UNIVERZA NA PRIMORSKEM
FAKULTETA ZA MATEMATIKO, NARAVOSLOVJE IN
INFORMACIJSKE TEHNOLOGIJE

Zaključna naloga

# Verjetnostna metoda

(The probabilistic method)

Ime in priimek: Neja Skočir
Študijski program: Matematika
Mentor: izr. prof. dr. Marko Orel

**Koper, avgust 2018**

# Ključna dokumentacijska informacija

Ime in PRIIMEK: Neja SKOČIR

Naslov zaključne naloge: Verjetnostna metoda

Kraj: Koper

Leto: 2018

Število listov: 38 Število referenc: 9

Mentor: izr. prof. dr. Marko Orel

Ključne besede: kombinatorika, verjetnostna metoda

**Izvleček:**
Zaključna naloga zajema nekaj osnov verjetnostne metode. Metoda je predstavljena tako, da je njena uporaba prikazana na več primerih iz različnih matematičnih področjih. V nalogi je predstavljenih tudi nekaj različnih načinov te metode. Prikazana je osnovna ideja metode, uporaba linearnosti pričakovane vrednosti, metoda prvega momenta, metoda drugega momenta in metoda eksponentnega momenta. Na koncu je opisan še Lovászov lokalni lema. Vsak izmed teh načinov je predstavljen preko vsaj enega primera.

# Key words documentation

Name and SURNAME: Neja SKOČIR

Title of final project paper: The probabilistic method

Place: Koper

Year: 2018

Number of pages: 38 Number of references: 9

Mentor: Assoc. Prof. Marko Orel, PhD

Keywords: combinatorics, probabilistic method

**Abstract:**
The final project paper covers some of the basics of the probabilistic method. The method is presented with examples from different areas of mathematics. Some of the approaches of the probabilistic method are also presented in this paper. Some applications of the basic method, the linearity of the expectation, the first moment method, the second moment method and the exponential moment method and the Lovász local lemma are included. Each of this approaches is presented with at least one example.

# Zahvala

Najprej bi se rada zahvalila mentorju dr. Marku Orlu za predlagano temo in pomoč med pisanjem zaključne naloge. Hvala, da ste mi bili vedno na voljo za vsako vprašanje in nasvet.
Zahvalila bi se tudi vsem profesorjem in asistentom, s katerimi sem se srečala skozi celoten študij.

Mama, hvala, da me imaš rada, da si mi vedno ob strani in da me vedno podpiraš na vsakem koraku. Tata, hvala za dano strast do reševanja logičnih in matematičnih problemov.
Hvala Roliju ter bratoma Niku in Maju, da ste vedno potiho verjeli vame.
Vesna in Igor, hvala, da sta poskrbela za Ario, ko sem v zadnjem letu obiskovala predavanja in bila ob tem brez skrbi vedoč, da je v dobrih rokah.
Hvala nonotom in nonam za spodbujanje in oporo v študijskih letih.
Hvala prijateljem in vsem sošolkam za lepo preživete študijske dni in za posojene zapiske, še posebej hvala prijateljici Sari. Kim in Nina hvala, da ste mi bile vedno ob strani, ko sem vaju najbolj potrebovala.

Posebna zahvala gre pa moji družini.
Miha, hvala, da lahko vedno računam nate, da me podpiraš in verjameš vame, da si moj najboljši prijatelj, partner in najboljši tatko najinima otrokoma.
Aria, hvala, ker si mi polepšala že skoraj dve leti in ker mi narišeš vsako jutro nasmeh na obraz in me vsak dan učiš biti boljša oseba. Hvala ti, da si mi pokazala, kaj je brezpogojna ljubezen in hvala, da si me naučila, da če si nekaj zares močno želiš, lahko s trudom tudi dosežeš.
Na koncu pa bi se rada zahvalila še moji mali štručki, ki je trenutno še samo moja in me med pisanjem zaključne naloge veselo brca v trebuščku in mi daje motivacijo, da diplomiram. Komaj čakam, da se jeseni tudi spoznava.

Hvala vsem, saj mi brez vas in vaše podpore to in še marsikaj drugega ne bi uspelo.

# Kazalo vsebine

**1 Uvod** **1**

**2 Osnovna metoda** **2**
2.1 Ramseyeva števila . . . . . 2
2.2 Barvanje hipergrafa . . . . . 4
2.3 Erdős-Ko-Radov izrek . . . . . 4

**3 Linearnost pričakovane vrednosti** **6**
3.1 Osnovni pojmi . . . . . 6
3.1.1 Hamiltonske poti v turnirju . . . . . 7
3.2 Brégmanov izrek . . . . . 8

**4 Metoda prvega momenta** **18**
4.1 Množice brez vsot . . . . . 19

**5 Metoda drugega momenta** **21**

**6 Metoda eksponentnega momenta** **24**

**7 Lovászov lokalni lema** **28**
7.1 Barvanje hipergrafa in lokalni lema . . . . . 30

**8 Zaključek** **31**

**9 Literatura** **32**

# Seznam kratic

*oz.* oziroma
*tj.* to je
*npr.* na primer

# 1 Uvod

Verjetnostna metoda je eno izmed najbolj močnih in široko uporabnih orodij v številnih matematičnih področjih, vendar jo najpogosteje srečamo v kombinatoriki. Je tehnika za dokazovanje obstoja kombinatoričnih objektov z določenimi lastnostmi. Zasnovana je na verjetnosti, uporablja pa se jo za dokazovanje izrekov, ki so popolnoma nepovezani z verjetnostjo.

Osnovno verjetnostno metodo lahko opišemo na sledeč način. Želimo dokazati obstoj kombinatoričnega objekta z določenimi lastnostmi. Včasih je konstruktivni dokaz lahko zelo težak. Zato skonstruiramo primeren verjetnostni prostor, izberemo en slučajen oz. na slepo izbran objekt in pokažemo, da je verjetnost, da ima željene lastnosti, strogo pozitivna. V tem primeru vemo, da tak objekt obstaja, saj bi bila v nasprotnem primeru verjetnost nična.

Verjetnostno metodo je prvi uporabil oz. vpeljal znan madžarski matematik Paul Erdős, ki je prispeval tako veliko k razvoju verjetnostne metode, da jo nekateri poimenujejo kar ≫Erdőseva metoda≪.

V nalogi si bomo najprej ogledali nekaj osnovnih primerov uporabe verjetnostne metode, ki je predstavljena v drugem poglavju. V tretjem poglavju je predstavljenih nekaj primerov z uporabo linearnosti pričakovane vrednosti. V nadaljnih poglavjih so predstavljene metoda prvega momenta, metoda drugega momenta in metoda eksponentnega momenta. V šestem poglavju pa je predstavljen še Lovászov lokalni lema in en primer njegove uporabe.

# 2 Osnovna metoda

## 2.1 Ramseyeva števila

**Definicija 2.1.** *Klika* v grafu je množica paroma sosednjih točk. *Neodvisna množica* v grafu je množica paroma nesosednjih točk.

Ramseyev izrek pravi, da vsak dovolj velik graf vsebuje ali kliko ali neodvisno množico določene, v naprej podane velikosti.

**Definicija 2.2.** Naj bosta $k, l \geq 2$ dve naravni števili. *Ramseyevo število* $R(k,l)$ je podano kot

$$R(k,l) = min\ \{n \in \mathbb{N}\text{: poljuben graf na } n \text{ vozliščih vsebuje kliko velikosti } k \text{ ali neodvisno množico velikosti } l\}.$$

Ramseyev izrek pove, da je za poljubni števili $k$ in $l$ Ramseyevo število $R(k,l)$ končno. Za nekatere majhne vrednosti $k$ in $l$ so vrednosti $R(k,l)$ znane, večina vrednosti $R(k,l)$ pa ni poznanih [5]. S pomočjo verjetnostne metode lahko dokažemo zanimivo spodnjo mejo za diagonalna Ramseyeva števila $R(k,k)$.

**Lema 2.3.** *Naj bo $k \geq 3$. Tedaj je*

$$\frac{2^{1+\frac{k}{2}}}{k!} < 1.$$

*Dokaz.* Uporabimo indukcijo na $k$. Za $k = 3$ velja

$$\frac{2^{1+\frac{k}{2}}}{k!} = \frac{2^{1+\frac{3}{2}}}{3!} = \frac{4 \cdot \sqrt{2}}{6} < 1.$$

Predpostavimo, da velja $\frac{2^{1+\frac{k}{2}}}{k!} < 1$, za nek $k \geq 3$. Tedaj je

$$\frac{2^{1+\frac{k+1}{2}}}{(k+1)!} = \frac{2^{1+\frac{k}{2}}}{k!} \cdot \frac{2^{\frac{1}{2}}}{k+1} < 1.$$

□

**Trditev 2.4.** *Za vsak $k \geq 3$ velja*

$$R(k,k) > 2^{k/2}.$$

*Dokaz.* Pokazali bomo, da za $n \leq 2^{k/2}$ obstaja graf na $n$ točkah, ki nima niti klike niti neodvisne množice velikosti $k$.
Naj bo graf $G$ poljuben slučajen graf na $n$ točkah, kjer je $n \leq 2^{k/2}$, pri čemer vsaka povezava obstaja z verjetnostjo $\frac{1}{2}$, neodvisno od ostalih povezav. Če izmed $n$ vozlišč našega grafa izberemo $k$ vozlišč, potem bo teh $k$ vozlišč tvorilo kliko velikosti $k$ natanko tedaj, ko bo med njimi vseh $\binom{k}{2}$ povezav. Verjetnost takega dogodka je enaka $(\frac{1}{2})^{\binom{k}{2}} = 2^{-\binom{k}{2}}$. Omenjenih $k$ vozlišč lahko izberemo na $\binom{n}{k}$ načinov.
Če z $A$ označimo dogodek, da graf $G$ vsebuje kliko velikosti $k$, potem velja

$$P(A) \leq \binom{n}{k} 2^{-\binom{k}{2}}.$$

Podobno vidimo, da velja tudi

$$P(B) \leq \binom{n}{k} 2^{-\binom{k}{2}},$$

kjer smo z $B$ označili dogodek, da graf G vsebuje neodvisno množico velikosti $k$. Ker je $n \leq 2^{k/2}$, sledi

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

Po lemi 2.3 vemo

$$\frac{2^{1+\frac{k}{2}}}{k!} < 1.$$

Unija dogodkov $A$ in $B$ je ravno dogodek, da graf $G$ vsebuje kliko velikosti $k$ ali neodvisno množico velikosti $k$.
Zato

$$\begin{aligned}P(A \cup B) = P(A) + P(B) - P(A \cap B) \leq P(A) + P(B) \\ \leq 2\binom{n}{k} 2^{-\binom{k}{2}} = \binom{n}{k} 2^{1-\binom{k}{2}} < 1.\end{aligned}$$

Torej je $P(A \cup B) < 1$ in verjetnost nasprotnega dogodka pozitivna. Zato za vsak $n \leq 2^{\frac{k}{2}}$ obstaja tak graf na $n$ točkah, ki ne vsebuje niti klike niti neodvisne množice velikosti $k$. □

Dokaz trditve 2.4 je povzet iz gradiva [4]. S tem primerom smo nakazali uporabo verjetnostne metode. Ta primer je prvi predstavil Paul Erdős leta 1947 v članku [3].

