za vsako netrivialno ničlo z funkcije ζ.

$\zeta(-1) = -\frac{B_2}{2} = -\frac{1}{12}$

„$\sum_{n=1}^{\infty} n = -\frac{1}{12}$“

Faulhaberjeva formula:

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

$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6} = \frac{n^3}{3} + \frac{n^2}{2} + \frac{n}{6}$

$\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4} = \frac{n^4}{4} + \frac{n^3}{2} + \frac{n^2}{4}$

$\sum_{i=1}^{n} i^k = \frac{1}{k+1} \sum_{l=0}^{k} \binom{k+1}{l} B_l \cdot n^{k+1-l}$

$= \frac{n^{k+1}}{k+1} + \frac{n^k}{2} + \sum_{l=1}^{\lfloor \frac{k}{2} \rfloor} \frac{(-1)^{l+1}\binom{k}{2l-1}}{2^{2l}(2^{2l}-1)} E_{2l-1} \cdot n^{k-1-2l}$

$= \log n + \gamma + \frac{1}{2n} - \sum_{k=1}^{\infty} \frac{B_{2k}}{2k \cdot n^{2k}}$

$= \log n + \gamma + \frac{1}{2n} - \sum_{k=1}^{\infty} \frac{(-1)^k E_{2k-1}}{2^{2k}(2^{2k}-1)n^{2k}}$,

kjer je $H_n = 1 + \frac{1}{2} + \cdots + \frac{1}{n}$ n-to harmoično število.

$A(n,k)$: število permutacij v S_n z $k-1$ spusti.

$A(n,k) = (n+1-k)A(n-1,k-1) + kA(n-1,k)$

$\frac{1}{1-x} = 1 + x + x^2 + \ldots \quad /'/ \cdot x$

$\frac{x}{(1-x)^2} = x + 2x^2 + 3x^3 + \ldots \quad /'/ \cdot x$

$\frac{x+x^2}{(1-x)^3} = x + 4x^2 + 9x^3 + \ldots \quad /'/ \cdot x$

$\frac{x+4x^2+x^3}{(1-x)^4} = x + 8x^2 + 27x^3 + \ldots$

$A_n(x) = \sum_k A(n,k)x^k$ eulerski polinom.

Izrek 2.8.2.

$\sum_m m^n x^m = \frac{A_n(x)}{(1-x)^{n+1}}$.

Dokaz 2.8.3.

Indukcija:

$n = 0$: $\frac{1}{1-x} = \frac{1}{1-x}$

$n-1 \to n$:

$$\sum_m m^{n-1} x^m = \frac{A_{n-1}(x)}{(1-x)^n} \quad /'/ \cdot x$$

$$x \cdot \sum_m m^{n-1} x^{m-1} = \frac{A_{n-1}'(x)(1-x)^n + A_{n-1}(x)n(1-x)^{n-1}}{(1-x)^{2n}} \stackrel{?}{=} \frac{A_n(x)}{(1+x)^{n+1}}$$

$[x^k]$: $(k+1)A(n-1,k-1) - kA(n-1,k) + nA(n-1,k) = A(n,k)$ ✓

$A_{n-1}(x) = \sum_k A(n-1,k)x^k$

$A'_{n-1}(x) = \sum_k kA(n-1,k)x^{k-1}$.

■

Izrek 2.8.4.
$\sum_{n,k} A(n,k)x^k \frac{y^n}{n!} = \frac{1-x}{1-xe^{y(1-x)}}$ - mešana rodovna funkcija (običajna v x, eksponentna v y).

Dokaz 2.8.5.
$\sum_{n,k} A(n,k)x^k \frac{y^n}{n!}$
$= (1-x)\left(\sum_n \frac{A_n(x)}{(1-x)^{n+1}} \cdot \frac{y^n}{n!}(1-x)^n\right)$
$= (1-x)\sum_n \left(\sum_m m^n x^m\right) \frac{y^n(1-x)^n}{n!}$
$= (1-x)\sum_m \left(\sum_n \frac{m^n y^n (1-x)^n}{n!}\right) x^m$
$= (1-x)\sum_m e^{y(1-x)}x^m$
$= \frac{1-x}{1-e^{y(1-x)}}$. ■

2.9 Izračun povprečij in variance

Koliko elementov ima v povprečju podmnožica $[n]$?
$\frac{\sum_{T\subseteq[n]}|T|}{2^n} = \frac{\sum_n k\binom{n}{k}}{2^n} = \frac{n\cdot 2^{n-1}}{2^n} = \frac{n}{2}$
$(1+x)^n = \sum_k \binom{n}{k}x^k \quad /'$
$n(1+x)^{n-1} = \sum_k k\binom{n}{k}x^{n-1}$
$x=1$:
$n\cdot 2^{n-1} = \sum_k k\binom{n}{k}$.
S končna množica.
$F(x) = \sum_{a\in S} x^{f(a)}$
$F(1) = |S|$
$F'(x) = \sum_{a\in S} f(a)\cdot x^{f(a)-1}$
$F'(1) = \sum_{a\in S} f(a)$
$\mu = \frac{F'(1)}{F(1)} = (\log' F)(1)$

$F(x) = (1+x)^n$

$\log F(x) = n \log(1+x)$

$\log^{'} F(x) = \frac{n}{1+x}$

$(\log^{'} F)(1) = \frac{n}{2}$

$\sigma^2 = E(x^2) - \mu^2$

$E(x^2) = \frac{\sum_n f^2(s)}{|S|}$

$F^{'}(x) + xF^{''}(x) = (xF^{'}(x))^{'} = \sum_{a \in S} f^2(a) x^{f(a)-1}$

$x = 1$:

$\sigma^2 = \frac{F^{'}(1)+F^{''}(1)}{F(1)} - \frac{F^{'}(1)^2}{F(1)^2} = \frac{F^{'}(1)}{F(1)} + \frac{F^{''}(1)F(1)-F^{'}(1)^2}{F(1)^2}$.

Torej

$\mu = (\log^{'} F)(1)$

$\sigma^2 = (\log^{'} F)(1) + (\log^{''} F)(1)$

$F(x) = (1+x)^n$

$\mu = \frac{n}{2}$

$\log^{'} F(x) = \frac{n}{1+x}$

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

$\sigma^2 = \frac{n}{2} - \frac{n}{4} = \frac{n}{4}$

$\frac{n}{2} \pm \frac{\sqrt{n}}{2}$.

Koliko ciklov ima v povprečju permutacija v S_n?

$\sum_{\pi \in S_n} x^{f(\pi)} = \sum_k c(n,k) x^k = x^{\overline{n}} = F(x)$

$\log F(x) = \log x + \log(x+1) + \cdots + \log(x+n-1)$

$\log^{'} F(x) = \frac{1}{x} + \cdots + \frac{1}{x+n-1}$

$\mu = H_n = \log n + \gamma + o(1)$

$\log^{''} F(x) = -\frac{1}{x^2} - \cdots - \frac{1}{(x+n-1)^2}$

$\sigma^2 = H_n - \sum_{i=1}^{n} i^2 = \log n + \gamma - \frac{\pi^2}{6} + o(1)$

$\log n \pm \sqrt{\log n}$.

2.10 Lagrangeeva inverzija

$K[x]$ algebra polinomov,

$K(x)$ obseg racionalnih funkcij (obseg ulomkov $K[x]$),

$K[[x]]$ algebra formalnih potenčnih vrst,
$K((x)) = \{\sum_{n\geq n_0} a_n x^n;\ n_0 \in \mathbb{Z}, a_i \in K\}$ obseg formalnih Laurentovih vrst (obseg ulomkov $K[[x]]$).
$\frac{F(x)}{G(x)} = \frac{F(x)}{x^m H(x)}, \frac{F(x)}{H(x)} \in K[[x]], H(0) \neq 0.$
Seštevanje, množenje, odvod, kompozitum, valuacija ($\in \mathbb{Z}$).
$res\, F(x) = [x^{-1}]F(x)$ residuum.

Lema 2.10.1. *$res\, F(x) = 0 \leftrightarrow F(x) = G'(x)$ za $K((x))$.*

Dokaz 2.10.2.
$(\Longleftarrow)$

$$\begin{aligned} F(x) &= \left(\sum_{n\geq n_0} b_n x^n\right)' = \left(\sum_{n\geq n_0} n b_n x^{n-1}\right) \\ [x^{-1}]F(x) &= 0 \cdot b_0 = 0. \end{aligned}$$

$(\Longrightarrow)$

$$\begin{aligned} F(x) &= \sum_{n\geq n_0} a_n x^n \\ G(x) &= \sum_{n\geq n_0} \frac{a_{n-1}x^n}{n} \\ a_{-1} &= 0. \end{aligned}$$

■

Lema 2.10.3.
$F(x) \in K((x)), F(x) \neq 0$, $res\, \frac{F'(x)}{F(x)} = v(F(x))$.

Dokaz 2.10.4.
$F(x) = x^{n_0} G(x)$
$n_0 = v(F(x))$
$G(x) \in K[[x]], G(0) \neq 0$
$\frac{F'(x)}{F(x)} = \frac{n_0 x^{n_0-1} G(x) + x^{n_0} x^{n_0} G'(x)}{x^{n_0} G(x)} = \frac{n_0}{x} + \frac{G'(x)}{G(x)}$
$\frac{G'(x)}{G(x)} \in K[[x]].$ ■

Lagrangeeva inverzija (1. verzija):

$F \in K[[x]]$

$v(F(x)) = 1$

$n \cdot [x^n] \left(F^{<-1>}(x)\right)^k = k \cdot [x^{-k}]F^{-n}(x);$

$F^{-n}(x) \in K((x)).$

Torej: $n \cdot [x^n]F^{<-1>}(x) = res\, F^{-1}(x).$

Dokaz 2.10.5. $\left(F^{<-1>}(x)\right)^k = \sum_{m \geq k} c_m x^m$

$x \leftrightarrow F(x)$

$x^k = \sum_{m \geq k} c_m (F(x))^m \quad /'$

$kx^{k-1} = \sum_{m \geq k} mc_m F^{m-1}(x)F'(x) \quad / : F^n(x)$

$\frac{kx^{k-1}}{F^n(x)} = \sum_{m \geq k} mc_m F^{m-n-1}(x)F'(x) \quad /res$

$[x^{-1}]\frac{kx^{k-1}}{F^n(x)} = [x^{-k}]\frac{k}{F^n(x)}$

$F^{m-n-1}(x)F'(x) = \frac{\left(F^{m-n}(x)\right)'}{m-n};\ m \neq n$

$res\left(F^{m-n-1}(x)F'(x)\right) = 0$ če $m \neq n$ in 1 sicer (lemi)

$\to n \cdot a_n \cdot 1$ (leva stran). ∎

Primer.

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

$F^{<-1>}(x) = ?$

$n[x^n]F^{<-1>}(x) = [x^{-1}]\left(\frac{1}{1-x^2}\right)^n = [x^{-n}]\frac{x^{-n}}{(1-x)^n}$

$\frac{1}{(1-x)^n} = \sum_m \binom{m+n-1}{n-1}x^m$

$[x^n]F^{<-1>}(x) = \frac{1}{n}\binom{2n-2}{n-1} = C_{n-1}.$

Še ena razlaga:

$y - y^2 = x$

$y^2 - y + x = 0 \implies y = \frac{1 \pm \sqrt{1-4x}}{2} \implies y = x\sum_n C_n x^n.$

Lagrangeeva inverzija (2. verzija)

$F(x) = xG(F(x))$

$F(x) \in K[[x]]$

$G(x) \in K[[x]], G(0) \neq 0, v(F) = 1$

$[x^k]F(k)^k = k[x^{n-k}]G(x)^n.$

Dokaz 2.10.6.
$f(x) := \frac{x}{G(x)}, v(f) = 1$
$f(F(x)) = \frac{F(x)}{G(F(x))} = 1 \rightarrow$ ima levi inverz, tudi desni.
$n[x^n]F(x)^k = k[x^n]\left(f^{<-1>}(x)\right)^k$
$= k[x^{-k}]f^{-k}(x) = k[x^{-k}]x^{-n}G^n(x).$ ■

Primer.

