Vjerojatnost da je slučajna matrica singularna

Jurčević, Jura

Vjerojatnost da je slučajna matrica singularna

Jurčević, Jura

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Jura Jurčević

VJEROJATNOST DA JE SLUČAJNA MATRICA SINGULARNA

Diplomski rad

Voditelj rada:
doc. dr. sc. Rudi Mrazović

Zagreb, rujan 2020.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Sadržaj

Uvod

U ovom radu promatramo slučajne $n \times n$ ± 1 matrice, pri čemu je slučajnost definirana uniformnom distribucijom, odnosno za svaki element matrice nezavisno jedan od drugog na slučajan (uniformni) način biramo 1 ili -1.
Za tako definirane matrice, zanima nas kako se ponaša $P_n = \mathbb{P}(M_n \text{ je singularna})$ kada n raste u beskonačnost.
Već je pokazano da $P_n \to 0$ i da vrijedi $P_n = O\left(\frac{1}{\sqrt{n}}\right)$. U ovom radu prezentiramo rezultat Kahna, Komlósa i Szemerédija koji su pokazali eksponencijalnu gornju među, odnosno da postoji ϵ takav da vrijedi $P_n < (1 - \epsilon)^n$.
U prvom poglavlju postavit ćemo problem i dati smjernice našem radu. U Poglavlju 2 dokazat ćemo pomoćni teorem koji je važan korak u dokazu naše tvrdnje, ali i kao samostalan rezultat. U Poglavlju 3 dokazat ćemo glavni teorem uz pomoć nekoliko lema za koje ćemo također pokazati da vrijede u istom poglavlju. Naposljetku, u posljednjem poglavlju iznijet ćemo neke primjene i posljedice naše tvrdnje na razna područja.

Poglavlje 1

O problemu

1.1 Postavljanje problema

Za početak, prisjetimo se definicije i jedne karakterizacije singularne matrice.

Definicija 1.1.1. *Kažemo da je matrica $A \in M_n(\mathbb{F})$ regularna ako postoji matrica $B \in M_n(\mathbb{F})$ takva da vrijedi $AB = BA = I$. U tom se slučaju matrica B zove multiplikativni inverz od A. Za matricu $A \in M_n(\mathbb{F})$ koja nema multiplikativni inverz kažemo da je singularna.*

Teorem 1.1.2. *Matrica $A \in M_n(\mathbb{F})$ je singularna ako i samo ako je* $\det A = 0$.

Od interesa će nam biti slučajne $n \times n$ ± 1 matrice, pri čemu je slučajnost definirana uniformnom distribucijom, odnosno za svaki element matrice nezavisno jedan od drugog na slučajan (uniformni) način biramo 1 ili -1.
Za tako definirane matrice, označimo s $P_n = \mathbb{P}(M_n \text{ je singularna})$. Zanima nas kako se ponaša P_n kada n raste u beskonačnost.

Propozicija 1.1.3. *Vrijedi*

$$P_n \geq (1 + o(1))\frac{n^2}{2^{n-1}}$$

Skica dokaza. Događaj $\{M_n$ ima bar dva retka ili stupca koji su jednaki do na predznak$\}$ podskup je događaja $\{M_n$ je singularna$\}$ pa vrijedi $P_n \geq \mathbb{P}(M_n$ ima bar dva retka ili stupca koji su jednaki do na predznak$) = (1 + o(1))2 \cdot \binom{n}{2} \cdot \frac{1}{2^{n-1}} = (1 + o(1))\frac{n(n-1)}{2^{n-1}} = (1 + o(1))\frac{n^2}{2^{n-1}}$.
Pojasnimo prvu jednakost, od n redaka (ili stupaca) biramo dva koja će biti jednaka što odgovara faktoru $\binom{n}{2}$. Nadalje, ta dva retka mogu biti jednaka na 2^{n+1} načina, a ukupno postoji

2^{2n} kombinacija za odabrati dva retka, to objašnjava faktor $\frac{1}{2^{n-1}} = \frac{2^{n+1}}{2^{2n}}$. Za kraj, pošto su slučajevi jednaki i za retke i za stupce, sve množimo s 2.
Sada objasnimo faktor $(1 + o(1))$. Primijetimo da koristimo aditivnost vjerojatnosti s obzirom na događaje koji nisu u potpunosti disjunktni, prvi i drugi redak mogu biti jednaki u isto vrijeme kada i drugi i treći, dva retka mogu biti jednaka u isto vrijeme kada i dva stupca. Dakle, koristit ćemo formulu uključivanja i isključivanja, ali svi ti presjeci događaja imaju iznimno male vjerojatnosti pa ih možemo obuhvatiti u član o(1). □

Već dugo se sluti da vrijedi

$$P_n = (1 + o(1))\frac{n^2}{2^{n-1}} \tag{1.1}$$

odnosno da glavni doprinos u P_n dolazi od matrica M_n koje sadrže dva retka ili stupca koji su jednaki do na predznak.

U ovom radu dajemo eksponencijalnu gornju među. Iskažimo glavni teorem koji daje navedenu među.

Teorem 1.1.4. *Postoji $\epsilon > 0$ za koji je $P_n < (1 - \epsilon)^n$.*

Teorem ćemo dokazati za $\epsilon = 0.001$ i $n \geq n_0$.

Naša želja za procjenom vjerojatnosti P_n motivirana je pitanjem o beskonačnoj sumi P_n-ova, tj. je li $\sum P_n < \infty$. Kada bismo dobili potvrdan odgovor, mogli bismo iskoristiti Borel-Cantellijevu lemu da zaključimo da je $\mathbb{P}\left(\limsup_{n\to\infty} P_n\right) = 0$, odnosno s vjerojatnosti 1 samo je konačno mnogo matrica M_n singularno. Jedan način za pokazati da je gornja suma konačna je dokazivanje Teorema 1.1.4.
Još nekoliko primjena i posljedica spomenut ćemo u Poglavlju 4. Od primjena je možda najinteresantniji Korolar 4.3.3. koji kaže da za odgovarajuću konstantu C, $n - C$ slučajnih $\{\pm 1\}$-vektora su ne samo (g.s.) nezavisni, nego ne razapinju nikoje druge $\{\pm 1\}$-vektore.

Problem procjenjivanja P_n usko je povezan s pitanjima iz raznih područja kao što su geometrija, logika i asocijativna sjećanja. U Poglavlju 4 govorit ćemo i o posljedicama na neka od tih područja.

U ostatku ovog poglavlja dat ćemo skicu i ideje dokaza Teorema 1.1.4. jedan od kojih je i Teorem 1.5.1. koji je važan u dokazu glavnog teorema, ali i kao samostalan rezultat.

1.2 Veliko O notacija

Prisjetimo se definicija asimptotskih oznaka koje ćemo u ovom radu koristiti.

Definicija 1.2.1. *Neka je f funkcija s realnim ili kompleksnim vrijednostima te neka je g funkcija s realnim vrijednostima. Neka su obje funkcije definirane na nekom neograničenom podkupu skupa realnih brojeva te neka je $g(x)$ strogo pozitivno za sve dovoljno velike vrijednosti od x.*
Tada je

$$f(x) = O(g(x)) \qquad za\ x \to \infty$$

ako postoji $M > 0, M \in \mathbb{R}$ i $x_0 \in \mathbb{R}$ takav da vrijedi $|f(x)| \leq Mg(x)$ za sve $x \geq x_0$.
Pišemo da je

$$f(x) = o(g(x)) \qquad za\ x \to \infty$$

ako za svaki $\epsilon > 0$ postoji N takav da vrijedi $|f(x)| \leq \epsilon g(x)$ za sve $x \geq N$.
Naposlijetku, pišemo da je

$$f(x) = \Omega(g(x)) \qquad za\ x \to \infty$$

ako vrijedi $\limsup_{x\to\infty} \left|\frac{f(x)}{g(x)}\right| > 0$.

Primijetimo da je druga oznaka jača od prve, da bi vrijedila prva jednakost uvjet mora biti ispunjen za neki M, a da bi vrijedila druga, uvjet mora biti ispunjen za svaki ϵ.
Dakle, svaka funkcija f koja je $o(g)$ je i $O(g)$, ali obrat ne vrijedi. Na primjer $2x^2 = O(x^2)$, ali $2x^2 \neq o(x^2)$.
Također, primijetimo da je $f(x) = \Omega(g(x))$ negacija od $f(x) = o(g(x))$.

1.3 Linearna algebra

Za $\underline{a} \in \mathbb{R}^n \setminus \{\underline{0}\}$, neka je

$$p(\underline{a}) = \mathbb{P}(\underline{\epsilon}^t \underline{a} = 0),$$

gdje je $\underline{\epsilon}$ određen uniformno iz $\{\pm 1\}^n$. Također, označimo s $E_{\underline{a}}$ događaj $\{M\underline{a} = \underline{0}\}$ gdje je $M = M_n$ slučajna $n \times n \pm 1$ matrica.
Uočimo, $M\underline{a} = \underline{0} \iff \underline{\epsilon}_1^t \underline{a} = \underline{\epsilon}_2^t \underline{a} = \cdots = \underline{\epsilon}_n^t \underline{a} = 0$ jer su retci matrice M slučajni vektori iz $\{\pm 1\}^n$ što je upravo $\underline{\epsilon}$. Dakle, možemo zaključiti da je $\mathbb{P}(E_{\underline{a}}) = p(\underline{a})^n$.
Također, ako vrijedi $\{M\underline{a} = \underline{0}\}$, tada se jedan redak matrice M može zapisati kao linearna kombinacija ostalih redaka pa je matrica M singularna, a vrijedi i obrat. Iz toga slijedi da je

$$P_n = \mathbb{P}\left(\bigcup_{\underline{a}\in\mathbf{Z}^n\setminus\{\underline{0}\}} E_{\underline{a}}\right).$$

Uočimo da smo do sad pisali da je $\underline{a} \in \mathbb{R}^n$, a u gornjem izrazu je $\underline{a} \in \mathbb{Z}^n$. Pojasnimo zašto možemo tako pisati.
Jedan smjer je trivijalan, pokažimo drugi. Pretpostavimo da postoji $\underline{a} \in \mathbb{R}^n \setminus \{\underline{0}\}$ takav da je $M\underline{a} = \underline{0}$. Jer je $\underline{a}$ netrivijalno, Gaussovim eliminacijama ćemo također dobiti netrivijalno rješenje. Također, pošto se matrica M sastoji od cjelobrojnih elemenata, Gaussove eliminacije dat će racionalno netrivijalno rješenje. Množenjem tog rješenja sa zajednčkim nazivnikom svih njegovih nazivnika dobit ćemo netrivijalno cjelobrojno rješenje, što smo i tražili.

