Математичка гимназија

Матурски рад
из математике

Вјероватносне методе у комбинаторици

Ученик
Сергеј Петковић, IVб

Ментор
Никола Митриновић

Београд, *28.05.2026*

Садржај

Ти видиш ствари које јесу, и питаш се зашто јесу.
Ја сањам о стварима које никада нису биле и питам се, зашто не?

Џорџ Бернард Шо

1

Увод

Стотинама година уназад, комбинаторне конструкције представљају занимање великих свјетских математичара. Онда када није очигледно како доказати да је неки математички објекат са задатим својствима непостојећи, експерти би се користили алгоритамским методама да, у коначном броју потеза, створе тражени објекат. Тежња ка оваквим рјешењима долазила је природно; најлакши начин да покажемо да неки предмет постоји јесте да читаоцу доказа „уперимо прстом" у један примјер траженог предмета.

На несрећу конструктивиста, показало се да постоје задаци које је врло тешко[1] (некада и немогуће) ријешити непосредно налазећи примјер рјешења. Увођењем аксиоме избора у теорију скупова и саме математичке фондације постале су неконструктивне. Било је потребно помирити се са чињеницом да постоје проблеми које није могуће нападати непосредно, већ се вриједи служити алгебарским методама, помоћу којих се могло утврдити постојање неког објекта, макар не знали увијек како да га конструишемо.

Из овог начина размишљања изродила се и вјероватносна метода[2], која је нашла успјеха на пољима гдје класични, алгоритамски приступ доказивању није. Показивање да постоји објекат са траженим својствима свео би се на показивање да је вјероватноћа да неки објекат у вјероватносном простору има тражене особине већа од нуле. Творцем ове методе сматра се мађарски математичар Пол Ердеш[3]. Стручњаци пишу да је Ердеш допринијео развоју методе у тој мјери да би је било погодно звати „Ердешевом методом ", и напо-

[1]Накнадно је увођење доказа потпомогнутих рачунарима допринијело томе да се изведу конструкције објеката какве би било практично немогуће урадити служећи се папиром и оловком.

[2]енгл. *probabilistic method*

[3]*Erdős Pál*(1913-1996)

мињу да његов допринос не лежи само у многобројним резултатима до којих је дошао, већ и у многобројним задацима и хипотезама које су мотивисале истраживања у овој области.

Циљ овог рада био је да читаоцима покажем нови приступ рјешавању комбинаторних проблема који је створен у прошлом вијеку. У том духу, текст се више бави методологијом рада него резултатима, и задаци и теореме су бирани да буду приступачне средњошколском нивоу. Наиме, нисам наводио најбоље могуће резултате уколико би њихово извођење било прекомјерно технички захтјевно.

Сам рад у себи садржи такмичарске задатке и професионалне теореме које су доказане вјероватносном методом. Наведен је кратки историјат ове технике, пратеће технике које су развијене уз њу, и утицај који је она имала на даљи развој комбинаторике. У раду подразумијевам познавање основних математичких појмова, попут Дирихлеовог принципа и основа теорије вјероватноће. Такође подразумијевам упознатост читаоца са неким познатим резултатима из анализе, попут Јенсенове неједнакости.

Захваљујем се свом ментору Николи Митриновићу на пруженим савјетима и стручној помоћи приликом израде овог текста. Такође, захвалност дугујем и Андријани Марјановић на пажљивом читању рада и драгоцјеним сугестијама.

2

Дефиниције и нотација

Да би се бавили вјероватносном методом, морамо да уведемо неке основне концепте из теорије вјероватноће.

2.1 Случајан догађај и вјероватноћа

Дефиниција. За случајан догађај E кажемо да има вјероватноћу једнаку

$$\mathbb{P}(E) = \frac{\text{број исхода који задовољавају } E}{\text{укупан број могућности}}$$

На примјер, ако случајну величину D дефинишемо као број који добијемо након бацања коцкице, важиће $\mathbb{P}(D = 1) = \mathbb{P}(D = 2) = \cdots = \mathbb{P}(D = 6) = \frac{1}{6}$, $\mathbb{P}(D = 13) = 0$ и $\mathbb{P}(D \geq 4) = \frac{1}{2}$.