(a) $S = \{k\}$
$k = 3$
a_n : število k-dreves na n vozliščih.
$v(x) = \sum_n a_n x^n$
$V(x) = x + xV^k(x) = x\left(1 + V^k(x)\right)$
$G(x) = (1+x)^n$
$n[x^n]V(x)[x^{n-1}]\left(1 + x^k\right)^n = k[x^{n-1}]\sum_{i=0}^n \binom{n}{i} x^{ki};$
$n = ki + 1, i \in \mathbb{N}, a_n = a_{ki+1} = \frac{1}{n} \cdots = \frac{1}{ki+1}\binom{ki+1}{i}.$

(b) Vpeta drevesa v K_n.
r_n: število vpetih dreves s korenom v K_n.
$R(x) = \sum_n \frac{r_n}{n!} x^n$ (vozlišča so označena).
Označimo drevo s korenom = koren + množica blokov, ki jim damo strukturo označenega drevesa s korenom.
$R(x) = xe^{R(x)}$
$G(x) = e^x$
$n[x^n]R(x) = [x^{n-1}]e^{nx}$
$e^n = \sum_k \frac{n^k x^k}{n!}$
$\frac{nr_n}{n!} = \frac{n^{n-1}}{(n-1)!}$
$r_n = n^{n-1}$
Število vpetih dreves v K_n je n^{n-2}.

2.11 Asimptotika koeficientov

$K = \mathbb{C}$

$F(x) = \sum_n a_n x^n$

$F(x) \in \mathbb{C}[[x]]$ ima pozitiven konvergenčni polmer

$R = \frac{1}{\limsup_{n\to\infty} \sqrt[n]{|a_n|}}$.

F je holomorfna v okolici 0.

Za $\forall \epsilon > 0$:

- $|a_n| < \frac{1}{R} + \epsilon$ za $\forall n \geq n_0$,
- $|a_n| > \frac{1}{R} - \epsilon$ za neskončno mnogo n.

Npr. $F(z) = \frac{1}{1-z} = 1 + z + z^2 + \dots$

$R = 1$,

$|a_n| < (1+\epsilon)^n$ za $\forall n$,

$|a_n| > (1-\epsilon)^n$ za vse sode n.

$R = \infty \implies F(z)$ cela funkcija.

$R < \infty \implies F(z)$ ima singularnost v z_0, $|z_0| = R$.

Definicija 2.11.1. f ima v z_0 pol reda r, če ima $f(z)(z-z_0)^r$ odpravljivo singularnost v z_0, $\lim_{z\to z_0} f(z)(z-z_0)^r \neq 0$.

Funkcija je meromorfna, če so vse singularnosti poli in množica polov nima stekališč (oz. je diskretna).

$f(z)(z-z_0)^r = b_0 + b_1(z-z_0) + b_2(z-z_0)^2 + \dots \quad / : (z-z_0)^n$

V kombinatoriki: $1 - \frac{z}{z_0}$, $b_i \mapsto b_{i-r}$

$f(z) = b_{-r} + b_{-r+1}\left(1 - \frac{z}{z_0}\right) + \dots + b_{-1}\left(1 - \frac{z}{z_0}\right)^{-1} + b_0 + b_1\left(1 - \frac{z}{z_0}\right) + \dots$

Glavni del (angl. principal part):

$PP_{f,z_0}(z) = b_{-r}\left(1 - \frac{z}{z_0}\right)^r + \dots + b_{-1}\left(1 - \frac{z}{z_0}\right)^{-1}$.

Če je z_0 edina singularnost na $|z| = R$:

$f(z) - PP_{f,z_0}(z)$ ima konvergenčni polmer $R' > R$.

$[z^n]PP_{f,z_0}(z) = \left(\sum_{i=1}^r b_{-i}\binom{n+i-1}{i-1}\right) z_0^n \sim \frac{b_{-r}n^{r-1}}{z_0^n(r-1)!}$.

$\forall \epsilon > 0 : [z^n]\,|f(z) - PP_{f,z_0}(z)| < \left(\frac{1}{R'} + \epsilon\right)^n$ za $n \geq n_0$.

$\frac{1}{R'} + \epsilon < \frac{1}{R}$

$\lim_{n\to\infty} \frac{\left(\frac{1}{R'}+\epsilon\right)^n}{\left(\frac{1}{R}\right)^n} = 0.$

Izrek 2.11.2.

$F(z) \in \mathbb{C}[[x]]$, $R \in (0,\infty)$, z_0 edina singularnost na $|z_0| = R$, z_0 je pol reda r. Potem je

$[z^n]F(z) \sim \frac{b_{-r}n^{r-1}}{z_0^n(r-1)!}$, kjer je

$b_{-r} = \lim_{z\to z_0} f(z)\left(1 - \frac{z}{z_0}\right)^r.$

Primer.

(1) $f(z) = \frac{1}{(1-z)(1-2z)}$
$R = \frac{1}{2}, z_0 = \frac{1}{2}, r = 1$
$\lim_{z\to\frac{1}{2}} \frac{1}{(1-z)(1-2z)}(1-2z) = 2 = b_{-1}$
$a_n \sim \frac{2}{\left(\frac{1}{2}\right)^n} = 2^{n+1}.$

(2) d_n: število premestitev v S_n
$\sum_n \frac{d_n}{n!} z^n = \frac{e^{-z}}{1-z}$
$z_0 = 1, r = 1$
$b_{-1} = \lim_{z\to 1} \frac{e^{-z}}{1-z}(1-z) = e^{-1}$
$\frac{d_n}{n!} \sim \frac{e^{-1}}{1\cdot 1} = \frac{1}{e}$
$d_n \sim \frac{n!}{e}.$
Koliko dober je za približek?
$\frac{e^{-z}}{1-z} - \frac{e^{-1}}{1-z}$ je cela funkcija.
$[z^n]$ (cela funkcija) $< \left(\frac{1}{R}+\epsilon\right)^n = \epsilon^n$ za $n \geq n_0$.
Koeficienti celih funkcij hitro padajo proti 0.
Ker je $z_0 = 1$ edini pol in ker je enostaven, je $\frac{b_{-1}}{z_0^n}$ odličen približek.
$d_n = \left[\frac{n!}{e}\right].$

(3) $\widetilde{B}(n)$: urejena Bellova števila
$\widetilde{B}(n) = \sum_k k!S(n,k)$
$\sum_n \widetilde{B}(n)\frac{z^n}{n!} = \frac{1}{1-(e^z-1)} = \frac{1}{2-e^z}.$
Poli so $\log 2 + 2k\pi i,\ k \in \mathbb{Z}$
$z_0 = \log 2, r = 1$

$b_{-1} = \lim_{z\to\log 2} \frac{1-\frac{z}{\log 2}}{2-e} \stackrel{L'H}{=} \lim_{z\to\log 2} \frac{-\frac{1}{\log 2}}{2} = \frac{1}{2\log 2} = \frac{1}{\log 4}$
$\widetilde{B}(n) \sim \frac{n!}{2(\log 2)^{n+1}}$
$\widetilde{B}(20) = 267\ldots 115$ (23 števk)
$\left[\frac{20!}{2(\log 2)^{21}}\right] = 267\ldots 088$
$\frac{\log 2}{\log 2+2\pi i} \doteq 0.11.$

(4) n hiš.

1. družina se vseli v naključno hišo,

2. družina se vseli v naključno naslednjo hišo,

a_n: pričakovano število zasedenih hiš, $\frac{n}{3} < a_n < \frac{n}{2}$?

$a_0 = 0, a_1 = 1, a_2 = 1, a_3 = \frac{1}{3}\cdot 1 + \frac{2}{3}\cdot 2 = \frac{5}{3}.$

$a_n = \frac{1}{n}\sum_{i=1}^{n}(a_{i-2} + a_{n-i-1} + 1) \quad / \cdot n$

$na_n = n + 2(a_0 + a_1 + \cdots + a_{n-2})$

$F(x) = \sum_n a_n x^n$

$xF'(x) + 2xF(x) + 2F(x) = \frac{x}{(1-x)^2} + \frac{2F(x)}{1-x}$ - linearna DE 1. reda.

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

$z_0 = 1, r = 2$

$b_{-2} = \lim_{z\to 1} \frac{1-e^{-2z}}{2(1-z)^2}(1-z)^2 = \frac{1-e^{-2}}{2\cdot 1!}$

$a_n \sim \left(\frac{1-e^{-2}}{2}\right)^n$

$\frac{1-e^{-2}}{2} \doteq 0.423 \in \left(\frac{1}{3}, \frac{1}{2}\right).$

Kaj pa, če imamo več singularnosti na $|z| = R$?

$z_1 \ldots z_k$ poli redov $r_1 \ldots r_k$

$[z^n]f(z) = \sum_{i=1}^{k} \frac{b_{-r_i} n^{r_i - 1}}{z_i^n (r_i-1)!} + O\left(\left(\frac{1}{R'}\right)^n\right)$, $R' > R$.

Primer.

$r(x) = \frac{1}{1-z} + \frac{1}{1+z} + \frac{1}{1-z^2}$

$a_n = 1 + (-1)^n + \frac{1}{2^n} \not\sim 1 + (-1)^n.$

V praksi štejejo le najvišji poli.

Primer.

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

Racionalna funkcija, poli

1 reda k, -1 reda $\lfloor \frac{k}{2} \rfloor$, $e^{\pm \frac{2\pi i}{3}}$ reda $\lfloor \frac{k}{3} \rfloor \dots$

1 ima najvišji red.

$z_0 = 1, r = k$

$b_{-k} = \lim_{z \to 1} \prod_{i=1}^{k} \frac{1}{1-z^i}(1-z)^k = \lim_{z \to 1} \prod_{i=1}^{k} \frac{1}{1+z+\dots+z^{i-1}} = \frac{1}{k!}$

$\overline{p_k}(n) \sim \frac{n^{k-1}}{k!(k-1)!}$

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

$p_k(n) \sim \frac{n^{k-1}}{k!(k-1)!}$.

(Šibke) kompozicije n s k členi

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

$\binom{n-1}{k-1} \sim \frac{n^{k-1}}{(k-1)!}$

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

Singularnosti so bistvene, množica singularnosti ima stekališča.

Lema 2.11.3.

$\alpha \in \mathbb{R}$.

$\lim_{x \to \infty} \frac{\Gamma(x+\alpha)}{x^\alpha \Gamma(x)} = 1$.

$\Gamma(x) = \int_0^x t^{x-1} e^{-t} dt$

$\Gamma(x+1) = x\Gamma(x)$

$\Gamma(n) = (n-1)!\ n = 1, 2, 3 \dots$

Γ lahko razširimo na $\mathbb{C} \setminus \{0, -1, -2 \dots\}$.

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

$\lim_{x \to \infty} \frac{\Gamma(x+\alpha)}{\sqrt{2\pi x}\left(\frac{x}{e}\right)^x} = 1$.

Dokaz 2.11.4.

$$
\begin{aligned}
\lim_{x \to \infty} \frac{\Gamma(x+\alpha)}{x^\alpha \Gamma(x)} &= \lim_{x \to \infty} \frac{\sqrt{2\pi(x+\alpha-1)}\left(\frac{x-\alpha-1}{e}\right)^{x+\alpha-1}}{x^\alpha \cdot \sqrt{2\pi(x-1)}\left(\frac{x-\alpha}{e}\right)^{x-1}} \\
&= \lim_{x \to \infty} \frac{1}{e^\alpha} \left(\left(1 + \frac{\alpha}{x-1}\right)^{\frac{x-1}{\alpha}} \right)^\alpha \\
&= \frac{e^\alpha}{e^\alpha} \\
&= 1.
\end{aligned}
$$

■

Lema 2.11.5.

$\beta \in \mathbb{R} \setminus \mathbb{N}$.
$\binom{\beta}{n} \sim \frac{(-1)^n}{\Gamma(-\beta) n^{\beta+1}}$.