Prva ideja za gornju među od P_n mogla bi biti $P_n \leq \sum \mathbb{P}(E_{\underline{a}})$, ali ta nejednakost ne daje ništa vrijedno.
Za $\underline{a}$-ove s malim $p(\underline{a})$ sljedeća lema daje korisnu gornju granicu.

Lema 1.3.1. *Za bilo koji p_0 takav da $0 < p_0 < 1$, vrijedi*

$$\mathbb{P}\left(\bigcup_{\underline{a}:p(\underline{a})\leq p_0} E_{\underline{a}}\right) \leq np_0.$$

Dokaz. Označimo s L_i događaj {i-ti redak matrice M je linearna kombinacija ostalih $n-1$ redaka}. Tada vrijedi $\mathbb{P}\left(\left(\bigcup_{\underline{a}:p(\underline{a})\leq p_0} E_{\underline{a}}\right) \cap L_i\right) \leq p_0$. Zaista, lijevu stranu možemo zapisati po formuli potpune vjerojatnosti kao
$\sum_s \mathbb{P}\left(\left(\bigcup_{\underline{a}:p(\underline{a})\leq p_0} E_{\underline{a}}\right) \cap L_i \middle| \text{realizacija u ne-}i\text{-tim retcima je } s\right) \mathbb{P}\left(\text{realizacija u ne-}i\text{-tim retcima je } s\right)$
pri čemu suma šeće po svim mogućim realizacijama ne-i-redaka. Sada pokažimo da je za proizvoljan fiksni s, $\mathbb{P}\left(\left(\bigcup_{\underline{a}:p(\underline{a})\leq p_0} E_{\underline{a}}\right) \cap L_i \middle| \text{realizacija u ne-}i\text{-tim retcima je } s\right) \leq p_0$.
Zbog uvjeta L_i, skup $\{\underline{a} : p(\underline{a}) \leq p_0, M\underline{a} = 0\}$ je već određen s realizacijom s pa je događaj na lijevoj strani podskup događaja $\{\epsilon^t \underline{a} = 0\} \cap L_i$ za proizvoljni $\underline{a}$ koji poništava i preostalih $n-1$ redaka i koji je takav da ja $p(\underline{a}) \leq p_0$. Taj događaj je podskup događaja $\{\epsilon^t \underline{a} = 0\}$, a njemu je vjerojatnost $p(\underline{a}) \leq p_0$.
Sada imamo

$$\sum_s \mathbb{P}\left(\left(\bigcup_{\underline{a}:p(\underline{a})\leq p_0} E_{\underline{a}}\right) \cap L_i \middle| \text{realizacija u ne-}i\text{-tim retcima je } s\right) \mathbb{P}\left(\text{realizacija u ne-}i\text{-tim retcima je } s\right) \leq$$
$$\sum_s p_0 \mathbb{P}\left(\text{realizacija u ne-}i\text{-tim retcima je } s\right) \leq p_0 \sum_s \mathbb{P}\left(\text{realizacija u ne-}i\text{-tim retcima je } s\right) \leq p_0.$$

Uočimo da ako vrijedi događaj $\bigcup_{\underline{a}:p(\underline{a})\leq p_0} E_{\underline{a}}$, onda postoji i takav da vrijedi L_i. Dakle, možemo koristiti zakon potpune vjerojatnosti,
$\mathbb{P}\left(\bigcup_{\underline{a}:p(\underline{a})\leq p_0} E_{\underline{a}}\right) = \sum_{i=1}^n \mathbb{P}\left(\left(\bigcup_{\underline{a}:p(\underline{a})\leq p_0} E_{\underline{a}}\right) \cap L_i\right) \leq np_0.$

□

Za baratati s velikim $p(\underline{a})$-ovima moramo nekako iskoristiti ovisnosti među $E_{\underline{a}}$-ovima. Okvir za to, temeljen na ideji da linearno zavisne $\underline{a}$-ove poništavaju isti M-ovi, daje sljedeća lema.

Lema 1.3.2. *Neka je S podskup skupa $\mathbb{R}^n \setminus \{\underline{0}\}$, $k = \dim\langle S \rangle$ odnosno dimenzija potprostora koji razapinje S te neka je $p(S) = \max\{p(\underline{a}) : \underline{a} \in S\}$. Tada je*

$$\mathbb{P}\left(\bigcup_{\underline{a}\in S} E_{\underline{a}}\right) \leq \binom{n}{k-1} p(S)^{n-k+1}.$$

Uočimo da je Lema 1.3.1. specijalan slučaj Leme 1.3.2. za $k = n$. Lemu 1.3.2. dokazat ćemo u Poglavlju 3. Faktor $\binom{n}{k-1}$ je malo pregrub, kasnije ćemo umjesto Leme 1.3.2. dati više tehničku Lemu 3.3.1. koja daje malo bolju vrijednost ϵ u Teoremu 1.1.4.

1.4 Potprostori

U dokazu Teorema 1.1.4. probat ćemo pokriti $\mathbb{Z}^n \setminus \{\underline{0}\}$ malim brojem potprostora nevelikih dimenzija te iskoristiti nejednakosti iz Leme 1.3.2. i njene profinjenije verzije. Dakle, koristit ćemo nejednadžbu

$$P_n = \mathbb{P}\left(\bigcup_{a\in\mathbb{Z}^n\setminus\{\underline{0}\}} E_{\underline{a}}\right) \leq \sum_{i\geq 0} \mathbb{P}\left(\bigcup_{a\in S_i} E_{\underline{a}}\right), \tag{1.2}$$

gdje je $\{S_i\}$ prigodni pokrivač prostora $\mathbb{Z}^n \setminus \{\underline{0}\}$.
S_0 ćemo odabrati kao $\{\underline{a} : p(\underline{a}) \leq p_0\}$ gdje je $p_0 \approx (1-\epsilon)^n$ i to tako da vrijedi $\dim(S_0) = n$. Za $i \neq 0$, $\dim(S_i)$ bit će otprilike γn gdje je $\gamma < 1$, detaljnije ćemo ju definirati kasnije.

Jedna zgodna i donekle prirodna ideja bila bi konstruirati S_i-eve kao $S(I) = \bigcap_{\underline{\epsilon}\in I} \underline{\epsilon}^{\perp}$ gdje je I skup linearno nezavisnih vektora iz $\{\pm 1\}^n$. Pozadina te ideje je da ukoliko $\underline{a} \in \mathbb{Z}^n$ zadovoljava uvjet $\underline{\epsilon}^t \underline{a} = 0$ za mnoge $\underline{\epsilon} \in \{\pm 1\}^n$, tada bi $\underline{a}$ trebao ležati i u mnogo $S(I)$-eva. Ispostavit će se da ova ideja ipak nije dovoljno dobra, ali će se moći iskoristiti da dođemo do korisnih S_i-eva. Naime, potprostori koje ćemo koristiti bit će oblika $S(I)$, ali će skup I sadržavati $(1-\gamma)n$ linearno nezavisnih vektora iz skupa $\{-1, 0, +1\}^n$, svaki s točno d ne-nul komponenti za neki $d \approx \mu n$, za neku malu konstantu μ.
Kasnije ćemo pokazati da nevelik broj takvih potprostora pokriva $\mathbb{Z}^n \setminus \{\underline{0}\}$.

Sada precizno definirajmo pojmove koji prirodno proizlaze iz gornje rasprave, a odnose se na vektore od točno d ne-nul koordinata.

Definicija 1.4.1. *Neka je V_d skup vektora $\underline{\epsilon} \in \{-1, 0, 1\}^n$ s točno d ne-nul koordinata. Tada je d-suma izraz oblika $\sum_{i=1}^{n} \underline{\epsilon}_i a_i$, pri čemu je $\underline{\epsilon} \in V_d$.*
Pišemo

$$\Sigma_d(\underline{a}) = \{\underline{\epsilon} \in V_d : \underline{\epsilon}^t \underline{a} = 0\}$$

i

$$\sigma_d(\underline{a}) = \mid \Sigma_d(\underline{a}) \mid .$$

Analogon od $p(\underline{a})$ za d-sume je

$$p_d(\underline{a}) = \frac{\sigma_d(\underline{a})}{\mid V_d \mid} = \frac{\sigma_d(\underline{a})}{\binom{n}{d} 2^d}.$$

1.5 Pomoćni teoremi

Kao što smo i prije spomenuli, sve $\underline{a}$-ove za koje je $p(\underline{a})$ malen, to jest $p(\underline{a}) < p_0 \approx (1-\epsilon)^n$ možemo staviti u jedan skup, S_0 koji po Lemi 1.3.1. ukupnoj ogradi u (1.2) pridonosi samo s np_0.
Zanima nas što možemo reći za $\underline{a}$-ove za koje je $p(\underline{a})$ velik. Na primjer, Erdos je u ([2]) primijetio da iz Spernerovog teorema (vidi [14]) slijedi da ako je $p(\underline{a})$ znatno veći od $n^{-\frac{1}{2}}$, tada $\underline{a}$ ima relativno malen nosač.
Drugi slučaj je dan teoremom Sarkozyja i Szemeredija (vidi [13]), koji kaže da ukoliko su $a_1, \ldots, a_n$ različiti, onda je $p(\underline{a}) = O\left(n^{-\frac{3}{2}}\right)$. Dakle, ako je $p(\underline{a})$ znatno veći od $n^{-\frac{3}{2}}$, onda $\underline{a}$ mora imati puno ponavljajućih komponenti. Ova tvrdnja zajedno s Lemom 1.3.2. daje gornju ogradu $P_n = O\left(n^{-\frac{3}{2}}\right)$.
Također, Halászevi teoremi u [3] i [4] kažu da, ukoliko je $p(\underline{a})$ znatno veći od $n^{\frac{-(2r+1)}{2}}$, onda mora biti priličan broj duplikata među sumama $\pm a_{i_1} \pm \cdots \pm a_{i_r}$.