## 2.2 Barvanje hipergrafa

**Definicija 2.5.** *Hipergraf* je par $(V, E)$, kjer je $V$ končna množica točk in $E$ množica hiperpovezav oz. družina podmnožic množice $V$.

**Definicija 2.6.** Hipergraf je *$n$-uniformen*, če ima vsak element množice $E$ moč $n$.

**Definicija 2.7.** Hipergraf je 2-*obarvljiv*, če obstaja tako barvanje točk oz. vozlišč, da nobena hiperpovezava ni monokromatska.

Trditev 2.8 je leta 1963 prvi dokazal Erdős v članku [2].

**Trditev 2.8.** *Naj bo $m(n)$ najmanjše število hiperpovezav v $n$-uniformnem hipergrafu, ki ni* 2-*obarvljiv. Tedaj velja*

$$m(n) \geq 2^{n-1}.$$

*Dokaz.* Naj bo $H = (V, E)$ $n$-uniformen hipergraf z manj kot $2^{n-1}$ hiperpovezavami. Pobarvajmo vsako točko naključno v modro ali rdečo z verjetnostjo $\frac{1}{2}$ neodvisno od ostalih točk. Za vsako hiperpovezavo $e \in E$ naj bo $A_e$ dogodek, da je $e$ monokromatska. Ker je v hiperpovezavi n točk, je verjetnost, da je cela hiperpovezava rdeča, enaka $\left(\frac{1}{2}\right)^n$. Podobno je verjetnost, da je hiperpovezava modra, enaka $\left(\frac{1}{2}\right)^n$. Zato je

$$P(A_e) = 2 \cdot (\tfrac{1}{2})^n = 2^{1-n}.$$

Ker dogodki niso nujno disjunktni, lahko uporabimo neenakost

$$P\left(\bigcup_{e \in E} A_e\right) \leq \sum_{e \in E} P(A_e) = |E| \cdot 2^{1-n} < 2^{n-1} \cdot 2^{1-n} = 1.$$

Verjetnost, da je kakšna hiperpovezava monokromatksa, je manjša od 1. Zato obstaja vsaj eno tako barvanje, da bo graf 2-obarvljiv. □

Dokaz trditve 2.8 smo povzeli iz knjige [1].

## 2.3 Erdős-Ko-Radov izrek

**Definicija 2.9.** Družina množic $\mathcal{F}$ je *presečna*, če za vsaki množici $A$, $B \in \mathcal{F}$ velja $A \cap B \neq \emptyset$.

Dokaz leme 2.10 in izreka 2.11 smo povzeli iz gradiv [1] in [4].

**Lema 2.10.** *Naj bo $X = \{0, 1, \ldots, n-1\}$ za $n \geq 2k$ in naj bo $\mathcal{F}$ presečna družina podmnožic množice $X$, ki so moči $k$. Za $0 \leq s \leq n-1$ naj bo $A_s = \{s, s+1, \ldots, s+k-1\} \subseteq X$, kjer je seštevanje potrebno razumeti po modulu $n$. Potem $\mathcal{F}$ vsebuje največ $k$ množic izmed množic $A_0, A_1, \ldots, A_{n-1}$.*

*Dokaz.* Naj bo $A_i = \{i, i+1, \ldots, i+k-1\} \in \mathcal{F}$ fiksna množica, kjer je $0 \leq i \leq n-1$. Vse ostale množice $A_s$, ki presekajo $A_i$ so: $A_{i-k+1}, \ldots, A_{i-1}, A_{i+1}, \ldots, A_{i+k-1}$. Te lahko razdelimo v pare oblike $(A_{i-j}, A_{i-j+k})$, kjer $1 \leq j \leq k-1$. Ker je vseh $A_s$ množic, ki presekajo $A_i$, $2k-2$, je vseh parov $k-1$. Predstavniki teh parov so med seboj disjunktni. S tem smo dokazali lemo, saj lahko $\mathcal{F}$ vsebuje največ enega predstavnika iz vsakega para. □

**Izrek 2.11. (Erdős-Ko-Radov izrek)** *Naj bo $n \geq 2k$, $|X| = n$ in naj bo $\mathcal{F}$ presečna družina podmnožic množice $X$, ki imajo vse moč $k$. Potem je*

$$|\mathcal{F}| \leq \tbinom{n-1}{k-1}.$$

*Dokaz.* Predpostavimo lahko, da je $X = \{0, \ldots, n-1\}$.
Naj bosta permutacija $\sigma : X \to X$ in $s \in \{0, \ldots, n-1\}$ izbrana na slepo in neodvisno. Naj bo $A_s = \{\sigma(s), \sigma(s+1), \ldots, \sigma(s+k-1)\} \subseteq X$, kjer seštevanje razumemo po modulu $n$. Če je $\sigma_0 : X \to X$ poljubna permutacija, tedaj iz leme 2.10 sledi

$$P(A_s \in \mathcal{F} | \sigma = \sigma_0) \leq \frac{k}{n}$$

in zato

$$P(A_s \in \mathcal{F}) = \sum_{\sigma_0 \in S_X} P(A_s \in \mathcal{F} | \sigma = \sigma_0) P(\sigma = \sigma_0) \leq \frac{k}{n} \sum_{\sigma_0 \in S_X} P(\sigma = \sigma_0) = \frac{k}{n}.$$

Pri tem smo s $S_X$ označili množico vseh permutacij množice $X$.
Ker je $A_s$ na slepo izbrana med vsemi $\binom{n}{k}$ podmnožicami, ki imajo moč $k$, sledi

$$P(A_s \in \mathcal{F}) = \frac{|\mathcal{F}|}{\binom{n}{k}}.$$

Posledično je

$$\frac{|\mathcal{F}|}{\binom{n}{k}} \leq \frac{k}{n}$$

in zato

$$|\mathcal{F}| \leq \frac{k}{n}\binom{n}{k} = \binom{n-1}{k-1}.$$

□

# 3 Linearnost pričakovane vrednosti

## 3.1 Osnovni pojmi

**Definicija 3.1.** *Pričakovana vrednost ali matematično upanje* slučajne spremenljivke $X$, definirane na verjetnostnem prostoru $(\Omega, \mathcal{M}, P)$, je definirana z Lebesgue-ovim integralom

$$E(X) = \int_\Omega X(\omega) dP(\omega).$$

Pri tem bomo vseskozi tiho predpostavljali, da je bodisi $X$ nenegativna slučajna spremenljivka bodisi $X \in L^1(\Omega, \mathcal{M}, P)$.

**Lema 3.2.** *Naj bodo $X_1, \ldots, X_n$ slučajne spremenljivke in $c_1, \ldots, c_n$ realna števila. Če je $X = c_1X_1 + \cdots + c_nX_n$, potem velja*

$$E(X) = c_1E(X_1) + \cdots + c_nE(X_n).$$

*Dokaz.* Iz lastnosti Lebesgue-ovega integrala sledi

$$\begin{aligned} E(c_1X_1 + \cdots + c_nX_n) &= \int_\Omega (c_1X_1 + \cdots + c_nX_n) dP \\ &= \int_\Omega c_1X_1 dP + \cdots + \int_\Omega c_nX_n dP \\ &= c_1 \int_\Omega X_1 dP + \cdots + c_n \int_\Omega X_n \\ &= c_1E(X_1) + \cdots + c_nE(X_n). \end{aligned}$$

□

**Definicija 3.3.** *Karakteristična slučajna spremenljivka* dogodka $A$ je podana s predpisom

$$\chi_A(\omega) = \begin{cases} 1, & \text{če } \omega \in A \\ 0, & \text{če } \omega \notin A \end{cases}$$

**Lema 3.4.** *Velja*

$$E(\chi_A) = P(A).$$

*Dokaz.* Iz lastnosti Lebesgue-ovega integrala sledi

$$E(\chi_A) = \int_\Omega \chi_A(\omega) dP(\omega) = \int_A dP = P(A).$$

□

Za pričakovano vrednost vsote karakterističnih slučajnih spremenljivk $X = \chi_{A_1} + \chi_{A_2} + \cdots + \chi_{A_n}$ velja

$$E(X) = P(A_1) + P(A_2) + \ldots + P(A_n).$$

Pri tem smo uporabili lemi 3.2 in 3.4.

**Primer 3.5.** Če za permutacijo $\sigma$ obstaja tak $i \in \{1, \ldots, n\}$, da velja $\sigma(i) = i$, potem pravimo, da je $i$ fiksna točka permutacije $\sigma$. Izračunajmo pričakovano število fiksnih točk na slepo izbrane permutacije $\sigma$ na množici $\{1, \ldots, n\}$.
Naj bo $X(\sigma)$ število fiksnih točk permutacije $\sigma$. Slučajno spremenljivko $X$ lahko zapišemo kot vsoto karakterističnih slučajnih spremenljivk. Velja namreč

$$X(\sigma) = \sum_{i=1}^{n} X_i(\sigma),$$

kjer je

$$X_i(\sigma) = \begin{cases} 1, & \text{če } \sigma(i) = i, \\ 0, & \text{sicer.} \end{cases}$$

Ker je

$$E(X_i) = P(\sigma(i) = i) = \frac{1}{n},$$

sledi

$$E(X) = \frac{1}{n} + \frac{1}{n} + \cdots + \frac{1}{n} = 1.$$

Izračunali smo, da je pričakovano število fiksnih točk na slepo izbrane permutacije enako 1.

### 3.1.1 Hamiltonske poti v turnirju

**Definicija 3.6.** *Turnir* je usmerjen graf tvorjen z določitvijo smeri vsake povezave v neusmerjenem polnem grafu. *Hamiltonska pot* v turnirju je usmerjena pot skozi vsa vozlišča turnirja.

Izrek 3.7 velja za prvo uporabo verjetnostne metode. Dokazal ga je Szele leta 1943 v članku [7]. Dokaz smo povezeli iz gradiv [1] in [4].