Користан је и концепт индикаторске промјењиве; за случајан догађај E означавамо ју са $I(E)$ и она узима вриједност 1 са вјероватноћом $\mathbb{P}(E)$ а вриједност 0 са вјероватноћом $1 - \mathbb{P}(E)$. Она нам „показује" да ли се догађај E десио или не, одатле и назив индикатор.

Како је вјероватноћа дефинисана преко броја повољних исхода, лако је видјети да је догађај E „могућ" ако и само ако $\mathbb{P}(E) > 0$.
За нас ће ова тврдња добити једно комбинаторно значење; објекат са својством E постојаће ако и само ако

$$\mathbb{P}(E(D)) > 0$$

у вјероватносном простору свих могућих објеката D.
Користићемо се и панданом ове тврдње за „немогуће" догађаје; рецимо да имамо догађаје $E_1, E_2, \ldots, E_n$ које желимо да избјегнемо. Ми заправо онда

желимо да избјегнемо њихову унију, и можемо то урадити ако и само ако

$$\mathbb{P}\left(\bigcap_{i\in\{1,\ldots,n\}} \overline{E_i}\right) > 0 \Longleftrightarrow \mathbb{P}\left(\bigcup_{i\in\{1,\ldots,n\}} E_i\right) < 1.$$

Ово се може примијенити и на комбинаторне објекте, објекат D који не посједује ни једну од непожељних особина $E_1, E_2, \ldots, E_n$ постоји ако и само ако важи горња процјена.

2.2 Математичко очекивање

Дефиниција. Случајна промјенљива D има математичко очекивање једнако

$$\mathbb{E}[D] = \sum_x \mathbb{P}(D = x) \cdot x$$

Математичко очекивање заправо представља просјечну вриједност случајне величине D. Следећа теорема посебно је корисна у израчунавању разних очекивања:

Теорема 1. *(линеарност очекивања)* За случајне величине X и Y, важи

$$\mathbb{E}[X + Y] = \mathbb{E}[X] + \mathbb{E}[Y]$$

Доказ.

$$\begin{aligned}
\mathbb{E}[X + Y] &= \sum_x \sum_y (x + y)\,\mathbb{P}(X = x \wedge Y = y) \\
&= \sum_x \sum_y x\,\mathbb{P}(X = x \wedge Y = y) + \sum_y \sum_x y\,\mathbb{P}(X = x \wedge Y = y) \\
&= \sum_x x\,\mathbb{P}(X = x) + \sum_y y\,\mathbb{P}(Y = y) \\
&= \mathbb{E}[X] + \mathbb{E}[Y]
\end{aligned}$$

□

Познато је и да важи $\mathbb{E}[cX] = c\,\mathbb{E}[X]$, те одатле произилази и корисна једнакост

$$\mathbb{E}\left[\sum c_i X_i\right] = \sum c_i\,\mathbb{E}[X_i].$$

Следећа лема могла би се узети за „камен темељац" овог рада:

Лема. *(математичко очекивање осигурава постојање)*
Ако важи

$$\mathbb{E}[D] \geq c$$

тада у простору вјероватноће постоји објекат чија вриједност D износи барем c, и постоји објекат чија вриједност D износи највише c.

Доказ леме је прилично једноставан и нећемо га наводити. Интуитивно, очекивање представља просјек вриједности D сумираних по свим објектима; ако би сваки објекат имао вриједност мању од c тада просјек не би могао бити c. Примијетимо да обрат ове леме не мора да важи, замислимо огроман простор вјероватноће у ком сви догађаји сем једнога долазе са вриједношћу c а један „одскаче" и узима вриједност $C >> c$. Нама би наша лема дала постојање објекта са вриједношћу свега мало већом од c, док заправо постоји много већи објекат са вриједношћу C.