U ovom radu dat ćemo drugačiji uvjet koji kaže da za d znatno manji od n, $p(\underline{a}) = p_n(\underline{a})$ je sklon biti značajno manji od $p_d(\underline{a})$. Ovo će biti jedan od najbitnijih koraka u dokazu Teorema 1.1.4.
U terminima slučajnih šetnji, gornji rezultat znači sljedeće. Neka su $a_1, \ldots, a_n$ cijeli brojevi i neka je $\mu \in (0, \frac{1}{2})$. Tada je vjerojatnost da se slučajna šetnja s koracima veličina $a_1, \ldots, a_n$ u trenutku n vrati u ishodište manja za faktor $O\left(\sqrt{\mu}\right)$ nego vjerojatnost da se "lijena" slučajna šetnja, koja se u koraku i pomiče za a_i ili $-a_i$, svaki s vjerojatnošću μ, a

inače ostaje gdje je, u trenutku n nađe u ishodištu.
Zanimljivo je da tvrdnja vrijedi za korake proizvoljnih dužina jer je u takvoj općenitosti teško dati čak i razumne procjene za vrijednosti od p_n.

Sada ćemo iskazati pomoćni teorem kojega smo spomenuli u poglavlju 1.1. Označimo sa $\mathrm{supp}(\underline{a})$ broj ne-nul komponenti u $\underline{a}$.

Teorem 1.5.1. *Neka je $0 < \lambda < 1$ i neka je k pozitivni cijeli broj takav da je $4\lambda k^2 < 1$. Ako je $\underline{a} \in \mathbb{Z}^n \setminus \{\underline{0}\}$, onda vrijedi*

$$p(\underline{a}) \leq \left[\frac{1}{k\,(1-4\lambda k^2)} + \frac{1}{1-4\lambda} e^{-(1-4\lambda)\,\mathrm{supp}(\underline{a})/\left(4k^2\right)} \right] Q_\lambda(\underline{a}), \tag{1.3}$$

gdje je $Q = Q_\lambda(\underline{a})$ definiran kao

$$Q = \sum_{d=0}^{n} \binom{n}{d} \left(\lambda e^{-\lambda}\right)^d \left(1 - \lambda e^{-\lambda}\right)^{n-d} p_d(\underline{a}) \tag{1.4}$$

Izbor $k = (12\lambda)^{-\frac{1}{2}}$ daje sljedeći korolar kojeg ćemo zbog važnosti ipak prozvati teoremom.

Teorem 1.5.2. *Za svaki λ postoji $K(\lambda)$ takav da, ukoliko je $(12\lambda)^{-\frac{1}{2}}$ cijeli broj i vrijedi $supp(\underline{a}) \geq K(\lambda)$, onda je $p(\underline{a}) < c_0 \sqrt{\lambda} Q$, pri čemu je $c_0 < 5.2$.*

Napomena 1.5.3. *Neka je $\mu = \lambda e^{-\lambda}$. Primjetimo da je težinska funkcija u Q, $\binom{n}{d} \left(\lambda e^{-\lambda}\right)^d \left(1 - \lambda e^{-\lambda}\right)^{n-d}$ upravo binomna distribucija, a znamo da ona najveće vrijednosti postiže oko očekivanja koje za ovu funkciju iznosi μn. Dakle, u sumu od Q će značajno pridonositi samo one vrijednosti od $p_d(\underline{a})$ za čiji d vrijedi $d \approx \mu n$.*
Prema tome, Teorem 1.5.2. daje sljedeće. Neka je $\mu > 0$. Ako su $a_1, \ldots, a_n$ ne-nul cijeli brojevi i mnogo (udio veći od $(1-\mu)^n$) od ukupno 2^n suma $\sum_{i=1}^n \epsilon_i a_i$ je jednako 0, onda, za neki $d \approx \mu n$ još veći udio od ukupno $\binom{n}{d}2^d$ d-suma iznosi 0. Uočimo, za $d \approx \mu n$ je veći omjer d-suma koje iznose 0 i ukupan broj d-suma, $\binom{n}{d}2^d$ od omjera suma $\sum_{i=1}^n \epsilon_i a_i$ koje su jednake 0 i ukupnog broja tih suma, 2^n. Taj omjer je veći za faktor $\sqrt{\frac{n}{d}}$.

Pogledajmo sada dva primjera vezana uz gornji teorem i napomenu.

Primjer 1.5.4. *Pokazano u (literatura - Imre Ruzsa, privatna komunikacija) Ako je $a_i = i^\alpha$, gdje je α pozitivni cijeli broj, onda za dovoljno velike d, n je $p(\underline{a}) \sim cn^{-\alpha-\frac{1}{2}}$ dok je $p_d(\underline{a}) \sim cn^{-\alpha} d^{-\frac{1}{2}}$.*

Primjer 1.5.5. *Neka su a_i slučajni cijeli brojevi iz skupa $\{1, 2, \ldots, M\}$, onda je $p(\underline{a}) \sim \frac{c}{M\sqrt{n}}$ i $p_d(\underline{a}) \sim \frac{c}{M\sqrt{d}}$.*

Primijetimo da u gornjim granicama iz Teorema 1.5.1. i 1.5.2. vrijednost Q nije najzgodnija niti jednostavna za baratati pa ćemo je u sljedećem raspisu probati pojednostaviti.
Neka je $\epsilon' > 0$ fiksan te neka je $q_\lambda(\underline{a}) = \max\{p_d(\underline{a}) :\mid d - \mu n \mid < \epsilon' n\}$.
Dakle, zbog prvog dijela napomene 1.5.3., promatramo d-ove koji su dovoljno blizu μn.
Sada je, zbog Chernoffove ograde,

$$Q_\lambda(\underline{a}) \leq q_\lambda(\underline{a}) + \sum_{|d-\mu n| \geq \epsilon' n} \binom{n}{d} \mu^d (1-\mu)^{n-d} \tag{1.5}$$

Sada definirajmo $DIV(\mu, \epsilon')$ kao

$$DIV(\mu, \epsilon') = \min\{D(\mu + \epsilon' \parallel \mu), D(\mu - \epsilon' \parallel \mu)\} = \begin{cases} D(\mu - \varepsilon' \parallel \mu) & \text{ako } \mu \leq 1/2 \\ D(\mu + \varepsilon' \parallel \mu) & \text{ako } \mu > 1/2 \end{cases}$$

pri čemu je $D(x \parallel \mu) = x \log(\frac{x}{\mu}) + (1-x) \log \frac{1-x}{1-\mu}$, informacija teoretske divergencije x od μ.
Sada jednadžba (1.5) postaje

$$Q_\lambda(\underline{a}) \leq q_\lambda(\underline{a}) + 2e^{-DIV(\mu,\epsilon')n} \tag{1.6}$$

Sada, prema Teoremu 1.5.2., uz pretpostavku $\text{supp}(\underline{a}) > K(\lambda)$, vrijedi

$$p(\underline{a}) \leq c_0 \sqrt{\lambda} \left(q_\lambda(\underline{a}) + 2e^{-DIV(\mu,\epsilon')n} \right) \tag{1.7}$$

gdje je $c_0 < 5.2$.

1.6 Skica dokaza glavnog teorema

Dokaz Teorema 1.1.4. otprilike će izgledati ovako.
Fiksirat ćemo mali λ i još manji ϵ. Vektore $\underline{a}$ za koje je $p(\underline{a}) < (1-\epsilon)^n$ stavit ćemo u S_0.
Za ostale vektore koristit ćemo S_i-eve temeljene na d-sumama čija je dimenzija γn, pri čemu je $\gamma = \epsilon \frac{n}{d}$, a d poprima vrijednosti u okolini od λn.
Razlika između d-suma i punih suma zbog koje smo i prešli na d-sume je u faktoru $\sqrt{\lambda}$ koji će biti dovoljno malen da se osigura eksponencijalna gornja međa.
Za dani σ, broj S_i-eva kojima pokrivamo $\underline{a}$-ove takve da vrijedi $q_\lambda(\underline{a}) = p_d(\underline{a})$ i $\sigma_d(\underline{a}) \approx \sigma$ otprilike iznosi $\left(\binom{n}{d} \frac{2^d}{\sigma} \right)^{(1-\gamma)n} \approx p_d(\underline{a})^{-(1-\gamma)n}$.

Poglavlje 2

Dokaz pomoćnog teorema

2.1 Halászeva nejednakost

U ovom odjeljku pripremit ćemo neke tehničke dijelove i dokazati Halászevu nejednakost, što ćemo iskoristiti u sljedećem odljeljku kako bismo dokazali Teorem 1.5.1.

Uočimo da vrijedi jednakost

$$\prod_{i=1}^{n} \cos \alpha_i = 2^{-n} \sum_{\underline{\epsilon}} \cos(\epsilon_1 \alpha_1 + \cdots + \epsilon_n \alpha_n),$$

pri čemu sumiramo po svim $\underline{\epsilon} \in \{\pm 1\}^n$.
Iskoristimo Eulerov zapis kompleksnog broja da zapišemo $\cos x = \frac{e^{ix}+e^{-ix}}{2}$ pa produkt zapišemo kao sumu po $\underline{\epsilon} \in \{\pm 1\}^n$ pri čemu su sumandi jednaki $e^{i\underline{\epsilon}\alpha} + e^{-i\underline{\epsilon}\alpha}$ a to je upravo $2\cos\left(\underline{\epsilon}\alpha\right)$.
Gornja jednakost daje, za sve $\underline{a} \in \mathbb{R}^n$,

$$p(\underline{a}) = 2^{-n} \frac{1}{2\pi} \int_0^{2\pi} \sum_{\underline{\epsilon}} \cos((\epsilon_1 \alpha_1 + \cdots + \epsilon_n \alpha_n)t)\, dt = \frac{1}{2\pi} \int_0^{2\pi} \prod_{i=1}^{n} \cos(a_i t)\, dt \tag{2.1}$$

Napomena 2.1.1. *Primijetimo kako je sredina u gornjoj jednakosti upravo Fourierova transformacija distribucije od* $\sum_{i=1}^{n} \epsilon_i a_i$ *pri čemu su* ϵ *uniformno odabrani iz* $\{\pm 1\}^n$. *To nije slučajno, naime, iz Essenove leme prozilazi da za bilo koju konačnu mjeru* μ *vrijedi*

$$\sup_y \int_{|x-y|\leq 1} \mu(dx) \leq c \int_{|t|\leq 1} |\phi(t)|\, dt,$$

gdje je $\phi(t)$ *Fourierova transformacija* $\phi(t) = \int e^{itx} \mu(dx)$ *i c konstanta.*

Prethodnu napomenu možemo iskoristiti kako bismo generalizirali Teorem 1.1.4. na slučajne matrice s proizvoljnim, nezavisnim, jednako distribuiranim netrivijalnim elementima (vidi [10]).