Dokaz 2.11.6.

$$\begin{aligned} &\lim_{n\to\infty} \frac{\beta(\beta-1)\dots(\beta-n+1)\Gamma(-\beta)}{n!(-1)^n} \\ &= \lim_{n\to\infty} \frac{n^{\beta+1}\Gamma(-\beta+n)}{\Gamma(n+1)} \\ &\overset{\text{lema}}{=} 1; \end{aligned}$$

$x = n - \beta,\ \alpha = \beta + 1$. ■

$z_0 \in \mathbb{R}$
$f(z) = \left(1 - \frac{z}{z_0}\right)^\beta g(z)$
$\beta \in \mathbb{Z} \setminus \mathbb{N}$: pol,
$\beta \notin \mathbb{Z} \setminus \mathbb{N}$: algebraična singularnost.
Tipično: $\beta = \frac{1}{2}$, npr. $f(z) = \sqrt{1-z}$.
g analitična v 0 s polmerom $> |z_0|$.

$$\begin{aligned} f(z) &= \left(1 - \frac{z}{z_0}\right)^\beta \left(b_0 + b_1\left(1 - \frac{z}{z_0}\right) + \dots\right) \\ &= b_0\left(1 - \frac{z}{z_0}\right)^\beta + b_1\left(1 - \frac{z}{z_0}\right)^{\beta+1} + \dots \end{aligned}$$

$[z^n]f(z) = b_0\binom{\beta}{n}\frac{(-1)^n}{z_0^n} + b_1\binom{\beta}{n}\frac{(-1)^n}{z_0^2} + \dots$
$b_0\binom{\beta}{n}\frac{(-1)^n}{z_0^n} \sim b_0 \cdot \frac{1}{\Gamma(-\beta)n^{\beta+1}z_0^n}$,
$b_1\binom{\beta+1}{n}\frac{(-1)^n}{z_0^n} \sim b_0 \cdot \frac{1}{\Gamma(-\beta-1)n^{\beta+2}z_0^n}$.
$\frac{1}{n^{\beta+1}} > \frac{1}{n^{\beta+2}} \to$ majhno.

Izrek 2.11.7.

$f(z) = \left(1 - \frac{z}{z_0}\right)^\beta g(z)$, $z_0 \in \mathbb{R}$, $\beta \in \mathbb{R} \setminus \mathbb{N}$, $g(z_0) \neq 0$, g holomorfna s konvergenčnim polmerom $> |z_0|$. Potem je

$$[z^n]f(z) \sim \frac{g(z_0)}{\Gamma(-\beta)n^{\beta+1}z_0^n}.$$

V posebnem: $b = -r$: $\frac{b_{-r} \cdot n^{r-1}}{\Gamma(r) z_0^n}$.

Primer.

(1) $F(x) = \sum_n C_n x^n$
$F(x) = 1 + xF^2(x)$
$F(x) = \frac{1-\sqrt{1-4x}}{2x}$
$xF(x) = \frac{1}{2} + \frac{1}{2}\sqrt{1-4x}$
$x_0 = \frac{1}{4}, \beta = \frac{1}{2}, g(x) = -\frac{1}{2}$
$C_{n-1} \sim \frac{-\frac{1}{2}}{\Gamma(-\frac{1}{2}) n^{\frac{3}{2}} \left(\frac{1}{4}\right)^n}$
$\Gamma\left(\frac{1}{2}\right) = \sqrt{\pi}$
$\Gamma\left(-\frac{1}{2}\right) = -\frac{1}{2}\Gamma\left(-\frac{1}{2}\right)$
$\Gamma\left(-\frac{1}{2}\right) = -2\sqrt{\pi}$
$C_{n-1} \sim \frac{-\frac{1}{2}4^n}{-2\sqrt{\pi} n^{\frac{3}{2}}} = \frac{4^{n-1}}{\sqrt{\pi} n^{\frac{3}{2}}}$.
D.N. Dokažite to formulo iz $C_n = \frac{1}{n+1}\binom{2n}{n}$ in Stirlingovo formulo.

(2) $M(k) = \sum_n M_n x^n$
$M(x) = 1 + xM(x) + x^2 M^2(x)$
$x^2 M^2 + (x-1)M + 1 = 0$
$M(x) = \frac{1-x-\sqrt{1-2x-3x^2}}{2x^2}$
$x^2 M = \frac{1-x}{2} - \frac{1}{2}\sqrt{(1-3x)(1+x)}$
$x_0 = \frac{1}{3}, \beta = \frac{1}{2}, g(x) = -\frac{1}{2}\sqrt{1+x}$
$M_{n-2} \sim \frac{-\frac{1}{2} \cdot \sqrt{\frac{4}{3}}}{-2\sqrt{\pi} n^{\frac{3}{2}} \left(\frac{1}{3}\right)^n}$
$M_n \sim \frac{3^{\frac{3}{2}} \cdot 3^n}{2\sqrt{\pi} n^{\frac{3}{2}}}$.

Kaj pa, če je $f(n)$ cela?

Izrek 2.11.8 (Haymanova metoda)**.** Naj bo $f(z)$ dopustna funkcija (brez definicije), npr. $f(z) = e^{P(z)}$, P polinom, $[z^n]f(z) > 0$ od nekega n naprej (npr. e^z, $e^{z+\frac{z^2}{2}}$, ne pa e^{z^2}).

$$\beta(z) := \frac{zf'(z)}{f(z)}.$$

Potem ima enačba $\beta(z) = n$ natanko eno pozitivno rešitev z_n.

$$[z^n]f(z) \sim \frac{f(z_n)}{z_0^n \sqrt{2\pi z_n} \beta'(z_n)}.$$

Primer.

(1) $f(z) = e^z$
$\beta(z) = \frac{ze^z}{e^z} = z$
$z_n = n$
$[z^n]f(z) \sim \frac{e^n}{n^n\sqrt{2\pi n}}$ - Stirlingova formula.

(2) $f(z) = e^{z+\frac{z^2}{2}}$
$\beta(z) = \frac{z \cdot e^{z+\frac{z^2}{2}}(1+z)}{e^{z+\frac{z^2}{2}}} = z^2 + z$
$z^2 + z + n = 0$
$z_n = \frac{-1+\sqrt{1+4n}}{2}$
$\frac{i_n}{n!} \sim \frac{e^{\left(\frac{-1+\sqrt{1+4n}}{2}\right)^2 + \frac{-1+\sqrt{1+4n}}{2}}}{\left(\frac{-1+\sqrt{1+4n}}{2}\right)^n \sqrt{2\pi \frac{-1+\sqrt{1+4n}}{2}} \sqrt{1+4n}} \sim \dots$

Poglavje 3

Incidenčne algebre in Möbiusova inverzija

3.1 Motivacija

$f, g : \mathbb{N} \to \mathbb{R}$
$g(n) = f(0) + f(1) + \cdots + f(n)$ $n \in \mathbb{N}$
$f(n) = g(n) - g(n-1)$
$(g(x) = \int_0^x f(t)dt,\ g'(x) = f(x))$.
$f, g : \mathbb{N} \setminus \{0\} \to \mathbb{R}$
$g(n) = \sum_{d|n} f(d)$
$f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d)$ klasična Möbiusova inverzija, μ klasična Möbiusova funkcija, $\mu(n) \in \{-1, 0, 1\}$.
$f, g : 2^{[n]} \to \mathbb{R}$
$g(T) = \sum_{S \subseteq T} f(S)$
$f(T) = \sum_{S \subseteq T} (-1)^{|T \setminus S|} g(S)$ - NVI.

3.2 Delno urejene množice

$(P, \leq)$ je delno urejena množica (dum) (angl. partially ordered set oz. poset);
refleksivnost: $x \leq x$, ansitimetričnost: $x \leq y, y \leq x \implies x = y$, tranzitivnost: $x \leq y, y \leq z \implies x \leq z$.

Primer.

(1) $([n], \leq) = \underline{n} = \mathbf{n}$
$(\mathbb{N}, \leq)$.

(2) $(D_n, |) = D_n$ delitelji n
$(\mathbb{N} \setminus \{0\}, |) = D$.

(3) $(2^{[n]}, \subseteq) = B_n$ Boolova algebra.

(4) $(\{\text{razdelitve } [n]\}, \leq)$
$\leq$: biti finejša $\pi \leq \sigma$: vsak blok v π je vsebovan v bloku v σ
$14 - 2 - 378 - 56 \leq 12456 - 378$.

(5) $(\text{podprostori } \mathbb{F}_q^n, \subseteq) = L_n(q)$.

$x \geq y \leftrightarrow y \leq x$
$x < y \leftrightarrow x \leq y, x \neq y$
$x < \cdot y \leftrightarrow x < y, \nexists z : x < z < y$
x predhodnik y, y predhodnik x
$(\mathbb{N}, \leq)$: $i < \cdot i + 1$
$B_n : A \subset \cdot A \cup \{i\}; i \notin A$
$D : r \mid \cdot s \leftrightarrow \frac{s}{r}$ praštevilo
$L_n(q) : U < \cdot V \leftrightarrow U \subseteq V, \dim V - \dim U = 1$
$\mathbb{R}$: nikoli ne velja $x < \cdot y$.
Hassejev diagram:
graf,
$V = P$,

$xy \in E \iff x < \cdot y$ ali $y < \cdot x$

$x < \cdot y \implies x$ pod y.

Hassejev diagram B_n je hiperkocka.

x maksimalen element, če velja $y \geq x \implies y = x$ (oz $\nexists y : y > x$)

x minimalen element, če velja $y \leq x \implies y = x$ (oz $\nexists y : y < x$).

P končna dum $\implies P$ ima maksimalen element.

x največji element: $y \leq x \; \forall y \in P$.

Nima največjega elementa.

x, y največja $\implies x \leq y, y \leq x \implies x = y$.

$\hat{0}$: najmanjši element (če $\exists$),

$\hat{1}$: največji element (če $\exists$).

P, Q dum.

$\varphi : P \to Q$ homomorfizem, če $x \leq_P y \implies \varphi(x) \leq_Q \varphi(y)$.

$\varphi : P \to Q$ izomomorfizem, če je bijektiven homomorfizem in je inverz tudi homomorfizem, oz. φ bijekcija, $x \leq_P y \iff \varphi(x) \leq_Q \varphi(y)$.

Bijektivni homomorfizem, ni izomorfizem.

$P \cong Q$ (P,Q izomorfna), če obstaja izomorfizem $\varphi : P \to Q$.

$B_3 \cong D_{30}$.

P, Q dum.

$P \times Q$ (množica $P \times Q$), $(x,y) \leq (x^{'},y^{'})$, če $x \leq_P x^{'}, y \leq_Q y^{v}, x, x^{'} \in P, y, y^{'} \in Q$ - kartezični produkt.

$P \sqcup Q = P \times \{0\} \cup Q \times \{1\}$.

$P + Q$ (množica $P \sqcup Q$), $x \leq y$ če $(x,y \in P, x \leq_P y)$ ali $(x,y \in Q, x \leq_Q y)$ - disjunktna unija.

$P \oplus Q$ (množica $P \sqcup Q$), $x \leq y$ če $(x,y \in P, x \leq_P y)$ ali $(x,y \in Q, x \leq_Q y)$ ali $(x \in P, y \in Q)$ - disjunktna vsota.

$\underline{1} \oplus \cdots \oplus \underline{1} \cong \underline{n}$

$\underline{2} \times \cdots \times \underline{2} \cong B_n$

$\varphi : \underline{2}^n \to B_n$

$\varphi(\epsilon_1 \ldots \epsilon_n) = \{i : \epsilon_i = 2\}$

$D_n \cong \underline{[0, \alpha_1]} \times \cdots \times \underline{[0, \alpha_k]}$

$n = p_1^{\alpha_1} \dots p_k^{\alpha_k},\ \alpha_i \geq 1$, delitelji $p_1^{\beta_1} \dots p_k^{\beta_k}, 0 \leq \beta_i \leq \alpha_i$.

Če je n produkt k različnih praštevil, je $D_n \cong B_k$.

Veriga je podmnožica P, če sta poljubna elementa primerljiva ($x \leq y$ ali $y \leq x$).

V $B_8 :\ \{\emptyset, \{1,5\}, \{1,2,5,7,8\}\}$,

v $D_12 :\ \{2,6,12\}$.