Овдје се и осликава мана вјероватносне методе, наиме она ријетко даје најбоље могуће резултате, и сами резултати су бољи што је простор вјероватноће „збијенији". Одавде се може наслутити и природа задатака рјешивих овом методом; што је више случајева једнакости у оптималној конструкцији, проблем више позива ка рјешавању алгебарским методама. Уколико постоји релативно мало оптималних конструкција, оне се врло често могу категоризовати и „напасти непосредно". Са друге стране, ако је оптималних конструкција много и не придржавају се неког правила (ако су оптималне конструкције „насумичне") онда вриједи покушати задатак „напасти" пробабилистичком методом.

Ради јасноће и интуитивног разумијевања, у остатку рада користићемо се мало непрецизнијим језиком. Када за објекат X кажемо да је насумичан, заправо ћемо подразумијевати да је X случајна величина добијена унифомном расподјелом по свим могућим објектима. Такође, неријетко ћемо интуитивно случајну промјенљиву X схватати као стварни објекат добијен из те униформне расподјеле, иако се ово не повинује потпуно аксиоматском темељу по ком радимо. Водимо се принципом да читаоци прво треба да стекну интуитивно разумијевање доказа, те да ће после сами бити способни ригорозно да га допуне.

3

Основна метода

3.1 Веза између вјероватносне методе и метода пребројавања

Вјероватносна метода сродна је другим методама пребројавања у комбинаторици. Штавише, само коришћење вјероватносне методе често у себи носи оквир других комбинаторних алата. Да бисмо ову везу показали, следећи задатак ријешићемо на два начина. Прво рјешење служиће се Дирихлеовим принципом а друго рјешење користиће вјероватносну методу.

Задатак. *(Канада 2009)* Са парчета картона осјечена су два круга различитих полупречника. Оба круга подијељена су на 200 једнаких лукова. Потом су на сваком кругу неких 100 лукова обојени бијелом бојом, а преосталих 100 црном бојом. Мањи круг је постављен на већи, тако да им се центри поклапају. Показати да је могуће ротирати мањи круг тако да се лукови на оба круга поклапају и да барем 100 лукова мањег круга стоје изнад лукова исте боје на већем кругу.

Рјешење. (класично рјешење) Посматрајмо свих 200 могућих ротација мањег круга. За одабрани лук s на мањем кругу, постоји тачно 100 ротација после којих ће се s упарити са луком исте боје. Ако сумирамо по свим могућим изборима s, два лука исте боје поклопиће се у свим ротацијама укупно $200 \cdot 100 = 20000$ пута. Сада, пошто има 200 могућих ротација, по Дирихлеовом принципу нека ротација имаће барем $20000 \div 200 = 100$ поклапања, што је и требало доказати. □

Рјешење. (вјероватносно рјешење) Посматрајмо насумичну ротацију мањег круга. Очекивана вриједност броја поклапања лукова једнака је:

$$\begin{aligned}\mathbb{E}[\#\text{ поклапања лукова}] &= \mathbb{E}\left[\sum_{i=1}^{200} I(\text{лук } i \text{ се поклапа са луком своје боје})\right] \\ &= \sum_{i=1}^{200} \mathbb{E}[I(\text{лук } i \text{ се поклапа са луком своје боје})] \\ &= \sum_{i=1}^{200} \mathbb{P}(\text{лук } i \text{ се поклапа са луком своје боје}) \\ &= \underbrace{\frac{1}{2}+\frac{1}{2}+\cdots+\frac{1}{2}}_{200 \text{ пута}} = 100\end{aligned}$$

зато што се сваки засебан лук поклапа са неким своје боје са вјероватноћом $\frac{100}{200} = \frac{1}{2}$. Коришћењем леме о очекиваној вриједности, одавде постоји нека ротација са барем 100 поклапања боја лукова, те смо готови. □

У првом доказу требало се досјетити да пребројимо број „добрих" поклапања за сваки засебан лук, потом сумирати по свим могућим луковима и употребити Дирихлеов принцип. У другом доказу нам ово све долази аутоматски; линеарност очекивања као да посједује уграђен апарат за рјешавање ове врсте проблема. Демонстрираћемо ово кроз још један примјер.

