Vjerojatnosne i analitičke metode u kombinatorici

Ideja ovih zabilješki je okupiti osnovnu teoriju i primjere/zadatke iz kombinatorike koji se tipično rješavaju vjerojatnosnim i analitičkim tehnikama. Materijali su podijeljeni u tri cjeline, upravo prema najčešćim trima takvim tehnikama:

1. vjerojatnosna metoda,
2. funkcije izvodnice,
3. Fourierova analiza.

Obzirom da su na pripremama godine 2014. bile obrađene cjeline 2 i 3, a godine 2015. cjelina 1, činilo mi se prirodnim objediniti zabilješke iz tih dviju godina.

1. Vjerojatnosna metoda

Pod *vjerojatnosnom metodom* se obično podrazumijeva primjena vjerojatnosnih tehnika kod determinističkih problema, u čijoj formulaciji nema ničeg "slučajnog" pa takva primjena može biti donekle neočekivana. Malo preciznije, pretpostavimo da želimo dokazati postojanje nekog "dobrog" objekta. Mi na skupu svih objekata definiramo neku vjerojatnosnu mjeru pa potom pokažemo da skup svih dobrih objekata ima pozitivnu mjeru, tj. da je pozitivna vjerojatnost da će slučajno odabrani objekt biti dobar. Kao posljedicu dobivamo da postoji barem jedan dobar objekt, ali ne mora odmah biti jasno kako ga doista naći. Korisnost vjerojatnosne metode najbolje se vidi iz brojnih primjera. Ponekad je potrebno maštovito preformulirati problem i definirati odgovarajući vjerojatnosni prostor. Najveći promotor vjerojatnosne metode bio je Paul Erdős.

Od vjerojatnosti će nam trebati samo najosnovniji pojmovi. *Prostor elementarnih događaja* Ω će kod nas uvijek biti neki konačni skup. *Vjerojatnost* je tada jednoznačno određena nenegativnim brojevima $(p_\omega)_{\omega\in\Omega}$ takvima da je $\sum_{\omega\in\Omega} p_\omega = 1$. U tom slučaju za svaki *događaj* A, što je naprosto proizvoljni podskup od Ω, definiramo njegovu vjerojatnost sa

$$\mathbb{P}(A) := \sum_{\omega\in A} p_\omega \in [0,1].$$

Po definiciji je očigledno

$$\mathbb{P}(A^c) = 1 - \mathbb{P}(A).$$

Lako je vidjeti da za bilo koje događaje $A_1, A_2, \ldots, A_n$ vrijedi

$$\mathbb{P}\Big(\bigcup_{i=1}^{n} A_i\Big) \le \sum_{i=1}^{n} \mathbb{P}(A_i).$$

Štoviše, ako su $A_1, A_2, \ldots, A_n$ međusobno disjunktni, imamo čak jednakost:

$$\mathbb{P}\Big(\bigcup_{i=1}^{n} A_i\Big) = \sum_{i=1}^{n} \mathbb{P}(A_i).$$

Događaji $A_1, A_2, \ldots, A_n$ su međusobno *nezavisni* ako za svaki podskup $I \subseteq \{1, 2, \ldots, n\}$ vrijedi

$$\mathbb{P}\Big(\bigcap_{i\in I} A_i\Big) = \prod_{i\in I} \mathbb{P}(A_i).$$

Intuitivno, pojavljivanje nekih od tih događaja ne utječe na vjerojatnosti pojavljivanja ostalih događaja. U vjerojatnosti često umjesto $\mathbb{P}(A_1 \cap A_2 \cap \cdots \cap A_n)$ pišemo naprosto $\mathbb{P}(A_1, A_2, \ldots, A_n)$. Na Ω se najčešće pretpostavlja tzv. *uniformna* vjerojatnost, tj. da je $p_\omega = 1/|\Omega|$ za svaki $\omega \in \Omega$, što znači da za svaki događaj A vrijedi

$$\mathbb{P}(A) = \frac{|A|}{|\Omega|} = \frac{\text{broj “povoljnih” mogućnosti}}{\text{broj svih mogućnosti}}.$$

Mi ćemo podrazumijevati da je to slučaj kad god nije rečeno drugačije.

Slučajna varijabla je ovdje naprosto proizvoljna funkcija $X \colon \Omega \to \mathbb{R}$. Njeno *očekivanje* je dano formulom

$$\mathbb{E}X := \sum_{\omega\in\Omega} p_\omega X(\omega).$$

Ukoliko X poprima međusobno različite vrijednosti $a_1, \ldots, a_m \in \mathbb{R}$, tada je

$$\mathbb{E}X = \sum_{i=1}^{m} \mathbb{P}(X = a_i)a_i$$

te općenitije

$$\mathbb{E}f(X) = \sum_{i=1}^{m} \mathbb{P}(X = a_i)f(a_i)$$

za bilo koju funkciju $f \colon \mathbb{R} \to \mathbb{R}$. Kažemo da brojevi $\mathbb{P}(X = a)$, $a \in \mathbb{R}$ određuju *razdiobu* od X. Očekivanje je linearno, tj.

$$\mathbb{E}(\alpha X + \beta Y) = \alpha\mathbb{E}X + \beta\mathbb{E}Y$$

za slučajne varijable X, Y i brojeve $\alpha, \beta \in \mathbb{R}$. Osim toga je i monotono, tj. ako za slučajne varijable X i Y vrijedi $X \leq Y$, tada je $\mathbb{E}X \leq \mathbb{E}Y$. Trivijalna (ali nama korisna) opservacija je da ako za neki $a \in \mathbb{R}$ vrijedi $\mathbb{E}X \geq a$ (respektivno $\mathbb{E}X \leq a$), tada postoji barem jedan $\omega \in \Omega$ takav da je $X(\omega) \geq a$ (respektivno $X(\omega) \leq a$). Slučajne varijable $X_1, X_2, \ldots, X_n$ su međusobno *nezavisne* ako za svaki izbor $a_1, a_2, \ldots, a_n \in \mathbb{R}$ vrijedi

$$\mathbb{P}(X_1 = a_1, X_2 = a_2, \ldots, X_n = a_n) = \prod_{i=1}^{n} \mathbb{P}(X_i = a_i).$$

U tom slučaju imamo

$$\mathbb{E}\Big(\prod_{i=1}^{n} X_i\Big) = \prod_{i=1}^{n} \mathbb{E}X_i$$

te, općenitije, za proizvoljne funkcije $f_1, f_2, \ldots, f_n \colon \mathbb{R} \to \mathbb{R}$ vrijedi

$$\mathbb{E}\Big(\prod_{i=1}^{n} f_i(X_i)\Big) = \prod_{i=1}^{n} \mathbb{E}f_i(X_i).$$

Poznata (i prilično jednostavna) činjenica je da uvijek možemo konstruirati prostor Ω i vjerojatnost $\mathbb{P}$ tako da $X_1, X_2, \ldots, X_n$ budu međusobno nezavisne slučajne varijable s unaprijed zadanim razdiobama.

Zadaci

1. (*Kraftova nejednakost*) Neka je $\mathcal{F}$ konačna kolekcija binarnih stringova konačne duljine takva da nikoji string iz $\mathcal{F}$ nije prefiks (tj. početni dio) nekog drugog stringa iz $\mathcal{F}$. Ako je N_i broj stringova u $\mathcal{F}$ duljine i, dokažite $\sum_i \frac{N_i}{2^i} \leq 1$.

   Rješenje. Neka je n najveća duljina nekog stringa iz $\mathcal{F}$. Za prostor elementarnih događaja Ω uzimamo skup svih stringova s duljine n. Za svaki $f \in \mathcal{F}$ promatramo događaj

   $$A_f := \{s \in \Omega \,:\, \text{string } f \text{ je prefiks stringa } s\}.$$

   Primijetimo da zbog slučajnosti of s imamo

   $$\begin{aligned}\mathbb{P}(A_f) &= \frac{\text{broj stringova duljine } n \text{ s unaprijed određenih } |f| \text{ bitova}}{\text{broj stringova duljine } n} \\ &= \frac{2^{n-|f|}}{2^n} = \frac{1}{2^{|f|}},\end{aligned}$$

   pri čemu nam $|f|$ označava duljinu stringa f.

   Događaji A_f i A_g su međusobno disjunktni za različite $f, g \in \mathcal{F}$. Naime, kad bi postojao string $s \in A_f \cap A_g$ i ako bez smanjenja općenitosti pretpostavimo $|f| \leq |g|$, tada bi f i g istovremeno bili prefiksi od s, što bi značilo da je f prefiks od g, a to je protivno pretpostavci na $\mathcal{F}$. Zbog disjunktnosti događaja A_f možemo računati:

   $$1 \geq \mathbb{P}\Big(\bigcup_{f\in\mathcal{F}} A_f\Big) = \sum_{f\in\mathcal{F}} \mathbb{P}(A_f) = \sum_{f\in\mathcal{F}} \frac{1}{2^{|f|}} = \sum_{i\geq 0} \frac{N_i}{2^i}.$$

2. (*Spernerov teorem*) Neka je $\mathcal{F}$ familija podskupova od $\{1, 2, \ldots, n\}$ takva da ne postoje $A, B \in \mathcal{F}$ za koje bi vrijedilo $A \subsetneqq B$. Dokažite $|\mathcal{F}| \leq \binom{n}{\lfloor n/2 \rfloor}$.

   Rješenje, prilagođeno iz knjige [1], poglavlje 11. Neka je Ω skup svih permutacija σ skupa $\{1, 2, \ldots, n\}$. Za svaki $A \in \mathcal{F}$ definiramo događaj

   $$\begin{aligned}C_A := \{\sigma \in \Omega \,:\, &\text{svaki element od } A \text{ prethodi svakom elementu} \\ &\text{od } A^c \text{ u slijedu } \sigma(1), \sigma(2), \ldots, \sigma(n)\}.\end{aligned}$$

   Drugim riječima, ako je $|A| = k$, tada $\sigma \in C_A$ znači

   $$A = \{\sigma(1), \sigma(2), \ldots, \sigma(k)\}.$$

   Za svaki $A \in \mathcal{F}$ zbog slučajnosti od σ imamo:

   $$\begin{aligned}\mathbb{P}(C_A) &= \frac{(\text{broj permutacija od } A)(\text{broj permutacija od } A^c)}{\text{broj permutacija od } \{1, 2, \ldots, n\}} \\ &= \frac{|A|!(n-|A|)!}{n!} = \frac{1}{\binom{n}{|A|}} \geq \frac{1}{\binom{n}{\lfloor n/2 \rfloor}},\end{aligned}$$

   radi poznatog svojstva binomnih koeficijenata: $\max_{0\leq k\leq n} \binom{n}{k} = \binom{n}{\lfloor n/2 \rfloor}$, tj. najveći element svakog retka Pascalovog trokuta nalazi se u "sredini".

S druge strane, za svake $A, B \in \mathcal{F}$, $A \neq B$ događaji C_A i C_B moraju biti disjunktni. Naime, pretpostavimo da postoji $\omega \in C_A \cap C_B$ i označimo $k = |A|$, $l = |B|$. Neka je bez smanjenja općenitosti $k \leq l$. To znači da je $A = \{\sigma(1), \sigma(2), \ldots, \sigma(k)\}$ i $B = \{\sigma(1), \sigma(2), \ldots, \sigma(k), \ldots, \sigma(l)\}$, iz čega slijedi $A \subseteq B$, što je kontradikcija. Konačno, iz disjunktnosti događaja C_A slijedi

$$1 \geq \mathbb{P}\Big(\bigcup_{A \in \mathcal{F}} C_A\Big) = \sum_{A \in \mathcal{F}} \mathbb{P}(C_A) \geq \frac{|\mathcal{F}|}{\binom{n}{\lfloor n/2 \rfloor}},$$

što nam daje $|\mathcal{F}| \leq \binom{n}{\lfloor n/2 \rfloor}$.

Primijetimo da je ograda $\binom{n}{\lfloor n/2 \rfloor}$ optimalna, jer se postiže ako je $\mathcal{F}$ familija svih podskupova od $\{1, 2, \ldots, n\}$ s točno $\lfloor n/2 \rfloor$ elemenata.

3. (*Zadatak iz članka [2]*) U svaku kućicu 100×100 tablice upisan je jedan od brojeva $1, 2, 3, \ldots, 5000$ i to tako da se svaki od tih brojeva pojavljuje točno dvaput. Dokažite da je moguće odabrati 100 kućica tablice tako da vrijedi:

   - u svakom retku je odabrana točno jedna kućica,
   - u svakom stupcu je odabrana točno jedna kućica,
   - brojevi u odabranim kućicama su međusobno različiti.

   Rješenje. Uzmimo slučajnu permutaciju $a_1, a_2, \ldots, a_{100}$ od $1, 2, \ldots, 100$, tj. Ω je kolekcija svih permutacija skupa $\{1, 2, \ldots, 100\}$. Pretpostavljamo da su sve permutacije jednako vjerojatne, tj. pojavljuju se s vjerojatnošću $1/100!$. Odaberemo li kućice (j, a_j); $j = 1, 2, \ldots, 100$, one će očigledno zadovoljavati prva dva uvjeta. Neka je A_k događaj da smo odabrali obje kućice s brojem k za fiksirani $k \in \{1, 2, \ldots, 5000\}$. Ako se te kućice nalaze u različitim recima i različitim stupcima, onda je $\mathbb{P}(A_k) = \frac{1}{100} \cdot \frac{1}{99}$, dok je inače $\mathbb{P}(A_k) = 0$. Dakle,

   $$\mathbb{P}\Big(\bigcup_{k=1}^{5000} A_k\Big) \leq \sum_{k=1}^{5000} \mathbb{P}(A_k) \leq 5000 \cdot \frac{1}{100} \cdot \frac{1}{99} = \frac{50}{99}$$

   pa je

   $$\mathbb{P}\Big(\bigcap_{k=1}^{5000} A_k^c\Big) \geq \frac{49}{99} > 0.$$

   Slijedi da za barem jedan odabir permutacije nemamo ponavljanja brojeva u odgovarajućim kućicama.

4. (*IMO Shortlist 2006. C3*) Neka je S konačni skup točaka u ravnini takav da nikoje tri od njih nisu kolinearne. Za svaki konveksni mnogokut M s vrhovima iz S neka $a(M)$ označava broj njegovih vrhova, a $b(M)$ broj točaka iz S koje leže izvan mnogokuta M. Napomenimo da se prazan skup, točka i dužina shvaćaju kao konveksni mnogokuti s redom 0, 1 i 2 vrha. Dokažite da za svaki $x \in \mathbb{R}$ vrijedi

   $$\sum_{\substack{M \text{ je konveksni mnogokut} \\ \text{vrhovi od } M \text{ su iz } S}} x^{a(M)}(1-x)^{b(M)} = 1.$$

Rješenje iz [3]. Primijetimo da je lijeva strana polinom u varijabli x. Po teoremu o jednakosti polinoma, dovoljno je jednakost provjeriti za beskonačno mnogo različitih vrijednosti od x, a mi ćemo to učiniti za sve $x \in [0,1]$.