Vratimo se na jednadžbu (2.1) i iskoristimo nejednakost $x \leq |x| \leq e^{-\frac{1-x^2}{2}}$, dobit ćemo

$$p(\underline{a}) \leq \frac{1}{2\pi} \int_0^{2\pi} \exp\left\{ \sum_{i=1}^{n} \frac{-(1-\cos^2(a_i t))}{2} \right\} dt$$

Sada ćemo iskoristiti trigonometrijski identitet $1 - \cos^2 \alpha = \frac{1-\cos(2\alpha)}{2}$ da bismo dobili

$$p(\underline{a}) \leq \frac{1}{2\pi} \int_0^{2\pi} \exp\left\{ -\frac{1}{4} \sum_{i=1}^{n} (1-\cos(2a_i t)) \right\} dt \tag{2.2}$$

Definirajmo funkciju f kao

$$f(t) = \frac{1}{4} \sum_{i=1}^{n} (1-\cos(2a_i t)).$$

Definirajmo još funkcije T i g kao

$$T(x) = \{t \in (0, 2\pi) : f(t) \leq x\}$$

$$g(x) = \frac{1}{2\pi} \mid T(x) \mid$$

gdje je $|\cdot|$ Lebesgueova mjera. Dakle, funkcija T vraća sve $t \in (0, 2\pi)$ koji su manji od argumenta x, a funkcija g daje njenu Lebesgueovu mjeru normiranu s $\frac{1}{2\pi}$.

Sada možemo (2.2) zapisati kao

$$p(\underline{a}) \leq \frac{1}{2\pi} \int_0^{2\pi} e^{-f(t)}\, dt = \int_0^{2\pi} \int_{f(t)}^{\infty} \frac{1}{2\pi} e^{-x}\, dx\, dt = \int_0^{\infty} e^{-x} g(x)\, dx \tag{2.3}$$

Sljedeća nejednakost, takozvana Halászeva vrlo je važna za dokaz Teorema 1.5.1.
Za svaki $x > 0$ i pozitivni cijeli broj k, uz pretpostavku da je $g(k^2 x) < 1$, vrijedi

$$g(x) \leq \frac{g(k^2 x)}{k} \tag{2.4}$$

Gornja pretpostavka $g(k^2 x) < 1$ vrijedi ukoliko je $k^2 x \leq \frac{\text{supp}(\underline{a})}{4}$ jer je $\frac{1}{2\pi} \int_0^{2\pi} f(t)\, dt = \frac{\text{supp}(\underline{a})}{4}$.
Ta jednakost jednostavno slijedi iz činjenice da, ukoliko je $a_i = 0$, onda je $\cos(2a_i t) = 1$ pa

taj a_i ne pridonosi u sumu od $f(t)$, a ukoliko je $a_i \neq 0$, onda je $\int_0^{2\pi} 1 - \cos(2a_i t)\, dt = 2\pi$ pa taj a_i u sumu od $f(t)$ pridonosi s $\frac{2\pi}{4}$.

Skicirat ćemo Halászev dokaz od (2.4). Za fiksni $k \geq 2$, neka je $T^*(x) = \{t_1 + \cdots + t_k : t_i \in T(x)\}$, pri čemu zbrajanje uzimamo modulo 2π. Tada tražena nejednakost slijedi iz

$$T^*(x) \subset T(k^2 x), \tag{2.5}$$

$$\frac{1}{2\pi} \mid T^*(x) \mid \geq \min\{kg(x), 1\}. \tag{2.6}$$

(2.5) slijedi iz identiteta

$$1 - \cos(\alpha) = 2\sin^2\left(\frac{\alpha}{n}\right)$$

i nejednakosti

$$\sin^2\left(\sum_{i=1}^{k} \alpha_i\right) \leq \left(\sum_{i=1}^{k} |\sin \alpha_i|\right)^2 \leq k \sum_{i=1}^{k} \sin^2 \alpha_i.$$

Dokaz (2.6) nalazi se u [3].
Sada kad imamo (2.5) i (2.6) nije teško uočiti da vrijedi (2.4). Naime, zbog (2.5) vrijedi $\mid T(k^2x) \mid > \mid T^*(x) \mid$, a zbog (2.6) je $\frac{1}{2\pi} \mid T(k^2x) \mid \geq kg(x)$, odnosno $\frac{g(k^2x)}{k} \geq g(x)$.

2.2 Dokaz

Dokažimo Teorem 1.5.1.

Dokaz. Fiksirajmo λ takav da $0 < \lambda < 1$.
Zapišimo $g(x)$ kao

$$g(x) = \frac{1}{2\pi} \left| \left\{ t \in (0, 2\pi) : \exp\left\{ \lambda \sum_i \cos(2a_i t) \right\} \geq \exp\{\lambda(n - 4x)\} \right\} \right| \tag{2.7}$$

što koristeći Markovljevu nejednakost možemo odozgo ograničiti s

$$\exp\{-\lambda(n - 4x)\} \frac{1}{2\pi} \int_0^{2\pi} \exp\left\{ \lambda \sum_i \cos(2a_i t) \right\} dt$$

Za, $|z| \leq 1$ vrijedi

$$e^{\lambda z} \leq e^{\lambda} - \lambda(1 - z)$$

što daje

$$\exp\left\{\lambda \sum_i \cos(2a_i t)\right\} \leq \prod \left(e^{\lambda} - \lambda + \lambda \cos(2a_i t)\right)$$

Sada se vratimo na (2.7) i iz gornjeg produkta izlučimo $e^{-\lambda}$

$$g(x) \leq e^{4\lambda x} \frac{1}{2\pi} \int_0^{2\pi} \prod \left(1 - \lambda e^{-\lambda} + \lambda e^{-\lambda} \cos(2a_i t)\right) dt$$

Iskoristimo $\mu = \lambda e^{-\lambda}$ i raspišimo produkt kao

$$\begin{aligned} e^{4\lambda x} \frac{1}{2\pi} \int_0^{2\pi} \prod \left(1 - \lambda e^{-\lambda} + \lambda e^{-\lambda} \cos(2a_i t)\right) dt &= e^{4\lambda x} \sum_d \sum_{i_1 < \cdots < i_d} \mu^d (1-\mu)^{n-d} \frac{1}{2\pi} \int_0^{2\pi} \prod_{j=1}^{d} \cos(2a_i t)\, dt \\ &= e^{4\lambda x} \sum_d \mu^d (1-\mu)^{n-d} \frac{\sigma_d(\underline{a})}{2^d} \\ &= e^{4\lambda x} \sum_d \binom{n}{d} \mu^d (1-\mu)^{n-d} p_d(\underline{a}) \\ &= e^{4\lambda x} Q \end{aligned}$$

Dakle, ovim računom pokazali smo da vrijedi

$$g(x) \leq e^{4\lambda x} Q. \tag{2.8}$$

Sada imamo sve što nam treba da završimo dokaz.
Neka je k pozitivni cijeli broj takav da je $4\lambda k^2 < 1$. Označimo sa $S = \frac{\operatorname{supp}(\underline{a})}{4k^2}$ i zapišimo (2.3) kao

$$p(\underline{a}) \leq \int_0^{\infty} e^{-x} g(x)\, dx = \int_0^{S} e^{-x} g(x)\, dx + \int_S^{\infty} e^{-x} g(x)\, dx.$$

Omeđimo prvo drugi integral i to tako da iskoristimo (2.8)

$$\int_S^{\infty} e^{-x} g(x) dx \leq \int_S^{\infty} e^{-x} e^{4\lambda x} Q dx = \frac{Q}{1-4\lambda} e^{-(1-4\lambda)S}$$

Promotrimo sada prvi integral. Za $x \in (0, S)$ vrijedi $k^2 x \leq k^2 S = \operatorname{supp} \frac{a}{4}$. Dakle, možemo primijeniti (2.4) pa dobijemo

$$\int_0^{S} e^{-x} g(x) dx \leq \int_0^{S} \frac{1}{k} g\left(k^2 x\right) e^{-x} dx \leq \frac{Q}{k} \int_0^{S} e^{-\left(1-4\lambda k^2\right)x} dx \leq \frac{Q}{k\left(1-4\lambda k^2\right)}.$$

Uočimo da smo u drugoj nejednakosti opet koristili (2.8).
Dakle, za fiksni λ, $0 < \lambda < 1$ pokazali smo da postoji pozitivni cijeli broj k takav da je $4\lambda k^2 < 1$ i da za sve $\underline{a} \in \mathbb{Z}^n \setminus \{0\}$ vrijedi

$$p(\underline{a}) \leq \frac{Q}{k\,(1-4\lambda k^2)} + \frac{Q}{1-4\lambda} e^{-(1-4\lambda)S} = \left[\frac{1}{k\,(1-4\lambda k^2)} + \frac{1}{1-4\lambda} e^{-(1-4\lambda)\,\mathrm{supp}(\underline{a})/\left(4k^2\right)} \right] Q_\lambda(\underline{a}),$$

gdje je $Q = Q_\lambda(\underline{a})$ definiran kao u (1.4) □

Poglavlje 3

Dokaz glavnog teorema

3.1 $\underline{a}$-ovi s mnogo nula

Ispostavit će se korisno pokazati da slučajevi $\underline{a}$-ova s puno nula ne pridonose mnogo gornjoj međi od P_n.
Sljedeće zapažanje je iz [1].
Za sve K vrijedi

$$\mathbb{P}\left(\bigcup_{\underline{a}:\mathrm{supp}(\underline{a})\leq K} E_{\underline{a}}\right) \leq \sum_{k=2}^{K} \binom{n}{k}\binom{n}{k-1}\left[2^{-k}\binom{k}{\lfloor k/2\rfloor}\right]^{n-k+1} \tag{3.1}$$

Posebno, vrijedi

$$\mathbb{P}\left(\bigcup_{\underline{a}:\mathrm{supp}(\underline{a})\leq n-3\frac{n}{\log_2 n}} E_{\underline{a}}\right) \leq n^3 2^{-n} \tag{3.2}$$

Napomena 3.1.1. *Ova gornja ograda čak se može i poboljšati mijenjanjem faktora* $\binom{n}{k-1}$ *za* $\binom{n-1}{k-2}$ *u* (3.1) *što daje ogradu* $(1+o(1))n^2 2^{-n}$. *Dakle, kao što smo i htjeli pokazati, vektori* $\underline{a}$ *s bar* $3\frac{n}{log_2 n}$ *nula ne ometaju dokaz Teorema 1.1.4., a čak ni eventualni dokaz tvrdnje* (1.1).