Задатак. *(Русија 1996.)* У Думи пресједава 1600 делегата. Делегати су формирали 16000 комитета, а у сваком комитету налази се по 80 чланова. Доказати да је могуће пронаћи два комитета који имају барем четири заједничка члана.

Рјешење. (методом двоструког пребројавања)
Претпоставимо супротно, нека свака два комитета имају максимално три заједничка члана. Пребројимо скупове $\{A, B, d\}$ такве да је делегат d члан комитета A и B. Означимо ову суму са T.
Како свака два комитета имају максимално три заједничка члана,
$3\binom{16000}{2} \geq T$. Са друге стране, ако делегат d учествује у a_d комитета,
$T = \sum \binom{a_d}{2}$, јер за сваког делегата можемо изабрати $\binom{a_d}{2}$ парова комитета таква да он пресједава у оба.
Такође, $\sum a_d = (\#\text{ чланстава међу свим комитетима}) = 16000 \cdot 80$.
Како је функција $\binom{X}{2}$ конвексна, примијењујући Јенсенову неједнакост добијамо:

$$3\binom{16000}{2} \geq T = \sum \binom{a_d}{2} \overset{\text{Јенсен}}{\geq} 1600 \cdot \binom{800}{2}.$$

Рачунском провјером добијамо да ово није тачно, те је почетно тврђење из задатка истинито. □

Рјешење. (вјероватносном методом) Узмимо два насумична различита комитета A и B, и означимо са X број делегата који су чланови оба комитета. Како X узима цјелобројне вриједности, по леми о очекиваној вриједности довољно је показати $\mathbb{E}[X] > 3$, јер би то повлачило да постоје неки комитети A и B са више од три заједничка члана, те би број заједничких чланова између ова два комитета био барем четири, што би завршило доказ. За сваког делегата d, нека a_d означава број комитета којима он припада. Сада

$$\begin{aligned}\mathbb{E}[X] &= \sum_{d=1}^{1600} \mathbb{P}(\text{делегат } d \text{ припада комитетима } A \text{ и } B) \\ &= \sum_{d=1}^{1600} \frac{\binom{a_d}{2}}{\binom{16000}{2}} \overset{\text{Јенсен}}{\geq} 1600 \frac{\binom{\frac{\sum a_i}{1600}}{2}}{\binom{16000}{2}} \\ &= 1600 \frac{\binom{80 \cdot 16000 \div 1600}{2}}{\binom{16000}{2}} = 1600 \frac{\binom{800}{2}}{\binom{16000}{2}} > 3.9952 > 3\end{aligned}$$

те је тврдња из задатка доказана. □

Поново, вјероватносна метода нам помаже да избјегнемо исписивање аргумента бројањем. Занимљива је и чињеница да је након примјене линеарности очекивања очигледан правац којим доказ требамо наставити - сума биномних коефицијената нас једноставно наводи да примијенимо Јенсенову неједнакост. Ова два примјера довољно су лака да је исписивање доказа „примитивним алатима" још увијек могуће. Ипак, како ствари постају компликованије и пребројавања постају сложенија, испоставља се да пробабилистичка метода одржава запис (и мисао) уреднијом.

Иако нисмо увели много теорије, досадашња запажања коришћена су за доказивање неких значајних теорема.

3.2 Докази неких теорема основном методом

Следећи резултат мађарског математичара Тибора Селеа[1] често се наводи као први доказ вјероватносном методом.

Дефиниција. *Турнир* је орјентисан прост граф у ком за свака два различита чвора A и B постоји грана која води из A у B, или она која води из B у A.

Дефиниција. *Хамилтонов пут* за дати граф јесте пут у графу који посјећује сваки чвор тачно једном.