Za Ω uzmimo skup svih bojenja točaka iz S u dvije boje (crvenu i plavu), pri čemu točke bojimo nezavisno, a svaka točka biva obojena crveno s vjerojatnosti x, odnosno plavo s vjerojatnosti $1-x$. Za svaki mnogokut M neka A_M označava događaj da su mu svi vrhovi obojeni crveno, a sve točke izvan M su obojene plavo. Najprije primijetimo da su svi ti događaji međusobno disjunktni i u uniji daju cijeli Ω. Drugim riječima, svako bojenje se nalazi u točno jednom od događaja A_M. Naime, za svako bojenje odgovarajući mnogokut je naprosto konveksna ljuska svih crvenih točaka iz S. Primijetimo da za svaki mnogokut M vrijedi $\mathbb{P}(A_M) = x^{a(M)}(1-x)^{b(M)}$ pa je doista

$$\sum_M x^{a(M)}(1-x)^{b(M)} = \sum_M \mathbb{P}(A_M) = \mathbb{P}(\Omega) = 1.$$

5. (*Zadatak prilagođen iz knjige [1]*) Neka su $v_1, v_2, \ldots, v_n \in \mathbb{R}^n$ takvi da je $\|v_i\| \le 1$, $i = 1, 2, \ldots, n$, pri čemu $\|\cdot\|$ označava euklidsku normu. Dokažite da za svake brojeve $p_1, p_2, \ldots, p_n \in [0,1]$ postoje $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n \in \{0,1\}$ takvi da vrijedi
$$\Big\| \sum_{i=1}^n \varepsilon_i v_i - \sum_{i=1}^n p_i v_i \Big\| \le \frac{\sqrt{n}}{2}.$$

Rješenje. Fiksirajmo koeficijente $p_1, \ldots, p_n$. Neka su $\epsilon_1, \ldots, \epsilon_n$ nezavisne slučajne varijable koje poprimaju vrijednosti u $\{0,1\}$ i čije razdiobe su dane sa
$$\mathbb{P}(\epsilon_i = 0) = 1 - p_i, \quad \mathbb{P}(\epsilon_i = 1) = p_i$$
za $i = 1, \ldots, n$. Promatramo slučajnu varijablu
$$X := \Big\| \sum_{i=1}^n \epsilon_i v_i - \sum_{i=1}^n p_i v_i \Big\|^2 = \sum_{i,j=1}^n (\epsilon_i - p_i)(\epsilon_j - p_j)\langle v_i, v_j \rangle,$$
pri čemu $\langle \cdot, \cdot \rangle$ označava standardni skalarni produkt. Primijetimo da je
$$\mathbb{E}(\epsilon_i - p_i) = (1-p_i)(0-p_i) + p_i(1-p_i) = 0$$
te
$$\mathbb{E}(\epsilon_i - p_i)^2 = (1-p_i)(0-p_i)^2 + p_i(1-p_i)^2 = p_i(1-p_i).$$
Nadalje, zbog nezavisnosti za $i \neq j$ imamo
$$\mathbb{E}(\epsilon_i - p_i)(\epsilon_j - p_j) = \mathbb{E}(\epsilon_i - p_i)\mathbb{E}(\epsilon_j - p_j) = 0.$$
Zato je
$$\mathbb{E}X = \sum_{i=1}^n \|v_i\|^2 \mathbb{E}(\epsilon_i - p_i)^2 \le \sum_{i=1}^n \underbrace{p_i(1-p_i)}_{\le 1/4} \le \frac{n}{4}.$$
Prema tome, postoji $\omega \in \Omega$ takav da za brojeve
$$\varepsilon_i := \epsilon_i(\omega) \in \{0,1\}$$

vrijedi

$$\Big\| \sum_{i=1}^{n} \varepsilon_i v_i - \sum_{i=1}^{n} p_i v_i \Big\|^2 = X(\omega) \leq \frac{n}{4},$$

što je trebalo dokazati.

Primijetimo da je ograda $\sqrt{n}/2$ optimalna za svaki prirodni broj n, jer se postiže kada su v_i vektori standardne ortonormirane baze od $\mathbb{R}^n$, a svi koeficijenti su $p_i = 1/2$. Zapravo, u tom slučaju nam svi izbori od ε_i daju istu vrijednost $\sqrt{n}/2$.

6. (*IMO Shortlist 1999. C4*) Neka je A neki skup od n ostataka modulo n^2. Pokažite da postoji skup B od n ostataka modulo n^2 takav da je barem pola ostataka modulo n^2 oblika $a+b$ za $a \in A$ i $b \in B$. (Napomenimo da se ostaci i zbrajaju modulo n^2.)

   Rješenje iz [3]. Nezavisno i uniformno biramo n ostataka modulo n^2, tj. preciznije, Ω je skup svih n-torki ostataka modulo n^2. Ako je B skup koji se sastoji od odabranih ostataka (koji se mogu i ponavljati), tada B ima najviše n elemenata, a ima smisla promatrati i slučajnu varijablu X koja je jednaka broju svih ostataka prikazivih u obliku $a+b$ za $a \in A$ i $b \in B$, tj. $X := \operatorname{card}(A+B)$.

   Za svaki ostatak i postoji točno n ostataka j takvih da je $i \in A+j \Leftrightarrow j \in i - A$. Zato je

$$\mathbb{P}(i \notin A+B) = \Big(\frac{n^2-n}{n^2}\Big)^n = \Big(1 - \frac{1}{n}\Big)^n$$

   pa imamo

$$\mathbb{P}(i \in A+B) = 1 - \Big(1 - \frac{1}{n}\Big)^n.$$

   Dakle,

$$\mathbb{E}X = \sum_i \mathbb{E}\mathbf{1}_{\{i \in A+B\}} = n^2\Big(1 - \Big(1 - \frac{1}{n}\Big)^n\Big) \geq n^2/2.$$

   Naime, $\big(1 - \frac{1}{n}\big)^n \leq \frac{1}{2}$ je ekvivalentno s $2^{-1/n} \geq 1 - \frac{1}{n}$, što pak slijedi iz poznate ocjene $e^x \geq 1 + x$ za $x \in \mathbb{R}$. Prema tome, moguće je odabrati n (ili manje) ostataka i okupiti ih u skup B s traženim svojstvom.

7. (*Iran, selekcijski test 2008. #6*) Na nekom turniru sudjeluje 799 natjecatelja i poznato je da svaka dva natjecatelja igraju točno jedan meč u kojem pobjeđuje jedan od njih. Dokažite da postoje skupovi A i B od po 7 natjecatelja takvi da je svaki natjecatelj iz A pobijedio svakog natjecatelja iz B.

   Rješenje iz [3]. Za svakog natjecatelja $j \in \{1, 2, \ldots, 799\}$ označimo s n_j broj natjecatelja koji su ga pobijedili. Neka je Ω kolekcija svih sedmočlanih skupova natjecatelja. Neka je X slučajna varijabla koja broji koliko natjecatelja su pobijedili svi članovi slučajno odabranog skupa, tj. za svaki $A \in \Omega$ definiramo

$$X(A) := \operatorname{card}\{j : \text{svaki član od } A \text{ je pobijedio } j\}.$$

Osim toga, za svakog natjecatelja j možemo definirati slučajnu varijablu

$$Y_j(A) := \begin{cases} 1 & \text{ako su svi članovi od } A \text{ pobijedili } j, \\ 0 & \text{inače.} \end{cases}$$

Očigledno je $X = \sum_{j=1}^{799} Y_j$ te $\mathbb{P}(Y_j = 1) = \binom{n_j}{7} / \binom{799}{7}$ pa je

$$\mathbb{E}Y_j = \binom{n_j}{7} \Big/ \binom{799}{7} \quad \text{i} \quad \mathbb{E}X = \sum_{j=1}^{799} \binom{n_j}{7} \Big/ \binom{799}{7}.$$

Kako znamo da je

$$\sum_{j=1}^{799} n_j = \text{broj mečeva} = \binom{799}{2}, \text{ tj. } \frac{1}{799} \sum_{j=1}^{799} n_j = 399,$$

zbog konveksnosti funkcije $\mathbb{N}_0 \to \mathbb{R}$, $x \mapsto \binom{x}{7}$ imamo

$$\frac{1}{799} \sum_{j=1}^{799} \binom{n_j}{7} \geq \binom{399}{7}.$$

(Za primjenu Jensenove nejednakosti bismo zapravo trebali imati konveksnu funkciju na $[0, +\infty\rangle$, no to se lako postigne tako da se funkcija na $\mathbb{N}_0$ linearno interpolira između susjednih cijelih brojeva.) Zato je

$$\mathbb{E}X \geq 799 \cdot \binom{399}{7} \Big/ \binom{799}{7} = 6.02549\ldots,$$

odakle zbog cjelobrojnosti slijedi da postoji sedmočlani skup A takav da je $X(A) \geq 7$ te za skup B sada naprosto treba uzeti nekih 7 natjecatelja koje su pobijedili svi natjecatelji iz A.

8. (*Erdős*) *Ramseyev broj* $R(k, k)$ je najmanji prirodni broj n takav da za svako bojenje bridova od K_n (tj. potpunog grafa s n vrhova) u dvije boje, crvenu i plavu, postoji k vrhova koji su povezani samo crvenom bojom ili postoji k vrhova koji su povezani samo plavom bojom. Moguće je pokazati da takav broj $R(k, k)$ uvijek postoji, ali može biti vrlo velik. Kao primjere je lako vidjeti $R(2, 2) = 2$ (trivijalno) i $R(3, 3) = 6$ (česti "zadačić" za osnovnu školu). Dokažite da za svaki $k \in \mathbb{N}$, $k \geq 4$ vrijedi $R(k, k) \geq 2^{k/2}$.

   Rješenje, prilagođeno iz knjige [1], poglavlje 1. Stavimo $n = \lfloor 2^{k/2} \rfloor$. Neka je Ω skup svih bojenja bridova od K_n u crvenu ili plavu boju. Dakle, $|\Omega| = 2^{\binom{n}{2}}$. Za fiksirani podskup S skupa vrhova označimo sa A_S događaj da su svi bridovi s krajevima u S istobojni. Ako je $|S| = k$, tada imamo

$$\mathbb{P}(A_S) = \frac{2 \cdot 2^{\binom{n}{2} - \binom{k}{2}}}{2^{\binom{n}{2}}} = 2^{1 - \binom{k}{2}}.$$

   Zato je vjerojatnost da se dogodio barem jedan od događaja A_S za neki k-člani skup vrhova S moguće ocijeniti:

$$\mathbb{P}\Big(\bigcup_{\substack{S \\ |S| = k}} A_S \Big) \leq \sum_{\substack{S \\ |S| = k}} \mathbb{P}(A_S) = \binom{n}{k} 2^{1 - \binom{k}{2}}.$$

Ukoliko još pokažemo $\binom{n}{k}2^{1-\binom{k}{2}} < 1$, tada će biti

$$\mathbb{P}\Big(\bigcap_{\substack{S \\ |S|=k}} A_S^c\Big) = \mathbb{P}\bigg(\Big(\bigcup_{\substack{S \\ |S|=k}} A_S\Big)^c\bigg) > 0$$

pa će postojati barem jedno bojenje za koje niti jedan podgraf određen skupom vrhova S takvim da je $|S| = k$ nema istobojne bridove. To će značiti $R(k,k) > n$, čime će biti dokazana tražena tvrdnja $R(k,k) \geq 2^{k/2}$.

Ocijenimo:

$$\begin{aligned} \binom{n}{k}2^{1-\binom{k}{2}} &= \frac{n(n-1)\cdots(n-k+1)}{k!}2^{1-\frac{k(k-1)}{2}} \\ &< \frac{n^k}{k!}2^{-\frac{k^2}{2}+\frac{k}{2}+1} = \frac{n^k}{2^{\frac{k^2}{2}}}\frac{2^{\frac{k}{2}+1}}{k!} < 1. \end{aligned}$$

Pritom smo koristili

$$n^k = \lfloor 2^{k/2} \rfloor^k \leq (2^{k/2})^k = 2^{k^2/2}$$

te nejednakost

$$k! \geq 2^{k/2+1}$$

za $k \in \mathbb{N}$, $k \geq 4$, koju je lako dokazati indukcijom.

9. (*Zadatak za vježbu iz knjige [1]*) Neka je (V, E) bipartitni graf s n vrhova i neka je svakom vrhu $v \in V$ pridružena konačna lista $S(v)$ od $|S(v)| > \log_2 n$ dozvoljenih boja. Dokažite da je moguće obojiti vrhove grafa (svaki u neku od njemu dozvoljenih boja) tako da nikoja dva istobojna vrha nisu spojena bridom.

   Rješenje. Neka je k najmanji prirodni broj strogo veći od $\log_2 n$, tj. $k = \lfloor \log_2 n \rfloor + 1$, tako da imamo $|S(v)| \geq k$ za svaki $v \in V$. Da je graf bipartitan znači da mu se skup vrhova V može particionirati u dva skupa V_1 i V_2 takva da svaki brid iz E ima jedan kraj u V_1, a drugi u V_2. Označimo sa $S := \bigcup_{v \in V} S(v)$ skup svih boja koje se pojavljuju u listama.