**Izrek 3.7.** *Obstaja turnir $T$ na $n$ točkah z vsaj $n! \cdot 2^{-(n-1)}$ Hamiltonskimi potmi.*

*Dokaz.* Naj bo X število Hamiltonskih poti v na slepo izbranem turnirju na $n$ točkah. Za vsako permutacijo $\sigma \in S_n$ naj bo $X_\sigma$ karakteristična slučajna spremenljivka, ki je enaka 1, če velja $(\sigma(i), \sigma(i+1)) \in T$ za $1 \leq i \leq n-1$, sicer pa zavzame vrednost 0. Potem velja

$$X = \sum_{\sigma \in S_n} X_\sigma.$$

Verjetnost, da bo posamezen par $(\sigma(i), \sigma(i+1))$ pravilno orientiran je enaka $\frac{1}{2}$. Vseh parov v Hamiltonski poti je natanko $n-1$. Zato je verjetnost, da bodo vsi pari $(\sigma(i), \sigma(i+1))$ pravilno orientirani, enaka $\frac{1}{2^{n-1}}$. Iz leme 3.4 sledi

$$E(X_\sigma) = \frac{1}{2^{n-1}}$$

in zato

$$E(X) = \sum_{\sigma \in S_n} E(X_\sigma) = \sum_{\sigma \in S_n} \frac{1}{2^{n-1}} = \frac{1}{2^{n-1}} \sum_{\sigma \in S_n} 1 = \frac{n!}{2^{n-1}} = n! \cdot 2^{-(n-1)}.$$

Naj bo $\{T_1, T_2, \ldots, T_{2^{\binom{n}{2}}}\}$ množica vseh turnirjev na točkah $\{1, 2, \ldots, n\}$. Tedaj je $E(X|T = T_i)$ število Hamiltonskih poti v turnirju $T_i$.
Ker je

$$\begin{aligned} n!2^{-(n-1)} = E(X) &= \sum_{i=1}^{2^{\binom{n}{2}}} E(X|T = T_i) P(T = T_i) \\ &= \sum_{i=1}^{2^{\binom{n}{2}}} E(X|T = T_i) \frac{1}{2^{\binom{n}{2}}}, \end{aligned}$$

obstaja tak $i$, da velja

$$E(X|T = T_i) \geq n!2^{-(n-1)}.$$

S tem je izrek dokazan. □

## 3.2 Brégmanov izrek

**Definicija 3.8.** *Permanenta* $n \times n$ matrike $A = [a_{ij}]$ je definirana kot

$$per(A) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} a_{i,\sigma(i)},$$

kjer je $S_n$ grupa vseh permutacij množice $\{1, \ldots, n\}$.

Trditev iz leme 3.9 je dobro poznana. Glej npr. [9].

**Lema 3.9.** *Če sta $P$ in $Q$ permutacijski matriki, ki sta enake velikosti, kot je matrika $A$, potem velja*

$$per(PAQ) = per(A).$$

Diskretno Jensenovo neenakost poznamo iz teorije mere. Dokaz bolj splošne formulacije najdemo npr. v knjigi [6].

**Lema 3.10. (Diskretna Jensenova neenakost)** *Naj bosta $-\infty \leq a < b \leq \infty$ in naj bo $f : (a, b) \to \mathbb{R}$ konveksna fukncija. Če velja $\sum_{i=1}^{r} \alpha_i = 1$, kjer je $\alpha_i \geq 0$ in $x_i \in (a, b)$ za vsak $i$, potem velja*

$$f\left(\sum_{i=1}^{r} \alpha_i x_i\right) \leq \sum_{i=1}^{r} (\alpha_i f(x_i)).$$

**Lema 3.11.** *Naj bo $r \in \mathbb{N}$ in $t = \frac{t_1+t_2+\cdots+t_r}{r}$, kjer je $t_i > 0$ za vsak $1 \leq i \leq r$. Tedaj velja*

$$\left(\prod_{j=1}^{r} t_j^{t_j}\right)^{\frac{1}{r}} \geq t^t.$$

*Dokaz.* Oglejmo si funkcijo $f(x) = x \ln(x)$ na intervalu $(0, \infty)$. Njen prvi in drugi odvod sta enaka $f'(x) = \ln(x) + 1$ in $f''(x) = \frac{1}{x}$. Ker je drugi odvod funkcije $f(x)$ pozitiven, vemo, da je $f$ konveksna na intervalu $(0, \infty)$.
Naj bosta $\alpha_i := \frac{1}{r}$ in $x_i := t_i$, za vsak $1 \leq i \leq r$. Potem je $t = \sum_{i=1}^{r} \alpha_i x_i$. Ker vemo, da je $\sum_{i=1}^{r} \alpha_i = 1$, iz leme 3.10 sledi

$$f\left(\sum_{i=1}^{r} \alpha_i x_i\right) \leq \sum_{i=1}^{r} \alpha_i f(x_i) = \frac{1}{r}\left(\sum_{i=1}^{r} f(x_i)\right) = \frac{1}{r}\left(\sum_{i=1}^{r} x_i \ln x_i\right).$$

Iz tega sledi

$$t \ln t \leq \frac{1}{r}\left(\sum_{i=1}^{r} t_i \ln t_i\right)$$

in zato

$$e^{t \ln t} \leq e^{\frac{1}{r}\left(\sum_{i=1}^{r} t_i \ln t_i\right)}.$$

Ker velja

$$e^{t \ln t} = e^{\ln t^t} = t^t,$$

sledi

$$t^t \leq e^{\frac{1}{r}\left(\sum_{i=1}^{r} t_i \ln t_i\right)} = \left(e^{\sum_{i=1}^{r} \ln t_i^{t_i}}\right)^{\frac{1}{r}} = \left(\prod_{i=1}^{r} e^{\ln t_i^{t_i}}\right)^{\frac{1}{r}} = \left(\prod_{i=1}^{r} t_i^{t_i}\right)^{\frac{1}{r}}.$$

□

Če je $Y \sim \binom{a_1,\ldots,a_s}{p_1,\ldots,p_s}$ slučajna spremenljivka, ki zavzame vrednosti $a_1, \ldots, a_s$ z verjetnostmi $p_1, \ldots, p_s$, potem je $\ln Y \sim \binom{\ln a_1,\ldots,\ln a_s}{p_1,\ldots,p_s}$.
Iz definicije pričakovane vrednosti vemo, da je

$$E(\ln Y) = \sum_{k=1}^{s} \ln P(Y = k) = \ln a_1 \cdot p_1 + \cdots + \ln a_s \cdot p_s.$$

Zato velja

$$e^{E(\ln Y)} = e^{\ln a_1 \cdot p_1 + \cdots + \ln a_s \cdot p_s} = \prod_{i=1}^{s} e^{\ln a_i p_i} = \prod_{i=1}^{s} e^{\ln a_i^{p_i}} = \prod_{i=1}^{s} a_i^{p_i}.$$

To pa je enako geometrijski sredini, ki jo označimo z $G(Y)$.

**Lema 3.12.** *Velja*

$$G(Y_1 \cdot Y_2) = G(Y_1) \cdot G(Y_2).$$

*Dokaz.* Ker je $G(Y) = e^{E(\ln Y)}$, sledi

$$\begin{aligned} G(Y_1 \cdot Y_2) =& e^{E(\ln(Y_1 \cdot Y_2))} = e^{E(\ln Y_1 + \ln Y_2)} \\ =& e^{E(\ln Y_1) + E(\ln Y_2)} = e^{E(\ln Y_1)} \cdot e^{E(\ln Y_2)} \\ =& G(Y_1) \cdot G(Y_2). \end{aligned}$$

□

Naj bo $A = [a_{ij}]$ matrika velikosti $n \times n$, kjer je $a_{ij} \in \{0, 1\}$. Naj bosta $S_n$ množica vseh permutacij množice $\{1, \ldots, n\}$ in $S$ množica vseh permutacij $\sigma \in S_n$ z lastnostjo, da velja $a_{i\sigma_i} = 1$ za vsak $i \in \{1, \ldots, n\}$. Naj bosta $\tau \in S_n$ in $\sigma \in S$ na slepo in neodvisno izbrani permutaciji. Naj bo $A^{(i)}$ matrika $A$ brez vrstic $\tau(1), \ldots, \tau(i)$ in brez stolpcev $\sigma(\tau(1)), \ldots, \sigma(\tau(i))$. Naj bo $R_{\tau(i)}$ število enk v vrstici $\tau(i)$ v matriki $A^{(i)}$ in naj bo $L = L(\tau, \sigma) = \prod_{1 \le i \le n} R_{\tau(i)}$.

**Trditev 3.13.** *Naj bodo $A$, $\tau$ in $\sigma$ kot zgoraj. Naj bo $per(A) \neq 0$, tj. $S \neq \emptyset$. Tedaj za slučajno spremenljivko $L = L(\tau, \sigma)$ velja*

$$G(L) \ge per(A).$$

*Dokaz.* Fiksirajmo $\tau_0 \in S_n$. Ker je $\sigma$ slučajna spremenljivka, vemo, da je tudi $L(\tau_0, \sigma)$ slučajna spremenljivka. Dovolj je pokazati, da velja $G(L(\tau_0, \sigma)) \ge per(A)$, saj je tedaj

$$G(L(\tau_0, \sigma)) = e^{E(\ln L(\tau_0, \sigma))} \ge per(A)$$

in zato

$$\ln e^{E(\ln L(\tau_0, \sigma))} \ge \ln per(A),$$

kar implicira

$$E\left(\ln L\left(\tau_0,\sigma\right)\right) \geq \ln per(A).$$

Iz povezave med pogojno in običajno pričakovano vrednostjo sledi

$$\begin{aligned} E\left(\ln L\left(\tau,\sigma\right)\right) &= \sum_{\tau_0\in S_n} E\left(\ln L\left(\tau,\sigma\right)|\tau=\tau_0\right) P\left(\tau=\tau_0\right) \\ &= \sum_{\tau_0\in S_n} E\left(\ln L\left(\tau_0,\sigma\right)\right)\frac{1}{n!} \geq \frac{1}{n!}\sum_{\tau_0\in S_n} \ln per(A) = \ln per(A) \end{aligned}$$

in posledično

$$G\left(L\left(\tau,\sigma\right)\right) = e^{E(\ln L(\tau,\sigma))} \geq e^{\ln per(A)} = per(A).$$

Neenakost $G(L) \geq per(A)$ pri fiksnem $\tau_0$ bomo pokazali s pomočjo indukcije na velikosti matrike. Privzamemo torej, da trditev velja za matrike velikosti $(n-1)\times(n-1)$. Ker se $per(A)$ ne spremeni, če matriki permutiramo stolpce, lahko brez škode za splošnost privzamemo, da so v prvi vrstici enke natanko v prvih $r$ stolpcih.
Da bo zapis nekoliko bolj preprost, privzamemo, da velja $\tau_0(1) = 1$. Za $j \in \{1,\ldots,r\}$ naj bo $t_j$ permanenta podmatrike, ki je dobljena iz $A$ na tak način, da ji odstranimo prvo vrstico in $j$-ti stolpec. Tedaj velja

$$t_j = |\{\sigma \in S : \sigma(1) = j\}|.$$

Tedaj je

$$per(A) = t_1 + \cdots + t_r.$$

Naj bo $t := \frac{t_1+\cdots+t_r}{r}$. Potem je $per(A) = t \cdot r$.
Velja

$$L\left(\tau_0,\sigma\right) = R_{\tau_0(1)}\cdot R_{\tau_0(2)}\cdots R_{\tau_0(n)} = R_1\cdot R_{\tau_0(2)}\cdots R_{\tau_0(n)} = r\cdot R_{\tau_0(2)}\cdots R_{\tau_0(n)}.$$