3.2 Lema Odlyzkovog tipa

Prisjetimo se, V_d je skup vektora s vrijednostima u $\{-1,0,1\}$ s točno d ne-nul koordinata. Također je korisno sljedeće opažanje.

Lema 3.2.1. *Neka je S D-dimenzionalni podskup od $\mathbb{R}^n$, tada vrijedi*

$$|S \cap V_d| \leq F(D,d) := \sum_{i=D-n+d}^{d} \binom{D}{i} 2^i$$

Dokaz. Bez smanjenja općenitosti, možemo pretpostaviti da je skup restrikcija vektora iz S na koordinate $\{1,\ldots,D\}$ dimenzije D. Prema tome, različiti vektori iz $S \cap V_d$ imaju različite restrikcije na te koordinate, ali bitno je da je svaki od njih vektor s vrijednostima $\{-1,0,1\}$ i to s ne manje od $D-n+d$ i ne više od d ne-nul koordinata. Očito je da svaki vektor iz $S \cap V_d$ ima najviše d ne-nul koordinata jer taj vektor mora biti iz V_d. Za najmanje moguće ne-nul koordinata, objašnjenje dolazi iz činjenice da je moguće da restringirani vektor iz $S \cap V_d$ ima najviše $n-d$ nula pa taj isti vektor mora imati bar $D-(n-d)$ ne-nul koordinata.
Kardinalnost skupa se sada dobije da prebrojimo sve moguće vektora sa svim mogućim brojnostima ne-nul koordinata. □

Slučaj $D = n$ poznat je kao Odlyzkov rezultat, navedimo ga kao korolar.

Korolar 3.2.2. *Za V podksup od $\mathbb{R}^n$ i vektor $\underline{r}$ odabran slučajno uniformno iz $\{\pm 1\}^n$, vrijedi*

$$\mathbb{P}\left(\underline{r} \in V^{\perp}\right) \leq 2^{-\dim(V)}$$

3.3 Profinjenje Leme 1.3.2.

Kao što smo i spomenuli, malo profinjenija verzija Leme 1.3.2. dat će nešto bolji ϵ u Teoremu 1.1.4, iskažimo ju.

Lema 3.3.1. *Pretpostavimo da k-dimenzionalni S podksup od $\mathbb{R}^n$ i vrijednosti p, ϵ'' zadovoljavaju*

$$p(S) \leq p$$

te još zadovoljavaju tehničke uvjete

$$p < \epsilon'' < \frac{1}{2}$$

$$p^{-1} 2^{-\epsilon'' n} < n^{-2}.$$

Tada, za dovoljno veliki n, vrijedi

$$\mathbb{P}\left(\bigcup_{\underline{a} \in S} E_{\underline{a}}\right) < \binom{n}{\epsilon'' n} p^{n-k+1}$$

U pripremi dokaza Lema 1.3.2. i 3.3.1. promotrimo sljedeće. Neka su $\underline{r}_1, \ldots, \underline{r}_n$ retci matrice M. Tada je nužni uvjet za događaj $E_S := \bigcup_{\underline{a} \in S} E_{\underline{a}}$ da postoji najviše $k-1$ indeksa $j \in [n] = \{1, \ldots, n\}$ za koje vrijedi

$$\dim \left\langle S \cap \bigcap_{l \leq j} \underline{r}_l^{\perp} \right\rangle < \dim \left\langle S \cap \bigcap_{l < j} \underline{r}_l^{\perp} \right\rangle \tag{3.3}$$

Pokažimo zašto je to nužni uvjet. Pogledajmo skup na lijevoj strani u (3.3). Dimenzija tog skupa je najviše k jer je to dimenzija od S, a najmanje 1 zato što je pretpostavka da se dogodio E_S pa ne može biti 0. Međutim, zbog nejednakosti (3.3) svi ti skupovi moraju imati različite dimenzije. Kada bi postojalo k takvih indeksa j, to znači da bi imali k skupova različitih dimenzija između 1 i k. Tada bi za svaku od dimenzija od 1 do k, postojao neki indeks j za koji bi skup na lijevoj strani u (3.3) imao tu dimenziju. Posebno, neka je j_0 indeks za koji skup na lijevoj strani u (3.3) ima dimenziju k. Iz nejednakosti (3.3) primijenjene na j_0, zaključujemo da skup na desnoj strani ima dimenziju $> k$, što je nemoguće jer je dimenzija od S jednaka k.

Skup $S \cap \bigcap_{l \leq j} \underline{r}_l^{\perp}$ označava sve $\underline{a} \in S$ koji su okomiti na svaki od prvih j redaka uključujući i j-ti redak dok skup s desne strane ne uključuje j-ti redak. Primijetimo da se dimenzija tih skupova neće razlikovati ukoliko je j-ti redak linearna kombinacija redaka prije njega presječeno na prostor S.
Označimo događaj iz (3.3) s F_j. Za $I \subset \{1, \ldots, n\}$ neka je H_I događaj $S \cap \bigcap_{i \in I} \underline{r}_i^{\perp} \neq \{\underline{0}\}$. Dakle, postoji $\underline{a} \in S$ takav da je $\underline{a}$ ortogonalan na sve retke s indeksom $i \in I$.
Sada smo spremni dokazati Lemu 1.3.2.

Dokaz. Iz gornje diskusije možemo uočiti da vrijedi

$$\mathbb{P}(E_S) \leq \sum_{J \subset [n], |J| = n-k+1} \mathbb{P}\left(H_{[n] \setminus J} \cap \bigcap_{j \in J} \overline{F}_j \right)$$

Događaj na desnoj strani označava da retci s indeksima $j \in J$ ne utječu na dimenziju skupa $S \cap \bigcap_{l \leq j} \underline{r}_l^{\perp}$ te da postoji $\underline{a} \in S$ koji poništava retke koji utječu na dimenziju takvih skupova, a onda i cijelu matricu M jer su retci s indeksima iz J linearne kombinacije ostalih redaka presječeno na prostor S.
Indeksa u J (za koje ne vrijedi F_j) ima $n-k+1$ jer smije postojati najviše $k-1$ indeksa za koje vrijedi F_j. Primijetimo, ako postoji $k-i$ takvih indeksa gdje je $1 < i < k-1$, taj događaj je podskup događaja da postoji $k-1$ indeks za koji vrijedi F_j. Naime, tih $k-1$ indeksa za koje je dimenzija skupova u (3.3) različita sigurno sadrži i manji broj indeksa, $k-i$ za koje je ta dimenzija različita jer je $k-1$ najveći broj indeksa za koje tako nešto

vrijedi.
Pokažimo da za svaki $J \subset [n]$ vrijedi

$$\mathbb{P}\left(H_{[n]\setminus J} \cap \bigcap_{j\in J} \overline{F}_j\right) \leq \mathbb{P}\left(\bigcap_{j\in J} \overline{F}_j | H_{[n]\setminus J}\right) \leq p(S)^{|J|}$$

Prva nejednakost slijedi iz definicije uvjetne vjerojatnosti. Fiksirajmo retke $\underline{r}_j$, $j \notin J$ koji zadovoljavaju $H_{[n]\setminus J}$.
Sada eventualni događaj $\overline{F}_j$ povlači da za $j \in J$, $\underline{r}_j$ se nalazi u $\left\langle S \cap \bigcap_{l<j} \underline{r}_l^{\perp} \right\rangle^{\perp}$, odnosno da je ortogonalan na svaki $\underline{a} \in S \cap \bigcap_{l<j} \underline{r}_l^{\perp}$. To vrijedi jer je $\underline{r}_j$ linearna kombinacija svojih prethodnika presječeno na S pa je ortogonalan na svaki $\underline{a} \in S$ koji je ortogonalan na te prethodnike.
Vjerojatnost događaja $\{\underline{r}_j$ je ortogonalan na svaki $\underline{a} \in S \cap \bigcap_{l<j} \underline{r}_l^{\perp}\}$ je najviše $p(S)$. Jer su retci birani nezavisno i jer takvih redaka mora biti $|J|$, zaključujemo da vrijedi i druga nejednakost.
Završimo sada dokaz, od n redaka izaberimo $k-1$ za koje vrijedi F_j i sjetimo se da je $|J| = n-k+1$

$$\mathbb{P}(E_S) \leq \begin{pmatrix} n \\ k-1 \end{pmatrix} p(S)^{n-k+1}$$

□

Pokažimo sada da vrijedi lema 3.3.1.