   Neka je $\Omega = \mathcal{P}(S)$, tj. sastoji se od svih podskupova skupa boja. Pretpostavljamo uniformnu vjerojatnost na Ω, što ima za posljedicu da se svaka boja $c \in S$ pojavljuje s vjerojatnosti $1/2$ u slučajno odabranom skupu $T \in \mathcal{P}(S)$ te s vjerojatnosti $1/2$ u njegovom komplementu T^c. Osim toga su događaji $\{T \in \Omega : c \in T\}$ međusobno nezavisni za različite $c \in S$. Nas zapravo zanimaju događaji

$$\begin{aligned} A_v &:= \{T \in \Omega \,:\, T \cap S(v) = \emptyset\} \quad \text{za } v \in V_1, \\ A_v &:= \{T \in \Omega \,:\, T^c \cap S(v) = \emptyset\} \quad \text{za } v \in V_2. \end{aligned}$$

   Primijetimo da za svaki $v \in V$ (neovisno je li u V_1 ili V_2) vrijedi

$$\mathbb{P}(A_v) = \frac{\text{broj podskupova od } S \setminus S(v)}{\text{broj podskupova od } S} = \frac{2^{|S \setminus S(v)|}}{2^{|S|}} = 2^{-|S(v)|} \leq 2^{-k} < \frac{1}{n}.$$

   Dakle,

$$\mathbb{P}\Big(\bigcup_{v \in V} A_v\Big) \leq \sum_{v \in V} \mathbb{P}(A_v) < n \cdot \frac{1}{n} = 1$$

pa je

$$\mathbb{P}\Big(\bigcap_{v\in V} A_v^c\Big) > 0.$$

Slijedi da postoji skup $T \in \Omega$ koji se ne nalazi niti u jednom od događaja A_v, $v \in V$. Za svaki vrh $v \in V_1$ imamo $T \cap S(v) \neq \emptyset$ pa v možemo obojiti u neku od boja iz T. S druge strane, za svaki $v \in V_2$ imamo $T^c \cap S(v) \neq \emptyset$ pa v možemo obojiti u neku od boja iz T^c. Dobiveno bojenje ne može kreirati bridove s istobojnim krajevima, naprosto jer su u V_1 korištene samo boje iz T, a u V_2 samo boje iz T^c.

Zadaci za samostalan rad

1. (*Zadatak iz knjige [1], poglavlje 15*) Neka je $n \geq 4$ prirodan broj. Dokažite da postoji bojenje bridova potpunog grafa K_n u dvije boje koje daje najviše $\binom{n}{4}/32$ jednobojnih kopija grafa K_4, tj. takvih podgrafova s četiri vrha da su svih 6 njihovih bridova iste boje.

   Rješenje. Za Ω uzmimo sva bojenja bridova od K_n u crvenu i plavu. U slučaju uniformne vjerojatnosti su obje boje jednako vjerojatne za svaki vrh te su bojenja vrhova međusobno nezavisna. Za svaki skup S od 4 vrha neka je A_S događaj da je pripadni podgraf (induciran sa S) jednobojan, tj. da su svi bridovi s krajevima iz S iste boje. Očigledno je $\mathbb{P}(A_S) = 2 \cdot (\frac{1}{2})^6 = 2^{-5}$. Nadalje, neka je N slučajna varijabla koja broji jednobojne kopije od K_4, tj. $N := \sum_{|S|=4} \mathbf{1}_{A_S}$. Kako imamo $\mathbb{E}N = \sum_{|S|=4} \mathbb{P}(A_S) = \binom{n}{4} \cdot 2^{-5}$, zaključujemo da postoji bojenje $\omega \in \Omega$ koje daje najviše $\binom{n}{4} \cdot 2^{-5}$ jednobojnih kopija od K_4.

2. (*Zadatak za vježbu iz knjige [1]*) Neka je $\{(A_i, B_i) : i = 1, 2, \ldots, m\}$ familija parova skupova cijelih brojeva takva da za svaki i vrijedi $|A_i| = k$, $|B_i| = \ell$, $A_i \cap B_i = \emptyset$ te da za svake $i \neq j$ vrijedi $(A_i \cap B_j) \cup (A_j \cap B_i) \neq \emptyset$. Dokažite $m \leq \frac{(k+\ell)^{k+\ell}}{k^k \ell^\ell}$.

   Rješenje. Stavimo $S := \bigcup_{i=1}^m (A_i \cup B_i)$. Za Ω uzmimo sve funkcije $f\colon S \to \{1, 2, \ldots, k+\ell\}$ i pretpostavimo uniformnu vjerojatnost. Promotrimo događaje

   $$C_i := \big\{ f \in \Omega \,:\, f(A_i) \subseteq \{1, \ldots, k\},\ f(B_i) \subseteq \{k+1, \ldots, k+\ell\} \big\}$$

   za $i = 1, 2, \ldots, m$. Obzirom da su A_i i B_i disjunktni, imamo

   $$\begin{aligned} \mathbb{P}(C_i) &= \frac{(\text{br. fja sa } A_i \text{ u } \{1,\ldots,k\})(\text{br. fja sa } B_i \text{ u } \{k+1,\ldots,k+\ell\})}{\text{broj funkcija sa } A_i \cup B_i \text{ u } \{1,\ldots,k+\ell\}} \\ &= \frac{k^k \ell^\ell}{(k+\ell)^{k+\ell}}. \end{aligned}$$

   Naime, broj odabira vrijednosti od f na $S \setminus (A_i \cup B_i)$ se pokrati kod prebrajanja. Tvrdimo da su ti događaji disjunktni. Naime, kad bi postojala $f \in C_i \cap C_j$ za neke $i \neq j$, tada bismo imali $f(A_i) \cap f(B_j) = \emptyset$ i $f(A_j) \cap f(B_i) = \emptyset$, što povlači $A_i \cap B_j = \emptyset$ i $A_j \cap B_i = \emptyset$, a to je u kontradikciji s pretpostavkom zadatka. Konačno, tražena nejednakost slijedi iz

$$1 \geq \mathbb{P}\Big(\bigcup_{i=1}^{m} C_i\Big) = \sum_{i=1}^{m} \mathbb{P}(C_i) = m \cdot \frac{k^k \ell^\ell}{(k+\ell)^{k+\ell}}.$$

3. (*Erdős*) *Hipergraf* je uređeni par (V, E) konačnog skupa vrhova V i familije E podskupova od V koje zovemo bridovi. Ako je (V, E) hipergraf u kojem svaki brid ima točno $n \geq 2$ vrhova i bridova ima $|E| \leq 2^{n-1}$, dokažite da se tada vrhovi V mogu obojiti u dvije boje tako da svaki brid sadrži vrhove obiju boja.

   Rješenje iz [4]. Neka Ω čine sva bojenja vrhova V u crvenu ili plavu boju. Uz pretpostavku uniforme vjerojatnosti je svaki vrh $v \in V$ obojen u crvenu ili plavu s vjerojatnostima $1/2$, a boje različitih vrhova su nezavisne. Neka slučajna varijabla N označava broj jednobojnih bridova iz E obzirom na promatrano slučajno bojenje.

$$\begin{aligned} \mathbb{E}N &= \sum_{e \in E} \mathbb{E}\mathbf{1}_{\{e \text{ je istobojan}\}} \\ &= \sum_{e \in E} \mathbb{P}(e \text{ je istobojan}) = \sum_{e \in E} 2 \cdot \Big(\frac{1}{2}\Big)^n = \frac{|E|}{2^{n-1}} \leq 1 \end{aligned}$$

   Dakle, $\mathbb{E}N \leq 1$. Razlikujemo dva slučaja.

   Slučaj 1. Ako je $P(N = 0) = 0$, tada je zapravo $N \geq 1$. Ako bi za neki $\omega \in \Omega$ bilo $N(\omega) > 1$, tada bismo imali $\mathbb{E}N > 1$, što bi bilo u kontradikciji s netom dobivenim $\mathbb{E}N \leq 1$. Dakle, N je identički jednaka 1, tj. svako bojenje daje točno jedan jednobojni brid. Ipak, to nije moguće. Naime, ako postoji samo jedan brid u E, tada je neka dva njegova vrha moguće različito obojiti pomoću nekog ω pa bi bilo $N(\omega) = 0$. Ako pak E sadrži barem dva brida, tada bi bojenje ω svih vrhova u crvenu dalo $N(\omega) = |E| \geq 2$. Kontradikcija.

   Slučaj 2. Neka je dakle $P(N = 0) > 0$. To znači da postoji bojenje ω takvo da je $N(\omega) = 0$, tj. bojenje koje ne daje niti jedan jednobojni brid.

4. (*Zadatak za vježbu iz knjige [1]*) Ako je (V, E) hipergraf takav da je $|V| = n$, $|E| = m \geq \frac{n}{3}$ i svaki brid sadrži točno 3 vrha, dokažite da postoji skup $S \subseteq V$ takav da je $|S| \geq \frac{2n^{3/2}}{3\sqrt{3m}}$ i da niti jedan brid iz E nije podskup skupa S.

   Rješenje. Neka prostor Ω čine svi podskupovi skupa vrhova, tj. $\Omega = \mathcal{P}(V)$. Ovog puta konstruiramo vjerojatnost tako da za svaki vrh v slučajni skup S sadrži v s vjerojatnosti p, tj. $\mathbb{P}(\{S \in \Omega : v \in S\}) = p$, te da su svi događaji $\{S \in \Omega : v \in S\}$, $v \in V$ međusobno nezavisni. (Dakle, bacanjem nesimetričnog novčića za svaki v odlučujemo hoćemo li ga staviti u S ili u S^c.) Parametar $p \in [0, 1]$ će biti odabran kasnije.

   Promotrimo slučajne varijable:

$$\begin{aligned} X &:= |S| = \text{broj odabranih vrhova}, \\ Y &:= |E \cap \mathcal{P}(S)| = \text{broj bridova koji su podskupovi od } S, \\ X_v &:= \mathbf{1}_{\{S \in \Omega : v \in S\}} \quad \text{za } v \in V, \\ Y_e &:= \mathbf{1}_{\{S \in \Omega : e \subseteq S\}} \quad \text{za } e \in E, \end{aligned}$$

tako da imamo $X = \sum_{v\in V} X_v$, $Y = \sum_{e\in E} Y_e$. Kako je $\mathbb{E}X_v = \mathbb{P}(\{S \in \Omega : v \in S\}) = p$ i $\mathbb{E}Y_e = \mathbb{P}(\{S \in \Omega : e \subseteq S\}) = p^{|e|} = p^3$, linearnost očekivanja daje $\mathbb{E}(X-Y) = np - mp^3$. Dakle, postoji skup $S \in \Omega$ takav da je $X(S) - Y(S) \geq np - mp^3$. Za svaki brid iz $E \cap \mathcal{P}(S)$ možemo odabrati jedan njegov vrh te ga izbaciti iz skupa S. Skup koji preostane imat će barem $np - mp^3$ vrhova i neće sadržavati (kao nadskup) niti jedan brid iz E.

Preostaje odabrati p tako da maksimizira funkciju $f\colon [0,1] \to \mathbb{R}$, $f(p) := np - mp^3$. Računanjem derivacije $f'(p) = n - 3mp^2$ lako nalazimo da se njen maksimum postiže u $p = \sqrt{\frac{n}{3m}}$, kada je $f(p) = np - mp^3 = \frac{2n^{3/2}}{3\sqrt{3m}}$.

5. (*Erdős*) Za svaki konačni skup $B \subseteq \mathbb{Z} \setminus \{0\}$ postoji podskup $A \subseteq B$ takav da je $|A| \geq \frac{|B|}{3}$ i da ne postoje $x, y, z \in A$ za koje bi vrijedilo $x + y = z$.

   Rješenje iz knjige [1], poglavlje 1. Fiksirajmo neki prosti broj $p = 3k + 2$ koji je veći od $2\max_{x\in B} |x|$. Promatrajmo skup B modulo p, tj. smatrajmo ga podskupom konačnog polja $\mathbb{Z}/p\mathbb{Z}$. Dovoljno je naći podskup A od B takav da je $|A| \geq |B|/3$ i da jednadžba $x + y = z$ (u $\mathbb{Z}/p\mathbb{Z}$, tj. modulo p) nema rješenja u skupu A.

   Uzmimo $\Omega = (\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}$ s uniformnom vjerojatnosti i neka je N slučajna varijabla definirana sa

$$N(a) := \text{broj elemenata od } aB \cap \{k+1, \ldots, 2k+1\}$$

   za svaki $a \in \Omega$. Imamo

$$\begin{aligned}\mathbb{E}N &= \sum_{b\in B} \mathbb{E}\mathbf{1}_{\{a\in\Omega\,:\,ab\in\{k+1,\ldots,2k+1\}\}} = \sum_{b\in B} \mathbb{E}\mathbf{1}_{\{a\in\Omega\,:\,a\in\{(k+1)b^{-1},\ldots,(2k+1)b^{-1}\}\}} \\ &= \sum_{b\in B} \frac{k+1}{3k+1} = |B| \cdot \frac{k+1}{3k+1} \geq \frac{|B|}{3}\end{aligned}$$

   pa postoji $a \in \mathbb{Z}/p\mathbb{Z}$, $a \neq 0$ takav da je $N(a) \geq |B|/3$, tj. da skup $aB \cap \{k+1, \ldots, 2k+1\}$ ima barem $|B|/3$ elemenata. Tada stavimo

$$A := B \cap \{a^{-1}(k+1), \ldots, a^{-1}(2k+1)\}.$$

   Kad bi postojali $x, y, z \in A$ takvi da je $x+y = z$, tada bi vrijedilo $ax+ay = az$, ali je i $ax, ay, az \in \{k+1, \ldots, 2k+1\}$, a zbroj modulo p nikoja dva broja iz $\{k+1, \ldots, 2k+1\}$ ne može upasti u taj isti skup. Dakle, A ima sva tražena svojstva.

6. (*Zadatak iz knjige [1], poglavlje 15*) Neka je $[a_{i,j}]_{1\leq i,j\leq n}$ matrica tipa $n \times n$ s elementima iz $[-1, 1]$. Dokažite da postoje $\varepsilon_1, \ldots, \varepsilon_n \in \{-1, 1\}$ takvi da vrijedi $\left|\sum_{j=1}^n \varepsilon_j a_{i,j}\right| \leq \sqrt{2n \ln(2n)}$ za sve $i = 1, \ldots, n$.

   Rješenje. Neka su $\epsilon_1, \ldots, \epsilon_n$ nezavisne slučajne varijable s vrijednostima u $\{-1, 1\}$ koje imaju simetričnu razdiobu, tj. $\mathbb{P}(\epsilon_i = -1) = \mathbb{P}(\epsilon_i = 1) = \frac{1}{2}$. Promatramo slučajne varijable $X_i := \sum_{j=1}^n \epsilon_j a_{i,j}$ za $i = 1, 2, \ldots, n$.