Geometrijska sredina slučajne spremenljivke $L\left(\tau_0,\sigma\right)$ je po lemi 3.12 enaka

$$G\left(L\left(\tau_0,\sigma\right)\right) = G(r)G\left(R_{\tau_0(2)}\cdots R_{\tau_0(n)}\right).$$

Ker je $r$ konstanta, sledi

$$G\left(L\left(\tau_0,\sigma\right)\right) = rG\left(R_{\tau_0(2)}\cdots R_{\tau_0(n)}\right).$$

Opazimo, da je $L\left(\tau_0',\sigma'\right) := R_{\tau_0(2)}\cdots R_{\tau_0(n)}|\{\sigma(1) = j\}$ izračun spremenljivke $L$ za ustrezno $(n-1)\times(n-1)$ matriko za nek fiksen $\tau_0'$ in poljuben $\sigma'$. Vemo, da je $L\left(\tau_0',\sigma'\right) = e^{E\left(\ln\left(R_{\tau_0(2)}\cdots R_{\tau_0(n)}\right)|\{\sigma(1)=j\}\right)}$. Po indukcijski predpostavki za vsak $j$ velja

$$G\left(e^{E\left(\ln\left(R_{\tau_0(2)}\cdots R_{\tau_0(n)}\right)|\{\sigma(1)=j\}\right)}\right) \geq t_j.$$

Torej je

$$E\left(\ln\left(R_{\tau_0(2)}\cdots R_{\tau_0(n)}\right)|\{\sigma(1)=j\}\right)\geq \ln t_j$$

in zato

$$\begin{aligned}E\left(\ln\left(R_{\tau_0(2)}\cdots R_{\tau_0(n)}\right)\right)&=\sum_{j=1}^{r}E\left(\ln\left(R_{\tau_0(2)}\cdots R_{\tau_0(n)}\right)|\{\sigma(1)=j\}\right)P(\sigma(1)=j)\\&\geq\sum_{j=1}^{r}(\ln t_j)\cdot\frac{t_j}{|S|}=\sum_{j=1}^{r}(\ln t_j)\cdot\frac{t_j}{per(A)}.\end{aligned}$$

Iz tega sledi

$$\begin{aligned}G(R_{\tau_0(2)}\cdots R_{\tau_0(n)})=&e^{E\left(\ln\left(R_{\tau_0(2)}\cdots R_{\tau_0(n)}\right)\right)}\geq e^{\sum_{j=1}^{r}(\ln t_j)\frac{t_j}{per(A)}}=\prod_{j=1}^{r}e^{(\ln t_j)\frac{t_j}{per(A)}}\\=&\prod_{j=1}^{r}e^{\ln\left(t_j^{\frac{t_j}{per(A)}}\right)}=\prod_{j=1}^{r}t_j^{\frac{t_j}{per(A)}}=\prod_{j=1}^{r}t_j^{\frac{t_j}{r\cdot t}}=\left(\prod_{j=1}^{r}\left(t_j^{t_j}\right)^{\frac{1}{r}}\right)^{\frac{1}{t}},\end{aligned}$$

kar implicira

$$G(L(\tau_0,\sigma))\geq r\cdot\left(\prod_{j=1}^{r}\left(t_j^{t_j}\right)^{\frac{1}{r}}\right)^{\frac{1}{t}}.$$

Iz leme 3.11 pa sledi

$$G(L(\tau_0,\sigma))\geq r\cdot\left(t^t\right)^{\frac{1}{t}}=r\cdot t=per(A),$$

kar smo želeli pokazati.

□

**Lema 3.14.** *Naj bodo $k$, $r_1$ in $n$ naravna števila, za katera velja $1\leq k\leq r_1\leq n$. Tedaj*

$$\sum_{t=0}^{n-r_1}\binom{t+r_1-k}{r_1-k}\binom{n-r_1-t+k-1}{k-1}=\binom{n}{r_1}$$

*Dokaz.* Če namesto simbola $k$ vpeljemo oznako $a:=r_1-k$, potem se enakost, ki jo želimo dokazati, spremeni v

$$\sum_{t=0}^{n-r_1}\binom{t+a}{a}\binom{n-1-t-a}{r_1-a-1}=\binom{n}{r_1}. \tag{3.1}$$

Če namesto simbola $r_1$ vpeljemo oznako $m:=n-r_1$, potem se enakost (3.1), ki jo želimo dokazati, spremeni v

$$\sum_{t=0}^{m}\binom{t+a}{a}\binom{n-1-t-a}{n-m-a-1}=\binom{n}{n-m}. \tag{3.2}$$

Ker je $\binom{t+a}{a} = \binom{t+a}{t}$, $\binom{n-1-t-a}{n-m-a-1} = \binom{n-1-t-a}{m-t}$ in $\binom{n}{n-m} = \binom{n}{m}$, vidimo, da je dovolj dokazati enakost

$$\sum_{t=0}^{m} \binom{t+a}{t}\binom{n-1-t-a}{m-t} = \binom{n}{m}. \tag{3.3}$$

Pri tem je $a = r_1 - k \geq 0$, $m = n - r_1 \geq 0$ ter $m + a = n - k \leq n - 1$. Enakost (3.3) za tovrstne parametre $a, m, n$ bomo dokazali z indukcijo glede na vrednost $m + a$. Denimo, da velja $m + a = 0$, tj. $m = 0 = a$. Tedaj je leva stran v enačbi (3.3) enaka

$$\sum_{t=0}^{0} \binom{t}{t}\binom{n-1-t}{-t} = \binom{0}{0}\binom{n-1}{0} = 1,$$

desna stran pa znaša $\binom{n}{0} = 1$. Baza indukcije je s tem pokazana. Naj bo $N \geq 0$ in privzemimo, da (3.3) velja za vse parametre $a, m, n$, kjer je $a+m \leq N$ ter $a+m \leq n-1$. Naj bo sedaj

$$a + m = N + 1$$

ter $a + m \leq n - 1$. Po indukcijski predpostavki tedaj veljajo enakosti

$$\sum_{t=0}^{m} \binom{t+(a-1)}{t}\binom{n-1-t-(a-1)}{m-t} = \binom{n}{m}, \tag{3.4}$$

$$\sum_{t=0}^{m-1} \binom{t+(a-1)}{t}\binom{(n-1)-t-(a-1)-1}{(m-1)-t} = \binom{n-1}{m-1}, \tag{3.5}$$

$$\sum_{t=0}^{m-1} \binom{t+a}{t}\binom{n-1-t-a}{(m-1)-t} = \binom{n}{m-1}, \tag{3.6}$$

$$\sum_{t=0}^{m-2} \binom{t+a}{t}\binom{(n-1)-1-t-a}{(m-2)-t} = \binom{n-1}{m-2}. \tag{3.7}$$

Za zaključek dokaza bomo trikrat uporabili identiteto iz Pascalovega trikotnika

$$\binom{x}{y} = \binom{x-1}{y} + \binom{x-1}{y-1}.$$

Iz Pascalove identite ter enačb (3.4)-(3.7) sledi

$$\begin{aligned}
&\sum_{t=0}^{m} \binom{t+a}{t}\binom{n-1-t-a}{m-t} \\
&= \sum_{t=0}^{m} \left(\binom{t+a-1}{t} + \binom{t+a-1}{t-1}\right) \\
&\qquad \cdot \left(\binom{n-1-t-a+1}{m-t} - \binom{n-1-t-a}{m-t-1}\right)
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{t=0}^{m} \binom{t+(a-1)}{t} \binom{n-1-t-(a-1)}{m-t} \\
&- \sum_{t=0}^{m-1} \binom{t+(a-1)}{t} \binom{(n-1)-t-(a-1)-1}{(m-1)-t} \\
&+ \sum_{s=0}^{m-1} \binom{s+a}{s} \binom{n-1-s-a}{(m-1)-s} \\
&- \sum_{s=0}^{m-2} \binom{s+a}{s} \binom{(n-1)-1-s-a}{m-2-s} \\
&= \binom{n}{m} - \binom{n-1}{m-1} + \binom{n}{m-1} - \binom{n-1}{m-2} = \binom{n}{m}.
\end{aligned}
$$

S tem je pokazan indukcijski korak. □

**Izrek 3.15. (Brégmanov izrek)** *Naj bo $A$ matrika velikosti $n \times n$ s koeficienti iz množice $\{0,1\}$. Naj bo $r_i$ število enk v $i$-ti vrstici za $(1 \leq i \leq n)$. Tedaj velja*

$$per(A) \leq \prod_{1 \leq i \leq n} (r_i!)^{\frac{1}{r_i}}.$$

*Dokaz.* Naj bo $S_n$ množica vseh permutacij množice $\{1, \ldots, n\}$ in $S$ množica tistih permutacij $\sigma \in S_n$, za katere velja $a_{i,\sigma_i} = 1$ za vsak $i \in \{1, \ldots, n\}$.
Če je $per(A) = 0$ je izrek očiten. Naj bo $per(A) > 0$ tj. $S \neq \emptyset$. Zaradi trditve 3.13 je dovolj pokazati, da velja

$$G(L(\tau, \sigma)) = \prod_{1 \leq i \leq n} (r_i!)^{\frac{1}{r_i}},$$

kjer sta $\tau \in S_n$ in $\sigma \in S$ neodvisno in na slepo izbrani permutaciji. Še več, to enakost je dovolj pokazati pri fiksnem $\sigma \in S$ in na slepo izbranem $\tau$, kar je utemeljeno v nadaljevanju.
Naj bo $\sigma_0 \in S$ fiksna permutacija in $\tau$ na slepo izbrana permutacija. Povzamemo, da je $G(L(\tau, \sigma_0)) = e^{E(\ln((L(\tau,\sigma_0))))}$ oziroma

$$E(ln(L(\tau, \sigma_0))) = \ln \prod_{1 \leq i \leq n} (r_i!)^{\frac{1}{r_i}}, \text{za vsak } \sigma_0 \in S.$$

Tedaj je

$$
\begin{aligned}
E(ln(L(\tau, \sigma_0))) &= \sum_{\sigma_0 \in S} E(ln(L(\tau, \sigma)))|\sigma = \sigma_0) P(\sigma = \sigma_0) \\
&= \sum_{\sigma_0 \in S} E(ln(L(\tau, \sigma)))) P(\sigma = \sigma_0)
\end{aligned}
$$

$$
\begin{aligned}
&= \sum_{\sigma_0 \in S} \ln \left( \prod_{1 \le i \le n} (r_i!)^{\frac{1}{r_i}} \right) P(\sigma = \sigma_0) \\
&= \ln \left( \prod_{1 \le i \le n} (r_i!)^{\frac{1}{r_i}} \right) \cdot \sum_{\sigma_0 \in S} P(\sigma = \sigma_0) \\
&= \ln \left( \prod_{1 \le i \le n} (r_i!)^{\frac{1}{r_i}} \right)
\end{aligned}
$$

in posledično

$$G(L(\tau, \sigma)) = \prod_{1 \le i \le n} (r_i!)^{\frac{1}{r_i}}.$$

V nadaljevanju naj bo $\sigma \in S$ fiksen.