Dokaz. Primijetimo da možemo pretpostaviti da vrijedi

$$\epsilon'' n \leq k \leq n - \epsilon'' n \tag{3.4}$$

jer u suprotnom zaključak slijedi iz Leme 1.3.2.
Neka je $I \subset [n]$ takav da $|I| \leq k-1$ te neka je $J = [n] \setminus I$, definirajmo

$$G_I = H_I \cap \bigcap_{i\in I} F_i, \qquad F_I = G_I \cap \bigcap_{j\in J} \overline{F}_j.$$

Uočimo da je zbog rasprave s početka ovog poglavlja kardinalitet od I manji ili jednak $k-1$. Intuitivno, u skupu G_I su svi $\underline{a} \in S$ koji su okomiti na sve $\underline{r}_i$, $i \in I$ pri čemu su svi ti retci linearno nezavisni presječeno na S. U skupu F_I su svi $\underline{a}$ koji su u G_I i za koje vrijedi da su svi ostali retci $\underline{r}_j$, $j \in J$ linearno zavisni presječeno na S.
Dakle, vrijedi

$$\mathbb{P}(E_S) \leq \sum_{I\subset[n],|I|\leq k-1} \mathbb{P}(F_I) \tag{3.5}$$

jer je događaj E_S podskup događaja $\bigcup_{I\subset[n],|I|\leq k-1} F_I$.
Za $j \in J$, neka je $t(j) = |I \setminus [j]|$. Tada vrijedi

$$\mathbb{P}(F_I) \leq \mathbb{P}\left(\bigcap_{j\in J} \overline{F}_j | G_I\right) \leq \prod_{j\in J} \min\{2^{-t(j)-1}, p(S)\} =: f(I). \tag{3.6}$$

Prva nejednakost opet slijedi iz formule uvjetne vjerojatnosti. Da bismo pokazali drugu, fiksirajmo retke $\underline{r}_i$, $i \in I$ takve da zadovoljavaju G_I. Tada događaj $\overline{F}_j$ zahtjeva da vrijedi

$$\underline{r}_j \in \left\langle S \cap \bigcap_{l<j} \underline{r}_l^{\perp} \right\rangle^{\perp}. \tag{3.7}$$

Sada iz G_I slijedi da vrijedi (ta mi nejednakost nije jasna)

$$\dim\left\langle S \cap \bigcap_{l<j} \underline{r}_l^{\perp} \right\rangle \geq \dim\left\langle S \cap \bigcap_{i} \underline{r}_l^{\perp} \right\rangle + t(j) \geq t(j) + 1.$$

Sada možemo iskoristiti Korolar 3.2.2. i zaključiti da se (3.7) događa s vjerojatnoću najviše $2^{-t(j)-1}$. Međutim, (3.7) također zahtjeva da je $\underline{r}_j$ ortogonalan na svaki $\underline{a} \in S \cap \bigcap_{l<j} \underline{r}_l^{\perp}$, a to se događa s vjerojatnošću najviše $p(S)$. Sada imamo drugu nejednakost u (3.6)
Promotrimo I kardinaliteta $k-1$. Stavimo $m = k - \epsilon'' n$ i pretpostavimo da je $|I \cap [m]| = i$. Tada je $t(j) \geq k - 1 - i$ za $j \in J \cap [m]$ te po (3.6)

$$f(I) \leq 2^{-(k-i)(m-i)} p(S)^{n-k-m+i+1}.$$

Kada bismo varirali I, dobili bismo

$$\sum_{I\subset[n],|I|=k-1} f(I) < \sum_{i=0}^{m} \binom{m}{i}\binom{n-m}{k-1-i} 2^{-(k-i)(m-i)} p(S)^{n-k-m+i+1} < (1+o(1))\binom{n-m}{k-1-m} p^{n-k+1} \tag{3.8}$$

pri čemu prva nejednakost slijedi iz gornjeg raspisa ograde od $f(I)$ i činjenice da od m indeksa biramo njih i koji su u I te od $n-m$ indeksa biramo njih $k-1-i$ koji su u I. Druga nejednakost slijedi iz uvjeta leme $p(S) \leq p$ te $p^{-1}2^{-\epsilon'' n} < n^{-2}$.
Za manje I-eve uočimo da za svaki $I \subset I' \subset [n]$ vrijedi

$$f(I) \leq p^{|I'\setminus I|} f(I').$$

Dakle, po (3.5) možemo pisati

$$\mathbb{P}(E_S) \leq \sum_{t=0}^{k-1} \sum_{I\subset[n],|I|=k-1-t} f(I) \leq \sum_{t=0}^{k-1} \frac{\binom{n}{k-1-t}}{\binom{n}{k-1}} p^t \sum_{I\subset[n],|I|=k-1} f(I) = X$$

pri čemu smo u drugoj nejednakosti iskoristili gornji raspis za male I te $|I' \setminus I| = t$.
Sada iskoristimo (3.8) da dobijemo

$$X < (1+o(1)) \sum_{t=0}^{k-1} \frac{\binom{n}{k-1-t}}{\binom{n}{k-1}} p^t \binom{n-m}{k-1-m} p^{n-k+1} = Y$$

Na kraju, iskoristimo (3.4) i činjenicu da je $p < \epsilon'' < \frac{1}{2}$ da dobijemo

$$\mathbb{P}(E_S) < Y < \binom{n}{\epsilon'' n} p^{n-k+1}$$

što je i trebalo pokazati. □

3.4 Konstrukcija skupova S_i

U ovom odjeljku konstruirat ćemo skupove S_i koje ćemo koristiti u Lemi 3.3.1.
Neka su $\lambda, \mu = \lambda e^{-\lambda}, \epsilon, \epsilon' = \alpha\mu$ male pozitivne konstante. Pretpostavimo da vrijedi

$$1 - \epsilon > e^{-DIV(\mu,\epsilon')} \tag{3.9}$$

Tada Teorem 1.5.2. i (1.7) daju da za svaki $\underline{a}$ takav da je

$$q_\lambda(\underline{a}) > (1-\epsilon)^n \qquad i \qquad \text{supp}(\underline{a}) > K(\lambda)$$

vrijedi

$$p(\underline{a}) < 5.2\sqrt{\lambda} q_\lambda(\underline{a}). \tag{3.10}$$

Fiksirajmo dva cijela broja d i σ tako da vrijedi

$$|d - \mu n| < \epsilon' n \tag{3.11}$$

i

$$(1-\epsilon)^n N \le \sigma \le N, \tag{3.12}$$

gdje je $N = N_d = |V_d| = \binom{n}{d} 2^d$.
Za takve d i σ definirajmo skupove

$$M(d,\sigma) = \{\underline{a} \in \mathbb{Z}^n \setminus \{\underline{0}\} : \text{supp}(\underline{a}) > K(\lambda), q_\lambda(\underline{a}) = p_d(\underline{a}), \sigma_d(\underline{a}) = \sigma\}.$$

Prisjetimo se, $\sigma_d(\underline{a})$ je definiran kao kardinalitet skupa svih $\epsilon \in V_d$ koji su ortogonalni na $\underline{a}$, $p_d(\underline{a}) = \frac{\sigma_d(\underline{a})}{N}$ te $q_\lambda(\underline{a}) = \max\{p_d(\underline{a}) : |d - \mu n| < \epsilon' n\}$.

Sada nije teško uočiti da svi vektori $\underline{a} \in M(d, \sigma)$ zadovoljavaju $q_\lambda(\underline{a}) > (1-\epsilon)^n$ i $\text{supp}(\underline{a}) > K(\lambda)$ a time i (3.10).
Definirajmo još $\delta = \frac{d}{n}, \gamma = \frac{\epsilon}{\delta}$ i

$$D = (1-\gamma)n, \tag{3.13}$$

izabrat ćemo parametre tako da vrijedi $d \leq \frac{D}{2}$, odnosno

$$\gamma \leq 1 - 2\delta \tag{3.14}$$

što povlači da vrijedi $F(D,d) = \sum_{i=D-n+d}^{d} \binom{D}{i} 2^i < 2\binom{D}{d} 2^d$.
Također primijetimo, jer vrijedi $\gamma < 1$, slijedi

$$(1-\gamma)^\delta < 1 - \epsilon. \tag{3.15}$$

$M(d, \sigma)$ pokrit ćemo skupovima S_i pri čemu će se svaki S_i sastojati od $\underline{a}$-ova koji su ortogonalni na D linearno nezavisnih vektora iz V_d. Prvo dajmo egzistenciju skupova na koji će $\underline{a}$-ovi biti ortogonalni.

Lema 3.4.1. *Postoji $m < (1+o(1))\left(\frac{N}{\sigma}\right)^D \log\binom{N}{\sigma}$ i skupovi $W_1, \ldots, W_m$ od kojih se svaki sastoji od D linearno nezavisnih vektora iz V_d, takvi da svaki σ-podskup od V_d sadrži bar jedan W_i.*

Dokaz. Fiksirajmo podskup $\Sigma \subset V_d$ takav da je $|\Sigma| = \sigma$ i neka je $q = \frac{\sigma}{N}$. Izaberimo $w_1, \ldots, w_D$ iz V_d uniformno i nezavisno jedan od drugog te definirajmo događaj F kao

$$F = \{w_1, \ldots, w_D \text{ su linearno nezavisni elementi od } \Sigma\}.$$

Tvrdimo da je

$$\mathbb{P}(F) = (1 - o(1))q^D.$$

Jer je $\mathbb{P}(w_1, \ldots, w_D \in \Sigma) = q^D$, dovoljno je pokazati da vrijedi

$$\mathbb{P}(F | w_1, \ldots, w_D \in \Sigma) = 1 - o(1). \tag{3.16}$$

Ta vjerojatnost je upravo jednaka vjerojatnosti $P := \mathbb{P}(v_1, \ldots, v_D \text{ su linearno nezavisni })$ gdje su $v_1, \ldots, v_D$ izabrani iz V_d uniformno i nezavisno jedan od drugog.
Vjerojatnost P možemo zapisati kao

$$P > 1 - \sum_{i=1}^{D} \mathbb{P}(v_i \in \langle v_1, \ldots, v_{i-1} \rangle),$$

odnosno kao 1− vjerojatnost da je neki v_i linearno zavisan koja je manja od vjerojatnosti da je neki v_i zavisan od svojih prethodnika. Tu vjerojatnost zbog Leme 3.2.1. možemo omeđiti na sljedeći način

$$\mathbb{P}\left(v_i \in \langle v_1, \ldots, v_{i-1}\rangle\right) \leq \frac{F(i-1,d)}{\sigma}$$

gdje je S iz leme upravo skup $\{\langle v_1, \ldots, v_{i-1}\rangle\}$ čija je dimenzija najviše $i-1$ pa je vjerojatnost da smo slučajno izabrali vektor v_i iz tog skupa jednaka $\frac{|S\cap V_d|}{\sigma} \leq \frac{F(i-1,d)}{\sigma}$. Sada P možemo ograničiti kao

$$1 - \sum_{i=1}^{D} \mathbb{P}\left(v_i \in \langle v_1, \ldots, v_{i-1}\rangle\right) \geq 1 - \sum_{i=1}^{D} \frac{F(i-1,d)}{\sigma} > 1 - D\frac{F(D,d)}{\sigma}.$$

Sada omeđimo faktor $\frac{F(D,d)}{\sigma}$, prvo iskoristimo (3.12) da dobijemo

$$\frac{F(D,d)}{\sigma} < 2\frac{D(D-1)\cdots(D-d+1)}{n(n-1)\cdots(n-d+1)}\frac{1}{(1-\epsilon)^n} < 2\left(\frac{D}{n}\right)^d \frac{1}{(1-\epsilon)^n}.$$