Теорема 2. Постоји турнир са n чворова који има барем $\frac{n!}{2^{n-1}}$ Хамилтонових путева.

Доказ. Посматрајмо насумичан турнир и нека X означава број његових Хамилтонових путева. Овај број можемо израчунати тако што за сваку пермутацију чворова σ утврдимо да ли постоји Хамилтонов пут који иде редослиједом те пермутације, тј. да ли важи да је $(\sigma(i), \sigma(i+1))$ грана за све $1 \leq i < n$. Нека је X_σ индикаторска промјењива која утврђује за задату пермутацију да ли је Хамилтонов пут у X. Тада:

$$\mathbb{E}[X] = \sum_{\sigma} \mathbb{E}[X_\sigma] = n! \left(\frac{1}{2}\right)^{n-1}$$

пошто пермутација σ има $n!$, свака грана у X_σ постоји са вјероватноћом $\frac{1}{2}$, а има $n-1$ грана. Сада пошто је $\mathbb{E}[X] = n! \cdot 2^{-(n-1)}$, постоји неки турнир са $n! \cdot 2^{-(n-1)}$ Хамилтонових путева, што је требало доказати. □

Показаћемо пар резултата о пресјецању графова.

Теорема 3. Нека је дат граф G са n чворова и e грана. Могуће је подијелити G на двије дисјунктне компоненте U и V, тако да је број грана између U и V барем $\frac{e}{2}$.

Доказ. Означимо са E скуп грана графа G. Изаберимо U насумично, тако што сваки чвор v убацујемо у U са вјероватноћом $\frac{1}{2}$. Поставимо $V = G \setminus U$. Сада за сваки чвор v:

$$\mathbb{P}(v \in U) = \frac{1}{2} \text{ и } \mathbb{P}(v \in V) = \mathbb{P}(v \notin U) = \frac{1}{2}.$$

[1] Tibor Szele(1918-1955)

Одатле, ако рачунамо број грана између U и V, он је једнак:

$$\begin{aligned}\mathbb{E}\left[\#\text{ грана између } U \text{ и } V\right] &= \sum_{\{u,v\}\in E} \mathbb{P}((u \in U \wedge v \in V) \vee (u \in V \wedge v \in U)) \\ &= \sum_{\{u,v\}\in E} \frac{1}{2} = \frac{1}{2}e\end{aligned}$$

па како је очекиван број грана једнак $\frac{1}{2}e$, неко пресјецање графа даће барем $\frac{1}{2}e$ грана. □

Неријетко у пробабилистичким доказима мијењање простора вјероватноће може побољшати резултат. Интуиција нам говори да када дијелимо граф на овај начин, у просјеку ћемо имати највише „премошћујућих" грана онда када двије компоненте имају отприлике исти број чворова. Користећи се овом хеуристиком, покажимо мало јаче тврђење:

Теорема 4. Граф G са $2n$ чворова и e грана може се подијелити на подграфа тако да је број грана између два дијела барем $\frac{n}{2n-1}e$.

Доказ. Слично као и у прошлом доказу, бирајмо насумично U, али сада униформно из скупа свих подграфова који имају n чворова.
Израчунајмо вјероватноћу за догађај да грана $\{u, v\}$ „премошћује" два дијела графа:

$$2\,\mathbb{P}\left(u \in U \wedge v \in V\right) = 2\frac{\binom{2n-2}{n-1}}{\binom{2n}{n}} = \frac{n}{2n-1}.$$

Горња вјероватноћа долази из опсервације да ако фиксирамо да су u и v на супротним компонентама графа, можемо да изаберемо који од њих је у компоненти U, изаберемо осталих $n-1$ чворова који ће такође ићи у U, и подијелимо са бројем свих могућих избора.
Ако израчунамо очекивану вриједност броја грана између U и V, из линеарности очекивања добићемо да је она једнака $\frac{n}{2n-1}e$, што имплицира резултат. Сличан резултат могао би се извести и да је G имао $2n-1$ грана. □