Par $(A, \sigma_0)$ zamenjajmo s parom $(AP, \sigma_0')$ na naslednji način. Matriko $A$ zamenjajmo z matriko $AP$, kjer je $P$ taka permutacijska matrika, da bo matrika $AP$ imela vse enke iz prve vrstice v prvih $r_1$ stolpcih, nova permutacija $\sigma_0'$ pa zadošča enakosti $\sigma_0'(1) = 1$. Seveda velja $per(A) = per(AP)$ in $G(L(A, \tau, \sigma_0)) = G(L(AP, \tau, \sigma_0'))$ pri čemer je $\tau$ slučajen.

Nadalje zamenjamo par $(AP, \sigma_0')$ s parom $(QAP, \sigma_0'')$ na naslednji način. Matriko $AP$ zamenjamo z matriko $QAP$, kjer je $Q$ taka permutacijska matrika, da ima matrika $QAP$ na diagonali matrike samo enke in velja $\sigma_0''(i) = i$ za vsak $i \in \{1, \ldots, n\}$. Pri tem smo z matriko $Q$ permutirali zgolj vrstice $2, 3, \ldots, n$.

Zato lahko v nadaljevanju brez škode za splošnost predpostavimo, da je A take oblike, da ima v prvi vrstici v prvih $r_1$ stolpcih enke naprej pa ničle in velja $\sigma_0(i) = i$ za vsak $i \in \{1, \ldots, n\}$. Naj bo $A^{(i)}$ matrika $A$ brez vrstic $\tau(1), \ldots, \tau(i)$ in brez stolpcev $\sigma(\tau(1)), \ldots, \sigma(\tau(i))$. Naj bo $R_{\tau(i)}$ število enk v vrstici $\tau(i)$ v matriki $A^{(i)}$ in naj bo $L = L(\tau, \sigma) = \prod_{1 \le i \le n} R_{\tau(i)}$. Potem pri fiksnem $\sigma_0$ velja

$$L(\tau, \sigma_0) = L = R_{\tau(1)} R_{\tau(2)} \cdots R_{\tau(n)} = R_1 R_2 \cdots R_n$$

in zato iz leme 3.12 sledi

$$G(L(\tau, \sigma_0)) = G(R_1) G(R_2) \cdots G(R_n).$$

Izračunajmo $G(R_1)$ oz. porazdelitev $R_1$.

Slučajna spremenljivka $R_1 = R_{\tau(\tau^{-1}(1)}$ je enaka številu enk v prvi vrstici v matriki $A^{(\tau^{-1}(1))}$ oz. število enk v prvi vrstici potem, ko smo $\tau^{-1}(1) - 1$ vrstic in stolpcev izbrisali iz matrike $A$.

Seveda $R_1$ zavzame vrednosti iz množice $\{1, 2, \ldots, r_1\}$.

Naj bo $k \in \{1, 2, \ldots, r_1\}$. Ker $\tau^{-1}(1) \sim \begin{pmatrix} 1 & 2 & \cdots & n \\ \frac{1}{n} & \frac{1}{n} & \ldots & \frac{1}{n} \end{pmatrix}$, sledi $\tau^{-1}(1) - 1 \sim \begin{pmatrix} 0 & 1 & \cdots & n-1 \\ \frac{1}{n} & \frac{1}{n} & \ldots & \frac{1}{n} \end{pmatrix}$

in zato

$$\begin{aligned}
P(R_1=k) =& \sum_{j=0}^{n-1} P(R_1=k|\tau^{-1}(1)-1=j)P(\tau^{-1}(1)-1=j)\\
=& \sum_{j=0}^{n-1} P(R_1=k|\tau^{-1}(1)-1=j)\frac{1}{n}\\
=& \sum_{j=0}^{r_1-k-1} P(R_1=k|\tau^{-1}(1)-1=j)\frac{1}{n} + \sum_{j=r_1-k}^{n-k} P(R_1=k|\tau^{-1}(1)-1=j)\frac{1}{n}\\
&+ \sum_{j=n-k+1}^{n} P(R_1=k|\tau^{-1}(1)-1=j)\frac{1}{n}.
\end{aligned}$$

Ker sta prva in zadnja vsota ničelni, sledi

$$\begin{aligned}
P(R_1=k) =& \sum_{j=r_1-k}^{n-k} P(R_1=k|\tau^{-1}(1)-1=j)\frac{1}{n}\\
=& \sum_{j=r_1-k}^{n-k} \frac{\binom{r_1-1}{r_1-k}\binom{n-r_1}{j-(r_1-k)}}{\binom{n-1}{j}}\frac{1}{n}\\
=& \binom{r_1-1}{r_1-k} \sum_{j=r_1-k}^{n-k} \frac{\frac{(n-r_1)!}{(n-j-k)!(j-r_1+k)!}}{\frac{(n-1)!n}{(n-1-j)!j!}}\\
=& \binom{r_1-1}{r_1-k}\frac{(n-r_1)!}{n!} \sum_{j=r_1-k}^{n-k} \frac{j!}{(j-r+k)!}\frac{(n-j-1)!}{(n-j-k)!}.
\end{aligned}$$

Če vpeljemo novo spremenljivko $t=j-(r_1-k)$, dobimo $j=t+r_1-k$, in zato

$$\begin{aligned}
P(R_1=k) =& \binom{r_1-1}{r_1-k}\frac{(n-r_1)!}{n!}\\
&\cdot \sum_{t=0}^{n-r_1} \frac{(t+r_1-k)!}{t!}\frac{(n-t-r_1+k-1)!}{(n-t-r_1)!}\cdot\frac{(r_1-k)!}{(r_1-k)!}\cdot\frac{(k-1)!}{(k-1)!}\\
=& \binom{r_1-1}{r_1-k}\frac{(n-r_1)!}{n!}(r_1-k)!(k-1)!\sum_{t=0}^{n-k} \frac{(t+r_1-k)!}{t!(r_1-k)!}\frac{(n-t-r_1+k-1)!}{(n-t-r_1)(k-1)!}\\
=& \frac{(r_1-1)!}{(k-1)!(r_1-k)!}\frac{(n-r_1)!}{n!}(r_1-k)!(k-1)!\\
&\cdot \sum_{t=0}^{n-k} \binom{t+r_1-k}{r_1-k}\binom{n-t-r_1+k-1}{k-1}.
\end{aligned}$$

Iz leme 3.14 sledi

$$\begin{aligned} P(R_1 = k) =& \frac{(n-r_1)!(r_1-1)!}{n!} \cdot \binom{n}{r_1} \\ =& \frac{(n-r_1)!r_1!}{n!r_1} \cdot \binom{n}{r_1} \\ =& \frac{1}{r_1\binom{n}{r_1}} \cdot \binom{n}{r_1} \\ =& \frac{1}{r_1}. \end{aligned}$$

Torej je $R_1 \sim \begin{pmatrix} 1 & 2 & \cdots & r_1 \\ \frac{1}{r_1} & \frac{1}{r_1} & \cdots & \frac{1}{r_1} \end{pmatrix}$ in zato $G(R_1) = 1^{\frac{1}{r_1}} 2^{\frac{1}{r_1}} \cdots r_1^{\frac{1}{r_1}} = (r_1!)^{\frac{1}{r_1}}$.
Enako pokažemo, da velja $R_i \sim \begin{pmatrix} 1 & 2 & \cdots & r_1 \\ \frac{1}{r_i} & \frac{1}{r_i} & \cdots & \frac{1}{r_i} \end{pmatrix}$ oz. $G(R_i) = (r_i!)^{\frac{1}{r_i}}$. Posledično dobimo

$$G(L(\tau, \sigma_0)) = \prod_{1 \leq i \leq n} (r_i!)^{\frac{1}{r_i}}.$$

□

# 4 Metoda prvega momenta

**Izrek 4.1. (Neenakost Markova)** *Naj bo $X$ nenegativna slučajna spremenljivka. Potem za vsako pozitivno število $\lambda$ velja*

$$P(X \geq \lambda) \leq \frac{E(X)}{\lambda}.$$

*Dokaz.* Naj bo $\chi_{(X \geq \lambda)}$ karakteristična funkcija. Tedaj velja

$$X \geq \lambda \cdot \chi_{(X \geq \lambda)}$$

in

$$E(X) \geq \lambda E(\chi_{(X \geq \lambda)}).$$

Iz leme 3.4 sledi

$$P(X \geq \lambda) \leq \frac{E(X)}{\lambda}.$$

□

**Primer 4.2.** Pogosta uporaba leme 3.2 je napovedovanje moči množice $B \subseteq A$, kjer je $A$ dana množica, $B$ pa je generirana naključno. Za $\chi_{(a \in B)}$ karakteristične funkcije velja

$$|B| = \sum_{a \in A} \chi_{(a \in B)}.$$

Iz leme 3.2 sledi

$$E(|B|) = \sum_{a \in A} E(\chi_{(a \in B)}),$$

iz leme 3.4 pa dobimo

$$E(|B|) = \sum_{a \in A} P(a \in B).$$

Lemo 4.3 in njegov dokaz smo povzeli iz knjige [8].

**Lema 4.3. (Borel-Cantellijev lema)** *Naj bo $A_1, A_2, \ldots$ tako zaporedje dogodkov, da velja $\sum_{n=1}^{\infty} P(A_n) < \infty$. Potem za vsako pozitivno število $M$ velja neenakost*

$$P(\textit{Zgodi se manj kot } M \textit{ dogodkov izmed } A_1, A_2, \ldots) \geq 1 - \frac{\sum_{n=1}^{\infty} P(A_n)}{M}.$$

*V posebnem, z verjetnostjo 1 se zgodi kvečjemu končno mnogo dogodkov $A_1, A_2, \ldots$*

Še ena uporabna formulacija leme 4.3 je sledeča. Če so $B_1, B_2, \ldots$ taki dogodki, da velja $\sum_n (1 - P(B_n)) < \infty$, potem se z verjetnostjo 1 zgodijo vsi dogodki $B_1, B_2, \ldots$ razen končno mnogo.