Sada ćemo iskoristiti (3.13) te (3.15) redom da bismo dobili

$$2\left(\frac{D}{n}\right)^d \frac{1}{(1-\epsilon)^n} < 2\frac{(1-\gamma)^{nd}}{(1-\epsilon)^n} = 2\left(\frac{(1-\gamma)^d}{1-\epsilon}\right)^n < 2\left(\frac{1-\epsilon}{1-\epsilon}\right)^n = 2$$

pa slijedi (3.16) što smo i htjeli pokazati.
Time je lema dokazana, za prigodni $m < (1+o(1))\left(\frac{N}{\sigma}\right)^D \log\binom{N}{\sigma}$ i D-podskupove $W_1, \ldots, W_m$ čije elemente biramo uniformno i nezavisno jedan od drugog iz V_d, očekivani broj σ-podskupova od V_d koji ne sadrže nezavisne W_i jednak je

$$\binom{N}{\sigma}\left(1-(1-o(1))q^D\right)^m < 1,$$

jer od N vektora biramo njih σ a vjerojatnost da su oni nezavisni je $(1-o(1))q^D$ i tako za m podskupova. Dakle, postoje W_i-ovi iz iskaza leme. □

Sada imamo sve što nam treba kako bismo definirali skupove S_i. Neka je

$$S_j = \langle W_j\rangle^{\perp} \cap M(d,\sigma).$$

Pretpostavimo da konstanta ϵ'' zadovoljava

$$\epsilon'' > -\log_2(1-\epsilon). \tag{3.17}$$

Primijenimo Lemu 3.3.1. za $S = S_j$, $k = D$, $p = p(\underline{a})$ te iskoristimo (3.10) i činjenicu da je $q_\lambda(\underline{a}) = p_d(\underline{a}) = \frac{\sigma_d(\underline{a})}{|V_d|} = \frac{\sigma}{N}$ kako bismo dobili

$$\mathbb{P}\left(\bigcup_{\underline{a}\in S_j} E_{\underline{a}}\right) \leq \binom{n}{\epsilon'' n}\left(\frac{5.2\sqrt{\lambda}\sigma}{N}\right)^D.$$

Jer imamo m takvih skupova koji pokrivaju $M(d,\sigma)$ i jer je $m < \left(\frac{N}{\sigma}\right)^D N$, slijedi

$$\mathbb{P}\left(\bigcup_{\underline{a}\in M(d,\sigma)} E_{\underline{a}}\right) < m\binom{n}{\epsilon'' n}\left(\frac{5.2\sqrt{\lambda}\sigma}{N}\right)^D \tag{3.18}$$

$$< N\binom{n}{\epsilon'' n}\left(5.2\sqrt{\lambda}\right)^D \tag{3.19}$$

$$< 2^{\left(H_2(\delta)+\delta+H_2(\epsilon'')+(1-\gamma)\log_2(5.2\sqrt{\lambda})\right)n} =: m_d \tag{3.20}$$

Prema tome, uz korištenje činjenice da za svaki d, $\underline{a}$-ova u $M(d,\sigma)$ ima najviše $N = N_d$, imamo

$$\mathbb{P}\left(\bigcup_{\underline{a}:\mathrm{supp}(\underline{a})>K(\lambda),q_\lambda(\underline{a})>(1-\epsilon)^n} E_{\underline{a}}\right) < \sum_d N_d m_d \tag{3.21}$$

pri čemu suma šeće po svima d za koje vrijedi (3.11).
Faktor N u gornjoj ogradi je znatno veći nego je potrebno pa ćemo ga modificirati kako bi kasnije dobili bolju gornju među.
Promotrimo particiju intervala $[(1-\epsilon)^n N, N]$ u intervale oblika

$$I = \left\{\sigma : \left(1+\frac{1}{n}\right)^t < \sigma \leq \left(1+\frac{1}{n}\right)^{t+1}\right\}.$$

Iskoristimo Lemu 3.4.1. kako bismo pokrili $\bigcup_{\sigma\in I} M(d,\sigma)$. Uočimo, do sad smo koristili Lemu 3.4.1. za pokrivanje pojedinačnog $M(d,\sigma)$.
Ova promjena nema nikakvog utjecaja na gornje račune i dopušta nam da (3.21) zamijenimo s

$$\mathbb{P}\left(\bigcup_{\underline{a}:\mathrm{supp}(\underline{a})>K(\lambda),q_\lambda(\underline{a})>(1-\epsilon)^n} E_{\underline{a}}\right) < n^2 \sum_d m_d. \tag{3.22}$$

Naposlijetku, definirajmo S_0 kao

$$S_0 = \left\{\underline{a} \in \mathbb{Z}^n \setminus \{\underline{0}\} : q_\lambda(\underline{a}) \leq (1-\epsilon)^n \text{ ili } \mathrm{supp}(\underline{a}) \leq K(\lambda)\right\}$$
$$= \mathbb{Z}^n \setminus \left\{\{\underline{0}\} \cup \bigcup_{d,\sigma} M(d,\sigma)\right\}.$$

Zbog (1.7) i (3.9) te uvjeta $q_\lambda(\underline{a}) \leq (1-\epsilon)^n$, $\text{supp}(\underline{a}) > K(\lambda)$, za izbor $\lambda = \frac{1}{108}$ vrijedi

$$p(\underline{a}) < (1-\epsilon)^n.$$

Zbog toga, po Lemi 1.3.1. i nejednakosti (3.2) slijedi ograda za $\underline{a} \in S_0$

$$\mathbb{P}\left(\bigcup_{\underline{a}\in S_0} E_{\underline{a}}\right) < n(1-\epsilon)^n + n^3 2^{-n}.$$

S tom nejednakosti i (3.22) na kraju imamo

$$P_n < n^2 \sum m_d + n(1-\epsilon)^n + n^3 2^{-n}. \tag{3.23}$$

3.5 Izbor parametara

Naposlijetku nam preostaje samo izabrati parametre. Dovoljno je samo izabrati λ i $\alpha = \frac{\epsilon'}{\mu}$ jer ostale vrijednosti slijede iz (3.9), (3.11), (3.14) te (3.17).
Jedan prikladan odabir je vrijednost $\lambda = \frac{1}{108}$ iz čega slijedi $k = 3$ i $\mu = \lambda e^{-\lambda}$ te $\alpha = 0.5$ iz čega slijedi $\epsilon' = 5\mu, \epsilon'' = 0.01$ te $\epsilon = 0.002$.
Analizirajmo sada vrijednost izraza iz (3.20), $H_2(\delta) + \delta + H_2(\epsilon'') + (1-\gamma)\log_2(5.2\sqrt{\lambda}) = \frac{1}{n}\log_2 m_d$.
Derivirajmo po δ i uočimo da su vrijednosti tog izraza u ekstremima $\delta = (1 \pm \alpha)\mu$ manje od $\log_2(1-\epsilon)$, a vrijednosti druge derivacije u točkama između ekstrema su pozitivne pa možemo zaključiti da je cijeli izraz manji od $\log_2(1-\epsilon)$.
Dakle, ograda u (3.23) za velike n u biti je jednaka drugom izrazu te ograde iz čega slijedi Teorem 1.1.4.

Poglavlje 4

Zaključci i posljedice

4.1 Poboljšanja gornje ograde

Rezultat iz našeg rada pokazan je 1995. godine u [5]. Od tada se gornja ograda poboljšala nekoliko puta.
U [6] je pokazano da vrijedi $P_n \leq 0.939^n$, a isti autori su u [7] dokazali nejednakost $P_n \leq \left(\frac{3}{4} + o(1)\right)^n$. Nakon toga, u [8] ograda je poboljšana na $\left(\frac{1}{\sqrt{2}} + o(1)\right)^n$. Najnoviji rezultat, star godinu dana, skoro je dokazao hipotezu (1.1) s početka ovog rada, a nalazi se u [9].

4.2 O distribuciji od $\det(M_n)$

Pogledajmo što možemo zaključiti o distribuciji od $\det(M_n)$. Pokažimo da je $\det(M_n)$ uvijek djeljiva s 2^{n-1}.
Neka je M $n \times n$ matrica čiji su elementi ± 1. Dodajmo prvi redak od M svim ostalim retcima, označimo tako dobivenu matricu s N. Primijetimo da su mogući elementi u donjim $n-1$ retcima od N $2, 0$ i -2 te da zbog svojstva determinante vrijedi $\det(M) = \det(N)$.
Iskoristimo Laplaceovu transformaciju po prvom retku kako bismo dobili

$$\det(N) = \sum_{j=1}^{n} (-1)^{j+1} N_{1j} \det(C_{1j})$$

gdje je C_{1j} $(n-1) \times (n-1)$ matrica bez prvog retka i j-tog stupca.
Jer su svi elementi od C_{1j} $2, 0$ ili -2 zaključujemo da $\det(C_{1j})$ može iznositi $2^{n-1}, 0$ ili -2^{n-1}. Iz toga, gornje jednakosti i činjenice da je $\det(M) = \det(N)$, slijedi da je $\det(M_n)$ uvijek djeljiva s 2^{n-1}.

Ono što nas zanima i što nije nerazumno za očekivati je neka vrsta distribucije na limesu.

Koristeći prethodne rezultate pokažimo da za svaki b vrijedi

$$\mathbb{P}\left(\det(M_n) = b\right) < (1-\epsilon)^n. \tag{4.1}$$

Ako definiramo $p^*(\underline{a}) = \max_c \mathbb{P}\left(\underline{\epsilon}^t\underline{a} = c\right)$, onda ograda Teorema 1.5.1. vrijedi i za $p^*(\underline{a})$ jer množenje integranada u (2.1) s $\cos(ct)$ daje $\mathbb{P}\left(\underline{\epsilon}^t\underline{a} = c\right)$ umjesto $p(\underline{a})$.
To povlači, kao i u dokazu Teorema 1.1.4., da s vjerojatnošću barem $1-(1-\epsilon)^n$ prvih $n-1$ redaka $\underline{r}_1, \ldots, \underline{r}_{n-1}$ matrice M poništava $\underline{a}$ za kojeg vrijedi $p^*(\underline{a}) > (1-\epsilon)^n$. No, za bilo koje takve retke $\underline{r}_1, \ldots, \underline{r}_{n-1}$ i $\underline{a}$, za bilo koji b vrijedi $\mathbb{P}\left(\det(M_n) = b\right) \leq p^*(\underline{a})$.
Međutim, sluti se da vrijedi puno jača ograda od one u (4.1). Očekuje se da je vjerojatnost u (4.1) za $b \neq 0$ otprilike $e^{-\Omega(n\log n)}$.