$x_0 < x_1 < \cdots < x_k$ veriga dolžine k,

$x_0 \leq x_1 \leq \cdots < x_k$ multiveriga dolžine k.

Antiveriga je podmnožica P, v kateri nobena različna elementa nista primerljiva.

$\binom{[n]}{k}$ antiveriga v B_n,

P antiveriga v D.

Stopničasta dum (angl. graded) je P z rangom, t.j.

$\rho : P \to \mathbb{N}$, če

$x < y \implies \rho(x) < \rho(y)$

$x <\cdot y \implies \rho(y) = \rho(x) + 1$.

V $\mathbb{N} :\ \rho = id$,

v $B_n :\ \rho(A) = |A|$,

v $D_n :\ \rho\left(p_1^{\alpha_1} \dots p_k^{\alpha_k}\right) = \alpha_1 + \cdots + \alpha_k$,

ni stopničasta.

Definicija 3.2.1. P je lokalno končna, če je za

$\forall x \leq y :\ [x,y] := \{z : x \leq z \leq y\}$ končna.

Npr. vsaka končna dum je lokalno končna.

$\mathbb{N}, D$ sta lokalno končni.

3.3 Incidenčna algebra

P lokalno končna dum.

$Int(P) := \{[x,y] : x \leq y\}$

$I(P,K) := \{f :\ Int(P) \to K\}$ incidenčna algebra.

$x \leq y: \ f([x,y]) = f(x,y)$ (krajšamo).
$(f+g)(x,y) = f(x,y) + g(x,y)$
$(\lambda f)(x,y) = \lambda \cdot f(x,y)$
$(f \cdot g)(x,y) = \sum_{x \leq z \leq y} f(x,z) \cdot g(z,y)$ - pomembno!

$$\begin{aligned}
(f \cdot g) \cdot h(x,y) &= \sum_{x \leq z \leq y} (f \cdot g)(x,z) \cdot h(z,y) \\
&= \sum_{x \leq z \leq y} \left(\sum_{x \leq q \leq z} f(x,w) g(w,z) \right) h(z,y) \\
&= \sum_{x \leq w \leq z \leq y} f(f,w) g(q,z) h(z,y) \\
&= \cdots = f \cdot (g \cdot h)(x,y).
\end{aligned}$$

(Nekomutativna algebra.)
$P = \underline{n}$.
$I(\underline{n}, k) \cong$ algebra zgornje trikotnih matrik nad K.
$f(i,j) \to [f(i,j)$ če $i \leq j, 0$ sicer$]_{i,j=1}^{n}$
$1 \leq i \leq j \leq n$
$(A \cdot B)_{ij} = \sum_{k=1}^{n} A_{ik} B_{kj} = \sum_{k=i}^{j} A_{ik} B_{kj}$
$\underline{1}(x,y) = \delta_{xy} = \begin{cases} 1 : x = y \\ 0 : x < y \end{cases}$ enota za množenje.
$f : \underline{1}(x,y) = \sum_{x \leq z \leq y} f(x,y) \cdot 1(z,y) = f(x,y)$, ker $\underline{1}(z,y) = 0$, razen za $z = y$.
$\underline{1} \cdot f = f$.

Trditev 3.3.1. $f \in I(\underline{n}, K)$ je obrnljiv $\iff$ $f(x,x) \neq 0$ za $\forall x \in P$.

Dokaz 3.3.2.
$(\Rightarrow)$:

$$\begin{aligned}
&f \cdot g = \underline{1} \\
&(f \cdot g)(x,x) = \sum_{x \leq z \leq x} f(x,z) g(z,x) = f(x,y) \cdot g(x,y) \\
&= \underline{1}(x,x) = 1 \\
&\implies f(x,x) \neq 0.
\end{aligned}$$

($\Leftarrow$):

$$\begin{aligned}
&\exists \text{ desni inverz:}\\
&f \cdot g = \underline{1}\\
&(f \cdot g)(x,x) = 1 = f(x,x) \cdot g(x,x)\\
&g(x,x) = \frac{1}{f(x,x)}.
\end{aligned}$$

Skonstruiramo rekurzivno glede na $|[x,y]|$:

$$\begin{aligned}
&|[x,y]| = 1 : \checkmark\\
&\text{Imamo } g(x^{'},y^{'}) \text{ za } |[x^{'},y^{'}]| < |[x,y]|\\
&g(x,y) = \frac{\sum \dots}{f(x,x)}.
\end{aligned}$$

Podobno za levi inverz, enaka. ■

$\zeta(x,y) = 1$ za $x \leq y$
$\zeta^2(x,y) = \sum_{x \leq z \leq y} \zeta(x,z)\zeta(z,y) = |[x,y]|$
$\zeta^3(x,y) = \sum_{x \leq w \leq z \leq y} \zeta(x,w)\zeta(w,z)\zeta(z,y) =$ število multiverig dolžine 3 med x in y
$\zeta^k(x,y) =$ število multiverig dolžine k med x in y.
$(\zeta - 1)(x,y) = \begin{cases} 1 : x < y \\ 0 : x = y \end{cases}$
$(\zeta - 1)^2 = |(x,y)|$ - dolžina odprtega intervala.
$(\zeta - 1)^k =$ število verig dolžine k med x in y $= 0$ od nekega k naprej.
$\underline{1} + (\zeta - 1) + (\zeta - 1)^2 + \dots$ je dobro definirana (končnost).
$(1 + (\zeta - 1) + \dots)(x,y) =$ število verig med x in y.
$(1 + (\zeta - 1) + \dots)(1 - (\zeta - 1)) = 1$
$(2 - \zeta)^{-1}(x,y) =$ število verig med x in y.

$$\begin{bmatrix} 1 & 1 & \dots & 1 \\ 0 & 1 & \dots & \\ \vdots & & \vdots & \\ & & & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & 1 & 2 & 4 & \dots & 2^{n-1} \\ & & \vdots & & & \vdots \\ & & & & & 2 \\ & & & & & 1 \\ & & & & & 1 \end{bmatrix}.$$

Število verig med i in j je 2^{j-i-1} za $j \geq i+1$.

3.4 Möbius funkcija in Möbiusova inverzija

$\mu := \zeta^{-1}$: inverz obstaja, ker je $\zeta(x,x) \neq 0$.

$\underline{4}$

$\zeta \cdot \mu = \underline{1}$

$x = y : \zeta(x,x) \cdot \mu(x,x) = 1 \implies \mu(x,x) = 1$

$x < y : \sum_{x \leq z \leq y} \zeta(x,z) \cdot \mu(z,y) = 0$

$\mu(x,y) = -\sum_{x < z \leq y} \mu(z,y)$

$\mu \cdot \zeta = \underline{1}$

$\sum_{x \leq z \leq y} \mu(x,z) = 0$

$\mu(x,y) = -\sum_{x \leq z < y} \mu(x,z)$

$\underline{4}$:

$\mu(i,i) = 1$

$\mu(i,i+1) = -\mu(i,i) = -1$

$\mu(i,i+2) = -\mu(i,i) - \mu(i,i+1) = 0$

$\mu(i,i+3) = -\mu(i,i) - \mu(i,i+1) - \mu(i,i+2) = 0$

v $\underline{n}$ in $(\mathbb{N}, \leq)$: $\mu(x,y) = \begin{cases} 1 : i = j \\ -1 : j = i+1 \\ 0 : j - i \geq 2 \end{cases}$

$\mu(a,a) = \mu(b,b) = \cdots = 1$

$\mu(a,b) = \mu(b,c) = \mu(c,e) = \mu(a,d) = \mu(d,e) = -1$

$\mu(a,b) = \mu(b,e) = 0$

$\mu(a,e) = 1.$

Izrek 3.4.1 (Möbiusova inverzija)**.** P dum, za $\forall x \in P$ $\{z \in P : \ z \leq x\}$ je končna ($\implies$ P je lokalno končna.)
$f, g : P \to K$

$$g(y) = \sum_{x \leq y} f(x) \iff f(y) = \sum_{x \leq y} \mu(x, y) g(x).$$

(Dobro definirano, ker je vsota končna.)

Dokaz 3.4.2.
($\Rightarrow$):

$$\begin{aligned}\sum_{x \leq y} \mu(x, y) g(x) &= \sum_{x \leq y} \mu(x, y) \sum_{z \leq x} f(z) \\ &= \sum_{z \leq y} \sum_{z \leq x \leq y} \mu(x, y) f(z) = f(y); \\ \text{ker} &\sum_{z \leq x \leq y} \mu(x, y) = \delta_{z,y}.\end{aligned}$$

($\Leftarrow$): podobno. ■

Primer.
$P = \underline{n}$
$g(j) = \sum_{i \leq j} f(i) \iff f(j) = \sum_{i=1}^{j} \mu(i,j) g(i) = g(j) - g(j-1)$ za $j \geq 2$, $f(1) = g(1)$.

Kako izračunati μ za $B_n, D_n, M_n, L_n(q)$?

Trditev 3.4.3.
P, Q lokalno končni $\implies$ $P \times Q$ lokalno končen.

$\mu_{P \times Q}\Big((x,y), (x', y')\Big) = \mu_P(x,y) \cdot \mu_Q(x', y').$

Dokaz 3.4.4.

$$
\begin{aligned}
&(\mu_{P\times Q}(\mu_P,\mu_Q))\Big((x,y),(x',y')\Big)\\
=&\sum_{(x,y)\le(x'',y'')\le(x',y')}\mu_P(x'',x')\mu_Q(y'',y')\\
=&\sum_{x\le x''\le x'}\sum_{y\le y''\le y'}\mu_P(x'',x')\cdot\mu_Q(y'',y')\\
&=\left(\sum_{x\le x''\le x'}\mu_P(x'',x')\right)\cdot\left(\sum_{y\le y''\le y'}\mu_P(y'',y')\right)\\
&=\delta_{x,x'}\cdot\delta_{y,y'}\\
&=\delta_{(x,y),(x',y')}.
\end{aligned}
$$

■

Primer.

(1) $B_n = \underline{2}\times\cdots\times\underline{2}$
$\mu(S,T)=\mu((\epsilon_1\ldots\epsilon_n),(\varphi_1\ldots\varphi_n))=\mu_{\underline{2}}(\epsilon_1,\varphi_1)\ldots\mu_{\underline{2}}(\epsilon_n,\varphi_n)=(-1)^{|T\setminus S|}$
$S\subseteq T$
$f,g:2^{[n]}\to K$
$g(T)=\sum_{S\subseteq T}f(S) \iff f(T)=\sum_{S\subseteq T}(-1)^{|T\setminus S|}g(S)$: NVI.

(2) $D_n=\underline{[0,\alpha_1]}\times\cdots\times\underline{[0,\alpha_k]}$
$n=p_1^{\alpha_1}\ldots p_k^{\alpha_k}$

$$
\begin{aligned}
\mu(r,s)&=\mu((\beta_1\ldots\beta_k),(\gamma_1\ldots\gamma_k))\\
&=\mu(\beta_1,\gamma_1)\ldots\mu(\beta_k,\gamma_k)\\
&=\begin{cases}(-1)^l: \frac{s}{r}\text{produkt } l \text{ različnih praštevil}\\ 0: p^2\mid\frac{s}{r},\ p \text{ praštevilo}\end{cases}\\
&=\mu\left(\frac{s}{r}\right)
\end{aligned}
$$

$r=p_1^{\beta_1}\ldots p_k^{\beta_k}$
$s=p_1^{\gamma_1}\ldots p_k^{\gamma_k}$
$0\le\beta_i\le\gamma_i\le\alpha_i$

$r = p_1^{\gamma_1-\beta_1} \cdots p_k^{\gamma_k-\beta_k}$

$\mu(n) = \begin{cases} (-1)^k : \ n \text{ produkt } k \text{ različnih praštevil} \\ 0 : \ p^2 \mid n \text{ praštevilo} \end{cases}$

$f, g : \mathbb{N} \setminus \{0\} \to K$

$g(n) = \sum_{d|n} f(d) \iff f(n) = \sum_{d|n} \mu(d,n) g(d) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d).$

P

$I(P,K) = \{f : Int(P) \to K\}$

$f \cdot g(x,y) = \sum_{x \le z \le y} f(x,z) g(z,y)$

$\zeta, \mu.$

Izrek 3.4.5.