*Dokaz.* Naj bo $X = \sum_{i=1}^{\infty} \chi_{A_i}$, kjer je $\chi_{A_i}$ karakteristična spremenljivka dogodka $A_i$ za $1 \leq i < \infty$. Pokazati moramo, da velja

$$P\left(X < M\right) \geq 1 - \frac{\sum_{i=1}^{\infty} P(A_i)}{M},$$

za vsak $M > 0$. Ker so slučajne spremenljivke $\chi_{A_i}$ nenegativne, iz znane posledice Lebesgue-ovega izreka o monotoni konvergenci sledi

$$E(X) = \sum_{i=1}^{\infty} E(\chi_{A_i}) = \sum_{i=1}^{\infty} P(A_i).$$

Iz neenakosti Markova dobimo

$$E(X) \geq M \cdot P(X \geq M) = M(1 - P(X < M)).$$

Posledično velja

$$M(1 - P(X < M)) \leq \sum_{i=1}^{\infty} P(A_i)$$

oz.

$$P(X < M) \geq 1 - \frac{\sum_{i=1}^{\infty} P(A_i)}{M}.$$

□

## 4.1 Množice brez vsot

**Definicija 4.4.** Aditivna množica $A \subseteq \mathbb{R}$ je *množica brez vsot*, če ne vsebuje takih elementov $x, y, z$, da velja $x + y = z$. Ekvivalentno, množica $A$ je brez vsot natanko tedaj, ko velja $A \cap (A + A) = \emptyset$.

Dokaz trditve 4.5 bomo povzeli iz knjige [1].

**Trditev 4.5.** *Naj bo $A$ aditivna množica neničelnih celih števil. Potem obstaja taka podmnožica $B$ množice $A$, ki je brez vsot in je velikosti $|B| > |A|/3$.*

*Dokaz.* Naj bo $A = \{a_1, a_2, \ldots, a_n\}$ in naj $p = 3k + 2$ praštevilo, tako da $p > 2 \max_{1 \leq i \leq n}\{|a_i|\}$. Naj bo $C = \{k + 1, k + 2, \ldots, 2k + 1\}$. Vemo, da je $C$ množica brez vsot in da je podmnožica ciklične grupe $\mathbb{Z}_p$. Opazimo tudi, da velja

$$\frac{|C|}{p - 1} = \frac{k + 1}{3k + 1} > \frac{1}{3}.$$

Naj bo $x \in \{1, \ldots, p-1\}$ na slepo izbran. Definirajmo števila $d_1, \ldots, d_n$ s predpisom $d_i \equiv xa_i \pmod{p}$ za vsak $i \in \{1, \ldots, n\}$.
Tedaj

$$P(d_i \in C) = \frac{|C|}{p-1} > \frac{1}{3}$$

in zato

$$E(|\{i : d_i \in C\}|) = E\left(\sum_{i=1}^{n} \chi_{(d_i \in C)}\right) = \sum_{i=1}^{n} E\left(\chi_{(d_i \in C)}\right) = \sum_{i=1}^{n} P(d_i \in C) > \sum_{i=1}^{n} \frac{1}{3} = \frac{n}{3}.$$

Zato obstajata taka $x \in \{1, \ldots, p-1\}$ in $B \subset A$, da velja $|B| > \frac{|A|}{3}$, kjer $xb \pmod{p} \in C$ za vsak $b \in B$. Vemo, da je $B$ množica brez vsot, saj če bi obstajala taka števila $b_1$, $b_2$ in $b_3 \in B$, za katera bi veljalo $b_1 + b_2 = b_3$, potem bi veljala enakost $xb_1 + xb_2 = xb_3$, kjer so $xb_1$, $xb_2$ in $xb_3 \in C$. Tako $C$ ne bi bila množica brez vsot, kar pa je v protislovju z začetno definicijo množice $C$. □

# 5 Metoda drugega momenta

**Definicija 5.1.** Naj bo $X$ slučajna spremenljivka. *Varianco* slučajne spremenljivke $X$ definiramo kot

$$Var(X) = E(X^2) - [E(X)]^2 = E\left((X - E(X))^2\right).$$

**Izrek 5.2. (Neenakost Čebiševa)** *Naj bo $X$ slučajna spremenljivka. Za vsak pozitiven $\lambda$ velja*

$$P(|X - E(X)| > \lambda Var(X)^{1/2}) \leq \frac{1}{\lambda^2}.$$

*Dokaz.* Dokazali bomo ekvivalentno neenakost

$$P(|X - E(X)|^2 > \lambda^2 Var(X)) \leq \frac{1}{\lambda^2}.$$

Z uporabo neenakosti Markova lahko hitro opazimo, da velja

$$P(|X - E(X)|^2 > \lambda^2 Var(X)) \leq \frac{E(|X - E(X)|^2)}{\lambda^2 Var(X)}.$$

Po definiciji variance pa sledi

$$P(|X - E(X)|^2 > \lambda^2 Var(X)) \leq \frac{1}{\lambda^2},$$

kar smo želeli pokazati. □

Uporaba neenakosti Čebiševa se pogosto imenuje *metoda drugega momenta*.

**Definicija 5.3.** Naj bosta $X$ in $Y$ slučajni spremenljivki. *Kovarianca* slučajnih spremenljivk $X$ in $Y$ je definirana kot

$$Cov(X, Y) = E(X \cdot Y) - E(X) \cdot E(Y).$$

**Lema 5.4.** *Naj bodo $X_1, X_2, \ldots X_r$ slučajne spremenljivke. Potem velja*

$$Var\left(\sum_{k=1}^{r} X_k\right) = \sum_{k=1}^{r} Var(X_k) + 2\sum_{k<l} Cov(X_k, X_l).$$

*Dokaz.* Iz linearnosti pričakovane vrednosti sledi

$$\begin{aligned} Var\left(\sum_{k=1}^{r} X_k\right) =& E\left(\left(\sum_{k=1}^{r} X_k\right)^2\right) - \left[E\left(\sum_{k=1}^{r} X_k\right)\right]^2 \\ =& E\left(\sum_{k=1}^{r} X_k^2 + 2\sum_{k<l} X_k X_l\right) - \left(\sum_{k=1}^{r} (E(X_k))^2 + 2\sum_{k<l} E(X_k)E(X_l)\right). \\ =& \sum_{k=1}^{r} E(X_k^2) + 2\sum_{k<l} E(X_k X_l) - \sum_{k=1}^{r} (E(X_k))^2 - 2\sum_{k<l} E(X_k)E(X_l) \\ =& \sum_{k=1}^{r} Var(X_k) + 2\sum_{k<l} Cov(X_k, X_l). \end{aligned}$$

□

**Definicija 5.5.** Naj bo $A = \{x_1, \ldots, x_k\}$ množica pozitivnih celih števil. Množici $A$ rečemo, da je množica *različnih vsot*, če so vse vsote $\sum_{i\in S} x_i, S \subseteq \{1, \ldots, k\}$ med seboj različne.

Dokaz trditve 5.6 smo povzeli iz knjige [1].

**Trditev 5.6.** *Naj $f(n)$ predstavlja maksimalen $k$, za katerega obstaja množica z različnimi vsotami $\{x_1, \ldots, x_k\} \subseteq \{1, \ldots, n\}$. Tedaj obstaja taka konstanta $C < \infty$, da velja*

$$f(n) \leq \log_2 n + \frac{1}{2}\log_2 \log_2 n + C$$

*za vsa naravna števila $n$.*

*Dokaz.* Naj bo množica $A = \{x_1, \ldots, x_k\} \subset \{1, \ldots, n\}$ fiksna množica z različnimi vsotami. Naj bo $\epsilon_i$ neodvisen za vsak $i \in \{1, \ldots, k\}$, za katerega velja $P(\epsilon_i = 1) = P(\epsilon_i = 0) = \frac{1}{2}$. Naj bo $X = \epsilon_1 x_1 + \cdots + \epsilon_k x_k$. Potem je pričakovana vrednost slučajne spremenljivke X enaka

$$E(X) = \frac{x_1 + \cdots + x_k}{2}$$

in varianca slučajne spremenljivke X enaka

$$Var(X) = \frac{x_1^2 + \cdots + x_k^2}{4}.$$

Hitro lahko opazimo, da je $Var(X) \leq \frac{n^2 k}{4}$.
Vemo, da je verjetnost $P(X = i)$ enaka 0 ali $\frac{1}{2^k}$. Naj bo $t := \frac{\lambda n\sqrt{k}}{2}$. Iz izreka 5.2 sledi

$$P\left(|X - E(X)| \geq \frac{\lambda n\sqrt{k}}{2}\right) \leq \frac{1}{\lambda^2}$$

za vsak $\lambda > 1$. Verjetnost nasprotnega dogodka je

$$P\left(|X - E(X)| < \frac{\lambda n\sqrt{k}}{2}\right) \geq 1 - \frac{1}{\lambda^2}.$$

Ker je vseh števil, ki so od $E(X)$ oddaljena manj kot $\frac{\lambda n\sqrt{k}}{2}$, kvečjemu $2 \cdot \frac{\lambda n\sqrt{k}}{2} + 1$, sledi

$$P\left(|X - E(X)| < \frac{\lambda n\sqrt{k}}{2}\right) \leq \frac{1}{2^k}\left(\lambda n\sqrt{k} + 1\right).$$

Iz tega sledi

$$n \geq \frac{2^k\left(1 - \frac{1}{\lambda^2}\right) - 1}{\lambda\sqrt{k}}.$$

Sledi

$$f(n) \leq \log_2 n + \frac{1}{2}\log_2\log_2 n + C.$$

□

Oglejmo si še en preprost primer uporabe metode drugega momenta.