Označimo $\beta := \sqrt{2n\ln(2n)}$ i $\alpha := \beta/n$. Zbog nezavisnosti možemo računati

$$\begin{aligned}
\mathbb{E}e^{\alpha X_i} &= \mathbb{E}e^{\alpha\sum_{j=1}^n \varepsilon_j a_{i,j}} = \mathbb{E}\prod_{j=1}^n e^{\varepsilon_j\alpha a_{i,j}} = \prod_{j=1}^n \mathbb{E}e^{\varepsilon_j\alpha a_{i,j}} \\
&= \prod_{j=1}^n \big(\tfrac{1}{2}\cdot e^{\alpha a_{i,j}} + \tfrac{1}{2}\cdot e^{-\alpha a_{i,j}}\big) = \prod_{j=1}^n \operatorname{ch}(\alpha a_{i,j}) \\
&\le \prod_{j=1}^n e^{\alpha^2 a_{i,j}^2/2} \le \prod_{j=1}^n e^{\alpha^2/2} = e^{\frac{\alpha^2 n}{2}} = e^{\frac{\beta^2}{2n}}
\end{aligned}$$

(zapravo uz strogu nejednakost na barem jednom od gornja dva mjesta) te potom ocjenjujemo vjerojatnosti događaja $\{\omega\in\Omega : |X_i(\omega)| > \beta\}$ kao

$$\begin{aligned}
\mathbb{P}(|X_i| > \beta) &= 2\mathbb{P}(X_i > \beta) = 2\mathbb{P}(e^{\alpha X_i} > e^{\alpha\beta}) \\
&\le 2e^{-\alpha\beta}\mathbb{E}e^{\alpha X_i} < 2e^{-\frac{\beta^2}{n}}e^{\frac{\beta^2}{2n}} = 2e^{-\frac{\beta^2}{2n}}.
\end{aligned}$$

Ovdje smo koristili poznatu Markov-Čebiševljevu nejednakost koja kaže da za slučajnu varijablu Y i za $\gamma > 0$ vrijedi $\mathbb{P}(|Y| > \gamma) \le \gamma^{-1}\mathbb{E}|Y|$. Dakle,

$$\mathbb{P}\Big(\bigcup_{i=1}^n \{|X_i| > \beta\}\Big) \le \sum_{i=1}^n \mathbb{P}(|X_i| > \beta) < 2ne^{-\frac{\beta^2}{2n}} = 2ne^{-\ln(2n)} = 1.$$

Stoga imamo $\mathbb{P}\big(\bigcap_{i=1}^n\{|X_i| \le \beta\}\big) > 0$ pa postoji $\omega\in\Omega$ takav da je $|X_i(\omega)| \le \beta$ za $i = 1,\ldots,n$, što znači da brojevi $\varepsilon_i := \epsilon(\omega)$ zadovoljavaju nejednakosti iz zadatka.

Korištena literatura i dodatni izvori zadataka

[1] N. Alon, J. H. Spencer, *The Probabilistic Method*, Wiley-Interscience Series in Discrete Mathematics and Optimization, treće izdanje, John Wiley & Sons, Inc., 2008.

[2] L. K. Ho, *Probabilistic Method*, Mathematical Excalibur, **14**, no.3, 2009.

[3] P.-S. Loh, *Probabilistic Methods in Combinatorics*, 2009.

[4] A. Milošević, *Primjene vjerojatnosne metode na determinističke igre*, diplomski rad, PMF—Matematički odsjek, Sveučilište u Zagrebu, 2015.

2. Funkcije izvodnice

Funkcije izvodnice su korisno analitičko oruđe za proučavanje nizova, posebno onih koji dolaze iz raznih kombinatornih problema prebrojavanja. Kao što ćemo vidjeti, usko su povezane uz rekurzivne relacije, traženje zatvorenih formula te ispitivanje asimptotskog ponašanja.

Obična funkcija izvodnica (ili samo funkcija izvodnica) niza $(a_n)_{n=0}^{\infty}$ je red potencija

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

Eksponencijalna funkcija izvodnica niza $(a_n)_{n=0}^{\infty}$ je obična funkcija izvodnica od $\left(\frac{a_n}{n!}\right)_{n=0}^{\infty}$, tj.

$$E(x) := \sum_{n=0}^{\infty} a_n \frac{x^n}{n!}.$$

Ako niz $(a_n)_{n=0}^{\infty}$ raste "razumno brzo", tada su funkcije A i E dobro definirane na nekom intervalu $\langle -r, r\rangle$ makar za dovoljno mali $r > 0$ i ponekad se mogu izračunati eksplicitne formule za $A(x)$ i $E(x)$. "Razumno brzo" u slučaju obične funkcije izvodnice znači: ne brže od svakog geometrijskog niza. Posebno je fascinantno što u nekim slučajevima imamo vrlo lijepe formule za $A(x)$ ili $E(x)$ makar je teško (ili čak nemoguće) napisati zatvorenu formulu za a_n. Obratno, iz formule za $A(x)$ ili $E(x)$ se razvojem u red potencija (barem načelno) mogu iščitati koeficijenti te dobiti formula za a_n. Ako je $A(x) = \sum_{n=0}^{\infty} a_n x^n$, tada obratno pišemo

$$a_n = [x^n]A(x),$$

tj. $[x^n]A(x)$ nam označava koeficijent uz x^n u razvoju od $A(x)$.

Slijede neki poznati razvoji koji se mogu koristiti.

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots = \sum_{n=0}^{\infty} \frac{x^n}{n!}, \quad \text{za } x \in \mathbb{R}$$

$$\cos x = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} + \dots = \sum_{n=0}^{\infty} (-1)^n \frac{x^{2n}}{(2n)!}, \quad \text{za } x \in \mathbb{R}$$

$$\sin x = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \dots = \sum_{n=0}^{\infty} (-1)^n \frac{x^{2n+1}}{(2n+1)!}, \quad \text{za } x \in \mathbb{R}$$

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

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

$$\frac{1}{(1-x)^{k+1}} = \sum_{n=0}^{\infty} \binom{n+k}{k} x^n, \quad \text{za } |x| < 1,\ k \in \mathbb{N}_0$$

$$(1+x)^\alpha = 1 + \binom{\alpha}{1} x + \binom{\alpha}{2} x^2 + \dots = \sum_{n=0}^{\infty} \binom{\alpha}{n} x^n, \quad \text{za } |x| < 1,$$

$$\text{pri čemu je } \binom{\alpha}{n} = \frac{\alpha(\alpha-1)\cdots(\alpha-n+1)}{n!}$$

$$\ln(1+x) = \frac{x}{1} - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \ldots = \sum_{n=1}^{\infty} (-1)^{n-1} \frac{x^n}{n}, \quad \text{za } |x| < 1$$

$$\operatorname{arctg} x = \frac{x}{1} - \frac{x^3}{3} + \frac{x^5}{5} - \frac{x^7}{7} + \ldots = \sum_{n=0}^{\infty} (-1)^n \frac{x^{2n+1}}{2n+1}, \quad \text{za } |x| < 1$$

Zadaci

1. Koja je obična funkcija izvodnica niza zadanog formulom $a_n = n^2$? Koja je eksponencijalna funkcija izvodnica tog istog niza?

   Rješenje.

$$\begin{aligned} A(x) &= \sum_{n=0}^{\infty} n^2 x^n = x^2 \sum_{n=2}^{\infty} n(n-1)x^{n-2} + x \sum_{n=1}^{\infty} n x^{n-1} \\ &= x^2 \sum_{n=0}^{\infty} \underbrace{(n+2)(n+1)}_{2\binom{n+2}{2}} x^n + x \sum_{n=0}^{\infty} (n+1)x^n \\ &= \frac{2x^2}{(1-x)^3} + \frac{x}{(1-x)^2} = \frac{x(1+x)}{(1-x)^3} \end{aligned}$$

$$\begin{aligned} E(x) &= \sum_{n=0}^{\infty} n^2 \frac{x^n}{n!} = \sum_{n=1}^{\infty} \frac{n x^n}{(n-1)!} = \sum_{n=1}^{\infty} \frac{\big((n-1)+1\big)x^n}{(n-1)!} \\ &= \sum_{n=2}^{\infty} \frac{x^n}{(n-2)!} + \sum_{n=1}^{\infty} \frac{x^n}{(n-1)!} = x^2 \sum_{n=0}^{\infty} \frac{x^n}{n!} + x \sum_{n=0}^{\infty} \frac{x^n}{n!} = x(1+x)e^x. \end{aligned}$$

2. Koliko ima permutacija skupa $\{1, 2, \ldots, n\}$ koje imaju najviše jedan "pad"? Dakle, traži se broj permutacija $p_1, p_2, \ldots, p_n$ od $1, 2, \ldots, n$ takvih da vrijedi $p_1 < \cdots < p_k$ i $p_{k+1} < \ldots < p_n$ za neki indeks k.

   Rješenje. Označimo traženi broj s a_n. Očigledno je $a_1 = 1$, $a_2 = 2$. Kasnije ćemo vidjeti da je praktično staviti $a_0 = 1$.

   Svaka permutacija od $1, 2, \ldots, n, n+1$ s opisanim svojstvom je ili identiteta ili ima točno jedan pad. Uzmemo li neku permutaciju od $1, 2, \ldots, n, n+1$ s najviše jednim padom i uklonimo element $n+1$, dobit ćemo permutaciju od $1, 2, \ldots, n$ koja opet ima najviše jedan pad. Ako ta permutacija ima točno jedan pad, tada broj $n+1$ možemo staviti na dva dozvoljena načina. Ako je pak ta permutacija identiteta, tada broj $n+1$ možemo staviti bilo gdje, tj. na $n+1$ načina. Dobili smo

$$a_{n+1} = 2(a_n - 1) + n + 1,$$

   tj. rekurzivnu relaciju

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

   Pomnožimo rekurziju s x^{n+1} i prosumirajmo po $n \in \mathbb{N}_0$.

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

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

Označimo li funkciju izvodnicu s $A(x)$, dobili smo (zbog $a_0 = 1$):

$$A(x) - 1 = 2xA(x) - \frac{x(1-2x)}{(1-x)^2},$$

tj.

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

Rastav na parcijalne razlomke daje

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

te razvojem u red potencija dobivamo

$$A(x) = \sum_{n=0}^{\infty} 2^n x^n + \sum_{n=0}^{\infty} x^n - \sum_{n=0}^{\infty} (n+1) x^n = \sum_{n=0}^{\infty} (2^n - n)\, x^n.$$

Zato je konačno

$$a_n = [x^n]A(x) = 2^n - n.$$

3. Na koliko načina se novčanica od 10 kuna može razmijeniti u kovanice?

Rješenje. Pretvorimo sve iznose u lipe, kako bi bili cjelobrojni. Zapravo tražimo koeficijent uz x^{1000} u produktu

$$\begin{aligned} f(x) = {} & \underbrace{(1 + x + x^2 + x^3 + \cdots)}_{\text{kovanice od 1 lp}} \underbrace{(1 + x^2 + x^4 + x^6 + \cdots)}_{\text{kovanice od 2 lp}} \\ & \cdot \underbrace{(1 + x^5 + x^{10} + x^{15} + \cdots)}_{\text{kovanice od 5 lp}} \underbrace{(1 + x^{10} + x^{20} + x^{30} + \cdots)}_{\text{kovanice od 10 lp}} \\ & \cdot \underbrace{(1 + x^{20} + x^{40} + x^{60} + \cdots)}_{\text{kovanice od 20 lp}} \underbrace{(1 + x^{50} + x^{100} + x^{150} + \cdots)}_{\text{kovanice od 50 lp}} \\ & \cdot \underbrace{(1 + x^{100} + x^{200} + x^{300} + \cdots)}_{\text{kovanice od 1 kn}} \underbrace{(1 + x^{200} + x^{400} + x^{600} + \cdots)}_{\text{kovanice od 2 kn}} \\ & \cdot \underbrace{(1 + x^{500} + x^{1000} + x^{1500} + \cdots)}_{\text{kovanice od 5 kn}}, \end{aligned}$$

koji se izračuna kao

$$\begin{aligned} & (1-x)^{-1}(1-x^2)^{-1}(1-x^5)^{-1}(1-x^{10})^{-1}(1-x^{20})^{-1} \\ & \cdot (1-x^{50})^{-1}(1-x^{100})^{-1}(1-x^{200})^{-1}(1-x^{500})^{-1}. \end{aligned}$$

Ako želimo razviti $f(x)$ u red potencija do člana x^{1000}, možemo u Mathematici koristiti naredbu

$$\mathrm{Series}[f[x], \{x, 0, 1000\}]\,.$$

Ovdje "0" naprosto znači da se razvija oko nule, tj. u potencije $(x-0)^n = x^n$, što ćemo mi uvijek raditi. Očitavanje koeficijenta uz x^{1000} daje

$$[x^{1000}]f(x) = 327631321.$$

4. (*Rumunjska 2003.*) Koliko n-znamenkastih brojeva sa znamenkama iz skupa $\{2,3,7,9\}$ je djeljivo s 3?

Rješenje iz [1]. Koristit ćemo karakterizaciju da je broj djeljiv s 3 ako i samo ako je zbroj njegovih znamenaka djeljiv s 3.

Promotrimo funkciju izvodnicu

$$f(x) := (x^2 + x^3 + x^7 + x^9)^n.$$

Njen koeficijent uz x^m nam govori koliko ima n-znamenkastih brojeva sa znamenkama iz skupa $\{2,3,7,9\}$ čiji zbroj znamenaka je upravo m. Uzmimo sada $\omega = e^{2\pi i/3} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$, tj. ω je primitivni kompleksni treći korijen iz jedinice. Primijetimo da za $m \in \mathbb{Z}$ vrijedi

$$1 + \omega^m + \omega^{2m} = \begin{cases} 3 & \text{ako je } m \text{ djeljiv s } p, \\ \frac{1-\omega^{3m}}{1-\omega^m} = 0 & \text{ako } m \text{ nije djeljiv s } 3. \end{cases}$$

Pogledajmo čemu je jednako

$$\frac{1}{3}\big(f(1) + f(\omega) + f(\omega^2)\big).$$

Ako raspišemo $f(x) = \sum_{m=0}^{9n} a_m x^m$, prema gornjoj formuli to je

$$\sum_{m=0}^{9n} a_m \frac{1}{3}(1 + \omega^m + \omega^{2m}) = \sum_{\substack{0 \le m \le 9n \\ m \text{ je djeljiv s } 3}} a_m,$$

što je upravo traženi broj.

S druge pak strane, direktno uvrštavanje daje

$$\begin{aligned} &\frac{1}{3}\big(f(1) + f(\omega) + f(\omega^2)\big) \\ &= \frac{1}{3}\Big(4^n + (\omega^2 + \omega^3 + \omega^7 + \omega^9)^n + (\omega^4 + \omega^6 + \omega^{14} + \omega^{18})^n\Big) \\ &= \frac{1}{3}\Big(4^n + 2(\underbrace{2 + \omega + \omega^2}_{1+0=1})^n\Big) = \frac{4^n + 2}{3} \end{aligned}$$

i to je željeni rezultat.

5. (*IMO 1995. #6*) Neka je $p \geq 3$ prost broj. Nađite broj svih p-članih podskupova od $\{1, 2, \ldots, 2p-1, 2p\}$ čiji zbroj elemenata je djeljiv s p.