P dum, $\{y \le x\}$ končen $\forall x \in P$,

$f, g : P \to K.$

$f(x) = \sum_{y \le x} g(y) \iff g(x) = \sum_{y \le x} \mu(y,x) f(y).$

Izrek 3.4.6.

P dum, $\{y \ge x\}$ končen $\forall x \in P$,

$f, g : P \to K.$

$f(x) = \sum_{y \ge x} g(y) \iff g(x) = \sum_{y \ge x} \mu(x,y) f(y).$

$B_n : \mu(S,T) = (-1)^{|T \setminus S|}$

$B_n \cong \underline{2} \times \cdots \times \underline{2}$

$\mu_{P \times Q} = \mu_P \cdot \mu_Q$

$D_n : \mu(r,s) = \begin{cases} (-1)^k : \ \frac{s}{r} \text{ produkt } k \text{ različnih praštevil} \\ 0 : \ p^2 | \frac{s}{r} \end{cases}.$

3.5 Mreže

Definicija 3.5.1.

$x \le y$:

y zgornja meja za x,

x spodnja meja za y.

P je mreža (angl. lattice?), če imata poljubna elementa najmanjšo zgornjo mejo in največjo spodnjo mejo.

$x \vee y$ spoj (angl, join),
$x \wedge y$ stik (angl. meet).
$x \wedge y \leq x, y \leq x \vee y$
$x, y \leq z \implies x \vee y \leq z$
$z \leq x, y \implies z \leq x \wedge y$.

Primer.

- 3 zgornje meje za x, y, noben ni $\leq$ od ostalih,
  ni mreža.
- $\underline{n}, \mathbb{N}$: $i \vee j = \max\{i, j\},\ i \wedge j = \min\{i, j\}$.
- $B_n : T \vee S = T \cup S,\ T \wedge S = T \cap S$.
- $D_n, D : r \vee s = l(r, s),\ r \wedge s = D(r, s)$.
- $L_n(q) : U \vee V = U + V,\ U \wedge V = U \cap V$.
- Π_n
  $\pi = 135 - 246, \sigma = 123 - 46 - 5$
  $\pi \wedge \sigma = \{$neprazni preseki bloka π in bloka $\sigma\}$
  $\pi \vee \sigma = \{$povezane konponente grafa, $V = [n], i \sim j$: i in j v istem bloku π ali $\sigma\}$
  $\pi \vee \sigma = 123456$.

P končna mreža $\implies$ ima največji in najmanjši element.
Največji: spoj vseh elementov $= \hat{1}$,
najmanjši: stik vseh elementov $= \hat{0}$.
$\forall x < y$:
$\sum_{x \leq z \leq y} \mu(x, z) = 0 \implies \mu(x, y) = -\sum_{x \leq z < y} \mu(x, z)$ ali
$\sum_{x \leq z \leq y} \mu(z, y) = 0 \implies \mu(x, y) = -\sum_{x < z \leq y} \mu(z, y)$.

Izrek 3.5.2.
P končna mreža,

$a \neq \hat{1}$.
$\mu(\hat{0}, \hat{1}) = -\sum_{x \neq \hat{0}, x \wedge a = \hat{0}} \mu(x, \hat{1})$.

Opomba. Vedno: $\mu(\hat{0}, \hat{1}) = -\sum_{x \neq \hat{0}} \mu(x, \hat{1})$.
Torej izrek nam omogoča, da $\mu(\hat{0}, \hat{1})$ izračunamo preko vsote z manj členi.

Tipično $a < \cdot \hat{1}$.

Dokaz 3.5.3.

$$\begin{aligned}
\sum_{x \wedge a = \hat{0}} \mu(x, \hat{1}) &= \sum_{x \in P} \mu(x, \hat{1}) \cdot 1(\hat{0}, x \wedge a) \\
&= \sum_{x \in P} \mu(x, \hat{1}) \sum_{y \leq x \wedge a} \mu(\hat{0}, y) \\
&\overset{(*)}{=} \sum_{x \in P} \mu(x, \hat{1}) \sum_{y \leq x, y \leq a} \mu(\hat{0}, y) \\
&= \sum_{y \leq a} \left(\sum_{x \geq y} \mu(x, \hat{1}) \right) \mu(\hat{0}, y) = 0;
\end{aligned}$$

ker $\sum_{x \geq y} \mu(x, \hat{1}) = 1(y, \hat{1}) = 0$, ker $y \leq a \neq \hat{1}$, oz. $y < \hat{1}$
(*): $y \leq x \wedge a \implies y \leq x \wedge y \leq a$. ■

Primer.

(a) B_n
$\mu_n = \mu(0, [n])$
$[S, T] \cong B_{|T \setminus S|}$
$[\{n\}, [n]] \cong B_{n-1}$
$A = [n-1]$
$\mu_n = \sum_{T \neq \emptyset, T \cap [n-1] = \hat{0}} \mu(T, [n]) = -\mu(\{n\}, [n]) = -\mu_{n-1}$
$\implies \mu_n = (-1)^n$
$\mu(S, T) = (-1)^{|T \setminus S|}$.

(b) D_n
$n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$
$a = p_1^{\alpha_1 - 1} \dots p_k^{\alpha_k}$

$\mu(1,n) = -\sum_{d|n, d\neq 1, D(d,a)=1} \mu(d,n)$
$= \begin{cases} 0: \ \alpha_1 \geq 2 \text{ (takega } d \text{ ni)} \\ -\mu(p_1,n): \ \alpha_1 = 1 \ (d = p_1) \end{cases}$
$-\mu(p_1,n) = -\mu(1, p_2^{\alpha_2} \dots p_n^{\alpha_n})$:
rekurzivno, $= 0$ če $\alpha_i \geq 2$, $(-1)^k$ sicer.

(c) $L_n(q)$
$\mu_n = \mu(0, \mathbb{F}_q^n)$
$[U,V] \cong L_{\dim V - \dim U}(q)$
$A = \Pi_q^{n-1} \times \{0\}$
$\mu_n = -\sum_{U\neq 0, U\cap A = 0} \mu(U, \Pi_q^n) = -q^{n-1}\mu_{n-1}$.
Linearna algebra: $\dim(U \cap A) + \dim(U + A) = \dim(U) + \dim(A)$:
$\dim(A) = n-1, \dim(U\cap A) = 0, \dim(U) \geq 1, \dim(U+A) \geq 0$
$n \geq \dim(U \cap A), \dim(U) + \dim(A) \geq n$
$\implies \dim(U) = 1, U = Lin\{u\}$; zadnja komponenta $\neq 0$, BŠS 1.
q^{n-1}: q možnosti za vsako od $n-1$ preostalih komponent.
$\mu_n = (-1)^n q^{\binom{n}{2}}$
$\mu(U,V) = (-1)^{\dim V - \dim U} q^{\binom{\dim V - \dim U}{2}}$.

(d) Π_n
$\mu := \mu(1-2-3\cdots-n, 123\dots n)$
$\alpha = 12\dots(n-1)-n$
$\mu_n = -\sum_{\pi\neq 1-2\dots n, \pi\wedge\alpha = 1-2\cdots-n} \mu(\pi, 12\dots n) = -(n-1)\mu_{n-1}$
$\pi = 1-2-\cdots-(i-1)-(in)-(i+1)-\cdots-(n-1)$
$[\pi, 12\dots n] \cong \Pi_{n-1}$
$\mu_n = (-1)^{n-1}(n-1)!$ (do μ_1, ne μ_0)
$[\pi,\sigma] \cong \pi_{\alpha_1} \times \cdots \times \pi_{\alpha_k}$,
kjer i-ti blok σ razpade na a_i blokov v π za $i = 1, 2\dots k$.
$\pi = 12-3-4-568-7$
$\sigma = 1247-56-8-3$
$a_1 = 3, a_2 = 2, a_1 = 1$
$\Pi_3 \times \Pi_2 \times \Pi_1$

$$\mu(\pi,\sigma) = (-1)^{a_1}(a_1-1)! \cdot (-1)^{a_2}(a_2-1)! \cdot (-1)^{a_3}(a_3-1)!.$$

3.6 Reducirane incidenčne algebre in Dirichletove rodovne funkcije

Primer.

- $\underline{n}, \mathbb{N}$
  $$\mu(i,j) = \begin{cases} 1: \ i=j \\ -1: \ j=i+1 \\ 0: \ j-i>1 \end{cases} \quad \text{- odvisen od } j-i.$$
- $B_n, B = \cup_{n=0}^{\infty} B_n = \{\text{končne podmnožice } \{1,2,3\dots\}\}$
  $\mu(S,T) = (-1)^{|T\setminus S|}$ - odvisen od $|T \setminus S|$.
- $L_n(q), L_q = \cup_{n=0}^{\infty} L_n(q)$ (dodamo $\times\{0\}^i$ na konec?)
  $\mu(U,T) = (-1)^{\dim V - \dim U}\dots$ - odvisen od $\dim V - \dim U$.
- D_n, D
  $\mu(r,s)$ - odvisen od $\frac{s}{r}$.

Vedno: $\mu(x,y) = \mu(x^{'},y^{'})$, če je $[x,y] \cong [x^{'},y^{'}]$.
(Primer zgoraj za $\mathbb{N}, B, L(q)$.)
V D: $[1,14] \cong [1,15] \cong B_2$, vendar $\frac{14}{1} \neq \frac{15}{1}$.

Izrek 3.6.1.
P lokalno končna dum.
$I_{\cong}(P,K) = \{f: \ Int(P) \to K: \ [x{,}y] \cong [x^{'},y^{'}] \implies f(x{,}y) = f(x^{'}{,}y^{'})\}$.
(npr. za $P = \underline{n}$ zgornje trikotne matrike, ki so konstantne na diagonali(ah?))
$(1, \ \mu, \zeta)$.
Potem velja $f,g \in I_{\cong}(P,I), \lambda \in K \implies f+g, \lambda \cdot f, f \cdot g \in I_{\cong}(P,K)$,
$f \in I_{\cong}(P,K)$ obrnljiv $\implies \ f^{-1} \in I_{\cong}(P,K)$,
$I_{\cong}(P,K)$ reducirana incidenčna algebra.

Dokaz 3.6.2.
$[x,y] \cong [x^{'},y^{'}]$
$(f+g)(x,y) = f(x,y) + g(x,y) = f(x^{'},y^{'}) + g(x^{'},y^{'}) = (f+g)(x^{'},y^{'})$,
$\lambda \cdot f$: podobno.
$(f \cdot g)(x,y) = \sum_{x \leq z \leq y} f(x,z) \cdot g(z,y)$
$(f \cdot g)(x^{'},y^{'}) = \sum_{x^{'} \leq z^{'} \leq y^{'}} f(x^{'},z^{'}) \cdot g(z^{'},y^{'})$
$\phi : [x,y] \to [x^{'},y^{'}]$ izomorfizem
$[\phi(z),\phi(w)] \cong [z,w]$
$f(x,z) = f(x^{'},z^{'}), g(z,y) = g(z^{'},y^{'})$
$f^{-1}(x,y) = f^{-1}(x^{'},y^{'})$ z indukcijo po $|[x,y]|$.
$|[x,y]| = 1$

$$x = x^{'}, y = y^{'}$$
$$f^{-1}(x,y) = \frac{1}{f(x,y)} = \frac{1}{f(x^{'},y^{'})} = f^{-1}(x^{'},y^{'})$$

$|[x,y]| > 1$

$$\sum_{x \leq z \leq y} f(x,z) f^{-1}(z,y) = \sum_{x < z \leq y} f(x,z) f^{-1}(z,y) + f(x,x) f^{-1}(x,y) = 0$$
$$\sum_{x^{'} \leq z^{'} \leq y^{'}} f(x^{'},z^{'}) f^{-1}(z^{'},y^{'}) = \sum_{x^{'} < z^{'} \leq y^{'}} f(x^{'},z^{'}) f^{-1}(z^{'},y^{'}) + f(x^{'},x^{'}) f^{-1}(x^{'},y^{'}) = 0;$$