**Trditev 5.7.** *Za vsak $m \geq 1$ velja*

$$\binom{2m}{m} \geq \frac{2^{2m}}{4\sqrt{m} + 2}.$$

*Dokaz.* Naj bo $X = X_1 + \cdots + X_{2m}$ slučajna spremenljivka, kjer so slučajne spremenljivke $X_1, \ldots, X_n$ neodvisne in vsaka zavzame vrednosti 0 ali 1 z verjetnostjo $\frac{1}{2}$. Vemo, da je $E(X) = m$ in $Var(X) = \frac{m}{2}$. Naj bo $t := \sqrt{m}$. Iz izreka 5.2 sledi

$$P(|X - m| > \sqrt{m}) \leq \frac{m}{2m} = \frac{1}{2}$$

in zato

$$P(|X - m| \leq \sqrt{m}) \geq \frac{1}{2}.$$

Verjetnost, da $X$ zavzame določeno vrednost $m + k$, kjer je $|k| \leq \sqrt{m}$, je enaka

$$P(X = m + k) = \binom{2m}{m + k}\frac{1}{2^{2m}}.$$

Ker je $\binom{2m}{m}$ največji binomski koeficient, sledi

$$P(X = m + k) \leq \binom{2m}{m}\frac{1}{2^{2m}}.$$

Posledično

$$\frac{1}{2} \leq P(|X - m| \leq \sqrt{m}) = \sum_{|k| < \sqrt{m}} P(X = m + k) \leq \left(2\sqrt{m} + 1\right)\binom{2m}{m}\frac{1}{2^{2m}}$$

in zato

$$\binom{2m}{m} \geq \frac{2^{2m}}{4\sqrt{m} + 2}.$$

□

# 6 Metoda eksponentnega momenta

Naj bo $X$ nenegativna slučajna spremenljivka in naj bosta $t > 0$ in $\lambda \in \mathbb{R}$.
Iz izreka 4.1 dobimo

$$P(X \geq \lambda) = P\left(e^{tX} \geq e^{t\lambda}\right) \leq \frac{E\left(e^{tX}\right)}{e^{t\lambda}} \tag{6.1}$$

in podobno

$$P(X \leq -\lambda) = P\left(e^{-tX} \geq e^{t\lambda}\right) \leq \frac{E\left(e^{-tX}\right)}{e^{t\lambda}}. \tag{6.2}$$

Spomnimo se znane Taylorjeve vrste za eksponentno funkcijo, ki je enaka

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots .$$

Zato velja

$$E(e^{tX}) = E\left(1 + tX + \frac{t^2X^2}{2!} + \frac{t^3X^3}{3!} + \cdots\right).$$

Z uporabo leme 3.2 in nekaj teorije mere sledi

$$E(e^{tX}) = 1 + tE(X) + t^2E\left(\frac{X^2}{2!}\right) + t^3\left(\frac{X^3}{3!}\right) + \cdots .$$

Količini $E\left(e^{tX}\right)$ rečemo *eksponentni moment* od slučajne spremenljivke $X$. Funkciji $t \mapsto E\left(e^{tX}\right)$ pravimo *momentna rodovna funkcija*. Uporabi neenakosti (6.1) in (6.2) pravimo *metoda eksponentnega momenta*.

**Lema 6.1.** *Če sta $X$ in $Y$ neodvisni slučajni spremenljivki, potem velja*

$$E(XY) = E(X)E(Y).$$

Trditev iz leme 6.1 poznamo iz verjetnosti.

**Lema 6.2.** *Če so $X_1, X_2, \ldots X_r$ neodvisne slučajne spremenljivke, potem velja*

$$Var\left(\sum_{k=1}^{r} X_k\right) = \sum_{k=1}^{r} Var(X_k)$$

*Dokaz.* Vemo, da je kovarianca dveh slučajnih spremenljivk enaka

$$Cov(X, Y) = E(X \cdot Y) - E(X) \cdot E(Y).$$

Ker so $X_1, X_2, \ldots, X_r$ neodvisne, po lemi 6.1 vemo, da je $Cov(X_k, X_l) = 0$ za vse $k, l \in \{1, \ldots, r\}$. Zato z uporabo leme 5.4 dobimo

$$Var\left(\sum_{k=1}^{r} X_k\right) = \sum_{k=1}^{r} Var(X_k),$$

kar smo želeli pokazati. □

**Lema 6.3.** *Naj bo $X$ taka slučajna spremenljivka, da velja $|X| \leq 1$ in $E(X) = 0$. Potem za vsak $-1 \leq t \leq 1$ velja*

$$E\left(e^{tX}\right) \leq e^{t^2 Var(X)}.$$

*Dokaz.* Vemo, da je $|tX| \leq 1$. Zato iz Taylorjevega razvoja eksponentne funkcije sledi

$$e^{tX} \leq 1 + tX + t^2X^2.$$

Posledično je

$$E\left(e^{tX}\right) \leq E\left(1 + tX + t^2X^2\right).$$

Iz leme 3.2 sledi

$$E\left(e^{tX}\right) \leq 1 + tE(X) + t^2E(X^2).$$

Ker je $E(X) = 0$, velja

$$E\left(e^{tX}\right) \leq 1 + t^2E(X^2) = 1 + t^2Var(X) \leq e^{t^2Var(X)}.$$

Pri tem smo uporabili znano neenakost $1 + y \leq e^y$. □

**Izrek 6.4. (Neenakost Chernoffa)** *Predpostavimo, da so $X_1, \ldots, X_n$ neodvisne slučajne spremenljivke, kjer je $|X_i - E(X_i)| \leq 1$ za vsak $i \in \{1, \ldots, n\}$.*
*Naj bo $X := X_1 + \cdots + X_n$ in naj bo $\sigma := \sqrt{Var(X)}$ standardna deviacija od $X$. Potem za vsak pozitiven $\lambda$ velja*

$$P(|X - E(X)| \geq \lambda\sigma) \leq 2\max(e^{-\lambda^2/4}, e^{-\lambda\sigma/2}).$$

*Dokaz.* Če odštejemo vsakemu $X_i$ konstanto, potem lahko privzamemo, da velja $E(X_i) = 0$ za vsak $i \in \{1, \ldots, n\}$. Opazimo, da

$$P(|X| \geq \lambda\sigma) = P(X \geq \lambda\sigma) + P(X \leq -\lambda\sigma).$$

Zaradi simetrije je dovolj pokazati, da velja

$$P(X \geq \lambda\sigma) \leq e^{-t\lambda\sigma/2},$$

kjer je $t := \min(\lambda/(2\sigma), 1)$. Če uporabimo neenakost (6.1) dobimo

$$P(X \geq \lambda\sigma) \leq \frac{E\left(e^{tX}\right)}{e^{t\lambda\sigma}} = e^{-t\lambda\sigma} E\left(e^{tX_1} \cdots e^{tX_n}\right).$$

Vemo, da so $X_i$ neodvisne slučajne spremenljivke. Zato so tudi $e^{tX_i}$ neodvisne. Z uporabo leme 6.1 dobimo neenakost

$$P(X \geq \lambda\sigma) \leq e^{-t\lambda\sigma} E(e^{tX_1}) \cdots E(e^{tX_n}).$$

Iz leme 6.3 sledi

$$\begin{aligned} P(X \geq \lambda\sigma) \leq & e^{-t\lambda\sigma} e^{t^2 Var(X_1)} \cdots e^{t^2 Var(X_n)} \\ = & e^{-t\lambda\sigma} e^{t^2 (Var(X_1) + \cdots + Var(X_n))} \end{aligned}$$

Z uporabo leme 6.2 dobimo

$$P(X \geq \lambda\sigma) \leq e^{-t\lambda\sigma} e^{t^2 (Var(X))} = e^{-t\lambda\sigma} e^{t^2\sigma^2}.$$

Dokaz je zaključen, saj vemo, da je $t \leq \lambda/(2\sigma)$. □

Dokaz izreka 6.4 smo povzeli iz knjige [8].

**Posledica 6.5.** *Naj bo $X = t_1 + t_2 + \cdots + t_n$, kjer so $t_i$ neodvisne slučajne spremenljivke, ki zavzamejo verjetnost 0 in 1 z verjetnostjo $\frac{1}{2}$. Potem za vsak $\epsilon > 0$ velja*

$$P(|X - E(X)| \geq \epsilon E(X)) \leq 2e^{-\min(\epsilon^2/4, \epsilon/2) E(X)}.$$

*Dokaz.* Hitro izračunamo, da je $|t_i - E(t_i)| \leq 1$. Uporabimo izrek 6.4 za $\lambda := \epsilon E(X)/\sigma$. Dobimo

$$P(|X - E(X)| \geq \epsilon E(X)) \leq 2 \max(e^{-\epsilon^2 E^2(X)/(4Var(X))}, e^{-\epsilon E(X)/2}).$$

Ker je $Var(t_i) = \frac{1}{4} < \frac{1}{2} = E(t_i)$, iz lem 3.2 in 6.2 sledi neenakost $Var(X) \leq E(X)$. Posledično velja

$$P(|X - E(X)| \geq \epsilon E(X)) \leq 2e^{-\min(\epsilon^2/4, \epsilon/2) E(X)}.$$

□

Dokaz posledice 6.5 smo povzeli iz knjige [8].

**Posledica 6.6.** *Naj bo $B \subseteq A$ naključna podmnožica množice $A$ z lastnostjo, da so dogodki $a \in B$ med seboj neodvisni za vse $a \in B$. Potem za vsak pozitiven $\epsilon$ in vsako končno množico $A' \subseteq A$ velja*

$$P\left(\left||B \cap A'| - \sum_{a \in A'} P(a \in B)\right| \geq \epsilon \sum_{a \in A'} P(a \in B)\right) \leq 2e^{-min(\epsilon^2/4, \epsilon/2) \sum_{a \in A'} P(a \in B)}.$$

*Dokaz.* Spomnimo se primera 4.2. Vemo, da je $E(|B \cap A'|) = \sum_{a \in A'} P(a \in B)$. Če uporabimo posledico 6.5, dobimo

$$P\left(||B \cap A'| - \sum_{a \in A'} P(a \in B)| \geq \epsilon \sum_{a \in A'} P(a \in B)\right) \leq 2e^{-min(\epsilon^2/4, \epsilon/2) \sum_{a \in A'} P(a \in B)}.$$

□

Dokaz posledice 6.6 smo povzeli iz knjige [8].

# 7 Lovászov lokalni lema

**Definicija 7.1.** Naj bodo $A_1, A_2, \ldots, A_n$ dogodki v verjetnostnem prostoru. Usmerjenemu grafu $D = (V, E)$, ki nima zank, kjer je $|V| = n$, pravimo *odvisnostni digraf* za dogodke $A_1, A_2, \ldots, A_n$, če je za vsak $i \in \{1, 2, \ldots, n\}$ dogodek $A_i$ neodvisen od vseh ostalih dogodkov $A_j$ za katere velja $(i, j) \notin E$.