Rješenje iz knjige [4]. Promotrimo funkciju izvodnicu

$$f(x, y) := \prod_{j=1}^{2p} (xy^j - 1).$$

Za $y = 1$ odmah vidimo da $f(x, 1)$ do na predznak prebrojava sve podskupove od $\{1, \ldots, 2p\}$, ali zanimljivo je uvrstiti i druge vrijednosti za y.

Označimo $\omega = e^{2\pi i/p}$, tj. ω je primitivni kompleksni p-ti korijen iz jedinice. Primijetimo da za $m \in \mathbb{Z}$ vrijedi

$$\sum_{k=0}^{p-1} \omega^{km} = \begin{cases} p & \text{ako je } m \text{ djeljiv s } p, \\ \frac{1-\omega^{pm}}{1-\omega^n} = 0 & \text{ako } m \text{ nije djeljiv s } p. \end{cases}$$

Pogledajmo sada što prebraja funkcija izvodnica

$$\frac{1}{p}\sum_{k=0}^{p-1} f(x, \omega^k).$$

Njezin koeficijent uz x^p je

$$-\sum_{\substack{S\subseteq\{1,\ldots,2p\}\\|S|=p}} \frac{1}{p}\sum_{k=0}^{p-1} \omega^{k(\text{zbroj elemenata od } S)} = -\sum_{\substack{S\subseteq\{1,\ldots,2p\}\\|S|=p\\ \text{zbroj elemenata od } S \text{ je djeljiv s } p}} 1$$

pa nakon množenja sa -1 dobivamo upravo broj koji se traži u zadatku.

S druge strane, za $k \in \{1, 2, \ldots, p-1\}$ imamo da su $k, 2k, \ldots, (p-1)k$ modulo p naprosto ispermutirani ostaci $1, 2 \ldots, p-1$, što nam daje

$$\begin{aligned} f(x, \omega^k) &= \prod_{j=1}^{2p}(x\omega^{jk} - 1) = \Big(\prod_{j=0}^{p-1}(x\omega^j - 1)\Big)^2 \\ &= \Big(\omega^{p(p-1)/2}\prod_{j=0}^{p-1}(x - \omega^{-j})\Big)^2 = \Big(\prod_{j=0}^{p-1}(x - \omega^{-j})\Big)^2 = (x^p - 1)^2, \end{aligned}$$

pri čemu smo koristili faktorizaciju polinoma pomoću njegovih kompleksnih nultočaka. Dakle,

$$\frac{1}{p}\sum_{k=0}^{p-1} f(x, \omega^k) = \frac{1}{p}(x-1)^{2p} + \frac{p-1}{p}(x^p - 1)^2,$$

a koeficijent posljednje funkcije izvodnice uz x^n iznosi

$$-\frac{1}{p}\binom{2p}{p} + \frac{p-1}{p}\cdot(-2).$$

Slijedi da je traženi broj jednak

$$\frac{\binom{2p}{p} + 2p - 2}{p}.$$

6. (*Euler*) Dokažite da je broj rastava prirodnog broja na različite pribrojnike jednak broju rastava prirodnog broja na neparne pribrojnike.

   Rješenje. Označimo:

$$\begin{aligned} R_n &= \text{broj rastava od } n \text{ na različite pribrojnike}, \\ N_n &= \text{broj rastava od } n \text{ na neparne pribrojnike}. \end{aligned}$$

$$\sum_{n=0}^{\infty} R_n x^n = (1+x)(1+x^2)(1+x^3)\cdots = \prod_{k=1}^{\infty}(1+x^k) = \prod_{k=1}^{\infty} \frac{1-x^{2k}}{1-x^k}$$

$$= \frac{\prod_{k=1}^{\infty}(1-x^{2k})}{\prod_{k=1}^{\infty}(1-x^k)} = \frac{1}{\prod_{\substack{k\in\mathbb{N}\\ k \text{ neparan}}}(1-x^k)} = \prod_{\substack{k\in\mathbb{N}\\ k \text{ neparan}}} \frac{1}{1-x^k}$$

$$= \prod_{\substack{k\in\mathbb{N}\\ k \text{ neparan}}} (1+x^k+x^{2k}+x^{3k}+\cdots) = \sum_{n=0}^{\infty} N_n x^n$$

Izjednačavanjem koeficijenata slijedi $R_n = N_n$.

7. (*Zadatak iz knjige [5], poglavlje 2*) Neka je D_n broj permutacija skupa $\{1,2,\ldots,n\}$ bez fiksnih točaka, tj. takvih bijekcija

$$f\colon \{1,2,\ldots,n\} \to \{1,2,\ldots,n\}$$

da za svaki x vrijedi $f(x) \neq x$. Često se kaže da je D_n broj deranžmana n-članog skupa. Još stavljamo $D_0 := 1$. Najprije izvedite formulu za eksponencijalnu funkciju izvodnicu niza $(D_n)_{n=0}^{\infty}$, a potom dokažite formulu

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

Rješenje. Svaka permutacija od $\{1,2,\ldots,n\}$ fiksira nekih k elemenata te potom "deranžira" preostalih $n-k$ elemenata. Kako se k-člani podskup može odabrati na $\binom{n}{k}$ načina, dobili smo formulu

$$n! = \sum_{k=0}^{n} \binom{n}{k} D_{n-k}.$$

Množenjem s $\frac{x^n}{n!}$ i zbrajanjem dobivamo

$$\sum_{n=0}^{\infty} x^n = \sum_{n=0}^{\infty}\sum_{k=0}^{n} \frac{x^k}{k!}\frac{D_{n-k}x^{n-k}}{(n-k)!}.$$

Na desnoj strani možemo prepoznati produkt redova po principu "svaki sa svakim":

$$\underbrace{\Big(\sum_{k=0}^{\infty} \frac{x^k}{k!}\Big)}_{=e^x}\Big(\sum_{m=0}^{\infty} \frac{D_m x^m}{m!}\Big).$$

Označimo li eksponencijalnu funkciju izvodnicu niza s $D(x)$, dobili smo

$$\frac{1}{1-x} = e^x D(x), \qquad \text{tj. } D(x) = \frac{e^{-x}}{1-x}.$$

Razvijmo sada ponovno $D(x)$ u red.

$$D(x) = \Big(\sum_{k=0}^{\infty} \frac{(-1)^k x^k}{k!}\Big)\big(1+x+x^2+x^3+\cdots\big).$$

Uspoređivanje koeficijenata uz x^n daje

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

8. (*Zadatak iz knjige [5], poglavlje 1*) Neka je B_n broj particija skupa od n elemenata, tzv. Bellov broj. Tako je npr.

$$B_0 := 1,\ B_1 = 1,\ B_2 = 2,\ B_3 = 5,\ B_4 = 15,\ B_5 = 52.$$

Najprije izvedite formulu za eksponencijalnu funkciju izvodnicu tog niza, a potom dokažite formulu

$$B_n = \frac{1}{e} \sum_{k=0}^{\infty} \frac{k^n}{k!}.$$

Rješenje. Diskutiranjem u kojem članu particije se nalazi broj $n+1$ i označavajući s k broj preostalih elemenata u tom članu dobivamo rekurzivnu relaciju

$$B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k.$$

Množenjem s $\frac{x^n}{n!}$ i zbrajanjem dobivamo

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

Na lijevoj strani prepoznajemo derivaciju:

$$\frac{d}{dx} \sum_{n=0}^{\infty} B_n \frac{x^n}{n!} = \sum_{n=1}^{\infty} B_n \frac{x^{n-1}}{(n-1)!},$$

dok na desnoj prepoznajemo produkt redova po principu "svaki sa svakim":

$$\underbrace{\Big(\sum_{m=0}^{\infty} \frac{x^m}{m!} \Big)}_{=e^x} \Big(\sum_{k=0}^{\infty} B_k \frac{x^k}{k!} \Big).$$

Označimo li eksponencijalnu funkciju izvodnicu niza s $B(x)$, dobili smo

$$B'(x) = e^x B(x).$$

Sada rješavamo tu diferencijalmu jednadžbu:

$$\frac{d}{dx}(\ln B(x)) = \frac{B'(x)}{B(x)} = e^x$$

$$\ln B(x) = e^x + C$$

$$B(x) = e^{e^x + C}$$

Konstanta C se odredi iz

$$1 = B_0 = B(0) = e^{1+C}, \qquad \text{tj. } C = -1.$$

Dakle,

$$B(x) = e^{e^x - 1}.$$

Iskoristimo sada dvaput razvoj eksponencijalne funkcije u red:

$$B(x) = \frac{1}{e} e^{e^x} = \frac{1}{e} \sum_{k=0}^{\infty} \frac{e^{kx}}{k!} = \frac{1}{e} \sum_{k=0}^{\infty} \sum_{n=0}^{\infty} \frac{(kx)^n}{k!n!} = \frac{1}{e} \sum_{n=0}^{\infty} \Big(\sum_{k=0}^{\infty} \frac{k^n}{k!} \Big) \frac{x^n}{n!}.$$

Uspoređivanje koeficijenata s $B(x) = \sum_{n=0}^{\infty} B_n \frac{x^n}{n!}$ daje traženu formulu.

Asimptotika nizova

Često je potrebno ustanoviti asimptotsko ponašanje (npr. brzinu rasta) nekog kombinatorno dobivenog niza, a funkcije izvodnice mogu pomoći kod toga.

Kažemo da su nizovi $(a_n)_{n=0}^{\infty}$ i $(b_n)_{n=0}^{\infty}$ asimptotski jednaki i pišemo $a_n \sim b_n$ ako vrijedi

$$\lim_{n \to \infty} \frac{a_n}{b_n} = 1.$$

Naprimjer, poznata Stirlingova formula se može zapisati

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

Sljedeći teorem je samo malo neprecizan jer želimo izbjeći previše tehničke pojmove.

Teorem 1. *(Iz članka [3]; vidjeti knjigu [2], poglavlje 11) Neka je* $(a_n)_{n=0}^{\infty}$ *kombinatorno dobiveni niz i neka njegova obična funkcija izvodnica* $A(x) = \sum_{n=0}^{\infty} a_n x^n$ *konvergira na intervalu* $[-r, r\rangle$ *za neki* $r > 0$. *Pretpostavimo da je ona oblika* $A(x) = f(x)g(x) + h(x)$, *pri čemu vrijedi:*

- $f(x) = \big(- \ln(1 - \frac{x}{r}) \big)^b (1 - \frac{x}{r})^c, \quad c \notin \mathbb{N}$ *i nije baš* $b = c = 0$,
- *postoji limes* $L := \lim_{x \uparrow r} g(x) \in \mathbb{R} \setminus \{0\}$,
- *postoji limes* $\lim_{x \uparrow r} h(x) \in \mathbb{R}$.

Ako je $c \neq 0$, *tada vrijedi*

$$a_n \sim \frac{L (\ln n)^b (1/r)^n}{n^{c+1} \Gamma(-c)},$$

a ako je $c = 0$, *tada vrijedi*

$$a_n \sim \frac{b L (\ln n)^{b-1} (1/r)^n}{n}.$$

Ovdje Γ označava gama-funkciju. Obično je dovoljno znati da je $\Gamma(k) = (k-1)!$ za $k \in \mathbb{N}$ te $\Gamma(1/2) = \sqrt{\pi}$, $\Gamma(-1/2) = -2\sqrt{\pi}$, $\Gamma(3/2) = \sqrt{\pi}/2$. Primijetimo još da je $x = r$ prvi "singularitet" funkcije $A(x)$.

Zadaci

9. Ako je D_n broj permutacija n-članog skupa bez fiksnih točaka, dokažite

$$D_n \sim \frac{n!}{e}.$$

Rješenje. Funkcija izvodnica od $D_n/n!$ je

$$D(x) = (1-x)^{-1}e^{-x}$$

pa primjenjujemo teorem za $r = 1$, $b = 0$, $c = -1$, $g(x) = e^{-x}$, $h(x) = 0$,

$$L = \lim_{x\uparrow 1} e^{-x} = e^{-1}.$$

Dobivamo

$$\frac{D_n}{n!} \sim \frac{L\ 1^n}{n^0\ \Gamma(1)} = L = \frac{1}{e}.$$

Napomenimo da se isti zaključak može izvesti i iz opće formule niza:

$$\lim_{n\to\infty} \frac{D_n}{n!} = \lim_{n\to\infty} \sum_{k=0}^{n} \frac{(-1)^k}{k!} = \sum_{k=0}^{\infty} \frac{(-1)^k}{k!} = e^{-1}.$$

Osim toga, ovdje nije teško dokazati i precizniju tvrdnju: D_n je najbliži cijeli broj broju $n!/e$.

10. (*Primjer iz knjige [2], poglavlje 11*) Neka je C_n broj načina na koje se može izračunati izraz $a_1 * a_2 * \cdots * a_n$ (koji ima $n-1$ znakova $*$) ukoliko je važan poredak vršenja operacije $*$. Naime, zagradama možemo odrediti redoslijed izvšavanja pa je npr. $C_4 = 5$, jer su mogućnosti

$$a_1 * (a_2 * (a_3 * a_4)), \quad a_1 * ((a_2 * a_3) * a_4), \quad (a_1 * a_2) * (a_3 * a_4),$$
$$(a_1 * (a_2 * a_3)) * a_4, \quad ((a_1 * a_2) * a_3) * a_4.$$

To su tzv. Catalanovi brojevi (pomaknuti za 1) i stavljamo $C_0 = 0$. Izvedite izraz za običnu funkciju izvodnicu niza $(C_n)_{n=0}^{\infty}$ pa potom odredite njegovu asimptotiku.

Rješenje. U izrazu $a_1 * a_2 * \cdots * a_n$ promotrimo instancu od $*$ koja se izvršava posljednja. Neka lijevo od nje ima k varijabli i desno od nje $n-k$ varijabli. Dobivamo rekurzivnu relaciju

$$C_n = \sum_{k=1}^{n-1} C_k C_{n-k}.$$

Pomnožimo je s x^n i prosumirajmo po $n \geq 2$.

$$\sum_{n=2}^{\infty} C_n x^n = \sum_{n=2}^{\infty} \sum_{k=1}^{n-1} C_k x^k C_{n-k} x^{n-k} = \sum_{k,m=1}^{\infty} C_k x^k C_m x^m.$$

Označimo li funkciju izvodnicu $C(x) := \sum_{n=0}^{\infty} C_n x^n$, dobivamo (zbog $C_1 = 1$):

$$C(x) - x = C(x)^2,$$

a rješavanje kvadratne jednadžbe po $C(x)$ daje

$$C(x) = \frac{1 - \sqrt{1-4x}}{2}.$$

Kako funkciju izvodnicu možemo zapisati

$$C(x) = \Big(1 - \frac{x}{1/4}\Big)^{1/2}\Big(-\frac{1}{2}\Big) + \frac{1}{2},$$

možemo primijeniti prethodni teorem uz $r = 1/4$, $b = 0$, $c = 1/2$, $g(x) = -1/2$, $L = -1/2$, $h(x) = 1/2$ pa imamo

$$C_n \sim \frac{(-1/2)\ 4^n}{n^{3/2}\ \Gamma(-1/2)} = \frac{4^{n-1}}{\sqrt{\pi}\, n^{3/2}}.$$

To je tražena asimptotika niza.