4.3 Još neke posljedice

Može se vidjeti da (3.20) zajedno s (3.1) daje sljedeće korolare.

Korolar 4.3.1. *Za svaki $\gamma > 0$ postoje konstante $C, \epsilon^* > 0$ takve da vrijedi*

$$\mathbb{P}\left(M_n\underline{a} = \underline{0} \text{ za } \underline{a} \text{ za koje vrijedi } supp(\underline{a}) > C \text{ i } p(\underline{a}) > (1-\epsilon^*)^n\right) < \gamma^n.$$

Korolar 4.3.2. *Za svaki $\gamma > 0$ postoji konstanta C takva da vrijedi*

$$\mathbb{P}\left(\ rang(M_n) < n - C\right) < \gamma^n.$$

Korolar 4.3.3. *Postoji konstanta C takva da za $r \leq n - C$ i $\underline{v}_1, \ldots \underline{v}_r$ izabrane na slučajan (uniformni) način i nezavisno jedan od drugog iz $\{\pm 1\}^n$ vrijedi*

$$\mathbb{P}\left(\underline{v}_1, \ldots \underline{v}_r \text{ su linearno nezavisni}\right) = (1+o(1))2\binom{r}{2}2^{-n}, \tag{4.2}$$

$$\mathbb{P}\left(\langle \underline{v}_1, \ldots \underline{v}_r \cap \{\pm 1\}^n \neq \{\underline{v}_1, \ldots \underline{v}_r\}\right) = (1+o(1))4\binom{r}{3}\left(\frac{3}{4}\right)^n. \tag{4.3}$$

Precizna vrijednost greške u (4.2) je $(1+o(1))8\binom{r}{4}\left(\frac{3}{8}\right)^n$ te u (4.3) $O\left(\left(\frac{7}{10}\right)^n\right)$. Potonji rezultat poboljšava vrijednost u [12] koja daje istu ogradu, ali uz uvjet $r < n - \frac{10n}{\log n}$. Kao što je tamo uočeno, ta greška nije najbolja moguća.
Slutimo da Korolar 4.3.2. vrijedi i uz pretpostavku $r \leq n-1$, ali očekujemo da eventualni

dokaz te trvdnje zahtjeva posla kao dokaz tvrdnje (1.1).

Označimo s T_n broj *threshold* funkcija s n varijabli, odnosno funkcija $f : \{\pm 1\}^n \to \{\pm 1\}$ oblika

$$f(\underline{x}) = \operatorname{sgn}(a_0 + a_1 x_1 + \cdots + a_n x_n)$$

pri čemu su $a_i \in \mathbb{R}$.
Ponašanje vrijednosti T_n tema je proučavana od strane raznih autora koji su utvrdili ograde $\binom{n}{2} < \log_2 T_n < n^2$ (vidi [11] za detalje i vezane rezultate). Zuev je u [15] pokazao da vrijedi $\log_2 T_n \sim n^2$, a njegova precizna vrijednost donje ograde je

$$T_n \geq \left(\begin{array}{c} 2^n \\ n - \frac{10n}{\log n} \end{array} \right) 2^{-\left(n - \frac{10n}{\log n}\right)} = 2^{n^2 - \frac{10n^2}{\log n} - O\left(n \log n\right)} \tag{4.4}$$

dok je gornja ograda jednaka

$$2 \sum_{i=0}^{n} \left(\begin{array}{c} 2^n - 1 \\ i \end{array} \right) = 2^{n^2 - n \log_2 n + O(n)} \tag{4.5}$$

Koristeći Korolar 4.3.3., (4.3) umjesto nekih rezultata koje je koristio Zuev, može se poboljšati donja međa (4.4) na $2^{n^2 - n \log_2 n - O(n)}$. Štoviše, ako je slutnja da se u Korolaru 4.3.3. $r \leq n - C$ može zamijeniti s $r \leq n - 1$ ispravna, onda se uz male izmjene argumenata u [15] može dobiti asimptotsko ponašanje ne samo za $\log T_n$ nego i za sami T_n, asimptotski bi se ponašao kao lijeva strana od (4.5).

Bibliografija

[1] B. Bollobás, *Random graphs*, Academic Press, New York, 1985.

[2] P. Erdős, *On a lemma of Littlewood and Offord*, Bulletin of the American Matemathical Society (1981), br. 51, 898–902.

[3] G. Halász, *On the distribution of additive arithmetic functions*, Acta Arithmetica (1975), br. 27, 143–152.

[4] _____, *Estimates for the concetration function of combinatorial number theory and probability*, Periodica Mathematica Hungarica (1977), br. 8, 197–211.

[5] Kahn J. i Komlós J. i Szemerédi E., *On the probability that a random* ±1*-matrix is singular*, American Mathematical Society (1995), br. 1, 223–240.

[6] Tao. T. i Vu V., *On random* ±1 *matrices: singularity and determinant*, Random Structures & Algorithms (2006), br. 1, 1–23.

[7] _____, *On the singularity probability of random Bernoulli matrices*, American Mathematical Society (2007), br. 3, 603–628.

[8] Bourgain J. i Vu V. H. i Wood P. M., *On the singularity probability of discrete random matrices*, Annals of Functional Analysis (2010), br. 2, 559–603.

[9] Tikhomirov K., *Singularity of random Bernoulli matrices*, Annals of Mathematics (2020), br. 2, 593–634.

[10] J. Komlós, *On the determinants of random matrices*, Studia Scientiarum Mathematicarum Hungarica (1968), br. 3, 387–399.

[11] S. Muroga, *Threshold logic and its applications*, Wiley, New York, 1971.

[12] A. M. Odlyzko, *On subspaces spanned by random selection of* ±1 *vectors*, Journal of Combinatorial Theory, Series A (1985), br. 47, 124–133.

[13] A. Sárközy i E. Szemeredi, *Über ein Problem von Erdős und Moser*, Acta Arithmetica (1965), br. 11, 205–208.

[14] E. Sperner, *Ein Satz über Untermenge einer endliche Menge*, Mathematische Zeitschrift (1928), br. 27, 544–548.

[15] Yu. A. Zuev, *Methods of geometry and probabilistic combinatorics in threshold logic*, Discrete Mathematics and Applications (1992), br. 2, 427–438.

Sažetak

U ovom radu promatramo slučajne $n \times n$ ± 1 matrice, pri čemu je slučajnost definirana uniformnom distribucijom, odnosno za svaki element matrice nezavisno jedan od drugog na slučajan (uniformni) način biramo 1 ili -1.
Za tako definirane matrice, zanima nas kako se ponaša $P_n = \mathbb{P}(M_n \text{ je singularna})$ kada n raste u beskonačnost.
Već je pokazano da $P_n \to 0$ i da vrijedi $P_n = O\left(\frac{1}{\sqrt{n}}\right)$. U ovom radu prezentiramo rezultat Kahna, Komlósa i Szemerédija koji su pokazali eksponencijalnu gornju među, odnosno da postoji ϵ takav da vrijedi $P_n < (1 - \epsilon)^n$.
U prvom poglavlju postavit ćemo problem te iskazati glavne rezultate i dati smjernice, odnosno način na koji ćemo te rezultate dokazati. U Poglavlju 2 dokazat ćemo pomoćni teorem koji je važan korak u dokazu naše tvrdnje, ali i kao samostalan rezultat. Jako važan, ako ne i najvažniji korak u tom dokazu je korištenje Halászeve nejednakosti. U Poglavlju 3 dokazat ćemo glavni teorem uz pomoć nekoliko lema za koje ćemo također pokazati da vrijede u istom poglavlju. Osim spomenutih lema, još jedan bitan korak u dokazu glavnog teorema je konstrukcija potprostora kojima ćemo pokriti sve vektore iz $\mathbb{Z}^n$. Naposljetku, u posljednjem poglavlju iznijet ćemo poboljšanja našeg rezultata. Također ćemo spomenuti neke primjene i posljedice naše tvrdnje na razna područja.

Summary

In this work we observe random $n \times n$ ± 1 matrices, where randomness is defined by the uniform distribution, that is we choose 1 or -1 for each element of the matrix independently of each other in a random (uniform) way.
For such random matrices, we are interested in how $P_n = \mathbb{P}(M_n \text{ is singular})$ behaves when n grows to infinity.
It has already been shown that $P_n \to 0$ and that $P_n = O\left(\frac{1}{\sqrt{n}}\right)$. In this paper, we give an exponential upper bound, i.e. we show that there exists an ϵ such that $P_n < (1-\epsilon)^n$.
In the first chapter, we will pose the problem and present the main results and give guidelines on how to prove these results. In Chapter 2 we will prove an auxiliary theorem which is an important step in proving our claim, but also as an independent result. A very important, if not the most important step in this proof is the use of Halász's inequality. In Chapter 3 we will prove the main theorem with the help of several lemmas which we will also prove in the same chapter. In addition to the these lemmas, another important step in the proof of the main theorem is the construction of subspaces by which we will cover all vectors from $\mathbb{Z}^n$. Finally, in the last chapter, we will present improvements to our bound. We will also mention some applications and consequences of our claim to various areas.

Životopis

Rođen sam 23.4.1996. godine u Karlovcu, Republika Hrvatska. Odrastao sam i živim u Slunju gdje sam od 2003.-2011. pohađao Osnovnu školu Slunj s odličnim uspjehom. Godine 2011. upisujem Prirodoslovno - matematičku gimnaziju u Karlovcu koju 2015. završavam također s odličnim uspjehom.
Na Prirodoslovno - matematički fakultet, smjer matematika upisujem se 2015. godine. Dana 17.7.2018. završavam taj studij s prosječnim uspjehom 3.900 i stječem titulu sveučilišnog prvostupnika matematike. Iste 2018. godine upisujem diplomski studij Financijske i poslovne matematike na Prirodoslovno - matematičkom fakultetu u svrhu čijeg završavanja sam napisao ovaj rad.