**Izrek 7.2. (Lovászov lokalni lema)** *Naj bodo $A_1, A_2, \ldots, A_n$ dogodki v verjetnostnem prostoru in naj bo $D = (V, E)$ njihov odvisnostni digraf. Naj bodo $x_1, x_2, \ldots, x_n$ taka realna števila, da velja $0 \leq x_i < 1$ in $P(A_i) \leq x_i \prod_{(i,j)\in E}(1 - x_j)$ za vsak $1 \leq i \leq n$. Potem velja*

$$P\left(\bigcap_{i=1}^{n} \overline{A_i}\right) \geq \prod_{i=1}^{n}(1 - x_i) > 0,$$

*pri čemer smo z $\overline{A_i}$ označili nasprotni dogodek dogodka $A_i$.*

*Dokaz.* Vemo, da imajo komplementarni dogodki $\overline{A_i}$ pozitivno verjetnost, želeli pa bi, da bi se vsi zgodili istočasno s pozitivno verjetnostjo. Da se to zgodi, moramo omejiti verjetnost dogodka $A_i$ pod pogojem, da se vsi ostali dogodki $A_j$ ne zgodijo.
Naj bo $S \subseteq \{1, \ldots, n\}$ in naj bo $i \notin S$. Najprej pokažemo, da za poljubno množico $S$ velja

$$P\left(A_i \middle| \bigcap_{j\in S} \overline{A_j}\right) \leq x_i.$$

To pokažemo z indukcijo na velikosti množice $S$.
Če je $S = \emptyset$, vemo, da trditev drži, saj velja neposredno iz predpostavke leme, da je

$$P(A_i) \leq x_i \prod_{(i,j)\in E} (1 - x_j) \leq x_i.$$

Predpostavimo, da trditev velja tudi za vsako množico $S'$, kjer $|S'| < |S|$.
Naj bosta $S_1 = \{j \in S : (i, j) \in E\}$ in $S_2 = S \backslash S_1$. Brez škode za splošnost lahko privzamemo, da velja $S_1 \neq \emptyset$, saj v nasprotnem trditev sledi neposredno iz predpostavke. Potem velja

$$P\left(A_i \middle| \bigcap_{j\in S} \overline{A_j}\right) = \frac{P\left(A_i \cap \bigcap_{j\in S_1} \overline{A_j} \middle| \bigcap_{l\in S_2} \overline{A_l}\right)}{P\left(\bigcap_{j\in S_1} \overline{A_j} \middle| \bigcap_{l\in S_2} \overline{A_l}\right)}.$$

Vemo, da je $A_i$ neodvisen od dogodkov $\{A_l : l \in S_2\}$. Zato lahko omejimo števec

$$P\left(A_i \cap \bigcap_{j\in S_1} \overline{A_j} \Big| \bigcap_{l\in S_2} \overline{A_l}\right) \leq P\left(A_i \Big| \bigcap_{l\in S_2} \overline{A_l}\right) = P(A_i) \leq x_i \prod_{(i,j)\in E} (1-x_j).$$

Naj bo $S_1 = \{j_1, j_2, \ldots, j_r\}$. Po indukcijski predpostavki lahko omejimo tudi imenovalec, velja

$$\begin{aligned} P\left(\overline{A_{j_1}} \cap \overline{A_{j_2}} \cap \cdots \cap \overline{A_{j_r}} \Big| \bigcap_{l\in S_2} \overline{A_l}\right) =& P\left(\overline{A_{j_1}} \Big| \bigcap_{l\in S_2} \overline{A_l}\right) P\left(\overline{A_{j_2}} | \overline{A_{j_1}} \cap \bigcap_{l\in S_2} \overline{A_l}\right) \cdots \\ & \cdots P\left(\overline{A_{j_r}} | \overline{A_{j_1}} \cap \overline{A_{j_2}} \cap \cdots \cap \overline{A_{j_{r-1}}} \cap \bigcap_{l\in S_2} \overline{A_l}\right) \\ \geq & (1-x_{j_1})(1-x_{j_2}) \cdots (1-x_{j_r}) \\ \geq & \prod_{(i,j)\in E} (1-x_j). \end{aligned}$$

Tako smo dobili oceno

$$P\left(A_i \Big| \bigcap_{j\in S} \overline{A_j}\right) = \frac{P\left(A_i \cap \bigcap_{j\in S_1} \overline{A_j} \Big| \bigcap_{l\in S_2} \overline{A_l}\right)}{P\left(\bigcap_{j\in S_1} \overline{A_j} \Big| \bigcap_{l\in S_2} \overline{A_l}\right)} \leq x_i.$$

Zato velja

$$\begin{aligned} P\left(\bigcap_{i=1}^{n} \overline{A_i}\right) =& P\left(\overline{A_1}\right) P\left(\overline{A_2} | \overline{A_1}\right) \cdots P\left(\overline{A_n} \Big| \bigcap_{i=1}^{n-1} \overline{A_i}\right) \\ =& \left(1 - P\left(A_1\right)\right) \left(1 - P\left(A_2 | \overline{A_1}\right)\right) \cdots \left(1 - P\left(A_n \Big| \bigcap_{i=1}^{n-1} \overline{A_i}\right)\right) \\ \geq & \prod_{i=1}^{n} (1-x_i). \end{aligned}$$

□

**Posledica 7.3. (Simetrični Lovászov lokalni lema)** *Naj bodo $A_1, A_2, \ldots, A_n$ taki dogodki v verjetnostnem prostoru, da velja $P(A_i) \leq p$ za vsak $i \in \{1, 2, \ldots, n\}$. Predpostavimo, da je vsak dogodek $A_i$ odvisen od kvečjemu $d$ dogodkov $A_j$. Če je $ep(d+1) \leq 1$, potem velja*

$$P\left(\bigcap_{i=1}^{n} \overline{A_i}\right) > 0.$$

*Dokaz.* Posledica očitno velja za $d = 0$, saj so si v tem primeru vsi dogodki med seboj neodvisni. Za $d \geq 1$ obstaja tak odvisnostni digraf $D(V, E)$ za dogodke $A_1, A_2, \ldots, A_n$,

kjer za vsak $i$, velja $|\{j : (i,j) \in E\}| \leq d$. Naj bo $x_i = \frac{1}{d+1}$ za vsak $i$. Uporabimo izrek 7.2 in dobimo

$$P\left(\bigcap_{i=1}^{d} \overline{A_i}\right) \geq \prod_{i=1}^{d}\left(1 - \frac{1}{d+1}\right) = \left(1 - \frac{1}{d+1}\right)^d > \frac{1}{e} > 0.$$

□

Dokaz leme 7.2 in posledice 7.3 smo povzeli iz gradiv [1], [4], [8].

## 7.1 Barvanje hipergrafa in lokalni lema

V poglavju 2.2 smo pokazali, da je vsak $k$-uniformni hipergraf z manj kot $2^{k-1}$ hiperpovezavami 2-obarvljiv. S pomočjo lokalnega leme lahko pokažemo soroden pogoj za 2-obarvljivost hipergrafa.

**Trditev 7.4.** *Naj bo $H = (V, E)$ hipergraf, v katerem ima vsaka hiperpovezava vsaj $k$ točk in seka kvečjemu $d$ drugih hiperpovezav. Če velja*

$$e(d+1) \leq 2^{k+1},$$

*potem je $H$ 2-obarvljiv.*

*Dokaz.* Prebarvajmo točke hipergrafa H neodvisno in z enako verjetnostjo v rdeče ali modro. Za vsako hiperpovezavo $f$, naj bo $A_f$ dogodek, da je $f$ monokromatska. Vemo, da je

$$P(A_f) = 2 \cdot \frac{1}{2^{|f|}}.$$

Ker ima vsaka hiperpovezava vsaj $k$ točk, sledi

$$P(A_f) \leq 2^{1-k}.$$

Opazimo tudi, da je vsak dogodek $A_f$ odvisen od kvečjemu $d$ od ostalih dogodkov $A_{f'}$, tj. tistih, kjer $f'$ seka. Ker je $ep(d+1) \leq 1$, lahko uporabimo posledico 7.3. In zato je verjetnost, da nobena hiperpovezava ni monokromatska, pozitivna. □

Dokaz trditve 7.4 smo povzeli iz gradiv [1] in [4].

# 8 Zaključek

V zaključni nalogi smo si ogledali nekaj osnovnih idej verjetnostne metode in nekaj primerov njene uporabe v različnih področjih matematike. Videli smo, kako lahko z verjetnostjo metodo dokažemo zanimivo spodnjo mejo za diagonalna Ramseyeva števila. Poiskali smo spodnjo mejo za najmanjše število hiperpovezav, da hipergraf ni 2-obarvljiv. Dokazali smo Erdős-Ko-Radov izrek, ki nam omeji moč presečne družine podmnožic poljubne množice. Izračunali smo pričakovano število fiksnih točk v permutaciji in določili spodnjo mejo hamiltonskih poti v turnirju. Dokazali smo Bregmanov izrek, ki omejuje parmanento kvadratne matrike s koeficienti iz množice $\{0, 1\}$. S pomočjo uporabe metode prvega momenta smo pokazali, da v kolikor je $A$ aditivna množica neničelnih celih števil, potem obstaja taka podmnožica množice $A$, ki je brez vsot in z močjo večjo od $|A|/3$. Z metodo drugega momenta smo omejili maksimalen $k$, za katerega obstaja množica $\{x_1, x_2, \ldots, x_k\} \subseteq \{1, 2, \ldots, n\}$ z različnimi vsotami. Na preprost način smo tudi navzdol omejili binomski koeficient $\binom{2m}{m}$. Z metodo eksponentnega momenta smo dokazali neenakost Chernoffa in dve uporabni posledici tega izreka. Na koncu je predstavljen še Lovászov lokalni lema in simetrični lokalni lema. S pomočjo uporabe tega izreka smo dobili drugačen pogoj za 2-obarvljivost hipergrafa, kot v drugem poglavju.

# 9 Literatura

[1] N. Alon in J. H. Spencer, *The Probabilistic Method*. Third Edition, John Wiley & Sons, Inc., Hoboken, New Jersey, 2008. *(Citirano na straneh 4, 7, 19, 22 in 30.)*

[2] P. Erdős, On a combinatorial problem. *Nordisk Mat. Tidskr.* 11 (1963) 5–10. *(Citirano na strani 4.)*

[3] P. Erdős, Some remarks on the theory of graphs. *Bull. Amer. Math. Soc.* 53 (1947) 292–294. *(Citirano na strani 3.)*

[4] J. Matoušek in J. Vondrák, *The Probabilistic Method*. Lecture notes, 2008. *(Citirano na straneh 3, 4, 7 in 30.)*

[5] S. Radziszowski, *Small Ramsey numbers*, Electron. J. Combin., Dynamic Survey #DS1. Mar 3, 2017. *(Citirano na strani 2.)*

[6] W. Rudin, *Real and Complex Analysis*, Third edition, McGraw-Hill, 1986. *(Citirano na strani 9.)*

[7] T. Szele, Kombinatorikai vizsgálatok az irányitott teljes gráffal. *Kapcsolatban, Mt. Fiz. Lapok* 50 (1943) 223–256. *(Citirano na strani 7.)*

[8] T. Tao in V. H. Vu, *Additive Combinatorics*. Cambridge University Press, 2006. *(Citirano na straneh 18, 26, 27 in 30.)*

[9] I. M. Wanless, Permanents. in L. Hogben (Ed.), *R. Brualdi*. A. Greenbaum. R. Mathias (Associate Eds.) Handbook of linear algebra. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2007. *(Citirano na strani 9.)*