Napomenimo da se razvojem od $C(x)$ u red može lako izvesti i poznata opća formula

$$C_n = \frac{1}{n}\binom{2n-2}{n-1}, \quad \text{za } n \in \mathbb{N}.$$

Zadaci za samostalan rad

1. Mea želi olimpijskoj ekipi podijeliti 20 jednakih čokolada. Ilko je postavio sljedeće uvjete na raspodjelu čokolada.

   - Adrian, Daniel i Erik mogu dobiti najviše po jednu čokoladu svaki.
   - Mislav i Petar moraju dobiti neparan broj čokolada.
   - Vlatka mora dobiti paran broj čokolada i to barem 2 čokolade.

   Na koliko načina Mea može podijeliti te čokolade?

   Rješenje. Tražimo koeficijent uz x^{20} nakon što se izmnoži produkt

   $$f(x) = (1+x)^3\Big(\sum_{k=0}^{\infty} x^{2k+1}\Big)^2\Big(\sum_{k=0}^{\infty} x^{2k+2}\Big).$$

   Izračunajmo zatvorenu formulu za $f(x)$.

   $$\begin{aligned} f(x) &= (1+x)^3x^4\Big(\sum_{k=0}^{\infty} x^{2k}\Big)^3 = (1+x)^3x^4\Big(\frac{1}{1-x^2}\Big)^3 \\ &= (1+x)^3x^4\frac{1}{(1-x)^3(1+x)^3} = \frac{x^4}{(1-x)^3}. \end{aligned}$$

   Nadalje, razvoj u red potencija koristeći jednu od standardnih formula daje

   $$f(x) = x^4\sum_{n=0}^{\infty}\binom{n+2}{2}x^n = \sum_{n=0}^{\infty}\frac{(n+2)(n+1)}{2}x^{n+4}.$$

   Član s potencijom x^{20} odgovara indeksu $n = 16$ pa možemo očitati koeficijent:

   $$[x^{20}]f(x) = \frac{18 \cdot 17}{2} = 153.$$

   Dakle, Mea može raspodijeliti čokolade na 153 načina.

2. (*Rezultat iz knjige [5], poglavlje 4*) Pretpostavimo da je skup nenegativnih cijelih brojeva particioniran na k beskonačnih aritmetičkih nizova s razlikama $d_1, d_2, \ldots, d_k$, pri čemu je $k \geq 2$ prirodan broj i $d_1 \geq d_2 \geq \ldots \geq d_k$. Dokažite da mora vrijediti $\sum_{j=1}^{k} \frac{1}{d_j} = 1$ i $d_1 = d_2$.

   Rješenje. Neka su aritmetički nizovi na koje je $\mathbb{N}_0$ rastavljen dani sa $(a_j + md_j)_{m=0}^{\infty}$, $j = 1, 2, \ldots, k$. Iz činjenice da oni particioniraju $\mathbb{N}_0$ slijedi

$$\sum_{n=0}^{\infty} x^n = \sum_{j=1}^{k} \sum_{m=0}^{\infty} x^{a_j + md_j},$$

   a sumiranje redova daje

$$\frac{1}{1-x} = \sum_{j=1}^{k} \frac{x^{a_j}}{1 - x^{d_j}}.$$

   Pomnožimo gornju jednakost s $1 - x$ i pustimo limes kada $x \to 1$. Zbog

$$\lim_{x \to 1} \frac{1-x}{1-x^{d_j}} = \lim_{x \to 1} \frac{1}{1 + x + x^2 + \cdots + x^{d_j - 1}} = \frac{1}{d_j}$$

   dobivamo

$$1 = \sum_{j=1}^{k} \frac{1}{d_j}.$$

   Zbog $k \geq 2$ mora biti $d_j \geq 2$ za svaki j. Pretpostavimo suprotno tvrdnji $d_1 = d_2$, da vrijedi $d_1 > d_2 \geq \ldots \geq d_k$. Rastavimo desnu stranu gornje jednakosti racionalnih funkcija na parcijalne razlomke nad poljem $\mathbb{C}$. Kod rastava od $\dfrac{x^{a_1}}{1 - x^{d_1}}$ se pojavljuje član $\dfrac{A}{x - e^{2\pi i/d_1}}$, $A \neq 0$, koji se ne pojavljuje na lijevoj strani, a ne može se ni pokratiti s drugim parcijalnim razlomcima na desnoj strani jer $e^{2\pi i/d_1}$ nije nultočka nijednog od polinoma $x^{d_j} - 1$, $j = 2, \ldots, k$. To je kontradikcija.

3. (*Primjer iz knjige [5], poglavlje 4*) Za cijeli broj $n \geq 0$ izračunajte

$$\sum_{k=0}^{n} \binom{n+k}{2k} 2^{n-k}.$$

   Rezultat zapišite kao zatvorenu formulu, bez suma i produkata.

   Rješenje. Označimo $a_n := \sum_{k=0}^{n} \binom{n+k}{2k} 2^{n-k}$ i neka je $A(x) = \sum_{n=0} a_n x^n$ funkcija izvodnica tog niza. Korištenjem standardnih formula za sume redova potencija možemo računati

$$\begin{aligned} A(x) &= \sum_{n=0}^{\infty} \sum_{k=0}^{n} \binom{n+k}{2k} 2^{n-k} x^n = \sum_{k=0}^{\infty} \sum_{n=k}^{\infty} \binom{n-k+2k}{2k} (2x)^{n-k} x^k \\ &= \sum_{k=0}^{\infty} x^k \sum_{n=0}^{\infty} \binom{n+2k}{2k} (2x)^n = \sum_{k=0}^{\infty} x^k \frac{1}{(1-2x)^{2k+1}} \\ &= \frac{1}{1-2x} \sum_{k=0}^{\infty} \left(\frac{x}{(1-2x)^2} \right)^k = \frac{1}{1-2x} \frac{1}{1 - \frac{x}{(1-2x)^2}} \end{aligned}$$

$$= \frac{1-2x}{1-5x+4x^2} = \frac{1-2x}{(1-x)(1-4x)}.$$

Rastav na parcijalne razlomke je

$$A(x) = \frac{1}{3} \cdot \frac{1}{1-x} + \frac{2}{3} \cdot \frac{1}{1-4x},$$

a potom razvijamo u red potencija koristeći standardne formule:

$$A(x) = \frac{1}{3}\sum_{n=0}^{\infty} x^n + \frac{2}{3}\sum_{n=0}^{\infty}(4x)^n = \sum_{n=0}^{\infty} \frac{2^{2n+1}+1}{3} x^n.$$

Uspoređivanje koeficijenata uz x^n daje

$$a_n = [x^n]A(x) = \frac{2^{2n+1}+1}{3}.$$

4. (*Primjer iz knjige [2], poglavlje 11*) Promotrimo izraz $0 \wedge 0 \wedge \cdots \wedge 0$, u kojem ima n nula i $n-1$ znakova potenciranja $\wedge$. Otprije znamo da se redoslijed izvršavanja operacija $\wedge$ može izvesti na C_n načina, pri čemu je C_n (pomaknuti) Catalanov broj. Neka je Z_n broj takvih evaluacija koje kao rezultat daju 0. Pritom smatramo da vrijedi: $0 \wedge 0 = 1$, $0 \wedge 1 = 0$, $1 \wedge 0 = 1$, $1 \wedge 1 = 1$. Dokažite da je $\lim\limits_{n\to\infty} \frac{Z_n}{C_n} = \frac{5-\sqrt{5}}{10}$.

   Napomena: Naprimjer, $Z_3 = 1$ jer je $(0 \wedge 0) \wedge 0 = 1 \wedge 0 = 1$ i $0 \wedge (0 \wedge 0) = 0 \wedge 1 = 0$.

   Rješenje. Praktično nam je staviti $Z_0 = 0$, a očigledno je $Z_1 = 1$. Svaka evaluacija koja daje vrijednost "0" mora biti oblika $A \wedge B$, pri čemu A predstavlja formulu s k nula koja se evaluira u 0, a B predstavlja formulu s $n-k$ nula koja se evaluira u 1. Na taj način dobivamo rekurzivnu relaciju

$$Z_n = \sum_{k=1}^{n-1} Z_k \left(C_{n-k} - Z_{n-k}\right).$$

   Pomnožimo je s x^n i prosumirajmo po $n \geq 2$.

$$\begin{aligned}\sum_{n=2}^{\infty} Z_n x^n &= \sum_{n=2}^{\infty}\sum_{k=1}^{n-1} Z_k x^k (C_{n-k} - Z_{n-k}) x^{n-k} \\ &= \Big(\sum_{k=1}^{\infty} Z_k x^k\Big)\Big(\sum_{m=1}^{\infty}(C_m - Z_m)x^m\Big)\end{aligned}$$

   Označimo sa $Z(x)$ funkciju izvodnicu od $(Z_n)_{n=0}^{\infty}$, a već prije smo s $C(x)$ označili funkciju izvodnicu niza $(C_n)_{n=0}^{\infty}$. Dobili smo kvadratnu jednadžbu po $Z(x)$,

$$Z(x) - x = Z(x)\big(C(x) - Z(x)\big),$$

   čije rješavanje daje

$$Z(x) = -\frac{1}{2}\big(1 - C(x)\big) + \frac{1}{2}\sqrt{\big(1 - C(x)\big)^2 + 4x}.$$

Odabrali smo pozitivni predznak ispred korijena jer mora biti $Z(0) = Z_0 = 0$.

Već smo bili izračunali

$$C(x) = \frac{1}{2} - \frac{1}{2}\sqrt{1-4x}.$$

"Prvi singularitet" funkcije $Z(x)$ je ili $r = \frac{1}{4}$ ili rješenje jednadžbe $\big(1 - C(x)\big)^2 + 4x = 0$. Posljednja jednadžba ima rješenje $x = -\frac{4}{9}$, ali je $\frac{4}{9} > \frac{1}{4}$ pa ostajemo kod $r = \frac{1}{4}$. Slutimo da se $Z(x)$ može prikazati u obliku

$$Z(x) = (1-4x)^{1/2} g(x) + Z(\tfrac{1}{4}).$$

Primijetimo da je

$$C(\tfrac{1}{4}) = \tfrac{1}{2}, \quad Z(\tfrac{1}{4}) = \tfrac{\sqrt{5}-1}{4}.$$

Trebamo izračunati

$$L = \lim_{x\uparrow 1/4} g(x) = \lim_{x\uparrow 1/4} \frac{Z(x) - Z(\frac{1}{4})}{(1-4x)^{1/2}}.$$

Supstitucijom

$$s = \sqrt{1-4x}, \quad x = (1-s^2)/4, \quad C(x) = (1-s)/2$$

taj limes postaje

$$\begin{aligned} L &= \lim_{s\downarrow 0} \frac{-(1+s)/2 + \sqrt{(1+s)^2/4 + (1-s^2)} - 2Z(\frac{1}{4})}{2s} \\ &= \lim_{s\downarrow 0} \frac{-s + \sqrt{5+2s-3s^2} - \sqrt{5}}{4s} = \lim_{s\downarrow 0} \frac{-s + \frac{2s-3s^2}{\sqrt{5+2s-3s^2}+\sqrt{5}}}{4s} \\ &= \lim_{s\downarrow 0} \frac{-1 + \frac{2-3s}{\sqrt{5+2s-3s^2}+\sqrt{5}}}{4} = \frac{-1+\frac{2}{2\sqrt{5}}}{4} = -\frac{5-\sqrt{5}}{20}. \end{aligned}$$

Konačno možemo primijeniti teorem o asimptotici nizova uz parametre

$$r = 1/4, \quad b = 0, \quad c = 1/2, \quad h(x) = Z(\tfrac{1}{4})$$

i dobiti

$$Z_n \sim \frac{L\, 4^n}{n^{3/2}\,\Gamma(-1/2)} = \frac{5-\sqrt{5}}{40} \frac{4^n}{n^{3/2}\sqrt{\pi}}.$$

Dijeljenje s formulom izvedenom na satu,

$$C_n \sim \frac{4^{n-1}}{n^{3/2}\sqrt{\pi}},$$

daje

$$\frac{Z_n}{C_n} \sim \frac{5-\sqrt{5}}{10}.$$

Korištena literatura i dodatni izvori zadataka

[1] Z. R. Abel, *Multivariate Generating Functions and Other Tidbits*, Mathematical reflections **2**, 2006.

[2] E. A. Bender, S. G. Williamson, *Foundations of Combinatorics with Applications*, Dover, 2006.

[3] P. Flajolet, A. Odlyzko, *Singularity Analysis of Generating Functions*, SIAM J. Disc. Math. **3** (1990), 216–240.

[4] Ž. Hanjš, *Međunarodne matematičke olimpijade*, treće izdanje, Element, Zagreb, 2000.

[5] H. S. Wilf, *generatingfunctionology*, A K Peters/CRC Press, treće izdanje, 2005.

3. Fourierova analiza

Fourierova analiza je posebno korisna kod kombinatornih problema koji se bave aritmetičkim strukturama, tj. kada uz same skupove promatramo i operaciju zbrajanja, a ponekad i operaciju množenja. Kako bismo izlaganje održali elementarnim, ovdje ćemo raditi samo na konačnim komutativnim grupama.