$f(x,z) = f(x^{'},z^{'})$,
$f(x,x) = f(x^{'},x^{'})$,
$f^{-1}(z,y) \overset{IP}{=} f^{-1}(z^{'},y^{'})$
$\implies \quad f^{-1}(x,y) = f^{-1}(x^{'},y^{'})$. ■

$\tau = \{$množica ekvivalenčnih razredov za $\cong\}$: množica tipov.
$\mathbb{N} : \tau \equiv \mathbb{N}$
$B : \tau \equiv \mathbb{N}$
$L(q) : \tau \equiv \mathbb{N}$
$[x,y]$ tipa α.
$f,g \in I_{\cong}(P,K), f \cdot g(x,y) = \sum_{x \leq z \leq y} f(x,z) g(z,y)$
$(f \cdot g)(\alpha) = \sum_{\beta,\gamma} \binom{\alpha}{\beta,\gamma} f(\beta) g(\gamma)$

$(f \cdot g)$ odvisen samo od tipa.
$\binom{\alpha}{\beta,\gamma}$:= število elementov $z \in [x,y]$; $[x,y]$ tipa α, da je $[x,z]$ tipa β, $[z,y]$ tipa γ.
Torej: $I_{\cong}(P,K)$ je izomorfna algebri preslikav $\tau \to K$ s produktom
$(f \cdot g)(\alpha) = \sum_{\beta,\gamma} \binom{\alpha}{\beta,\gamma} f(\beta)g(\gamma)$.
$\mathbb{N}$

$$\binom{n}{i,j} = \begin{cases} 1: & i+j=n \\ 0: & \text{sicer} \end{cases}$$

$$f \cdot g(n) = \sum_{k=0}^{n} f(k)g(n-k)$$

$$I_{\cong}(\mathbb{N},K) \cong K[[x]]$$

$$f \to \sum_n f(n)x^n$$

B

$$\binom{n}{i,j} = \begin{cases} \binom{n}{i}: & i+j=n \\ 0: & \text{sicer} \end{cases}$$

$$f \cdot g(n) = \sum_{k=0}^{n} \binom{n}{k} f(k)g(n-k)$$

$$I_{\cong}(B,K) \cong K[[x]]$$

$$f \to \sum_n \frac{f(n)}{n!} x^n$$

L_q

$$\binom{n}{i,j} = \begin{cases} \binom{n}{i}_q: & i+j=n \\ 0: & \text{sicer} \end{cases}$$

$$f \cdot g(n) = \sum_{k=0}^{n} \binom{n}{k}_q f(k)g(n-k)$$

$$I_{\cong}(L(q),K) \cong K[[x]]$$

$$f \to \sum_n \frac{f(n)}{\underline{n!}} x^n$$

$\mathbb{N}$

$$\zeta \to \frac{1}{1-x}$$

$\mu \to \left(\frac{1}{1-x}\right)^{-1} = 1-x$, torej $\mu(0) = 1, \mu(1) = -1, \mu(2) = \mu(3) = \cdots = 0$

$\zeta^k \to \left(\frac{1}{1-x}\right)^k = \sum_n \binom{n+k-1}{k-1} x^n$

$\zeta^k(n)$: število multiverig dolžine k med 0 in n

$0 \leq i_1 \leq \cdots \leq i_{k-1} \leq n$.

Kombinacije s ponavljanjem: $\binom{(n+1)+(k-1)-1}{k-1} = \binom{n+k-1}{k-1}$

$(\zeta - 1)^k \to \left(\frac{x}{1-x}\right)^k = \sum_k \binom{n-1}{k-1} x^n$

$0 < i_1 < \cdots < i_{k-1} < n$

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

$(2-\zeta)^{-1} \to \left(2 - \frac{1}{1-x}\right)^{-1} = \left(\frac{2-2x-1}{1-x}\right)^{-1} = \frac{1-x}{1-2x} = 1 + \sum_{n=1}^{\infty} 2^{n-1} x^n$

$(2-\zeta)^{-1}(n)$: število vseh verig med 0 in n:

$0 < i_1 < \cdots < i_{k-1} < n$

2^{n-1}, $n \geq 1$: izberem ali ne.

B

$\zeta \to e^x$

$\mu \to e^{-x}$, torej $\mu(n) = (-1)^n$

$\zeta^k \to e^{kx} = \sum_n \frac{k^n}{n!} x^n$

$\zeta^k(n)$: število multiverig $\emptyset \subseteq A_1 \subseteq \cdots \subseteq A_{k-1} \subseteq [n]$.

Za $\forall j = 1, 2 \ldots n$ izberemo A_i, v katerem se j prvič pojavi; k izbir, n-krat izbiramo $\to k^n$

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

$(\zeta - 1)^k(n)$: število verig $\emptyset \subseteq A_1 \subset \cdots \subset A_{k-1} \subseteq [n]$

$(A_1, A_2 \setminus A_1, A_3 \setminus A_2 \ldots)$ urejena razdelitev na k blokov.

Spomnimo se: $\mu(r,s) = \mu(r^{'},s^{'})$, če je $\frac{s}{r} = \frac{s^{'}}{r^{'}}$.
$[r,s] \sim [r^{'},s^{'}]$, če je $\frac{s}{r} = \frac{s^{'}}{r^{'}}$.
$I_{\sim}(D,K) = \{f : Int(D) \to K : \; [r,s] \sim [r^{'},s^{'}] \implies f(r,s) = f(r^{'},s^{'})\}$ je tudi podlagebra (dokaz podoben).
$\tau \equiv \mathbb{N} \setminus \{0\}$

$$\binom{n}{i,j} = \begin{cases} 1 : \; i \cdot j = n \\ 0 : \; \text{sicer} \end{cases}$$

$f * g(n) = \sum_{i,j} \binom{n}{i,j} f(i)g(j) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right)$ Dirichletova konvolucija.
Dirichletove rodovne funkcije:
$\{\sum_{n=1}^{\infty} \frac{a_n}{n^s};\; a_i \in K\}$
$\sum_{n=1}^{\infty} \frac{a_n}{n^s} \cdot \sum_{n=1}^{\infty} \frac{b_n}{n^s} = \sum_{n=1}^{\infty} \frac{\sum_{d|n} a_d b_{\frac{n}{d}}}{n^s}$
$f \to \sum_n \frac{f(n)}{n^s}$ izomorfizem algeber.
$\zeta \to \zeta(s)$ (Riemmanova) funkcija ζ.
če $\sum_n \frac{a_n}{n^s}$ in $\sum_n \frac{b_n}{n^s}$ konvergirata:
$\left(\frac{a_1}{1^s} + \frac{a_2}{2^s} + \frac{a_3}{3^s} + \dots\right) \cdot \left(\frac{b_1}{1^s} + \frac{b_2}{2^s} + \frac{b_3}{3^s} + \dots\right)$
$\left[\frac{1}{6^s}\right]$: $a_1b_6 + a_2b_3 + a_3b_2 + a_6b_1$ (množenje kot dejanske funkcije).

(P,K)
$(r,s) \sim (r^{'},s^{'}) \iff \frac{s}{r} = \frac{s^{'}}{r^{'}}$
$I_{\sim}(P,K) = \{f : Int(P) \to K : (r,s) \sim (r^{'},s^{'}) \implies f(r,s) = f(r^{'},s^{'})\}$
$f{*}g(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right)$ - odvisno samo od kvocientov: pišemo en argument.
$\left\{\sum_{n=1}^{\infty} \frac{a(n)}{n^s} : a(n) \in K\right\}$ Dirichletove rodovne funkcije.
$\sum_{n=1}^{\infty} \frac{a(n)}{n^s} \cdot \sum_{n=1}^{\infty} \frac{b(n)}{n^s} = \sum_{n=1}^{\infty} \frac{\sum_{d|n} a(d)b\left(\frac{n}{d}\right)}{n^s}$.
Izomorfizem
$I_{\sim}(P,K) \to$ Dirichletove rodovne funkcije
$Drf : f \mapsto \sum_{n=1}^{\infty} \frac{f(n)}{n^s}$
$Drf(\zeta) = \zeta(s)$
$K = \mathbb{C}$
$\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ konvergira za $s_0 \implies$ konvergira za $\forall s :\; Re\ s > Re\ s_0$.
$\zeta(s)$ konvergira za $Re\ s > 1$.

Definicija 3.6.3.

$f : \mathbb{N} \setminus \{0\} \to \mathbb{C}$ je multiplikativna, če je $f(1) = 1$ in $f(ab) = f(a)f(b)$ za $D(a,b) = 1$.

Ekvivalentno: $f\left(p_1^{\alpha_1} \dots p_k^{\alpha_k}\right) = f\left(p_1^{\alpha_1}\right) \dots f\left(p_k^{\alpha_k}\right)$.

Trditev 3.6.4. f multiplikativna $\iff Drf(f) = \prod_{p \text{ prašt.}} \left(1 + \frac{f(p)}{p^2} + \frac{f(p^2)}{p^{2s}} + \dots\right)$.

Dokaz 3.6.5. Pogledamo $\left[\frac{1}{n^s}\right]$ na obeh straneh. ■

Primer. $\zeta(s) = \prod_{p \text{ prašt.}} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \dots\right) = \prod_{p \text{ prašt.}} \frac{1}{1 - \frac{1}{p^s}}$.

Posledica 3.6.6.

f, g multiplikativna $\implies f * g$ multiplikativna,

f multiplikativna $\implies f^{-1}$ multiplikativna.

Dokaz 3.6.7.

DN: direktno iz definicije.

Preko trditve:

$Drf(f * g) \stackrel{?}{=} Drf(f) \cdot Drf(g)$

$\left(1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \dots\right) \cdot \left(1 + \frac{g(p)}{p^s} + \frac{f(g^2)}{p^{2s}} + \dots\right) = 1 + \frac{f(p)+g(p)}{p^s} + \frac{f(p^2)+f(p)g(p)+g(p^2)}{p^{2s}} + \dots$

$Drf(f^{-1}) = \frac{1}{Drf(f)}$

$\frac{1}{1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \dots} = 1 - \left(\frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \dots\right) - \left(\frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \dots\right)^2 + \dots$

Oboje ustrezne oblike. ■

Opomba. f, g multiplikativni: $f * g\left(p^k\right) = \sum_{i=0}^k f\left(p^i\right) g\left(p^{k-i}\right)$.

Primer.

$Drf(\mu) = Drf(\zeta^{-1}) = \frac{1}{Drf(\zeta)} = \frac{1}{\zeta(s)} = \prod_{p \text{ prašt.}} \left(1 - \frac{1}{p^s}\right) = \sum_{n=1}^\infty \frac{\mu(n)}{n^s}$

$$\mu\left(p^k\right) = \begin{cases} 1 : & k = 0 \\ -1 : & k = 1 \\ 0 : & k \geq 2 \end{cases} .$$

$Drf\left(n^k\right) = \sum_{n=0}^\infty \frac{n^k}{n^s} = \zeta(s-k);\ Re\ s > k + 1.$

$\zeta^2(s) = ?$

$\zeta * \zeta(s) = \sum_{d|n} \zeta(d) \cdot \zeta\left(\frac{n}{d}\right) = \tau(n)$: število deliteljev n.

$\zeta^2(s) = \sum_{n=1}^\infty \frac{\tau(s)}{n^s}$

$\zeta * \zeta(p^k) = \sum_{i=0}^{k} 1 = k+1$

$\zeta * \zeta\,[p_1^{\alpha_1} \cdot p_k^{\alpha_k}] = (\alpha_1+1)\ldots(\alpha_k+1) = \tau(n)$

$\zeta(2s) = \sum_{n=1}^{\infty} \frac{1}{n^{2s}}$

$a(n) = \begin{cases} 1: \ n = m^2 \\ 0: \ \text{sicer} \end{cases}$ - multiplikativna funkcija.