У општем случају, утврђивање да ли за дати граф постоји пресјек дате величине компутационално је тежак. Неки алгоритми за проналажење „малих" пресјека су мотивисани горе наведеним доказима. Један грамзиви алгоритам за прву варијанту доказа извео би се овако: на почетку изаберимо произвољно разбијање графа $G = U \cup V, U \cap V = \emptyset$ и у сваком потезу ако неки чвор v припада компоненти у којој има више од половине својих грана, пребацимо га у другу компоненту. Може се показати да ће се овај алгоритам завршити, и да ће након његовог завршетка величина добијеног пресјека бити макар $\frac{e}{2}$.

Процес претварања вјероватносног доказа у ефикасан детерминистички алгоритам назива се *дерандомизација* (енгл. *derandomization*) и представља плодну област истраживања модерних рачунарских наука.

Следећа теорема о балансирању вектора такође долази уз ефикасан грамзиви алгоритам.

Теорема 5. Нека су дати вектори $v_1, v_2, \ldots, v_n \in \mathbb{R}^n$ и нека за све важи $|v_i| = 1$. Тада постоји избор знакова $\epsilon_1, \epsilon_2, \ldots, \epsilon_n = \pm 1$ такви да

$$|\epsilon_1 v_1 + \cdots + \epsilon_n v_n| \leq \sqrt{n}.$$

Доказ. Бирајмо $\epsilon_1, \epsilon_2, \ldots, \epsilon_n$ уз помоћ n бацања новчића. Дефинишимо случајну промјенљиву

$$X = |\epsilon_1 v_1 + \cdots + \epsilon_n v_n|^2.$$

Тада

$$X = \sum_{i=1}^{n} \sum_{j=1}^{n} \epsilon_i \epsilon_j v_i \cdot v_j$$

Те важи

$$\mathbb{E}[X] = \sum_{i=1}^{n} \sum_{j=1}^{n} v_i \cdot v_j \, \mathbb{E}[\epsilon_i \epsilon_j]$$

Уколико $i \neq j$, случајне величине ϵ_i и ϵ_j су независне и $\mathbb{E}[\epsilon_i \epsilon_j] = \mathbb{E}[\epsilon_i]\,\mathbb{E}[\epsilon_j] = 0$, Уколико $i = j$, тада $\mathbb{E}[\epsilon_i \epsilon_j] = \mathbb{E}[\epsilon_i^2] = 1$, те је коначна очекивана вриједност једнака

$$\mathbb{E}[X] = \sum_{i=1}^{n} v_i \cdot v_i = n$$

те постоји избор знакова који даје $X \leq n$, и корјеновањем добијамо тражени резултат. □

Грамзиви резултат за балансирање вектора ишао би овако: у i-том кораку подразумијевајмо да смо израчунали досадашњу векторску суму $w = \epsilon_1 v_1 + \cdots + \epsilon_{i-1} v_{i-1}$. Сада бирајмо знак ϵ_i такав да је угао између w и $\epsilon_i v_i$ оштар (или прав). Овај алгоритам не даје најмању могућу удаљеност w од координатног почетка, али осигурава да ће на крају вриједити $|w| \leq \sqrt{n}$.

Доказ следеће теореме брилијантно је дјело Пола Ердеша, и демонстрира како се вјероватносна метода може искористити у неочекиваним ситуацијама.

Теорема 6. Скуп цијелих бројева B назовимо *изванредним* ако ни за која три броја $a, b, c \in B$ не важи $a + b = c$. За сваки скуп B можемо изабрати његов подскуп A такав да је A изванредан и $|A| > \frac{|B|}{3}$.