Za prirodni broj d označimo sa $\mathbb{Z}_d$ skup ostataka pri dijeljenju s d, tj.

$$\mathbb{Z}_d := \{0, 1, 2, 3, \ldots, d-2, d-1\}.$$

Neka se na skupu $\mathbb{Z}_d$ podrazumijevaju operacije zbrajanja i množenja modulo d, tj. nakon izvršenog zbrajanja ili množenja još podijelimo rezultat s d i uzmemo samo ostatak pri dijeljenju. Tako npr. na $\mathbb{Z}_4$ imamo tablice zbrajanja i množenja:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Fiksirajmo sada $n \in \mathbb{N}$ i $d_1, \ldots, d_n \in \mathbb{N} \setminus \{1\}$. Kada pišemo

$$\mathbb{A} = \mathbb{Z}_{d_1} \oplus \mathbb{Z}_{d_2} \oplus \cdots \oplus \mathbb{Z}_{d_n},$$

tada smatramo da je $\mathbb{A}$ Kartezijev produkt skupova $\mathbb{Z}_{d_1}, \ldots, \mathbb{Z}_{d_n}$ na kojem se promatra zbrajanje po koordinatama. Drugim riječima, elementi od $\mathbb{A}$ su n-torke $x = (x_1, x_2, \ldots, x_n)$ koje se zbrajaju kao:

$$(x_1, x_2, \ldots, x_n) + (y_1, y_2, \ldots, y_n) := (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n).$$

Često pišemo samo $\mathbf{0}$ umjesto n-torke samih nula, $(0, 0, \ldots, 0)$. Tako npr. operacija zbrajanja na $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ glasi:

+	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	(0,0)	(0,1)	(1,0)	(1,1)
(0,1)	(0,1)	(0,0)	(1,1)	(1,0)
(1,0)	(1,0)	(1,1)	(0,0)	(0,1)
(1,1)	(1,1)	(1,0)	(0,1)	(0,0)

Kažemo da je $(\mathbb{A}, +)$ primjer konačne komutativne grupe i (preciznije) da je $\mathbb{A}$ direktna suma konačno mnogo konačnih cikličkih grupa. Zapravo, svaka konačna komutativna grupa ima strukturu kao gornji primjer za određene parametre n i $d_1, \ldots, d_n$.

Definirajmo preslikavanje

$$E\colon \mathbb{A} \times \mathbb{A} \to \mathbb{C}, \quad E(x, \xi) := \big(e^{2\pi i/d_1}\big)^{x_1\xi_1} \big(e^{2\pi i/d_2}\big)^{x_2\xi_2} \cdots \big(e^{2\pi i/d_n}\big)^{x_n\xi_n}$$
$$\text{za } x = (x_1, x_2, \ldots, x_n),\ \xi = (\xi_1, \xi_2, \ldots, \xi_n) \text{ iz } \mathbb{A}.$$

Primijetimo da E poprima vrijednosti u kompleksnim brojevima modula 1. Jedini razlog zašto lijevi argument pišemo latiničnim slovom x, a desni grčkim slovom

ξ, je kako bismo naglasili da oni žive u dvije različite "kopije" od $\mathbb{A}$, povezane preslikavanjem E.

To preslikavanje ima sljedeća očigledna svojstva.

$$E(x+y,\xi) = E(x,\xi)E(y,\xi), \quad E(x,\xi+\zeta) = E(x,\xi)E(x,\zeta),$$

$$E(\mathbf{0},\xi) = 1, \quad E(x,\mathbf{0}) = 1, \quad E(-x,\xi) = \overline{E(x,\xi)}, \quad E(x,-\xi) = \overline{E(x,\xi)},$$

$$\sum_{x\in\mathbb{A}} E(x,\xi) = \begin{cases} |\mathbb{A}| & \text{ako je } \xi = \mathbf{0} \\ 0 & \text{ako je } \xi \neq \mathbf{0} \end{cases} \qquad \sum_{\xi\in\mathbb{A}} E(x,\xi) = \begin{cases} |\mathbb{A}| & \text{ako je } x = \mathbf{0} \\ 0 & \text{ako je } x \neq \mathbf{0} \end{cases}$$

Naprimjer, posljednja formula slijedi za $x = (x_1, x_2, \ldots, x_n)$, $\xi = (\xi_1, \xi_2, \ldots, \xi_n)$ iz jednakosti

$$\sum_{\xi\in\mathbb{A}} E(x,\xi) = \Big(\sum_{\xi_1=0}^{d_1-1} \big(e^{2\pi i x_1/d_1}\big)^{\xi_1} \Big) \cdots \Big(\sum_{\xi_n=0}^{d_n-1} \big(e^{2\pi i x_n/d_n}\big)^{\xi_n} \Big).$$

Preostaje primijetiti da za $x_j \neq 0$ vrijedi $e^{2\pi i x_j/d_j} \neq 1$ pa formula za parcijalnu sumu geometrijskog reda daje

$$\sum_{\xi_j=0}^{d_j-1} \big(e^{2\pi i x_j/d_j}\big)^{\xi_j} = \frac{1-e^{2\pi i x_j}}{1-e^{2\pi i x_j/d_j}} = \frac{1-1}{1-e^{2\pi i x_j/d_j}} = 0,$$

dok za $x_j = 0$ imamo

$$\sum_{\xi_j=0}^{d_j-1} \big(e^{2\pi i x_j/d_j}\big)^{\xi_j} = \sum_{\xi_j=0}^{d_j-1} 1 = d_j.$$

Produkt "preživi" samo kada je $x_1 = \cdots = x_n = 0$ i tada je jednak $d_1 \cdots d_n = |\mathbb{A}|$.

Zadaci

1. Koliko se najviše može odabrati međusobno okomitih "vektora" iz skupa $\{-1,1\}^{1024}$?

   Napomena: Vektori $u, v \in \mathbb{R}^n$, $u = (u_1, \ldots, u_n)$, $v = (v_1, \ldots, v_n)$ su okomiti ako i samo ako je njihov skalarni produkt jednak 0, tj. vrijedi $u \cdot v = \sum_{j=1}^{n} u_j v_j = 0$.

   Rješenje. U prostoru $\mathbb{R}^n$ može postojati najviše n u parovima okomitih nenul vektora. Zato će u našem zadatku odgovor biti 1024 ako još pronađemo primjer koji ima točno 1024 vektora.

   Promotrimo grupu $\mathbb{A} = \mathbb{Z}_2^{10} = \underbrace{\mathbb{Z}_2 \oplus \cdots \oplus \mathbb{Z}_2}_{10}$. Očigledno $\mathbb{A}$ ima $2^{10} = 1024$ elemenata. Za svaki $x \in \mathbb{A}$ promotrimo vektor

   $$v^x := \big(E(x,\xi) : \xi \in \mathbb{A}\big)$$

   duljine $|\mathbb{A}| = 1024$. Kako se u formuli za E sada pojavljuju samo drugi korijeni iz jedinice (tj. samo potencije od -1), zaključujemo da sve koordinate vektora pripadaju skupu $\{-1,1\}$. Iz svojstava od E se odmah vidi da su vektori v^x međusobno okomiti:

$$v^x \cdot v^y = \sum_{\xi\in\mathbb{A}} E(x,\xi)E(y,\xi) = \sum_{\xi\in\mathbb{A}} E(x,\xi)\overline{E(y,\xi)} = \sum_{\xi\in\mathbb{A}} E(x-y,\xi) = 0$$

ako je $x \neq y$.

Konačno možemo uvesti ključni pojam Fourierove analize. Fourierova transformacija funkcije $f\colon \mathbb{A}\to\mathbb{C}$ je nova funkcija $\hat{f}\colon \mathbb{A}\to\mathbb{C}$ definirana formulom

$$\hat{f}(\xi) := \sum_{x\in\mathbb{A}} f(x)E(x,\xi) \quad \text{za svaki } \xi\in\mathbb{A}.$$

Naprimjer:

(a) Ako je $\mathbb{A}=\mathbb{Z}_4$ i ako funkcije na $\mathbb{A}$ pišemo kao uređene četvorke

$$f = (f_0, f_1, f_2, f_3),$$

tada je

$$\hat{f} = \big(f_0+f_1+f_2+f_3,\ f_0+if_1-f_2-if_3,\ f_0-f_1+f_2-f_3,\ f_0-if_1-f_2+if_3\big).$$

(b) Ako je $\mathbb{A}=\mathbb{Z}_2\oplus\mathbb{Z}_2$ i ako funkcije na $\mathbb{A}$ pišemo kao uređene četvorke

$$f = (f_{00}, f_{01}, f_{10}, f_{11}),$$

tada je

$$\begin{aligned}\hat{f} = \big(&f_{00}+f_{01}+f_{10}+f_{11},\quad f_{00}-f_{01}+f_{10}-f_{11},\\ &f_{00}+f_{01}-f_{10}-f_{11},\quad f_{00}-f_{01}-f_{10}+f_{11}\big).\end{aligned}$$

Neka svojstva Fourierove transformacije su dana u sljedećem teoremu.

Teorem 2. *(a) Vrijedi sljedeća formula inverzije:*

$$\sum_{\xi\in\mathbb{A}} \hat{f}(\xi)\overline{E(x,\xi)} \;=\; |\mathbb{A}|f(x) \quad \textit{za svaki } x\in\mathbb{A}.$$

Njom se polazna funkcija f može rekonstruirati iz svoje Fourierove transformacije.
Posebno, Fourierova transformacija je injektivna, tj. $\hat{f}=\hat{g}$ implicira $f=g$.

(b) Vrijedi Plancherelov identitet:

$$\sum_{\xi\in\mathbb{A}} |\hat{f}(\xi)|^2 \;=\; |\mathbb{A}|\sum_{x\in\mathbb{A}} |f(x)|^2$$

i općenitije:

$$\sum_{\xi\in\mathbb{A}} \hat{f}(\xi)\overline{\hat{g}(\xi)} \;=\; |\mathbb{A}|\sum_{x\in\mathbb{A}} f(x)\overline{g(x)}.$$

(c) Ako je funkcija h definirana kao tzv. konvolucija od f i g,

$$h(x) := \sum_{y\in\mathbb{A}} f(x-y)g(y) \quad \textit{za svaki } x \in \mathbb{A},$$

što pišemo $h = f * g$, tada vrijedi

$$\hat{h}(\xi) = \hat{f}(\xi)\hat{g}(\xi) \quad \textit{za svaki } \xi \in \mathbb{A}.$$

Drugim riječima, Fourierova transformacija prevodi konvoluciju u obični produkt.

(d) Fourierova transformacija je linearna, tj.

$$\widehat{\alpha f + \beta g} = \alpha\hat{f} + \beta\hat{g}.$$

Dokaz. (a)

$$\begin{aligned}\sum_{\xi\in\mathbb{A}} \hat{f}(\xi)\overline{E(x,\xi)} &= \sum_{\xi\in\mathbb{A}}\sum_{y\in\mathbb{A}} f(y)E(y,\xi)\overline{E(x,\xi)} \\ &= \sum_{y\in\mathbb{A}} f(y) \sum_{\xi\in\mathbb{A}} E(y-x,\xi) = |\mathbb{A}|f(x)\end{aligned}$$

(b)

$$\begin{aligned}\sum_{\xi\in\mathbb{A}} \hat{f}(\xi)\overline{\hat{g}(\xi)} &= \sum_{\xi\in\mathbb{A}}\sum_{x,y\in\mathbb{A}} f(x)\overline{g(y)}E(x,\xi)\overline{E(y,\xi)} \\ &= \sum_{x,y\in\mathbb{A}} f(x)\overline{g(y)}\sum_{\xi\in\mathbb{A}} E(x-y,\xi) = |\mathbb{A}|\sum_{x\in\mathbb{A}} f(x)\overline{g(x)}\end{aligned}$$

(c)

$$\begin{aligned}\hat{h}(\xi) &= \sum_{x\in\mathbb{A}}\Big(\sum_{y\in\mathbb{A}} f(x-y)g(y)\Big)E(x,\xi) \\ &= \sum_{x,y\in\mathbb{A}} f(x-y)E(x-y,\xi)\ g(y)E(y,\xi) \\ &= \sum_{z,y\in\mathbb{A}} f(z)E(z,\xi)\ g(y)E(y,\xi) \\ &= \Big(\sum_{z\in\mathbb{A}} f(z)E(z,\xi)\Big)\Big(\sum_{y\in\mathbb{A}} g(y)E(y,\xi)\Big) = \hat{f}(\xi)\hat{g}(\xi)\end{aligned}$$

(d)

$$\begin{aligned}(\widehat{\alpha f + \beta g})(\xi) &= \sum_{x\in\mathbb{A}}\big(\alpha f(x) + \beta g(x)\big)E(x,\xi) \\ &= \alpha\sum_{x\in\mathbb{A}} f(x)E(x,\xi) + \beta\sum_{x\in\mathbb{A}} g(x)E(x,\xi) \\ &= \alpha\hat{f}(\xi) + \beta\hat{g}(\xi)\end{aligned}$$

□

Zadaci

2. (*Bourgain, preuzet iz knjige [2], poglavlje 4*) Neka je p prost broj i $S \subseteq \{1, 2, 3, \ldots, p-1\}$ takav da je $|S| > p^{3/4}$. Dokažite da za svaki cijeli broj m postoje $a_1, a_2, b_1, b_2, c_1, c_2 \in S$ takvi da vrijedi

$$m \equiv a_1 a_2 + b_1 b_2 + c_1 c_2 \pmod{p}.$$

Rješenje. Prisjetimo se da je $\mathbb{Z}_p$ zapravo polje, tj. svaki $s \in \mathbb{Z}_p \setminus \{0\}$ ima inverzni (tj. recipročni) element s^{-1}. U kompaktnijoj skupovnoj notaciji želimo dokazati

$$\mathbb{Z}_p = A \cdot A + A \cdot A + A \cdot A.$$

Promotrimo funkciju $f\colon \mathbb{Z}_p \to \mathbb{C}$, $f := \sum_{s\in S} \chi_{s\cdot S}$, gdje χ označava karakterističnu funkciju skupa. Naprije primijetimo da je

$$\begin{aligned}(f * f * f)(x) &= \sum_{\substack{a,b,c\in\mathbb{Z}_p\\ a+b+c=x}} f(a)f(b)f(c) = \sum_{\substack{a_1,b_1,c_1\in S\\ a,b,c\in\mathbb{Z}_p\\ a+b+c=x}} \chi_{a_1\cdot S}(a)\,\chi_{b_1\cdot S}(b)\,\chi_{c_1\cdot S}(c)\\ &= \sum_{\substack{a_1,b_1,c_1\in S\\ a_2,b_2,c_2\in S\\ a_1a_2+b_1b_2+c_1c_2=x}} 1 \;=\; \text{broj traženih prikaza od } x\end{aligned}$$

pa zapravo trebamo dokazati da je $(f * f * f)(x) > 0$ za svaki $x \in \mathbb{Z}_p$.