$a(p^k) = \begin{cases} 1: \ k \text{ sod} \\ 0: \ k \text{ lih} \end{cases}$

$\frac{1}{\zeta(2s)} = \frac{1}{\prod_{p \text{ prašt.}}\left(1+\frac{1}{p^{2s}}+\frac{1}{p^{4s}}+\ldots\right)}$

$\overset{\text{geom.}}{=} \prod_{p \text{ prašt.}}\left(1 - \frac{1}{p^{2s}}\right) = \sum_{n=1}^{\infty} \frac{b(n)}{n^s}$

$b(p^k) = \begin{cases} 1: \ k = 0 \\ -1: \ k = 2 \\ 0: \ \text{sicer} \end{cases}$

$\frac{\zeta^2(s)}{\zeta(2s)} = ?$

$\sum_{n=0}^{\infty} \frac{c(n)}{n^s}$

$k \geq 2:$

$c(p^k) = \sum_{i=0}^{k} b(p^i)c(p^{k-i}) = 1 \cdot \tau(p^k) - 1 \cdot \tau(p^{k-2}) = k+1-(k-1) = 2$

$k = 1$:

$c(p) = 1 \cdot \tau(1) = 2$ (potrebno preveriti zarabi b)

$c(p^0) = 1$

$c(n) = 2^{\omega(n)}$, $\omega(n)$: število praštevilskih deliteljev.

$\frac{\zeta^2(s)}{\zeta(2s)} = \sum_{n=1}^{\infty} \frac{2^{\omega(n)}}{n^s}$

$\sum_{n=1}^{\infty} \frac{2^{\omega(n)}}{n^s} = \frac{\zeta^2(2)}{\zeta(4)} = \frac{\left(\frac{\pi^2}{6}\right)^2}{\frac{\pi^2}{90}} = \frac{5}{2}$ (konvergira počasi).

Poglavje 4

Upodobitve grup in Polyeva teorija

4.1 Permutacijske upodobitve

Definicija 4.1.1.
$(G, \circ)$ grupa, e enota.
Delovanje grupe G na množici X je preslikava $\vartheta : G \times X \to X$,
$(g, x) \mapsto \vartheta(g, x) = g \cdot x$ (ni množica v grupi), za katero velja:

- $\vartheta(e, x) = x \; \forall x \in X$ $[e \cdot x = x]$
- $\vartheta(g \circ h, x) = \vartheta(g, \vartheta(h, x)) \; \forall x \in X, g, h \in G$ $[(g \cdot h) \cdot x = g \cdot (h \cdot x)]$ (ni asociativnost).

ϑ delovanje G na X.
$\Theta : G \to S_X$
$\Theta(g)(x) = \vartheta(g, x)$
$\Theta(g)$ je bijekcija: inverz je $\Theta(g^{-1})$.
$\Theta(g)(\Theta(g^{-1})(x)) = \Theta(g)(\vartheta(g^{-1}, x)) = \vartheta(g, \vartheta(g^{-1}, x))$
$= \vartheta(g \circ g^{-1}, x) = \vartheta(e, x) = x$.
Θ je homomorfizem:

$\Theta(g \cdot h)(x) = \vartheta(g \cdot h, x)$
$\Theta(g)(\Theta(h)(x)) = \vartheta(g, \vartheta(h, x))$.
Obratno: $\Theta : G \to S_X$, homomorfizem je
$\vartheta : G \times X \to X$
$\vartheta(g, x) = \Theta(g)(x)$ delovanje.
Če je Θ injektiven homomorfizem ($ker\, \Theta$ trivialno), je delovanje zvesto (angl. faithful).
Torej: $g \cdot x = x \; \forall x \in X \implies g = e$.
V tem primeru je $G \cong \Phi(G)$, BŠS $G \leq S_X, G$ permutacijska grupa.
Zvesto delovanje $\equiv$ permutacijska grupa $\equiv$ zvesta permutacijska upodobitev.
$G \to S_X$ permutacijska upodobitev.
Odslej: X, G končni, delovanje zvesto ($G \leq S_X$).
$x \sim y$, če $\exists g \in G : \; g \cdot x = y$ ekvivalenčna relacija.
$x \in X : Gx = \{g \cdot x : \; g \in G\}$ orbita x.
X/G množica orbit.
$g \in G : x^g = \{x \in X : g \cdot x = x\}$ množica negibnih točk g.
$x \in X : G_x = \{x \in X : g \cdot x = x\}$ stabilizator x.
$G_x \leq G$.
$g, h \in G_x, g \cdot x = x, h \cdot x = x \implies (g \cdot h) \cdot x = g \cdot (h \cdot x) = g \cdot x = x \implies g \cdot h \in X$
$g \in G_x, g \cdot x = x \implies g^{-1} \cdot (g \cdot x) = g^{-1} \cdot x = (g^{-1} \cdot g) \cdot x = x$
$\implies g^{-1}(x) = x \implies g^{-1} \in G_x$.
V splošnem ni $G_x \lhd G$.

Trditev 4.1.2. $\forall x \in X : |G| = |G_x| \cdot |Gx|$.

Dokaz 4.1.3.
$H \leq G, G/H = \{g \cdot H : g \in G\}$ kvocientna množica (množica levih odsekov).
Levi odseki so disjunktni, neprazni in enako močni ($e \cdot H \to g \cdot H, h \cdot gh$ bijekcija).
$\implies |G/H| = \frac{|G|}{|H|}$.
$|G/G_x| = \frac{|G|}{|G_x|}$.
Iščemo bijekcijo $Gx \to G/G_x$.

$\phi(g \cdot x) = g \cdot G_x$.
Dobra definiranost ($\Longrightarrow$) in injektivnost ($\Longleftarrow$):
$gx = hx \iff (h^{-1}g)x = x \iff h^{-1}g \in G_x \iff h^{-1}gG_x = G_x \iff gG_x = hG_x$.
Sujrektivnost:
$g \cdot G_x = \phi(g \cdot x)$. ■

Izrek 4.1.4 (Burnsideova lema)**.** $|X/G| = \frac{1}{|G|} \sum_{g \in G} |x^g|$.
Število orbit = povprečno število negibnih točk.

Dokaz 4.1.5.

$$\begin{aligned}
\sum_{g \in G} |x^g| &= \sum_{g \in G} \sum_{x \in x^g} 1 \\
&= \sum_{x \in X} \sum_{g \in G, gx = x} 1 \\
&= \sum_{x \in X} |G_x| \\
&\overset{\text{trd.}}{=} \sum_{x \in X} \frac{|G|}{|Gx|} \\
&= |G| \sum_{\sigma \in X/G} \frac{1}{|\sigma|} \\
&= |G| \cdot |X/G|.
\end{aligned}$$

σ: orbita. ■

4.2 Polyeva teorija

Polya.
$x = [n], G = C_n = \{(12 \dots n)^i : \ 0 \le i \le n-1\}$
$n = 4 : C_4 = \{(1234), (13)(24), (1432), id\}$
$\vartheta : \mathbb{Z}_4 \times [4] \to [4]$
$\vartheta(i, x) = x + i (\mathrm{mod}\ 4)$
$0 \cdot x = x, 1 \cdot x = x + 1, 2 \cdot x = x + 2, 3 \cdot x = x + 3$
$\Theta : Z_4 \to S_4$

$i \mapsto (x \mapsto x + i)$

$0 \mapsto id, 1 \mapsto (1234), 2 \mapsto (13)(24), 3 \mapsto (1432)$

$\Theta(Z_4) = C_4$

G zvesto delovanje na X, ϑ.

R množica barv, $|R| = r$.

Barvanje $b : X \to R$.

Trditev 4.2.1.
$\widehat{\vartheta}(g,b)(x) = b(\vartheta(g^{-1},x))$ oz. $(\hat{g} \cdot b)(x) = b(g^{-1}x)$.
Delovanje na R^X (množica barvanj na X).
Če je $r > 1$, je to delovanje zvesto.

Dokaz 4.2.2.
$\widehat{\vartheta}(e,b)(x) = b(\vartheta(e^{-1},x)) = b(x) \implies \widehat{\vartheta}(e,b) = b$

$\widehat{\vartheta}(g \circ h, b)(x) = b(\vartheta((g \circ h)^{-1}, x)) = b(\vartheta(h^{-1}, \vartheta(g^{-1}, x)))$

$\widehat{\vartheta}(g, \widehat{\vartheta}(h, b))(x) = \widehat{\vartheta}(h, b)(\vartheta(g^{-1}, x)) = b(\vartheta(h^{-1}, \vartheta(g^{-1}, x)))$

$\widehat{\vartheta}(g, b) = b$ za $\forall b \in R^X$.

$1, 2 \in R$.

Izberemo $x_0 \in X$.

$b(x) = \begin{cases} 1 : & x = x_0 \\ 2 : & x \neq x_0 \end{cases}$

$\widehat{\vartheta}(g, b)(x) = b(x)\ \forall x \in X$

$b(\vartheta(g^{-1}, x)) = b(x)\ \forall x \in X$

$x = \vartheta(g, x)$

$b(x_0) = b(\vartheta(g, x_0)) = 1 \implies \vartheta(g, x_0) = x_0 \overset{\vartheta \text{ zvesto}}{\implies} g = e.$ ∎

Torej za $r > 1$ lahko uporabimo Burnsideovo lemo za $\widehat{\vartheta}$.

Število orbit = število neekvivalentnih barvanj.

$g \in G$, kaj so negibna barvanja?

$g =$ rotacija $\pi/4$: vse točke iste barve: r negibnih barvanj.

$g =$ rotacija $\pi/2$: cikla vsak iste barve: r^2 negibnih barvanj.

$\widehat{\vartheta}(g, b) = b$

$b(g^{-1}(x)) = b(x)\ \forall x \in X$.
Za $\forall x \in X$ sta x in $g^{-1}x$ iste barve.
Za $\forall x \in X$ sta x in gx iste barve.
Za $\forall x \in X$ sta gx in g^2x iste barve.
$x, gx, g^2x, g^3x \dots$ iste barve.
Vsi elementi v elem ciklu $g \in S_X$ iste barve $\implies$ b negibno barvanje za g.

Izrek 4.2.3 (Polyev)**.**
G zvesto delovanje na X,
R množica barv, $r = |R|$.
Število neekvivalentnih barvanj X z barvami iz R je $\frac{1}{|G|}\sum_{g\in G} r^{c(G)}$, kjer je $c(g)$ število ciklov g kot elementov S_X (torej število ciklov $\Theta(g)$) (tudi za $r = 1$ (nezvesto)).

Primer.
C_4
$\frac{1}{4}\left(r^4 + r^2 + 2r\right)$
D_4 diedrska grupa
$D_4 = C_4 \cup \{(14)(23), (12)(34), (13), (24)\}$
$\frac{1}{8}\left(r^4 + r^2 + 2r + 2r^2 + 2r^3\right) = \frac{1}{8}\left(r^4 + 2r^3 + 3r^2 + 2r\right)$.
$r = 2$:
$\frac{1}{8}(16 + 16 + 12 + 4) = 6$.

G zvesto deluje na X.
$G \leq S_X$.
Polya: število neekvivalentnih barvanj je $\frac{1}{|G|}\sum_{g\in G} r^{c(G)}$.

Primer.
S_n deluje na $[n]$.
$\pi \cdot i = \pi(i)$
$\frac{1}{n!}\sum_{\pi\in S_n} r^{c(\pi)} = \frac{1}{n!}\sum_k c(n,k)r^k$.
b_1 in b_2 sta neekvivalentni barvanji $\iff$ $\left|b_1^{-1}(i)\right| = \left|b_2^{-1}(i)\right|$ za $\forall i = 1, 2 \dots r$.
($\Rightarrow$ velja vedno.)

λ_i: število točk barve i, $\lambda_i \geq 0$.

$\lambda_1 + \cdots + \lambda_r = n \implies$ šibke kompozicije.

$\binom{n+r-1}{r-1} = \frac{(n+r-1)!}{(r-1)!n!} = \frac{1}{n!} \sum_k c(n,k) r^k$.

Definicija 4.2.4.

$G \leq S_X$, $|X| = n$.

$Z_G(t_1 \dots t_n) = \frac{1}{|G|} \sum_{g \in G} \prod_{c \text{ cikel G}} t_{|c|}$: ciklični indeks permutacijske grupe.