Доказ. Нека $B = \{b_1, b_2, .., b_n\}$ и $b_i \neq b_j$ за $i \neq j$.
Узмимо прост број[2] $p = 3k + 2$ такав да вриједи $p > 2 \max_{1 \leq i \leq n} |b_i|$.
Умјесто да доказујемо да је скуп изванредан у $\mathbb{Z}$, довољно је да докажемо да је изванредан у пољу $\mathbb{Z}_p$. Формално, пронаћи ћемо скуп A такав да ни за која три броја $a, b, c \in A$ не важи $a + b \equiv_p c$. Одатле ће вриједити да ни за која три броја не важи $a + b = c$, јер у противном $p | a + b - c = 0$.
Никоја два различита елемента b_i, b_j нису једнака у $\mathbb{Z}_p$, јер $0 < |b_i - b_j| < p$ по конструкцији.

Дефинишимо $M = \{k + 1, k + 2, ..., 2k + 1\}$. Лако је провјерити да је овај скуп изванредан, а такође важи да је $r \cdot M$ такође изванредан скуп за свако цјелобројно r које није дјељиво са p (овдје скупом $r \cdot M$ подразумијевамо скуп добијен множећи сваки елемент M са r). Ово важи зато што ако би за нека три елемента из $r \cdot M$ вриједило $ra + rb = rc$, тада би у оригиналном скупу M важило $a + b = c$, што би дало контрадикцију. (пошто је $\mathbb{Z}_p$ поље, дијељење је дозвољено ако претпоставимо да $r \neq p$).
Сада би било довољно доказати да за неко r важи $|B \cap rM| > \frac{|B|}{3}$. Умјесто да пронађемо овакво r директно, доказаћемо његово постојање пробабилистички. За свако r пишимо $X_r = B \cap rM$. Очекивана вриједност $|X_r|$ може се израчунати тако што за сваки елемент из rM провјеримо да ли је и елемент скупа B:

$$\mathbb{E}[X_r] = \sum_{x=k+1}^{2k+1} \mathbb{P}(rx \in B).$$

Из теорије бројева знамо да је $\{x, 2x, 3x, ..., (p-1)x\}$ потпун систем остатака, тј. да је једнак скупу $\{1, 2, ..., p-1\}$ у $\mathbb{Z}_p$. Одатле је $\mathbb{P}(rx \in B) = \frac{|B|}{p-1}$ те:

$$\mathbb{E}[X_r] = \sum_{x=k+1}^{2k+1} \frac{|B|}{p-1} = (k+1)\frac{|B|}{p-1} = (k+1)\frac{|B|}{3k+1} > \frac{|B|}{3}$$

што имплицира тражени резултат. □

[2]Постојање оваквог простог броја технички је резултат из теорије бројева и не тиче се теме овог рада. У сваком случају, наша интуиција познаје постојање p за прихватљиво; прости бројеви се понашају „насумично" и нема разлога да очекујемо да само коначно много пута долазе са остатком 2 при дијељењу са тројком. Потражити *Дирихлеову теорему о аритметичким низовима.*

Прикажимо један доказ мало другачији од осталих из овог одјељка. Присјетимо се опет дефиниције турнира као простог оријентисаног графа, тако да за свака два чвора A, B важи $A \to B$ или $B \to A$. Граф турнир можемо дословно посматрати као турнир, гдје сваки чвор представља неког играча, сваки играч је играо против сваког другог тачно једном и у свакој игри имамо тачно једног побједника. Тада важи $A \to B$ ако је A побиједио B, а $B \to A$ ако важи супротно.

За турнир T од n играча и природан број k кажемо да T има својство S_k ако за сваки скуп од k играча постоји један играч који их је све побиједио. Рецимо, за граф који је усмјерен троугао, $T_3 = (V, E)$, $V = \{1, 2, 3\}$ и $E = \{(1, 2), (2, 3), (3, 1)\}$ важи да има својство S_1.
Да ли је тачно да за свако k постоји турнир са својством S_k? Ердеш је показао да је одговор потврдан, те да се може врло лако добити вјероватностном методом. Штавише, испоставља се да нам вјероватносна метода даје врло добру процјену колико је најмање чворова потребно за такав турнир.