Fourierova transformacija od f je

$$\hat{f}(\xi) = \sum_{s\in S}\sum_{x\in\mathbb{Z}_p} \chi_{sS}(x) e^{2\pi i x\xi/p} = [x = sy] = \sum_{s\in S}\sum_{y\in S} e^{2\pi i s y\xi/p} = \sum_{s\in S} \hat{\chi}_S(s\xi).$$

Imamo $\hat{f}(\xi) = |S|^2$. Za $\xi \neq 0$ su elementi $s\xi$ svi međusobno različiti kako s varira pa aritmetičko-kvadratna nejednakost i Plancherelov identitet daju

$$\begin{aligned}|\hat{f}(\xi)| &\leq |S|^{1/2}\Big(\sum_{s\in S} |\hat{\chi}_S(s\xi)|^2\Big)^{1/2} \leq |S|^{1/2}\Big(\sum_{\xi\in\mathbb{Z}_p} |\hat{\chi}_S(\xi)|^2\Big)^{1/2}\\ &= |S|^{1/2}\Big(p\sum_{x\in\mathbb{Z}_p} |\chi_S(x)|^2\Big)^{1/2} = |S|^{1/2}p^{1/2}|S|^{1/2} = p^{1/2}|S|.\end{aligned}$$

Zbog nejednakosti Minkowskog imamo

$$\begin{aligned}\Big(\sum_{\xi\in\mathbb{Z}_p} |\hat{f}(\xi)|^2\Big)^{1/2} &\leq \sum_{s\in S}\Big(\sum_{\xi\in\mathbb{Z}_p} |\hat{\chi}_{sS}(\xi)|^2\Big)^{1/2}\\ &= \sum_{s\in S} p^{1/2}\Big(\sum_{x\in\mathbb{Z}_p} |\chi_{sS}(x)|^2\Big)^{1/2} = |S|p^{1/2}|S|^{1/2} = p^{1/2}|S|^{3/2}.\end{aligned}$$

Konačno, zbog $(f * f * f)\hat{}(\xi) = \hat{f}(\xi)^3$ i formule inverzije imamo

$$(f * f * f)(x) = \mathrm{Re}(f * f * f)(x) = \frac{1}{p}\mathrm{Re}\sum_{\xi\in\mathbb{Z}_p} \hat{f}(\xi)^3 e^{-2\pi i x\xi/p}$$

$$
\begin{aligned}
&\geq \frac{1}{p}\hat{f}(0)^3 - \frac{1}{p}\sum_{\xi\in\mathbb{Z}_p\setminus\{0\}} |\hat{f}(\xi)|^3 \\
&\geq p^{-1}|S|^6 - p^{-1}p^{1/2}|S|\sum_{\xi\in\mathbb{Z}_p} |\hat{f}(\xi)|^2 \\
&\geq p^{-1}|S|^6 - p^{-1/2}|S|p|S|^3 = p^{-1}|S|^6 - p^{1/2}|S|^4 \\
&= p^{-1}|S|^4\big(|S|^2 - p^{3/2}\big) > 0.
\end{aligned}
$$

Naime, po pretpostavci zadatka je $|S| > p^{3/4}$, tj. $|S|^2 > p^{3/2}$.

Princip neodređenosti

Za funkciju $f\colon \mathbb{A} \to \mathbb{C}$ na konačnoj abelovoj grupi $\mathbb{A}$ označimo

$$
\begin{aligned}
\operatorname{supp}(f) &:= \{x \in \mathbb{A} : f(x) \neq 0\}, \\
\operatorname{supp}(\hat{f}) &:= \{\xi \in \mathbb{A} : \hat{f}(\xi) \neq 0\}.
\end{aligned}
$$

Kratica "supp" dolazi od engleske riječi "support" koja se na hrvatski prevodi kao "nosač" funkcije.

Teorem 3. (Princip neodređenosti; *iz članka [1]*)

(a) Za svaku funkciju $f\colon \mathbb{A} \to \mathbb{C}$ koja nije identički jednaka konstanti 0 vrijedi

$$|\operatorname{supp}(f)|\,|\operatorname{supp}(\hat{f})| \geq |\mathbb{A}|.$$

(b) Za svaku funkciju $f\colon \mathbb{Z}_p \to \mathbb{C}$, gdje je p prost broj, koja nije identički jednaka konstanti 0 vrijedi

$$|\operatorname{supp}(f)| + |\operatorname{supp}(\hat{f})| \geq p + 1.$$

Obratno, za svake skupove $A, B \subseteq \mathbb{Z}_p$ koji zadovoljavaju $|A| + |B| \geq p + 1$ postoji funkcija $f\colon \mathbb{Z}_p \to \mathbb{C}$ takva da je $\operatorname{supp}(f) = A$ i $\operatorname{supp}(\hat{f}) = B$.

Zadaci

3. Dokažite (a) dio principa neodređenosti. (Dokaz (b) dijela je puno teži i nije sasvim elementaran.)

   Rješenje. Korištenjem nejednakosti trokuta, Cauchy-Schwarz nejednakosti i Plancherelovog identiteta dobivamo

$$
\begin{aligned}
\sup_{\xi\in\mathbb{A}} |\hat{f}(\xi)| = \sup_{\xi\in\mathbb{A}} \Big|\sum_{x\in\mathbb{A}} f(x)E(x,\xi)\Big| &\leq \sum_{x\in\mathbb{A}} |f(x)| = \sum_{x\in\operatorname{supp}(f)} |f(x)| \\
&\leq \Big(\sum_{x\in\operatorname{supp}(f)} 1^2\Big)^{1/2}\Big(\sum_{x\in\operatorname{supp}(f)} |f(x)|^2\Big)^{1/2} \\
&= |\operatorname{supp}(f)|^{1/2}\Big(\sum_{x\in\mathbb{A}} |f(x)|^2\Big)^{1/2}
\end{aligned}
$$

$$
\begin{aligned}
&= |\operatorname{supp}(f)|^{1/2}\Big(|\mathbb{A}|^{-1}\sum_{\xi\in\mathbb{A}}|\hat{f}(\xi)|^2\Big)^{1/2} \\
&= |\mathbb{A}|^{-1/2}|\operatorname{supp}(f)|^{1/2}\Big(\sum_{\xi\in\operatorname{supp}(\hat{f})}|\hat{f}(\xi)|^2\Big)^{1/2} \\
&\le |\mathbb{A}|^{-1/2}|\operatorname{supp}(f)|^{1/2}|\operatorname{supp}(\hat{f})|^{1/2}\sup_{\xi\in\mathbb{A}}|\hat{f}(\xi)|.
\end{aligned}
$$

Ako f nije identički jednaka 0, tada ni $\hat{f}$ nije identički jednaka 0 pa je $\sup_{\xi\in\mathbb{A}}|\hat{f}(\xi)| > 0$. Dijeljenjem s tim faktorom dobivamo traženu nejednakost.

4. (*Rezultat iz članka [1].*) Neka je p prost broj i neka je $S := \{z \in \mathbb{C} : z^p = 1\}$ skup p-tih korijena iz jedinice. Nadalje, neka su $c_0, c_1, c_2, \ldots, c_{p-1} \in \mathbb{C}$, među kojima je točno $k \ge 1$ brojeva različito od 0. Dokažite da je moguće odabrati podskup $T \subseteq S$ koji ima $|T| = p - k + 1$ elemenata i takav je da za svaki $z \in T$ vrijedi $\sum_{j=0}^{p-1} c_j z^j \neq 0$.

   Rješenje. Promotrimo funkciju

$$f\colon \mathbb{Z}_p \to \mathbb{C}, \qquad f(x) := \sum_{j=0}^{p-1} c_j (e^{-2\pi i x/p})^j.$$

   Zapravo trebamo dokazati da postoji barem $p - k + 1$ različitih $x \in \mathbb{Z}_p$ takvih da je $f(x) \neq 0$, tj. trebamo pokazati $|\operatorname{supp}(f)| \ge p - k + 1$.

   Primijetimo da je

$$\hat{f}(\xi) = \sum_{x\in\mathbb{Z}_p}\Big(\sum_{j\in\mathbb{Z}_p} c_j e^{-2\pi i x j/p}\Big) e^{2\pi i x\xi/p} = \sum_{j\in\mathbb{Z}_p} c_j \sum_{x\in\mathbb{Z}_p} e^{2\pi i x(\xi-j)/p} = p\, c_\xi.$$

   Po pretpostavci zadatka je točno k od brojeva $\hat{f}(0), \hat{f}(1), \ldots, \hat{f}(p-1)$ različito od 0, tj. $|\operatorname{supp}(\hat{f})| = k$. Po (b) dijelu principa neodređenosti imamo

$$|\operatorname{supp}(f)| \ge p + 1 - |\operatorname{supp}(\hat{f})| = p - k + 1.$$

5. (*Cauchy-Davenportov teorem*) Ako je p prost broj i ako su $A, B \subseteq \mathbb{Z}_p$ neprazni, dokažite da tada vrijedi

$$|A + B| \ge \min\big\{|A| + |B| - 1,\, p\big\}.$$

   Pritom, kao i obično, označavamo

$$A + B := \{a + b \,:\, a \in A,\, b \in B\}.$$

   Rješenje iz članka [1]. Najprije tvrdimo da možemo naći skupove $X, Y \subseteq \mathbb{Z}_p$ takve da je

$$|X| = p + 1 - |A|, \quad |Y| = p + 1 - |B|, \quad |X \cap Y| = \max\big\{|X| + |Y| - p,\, 1\big\}.$$

   Razlikujemo dva slučaja.

(1°) Ako je $|A|+|B| \leq p+1$, tada možemo uzeti

$$X=\{0,1,\ldots,p-|A|\}, \quad Y=\{|B|-1,|B|,\ldots,p-1\}.$$

(2°) Ako je $|A|+|B| > p+1$, tada možemo uzeti

$$X=\{0,1,\ldots,p-|A|\}, \quad Y=\{p-|A|,p-|A|+1,\ldots,2p-|A|-|B|\}.$$

Prema (b) dijelu principa neodređenosti postoje funkcije $f,g\colon \mathbb{Z}_p \to \mathbb{C}$ takve da je

$$\operatorname{supp}(f)=A, \quad \operatorname{supp}(\hat{f})=X, \quad \operatorname{supp}(g)=B, \quad \operatorname{supp}(\hat{g})=Y.$$

Promotrimo funkciju $f*g$. Iz definicije konvolucije

$$(f*g)(x) := \sum_{y\in\mathbb{Z}_p} f(x-y)g(y)$$

se odmah vidi

$$\operatorname{supp}(f*g) \subseteq \operatorname{supp}(f)+\operatorname{supp}(g)=A+B,$$

dok iz svojstva

$$(\widehat{f*g})(\xi)=\hat{f}(\xi)\hat{g}(\xi)$$

slijedi

$$\operatorname{supp}(\widehat{f*g})=\operatorname{supp}(\hat{f})\cap\operatorname{supp}(\hat{g})=X\cap Y.$$

Konačno, korištenjem (b) dijela principa neodređenosti dobivamo

$$|A+B|+|X\cap Y|=\big|\operatorname{supp}(f*g)\big|+\big|\operatorname{supp}(\widehat{f*g})\big| \geq p+1,$$

što je upravo

$$|A+B| \geq p+1-\max\big\{p+2-|A|-|B|,\, 1\big\}=\min\big\{|A|+|B|-1,\, p\big\}.$$

Zadaci za samostalan rad

1. Neka je n prirodan broj. Označimo s $\mathcal{P}_n$ familiju svih 2^n podskupova skupa $\{1,2,\ldots,n\}$. Za svaki $S\in\mathcal{P}_n$ dan je realni broj a_S i pretpostavimo da je točno $k\geq 1$ od tih brojeva a_S različito od 0. Dokažite da jednadžba

$$\sum_{S\in\mathcal{P}_n} a_S \prod_{j\in S} x_j = 0$$

ima najviše $\frac{2^n(k-1)}{k}$ rješenja u skupu $\{-1,1\}^n$, tj. ima najviše toliko n-torki $(x_1,x_2,\ldots,x_n)$ koje zadovoljavaju jednadžbu i za svaki indeks j je ili $x_j=-1$ ili $x_j=1$.

Napomena: Za $S=\emptyset$ produkt $\prod_{j\in S} x_j$ uvijek interpretiramo kao broj 1. Naprimjer, za $n=2$ jednadžba glasi

$$a_\emptyset + a_{\{1\}}x_1 + a_{\{2\}}x_2 + a_{\{1,2\}}x_1x_2 = 0.$$

Rješenje. Promotrimo grupu

$$\mathbb{A} = \mathbb{Z}_2^n = \underbrace{\mathbb{Z}_2 \oplus \cdots \oplus \mathbb{Z}_2}_{n} = \{0,1\}^n$$

i uspostavimo bijektivnu korespondenciju

$$\mathcal{P}_n \to \mathbb{A}, \qquad S \mapsto \text{karakteristična funkcija skupa } S$$

s inverzom

$$\mathbb{A} \to \mathcal{P}_n, \qquad (z_1, \ldots, z_n) \mapsto \{j \in \{1, 2, \ldots, n\} : z_j = 1\}.$$

Dakle, skupu $S \in \mathcal{P}_n$ odgovara n-torka $z = (z_1, \ldots, z_n)$ takva da je $z_j = 1$ za $j \in S$ i $z_j = 0$ za $j \in S^c$. Tada umjesto a_S pišemo a_z.

Definiramo funkciju $f\colon \mathbb{A} \to \mathbb{C}$,

$$f(y_1, \ldots, y_n) := \sum_{S \in \mathcal{P}_n} a_S \prod_{j \in S} (-1)^{y_j} = \sum_{z=(z_1,\ldots,z_n) \in \mathbb{A}} a_z \prod_{j=1}^{n} (-1)^{y_j z_j},$$

tj.

$$f(y) := \sum_{z \in \mathbb{A}} a_z\, E(y, z).$$

Primijetimo da zapravo želimo pobrojati rješenja $(y_1, \ldots, y_n) \in \mathbb{A}$ jednadžbe $f(y_1, \ldots, y_n) = 0$. Trebamo dokazati da je $|\operatorname{supp}(f)| \geq \frac{2^n}{k}$, jer će tada broj rješenja biti najviše $2^n - \frac{2^n}{k}$.

Zbog $E(y, z) \in \{-1, 1\} \subset \mathbb{R}$ imamo

$$\hat{f}(\xi) = \sum_{y \in \mathbb{A}} \Big(\sum_{z \in \mathbb{A}} a_z \overline{E(y, z)} \Big) E(y, \xi) = \sum_{z \in \mathbb{A}} a_z \sum_{y \in \mathbb{A}} E(y, \xi - z) = 2^n a_\xi.$$

Po pretpostavci zadatka je $|\operatorname{supp}(\hat{f})| = k$. Zato (a) dio principa neodređenosti primijenjen na grupu $\mathbb{A}$ daje

$$|\operatorname{supp}(f)| \geq \frac{|\mathbb{A}|}{|\operatorname{supp}(\hat{f})|} = \frac{2^n}{k}.$$

Korištena literatura i dodatni izvori zadataka

[1] T. Tao, *An uncertainty principle for cyclic groups of prime order*, Math. Res. Lett. **12** (2005), 121–127.

[2] T. Tao, V. Vu, *Additive Combinatorics*, Cambridge University Press, 2006.