$X = [4]$

$G = C_4$

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

Polya: število neekvivalentnih barvanj $= Z_G(r, r \dots r)$.

Izrek 4.2.5 (Posplošitev Polyevega izreka)**.** $B(\beta_1 \dots \beta_r)$: število neekvivalentnih barvanj, pri čemer je β_i elementov X barve i.

$\sum_{(\beta_1 \dots \beta_r)} B(\beta_1 \dots \beta_r) u_1^{\beta_1} \dots u_r^{\beta_r} = Z_G(u_1 + \cdots + u_r, u_1^2 + \cdots + u_r^2, \dots u_1^n + \cdots + u_r^n)$.

Primer.

Od prej, $r = 2$.

$$\begin{aligned} {}_{C_4}(u_1+u_2, u_1^2+u_2^2, u_1^3+u_2^3, u_1^4+u_2^4) &= \frac{1}{4}\left((u_1+u_2)^4 + 2(u_1^4+u_2^4) + (u_1+u_2)^2\right) \\ &= u_1^4 + u_2^4 + u_1^3 u_2 + 2u_1^2 u_2^2 + u_1 u_2^3 + u_2^4. \end{aligned}$$

Dokaz 4.2.6.

G zvesto deluje na $\{b : X \to R : |b^{-1}(i)| = \beta_i\}$.

Burnsideova lema: $B(\beta_1 \dots \beta_r) = \frac{1}{|G|} \sum_{g \in G}$ število neekvivalentnih barvanj za g.

Še vedno: elementi enega cikla g so iste barve.

Vsota dolžin ciklov barve i mora biti β_i.

$$\left[u_1^{\beta_1} \dots u_r^{\beta_r}\right] Z_G(u_1 + \cdots + u_r, \dots u_1^n + \cdots + u_r^n) = \left[u_1^{\beta_1} \dots u_r^{\beta_r}\right] \frac{1}{|G|} \sum_{g \in G} \prod_{c \text{ cikel } g} \left(u_1^{|c|} + \cdots + u_r^{|c|}\right).$$

Isto (distributivnost, vsota ...).

Za vsak cikel izberem u_i.

Vsota dolžin z izbranim u_i mora biti β_i. ∎

Opomba.
$|X^g| = \left|X^{g'}\right|$
$g, g' \in G$, $g' = hgh^{-1}$ za nek $h \in G : g, g'$ konjugirana.
$g \cdot x = x$
$g'(hx) = hgh^{-1}(hx) = hx$
$x \mapsto h \cdot x$ je bijekcija iz X^g v $X^{g'}$.
(Inverz je $x \mapsto h^{-1}x$.)
Število negibnih točk je konstantno na konjugiranostnih razredih.
V S_n: permutaciji sta konjugirani $\iff$ imata iste dolžine ciklov.
$\pi = \ldots (i\ \pi(i)\ \pi^2(i) \ldots)$
$\tau\pi\tau^{-1} = \ldots (\pi(i)\ \tau(\pi(i))\ \tau(\pi^2(i)) \ldots)$.

Upodobitev grupe G je homomorfizem.
$G \to GL_d$
GL_d: grupa obrnljivih matrik velikosti $d \times d$.
Karakter upodobitve ρ je $\chi(g) = sl_\rho(g)$, sl: sled.
Izkaže se: do izomorfizma natančno določa upodobitev
$\chi(hgh^{-1}) = sl_\rho(hgh^{-1}) = sl_\rho(h) \cdot sl_\rho(g) \cdot sl_\rho(h^{-1}) = sl_\rho(g)$;
$sl(ABA^{-1}) = sl(A^{-1}AB) = sl(B)$.
Permutacijska upodobitev:
$G \to S_n \to GL_n$
$$3\ 1\ 2 \mapsto \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$
$\pi \mapsto A$
$$A_{ij} = \begin{cases} 1 : & i = \pi(j) \\ 0 : \text{sicer} \end{cases}.$$
Karakter te upodobitve je število negibnih točk.

4.3 Primeri

G zvesto deluje na X.

$|G| = |Gx| \cdot |G_x|$

G grupa rotacij $\mathbb{R}^3$, ki ohranja kocko.

G zvesto deluje na $X = \{\text{ploskve kocke}\}$.

$|Gx| = G$: vse ploskve.

$|G_x| = 4$: rotacija.

id	1
90°, ploskev	6
180°, ploskev	3
180°, robova	6
180°, oglišči	8

$G \cong S_4$

G deluje na dolgih diagonalah (dobimo vse permutacije teh).

Definicija 4.3.1.

$x = x_1 \dots x_n \in [n]^n$ je parkirna funkcija, če velja $y_i \leq i; i = 1, 2 \dots n$, kjer je $y_1 \dots y_n$ šibko naraščajoča permutacija x.

$PF_n = \{\text{parkirne funkcije dolžine } n\}$.

$PF_1 = \{1\}$,

$PF_2 = \{11, 12, 21\}$

$PF_3 = \{111, 112, 121, 211, 122, 212, 221, 113, 131, 311, 123, 132, 213, 231, 312, 321\}$.

n avtov, n označenih parkirnih mest, vsak voznik ima izbrano parkirno mesto, vsak se zapelje do želenega in parkira na 1. prostem mestu.

121 $\underline{1}$ _ $\underline{3}$

311 $\underline{2}$ $\underline{3}$ $\underline{1}$

313 $\underline{2}$ _ $\underline{1}$: ne gre.

Trditev 4.3.2. $x \in [n]^n$ je parkirna funkcija $\iff$ vsi avtomobili parkirajo.

Dokaz 4.3.3.

($\Leftarrow$)
Če je $y_i > i$, je $y_i, y_{i+1} \dots y_n \geq i+1$
Voznikov: $n-i+1$, mest: $n-i$, za vsaj enega voznika zmanjka parkirnih mest.
($\Rightarrow$) z indukcijo.
$x_1 = k$
$\_\,\_\,\_\,\underline{x}\,\_\,\_$
$$x_i' := \begin{cases} x_{i+1} : \ x_{i+1} \leq k \\ x_{i+1} - 1 : \ x_{i+1} > k \end{cases}$$
$i \leftarrow i+1$: se zamakne.
x_i' je tudi parkirna funkcija.
$y_i \leq i \iff y_i - 1 \leq i - 1$.
Po indukciji lahko tudi ostali parkirajo. ■

Izrek 4.3.4.
$|PF_n| = (n+1)^{n-1}$
$\psi : PF_n \to \mathbb{Z}_{n+1}^{n-1}$ bijekcija
$x \mapsto (x_2 - x_1, x_3 - x_2 \dots x_n - x_{n-1}) \pmod{n+1}$.

$11 \to 0$
$12 \to 1$
$21 \to 2$

Dokaz 4.3.5.
Dodamo še parkirno mesto 0, avto se lahko vrne na začetek, izbere $\mathbb{Z}_{n+1}^n$.
00 $\underline{1}\,\underline{2}\,\_$
01 $\underline{1}\,\underline{2}\,\_$
02 $\underline{1}\,\_\,\underline{2}$
10 $\underline{2}\,\underline{1}\,\_$
11 $\_\,\underline{1}\,\underline{2}$
12 $\_\,\underline{1}\,\underline{2}$
20 $\underline{2}\,\_\,\underline{1}$
21 $\_\,\underline{2}\,\underline{1}$

22 $\underline{2}\_\underline{1}$

Vsi lahko parkirajo, eno mesto je prosto.

x in $x + (k, k \dots k)$: zamaknjeno na k mest.

V vsakem (levem) odseku podgrupe, generirane z $(1, 1 \dots)$ je natanko en element v PF_n

$\implies \ |PF_n| = \frac{|Z_{n+1}^n|}{n+1} = (n+1)^{n-1}$.

Inverz of ψ :

$\mathbb{Z}_{n+1}^{n-1} \to PF_n$

$(a_1, a_2 \dots a_{n-1}) \mapsto (x_1, x_1 + a_1, x_1 + a_1 + a_2 \dots)$.

Obstaja natanko en x_1, da je to parkirna funkcija. ■

Delovanje S_n na PF_n.

$\pi \cdot x_1 \dots x_n = x_{\pi^{-1}(1)} \dots x_{\pi^{-1}(n)}$.

Zvesto: ✓

Koliko je negibnih točk π?

BŠS: $\pi = (1\ 2 \dots \lambda_1)(\lambda_1 + 1 \dots \lambda_1 + \lambda_2) \dots$

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

$\pi \cdot x = x$

$\pi \cdot x_1 \dots x_8 = x_3 x_1 x_2 x_3\, x_7 x_5 x_6\, x_8$.

Če $x_1 = x_2 = x_3 = x_4$ in $x_5 = x_6 = x_7$.

$\psi(x_1 \dots x_8) = (0, 0, 0, -, 0, 0, -)$

$|PF_n(\pi)| = (n+1)^{c(\pi)-1}$.

Burnsideova lema:

$$\begin{aligned}
\text{število orbit} &= \frac{1}{n!} \sum_{\pi \in S_n} (n+1)^{c(\pi)-1} \\
&= \frac{1}{n!(n+1)} \sum_k c(n,k)(n+1)^n \\
&= \frac{1}{n!(n+1)} (n+1)^{\overline{n}} \\
&= \frac{(n+1)(n+2)\dots 2n}{n!(n+1)} \cdot \frac{n!}{n!} \\
&= \frac{1}{n+1} \binom{2n}{n} = c_n.
\end{aligned}$$

Predstavniki orbit za $n = 3$.

Zarotirane Dyckove poti.

Ciklični indeks za kocko:

$x = \{\text{oglišča kocke}\}$

$Z_G(t_1 \dots t_8) = \frac{1}{24}\left(t_1^8 + 6t_4^2 + 3t_2^4 + 6t_2^4 + 8t_1^2 t_3^2\right)$.

Pobarvamo z r barvami:

$\frac{1}{24}\left(r^8 + 17r^4 + 6r^2\right)$.

Ciklični indeks za C_n:

$C_n = \{(1\ 2 \dots n)^i\ 1 \leq i \leq n\}$

$(123456)^2 = (135)(246)$

$(123456)^3 = (14)(25)(36)$

$(12 \dots n)^i D(n, i = 1) \implies$ cikel dolžine n.

$(12 \dots n)^d = (1\ d+1 \dots)(2\ d+2 \dots)$

d ciklov dolžine n.

$(12 \dots n)^i = \left((12 \dots n)^d\right)^i$

$d = D(n, i)$

$n = n^{'} d$

$i = i^{'} d$

$D(n^{'}, i^{'}) = 1$

$(12 \dots n)^d$: d ciklov dolžine $n^{'}$.

$Z_{C_n}(t_1 \dots t_n) = \frac{1}{n!} \sum_{d|n} \phi\left(\frac{n}{d}\right) t_{\frac{n}{d}}^{d}$.

Za dane d in $\frac{n}{d}$: koliko je $i \in [n]$, da je $D(n, i) = d$

$i = i^{'} \cdot d,\ 1 \leq i^{'} \leq \frac{n}{d} = n^{'}$

$n = n^{'} \cdot d$

$D(i, n) = D(i^{'} \cdot d, n^{'} \cdot d) = d = d \cdot D(n^{'}, i^{'})$.

Torej: koliko je $i^{'} \in \left[\frac{n}{d}\right]$, da je $D(n^{'}, i^{'}) = 1$:

$\phi\left(\frac{n}{d}\right)$.

Izrek 4.3.6.

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

$$Z_{D_n}(t_1 \dots t_n) = \frac{1}{n} \sum_{d|n} \phi(d) t_d^{\frac{n}{d}} + \begin{cases} \frac{1}{2} t_1 t_2^{\frac{n-1}{2}} : n \text{ lih} \\ \frac{1}{4} t_1^2 t_2^{\frac{n}{2}-1} + \frac{1}{4} t_2^{\frac{n}{2}} : n \text{ sod} \end{cases}$$

Primer.

Ogrlice: iste, če eno iz druge dobim z rotacijo.

$\frac{1}{n}\sum_{d|n}\phi(d)r^{\frac{n}{d}}$.

Zapostnice: iste, če eno iz druge dobim z rotacijo ali zrcaljenjem.

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