Теорема 7. Ако важи $\binom{n}{k}(1 - 2^{-k})^{n-k} < 1$, постоји турнир са n играча који има својство S_k.

Доказ. Изаберимо насумичан турнир са n чворова, тако што ћемо за свака два играча i и j бацањем новчића одредити да ли важи $i \to j$ или $j \to i$.
Нека је K неки скуп од k чворова. Нека је A_K догађај да не постоји чвор који побјеђује све чворове из K. Наш циљ је да све ове догађаје избјегнемо.
Вјероватноћа $\mathbb{P}(A_K) = (1 - 2^{-k})^{n-k}$. Ово је тако зато што за сваки чвор ван K морамо осигурати да он не побјеђује ни један чвор из K, то радимо са вјероватноћом $1 - 2^{-k}$ те онда множимо вјероватноће тих $n - k$ догађаја. Сада важи

$$\mathbb{P}\left(\bigcup_{|K|=k} A_K\right) \leq \sum_{|K|=k} \mathbb{P}(A_K) = \binom{n}{k} \cdot (1 - 2^{-k})^{n-k} < 1$$

те је вјероватноћа уније свих „лоших" догађаја мања од 1. Ово значи да постоји турнир за ког сваки скуп K има чвор који побјеђује свакога из K, те је тврдња теореме тачна. □

Вриједи оставити двије напомене. За почетак, $\lim_{n\to\infty} \binom{n}{k}(1 - 2^{-k})^{n-k} = 0$, те смо за свако природно k осигурани да ће дати израз постати мањи од један за неко довољно велико n. Такође, примијетимо да се овај доказ разликује од осталих; умјесто да докажемо постојање конструкције рачунањем очекиване вриједности ми смо издвојили скуп непожељних догађаја и процијенили вјероватноћу са којом их можемо избјећи. Ову идеју ћемо надоградити у следећој глави.

3.3 Туранова теорема

Назовимо скуп чворова графа *независним* уколико не постоји грана између икоја два чвора из скупа. Следећа теорема бави се постојањем независног скупа дате величине у произвољном графу. Први ју је доказао Пол Туран[3], свој доказ је дао и Ердеш, али ми ћемо приказати вјероватносни доказ Алона и Спенсера[4].

Теорема 8. У графу G са n чворова, ако чворови имају просјечан степен d тада постоји независан скуп величине барем $\frac{n}{d+1}$.

Доказ. Нека чвор i има степен d_i, за $1 \leq i \leq n$.
Узмимо $\pi = (\pi_1, \pi_2, \ldots, \pi_n)$ за насумичну пермутацију чворова графа G. Претпоставимо да идемо редом по овој пермутацији и сваки пут када можемо да убацимо нови чвор у независан скуп, да га и убацимо. Формално, за свако i убацићемо чвор π_i у независни скуп ако ни један од чворова $\pi_1, \pi_2, \ldots, \pi_{i-1}$ није сусједан π_i. Нека τ означава кардиналност независног скупа добијеног на овај начин. Очигледно

$$\begin{aligned}
\mathbb{E}[\tau] &= \sum_{i=1}^{n} \mathbb{P}(\text{чвор } i \text{ нема сусједа међу } 1, 2, \ldots, i-1) \\
&= \sum_{i=1}^{n} \mathbb{P}(\text{чвор } i \text{ појављује се прије својих сусједа у } \pi) \\
&= \sum_{i=1}^{n} \frac{d_i!}{(d_i+1)!} = \sum_{i=1}^{n} \frac{1}{d_i+1}
\end{aligned}$$

Сада знамо да, узимајући неку пермутацију π, можемо изградити независни скуп величине барем $\sum_{i=1}^{n} \frac{1}{d_i+1}$. Примијењујући Јенсенову неједнакост (пошто је фунцкија $\frac{1}{x+1}$ конвексна на $[1, +\infty)$, тај независни скуп имаће барем $\frac{n}{d+1}$ чворова, те је тврђење доказано. □

Процјена је строга, једнакост се постиже за граф састављен од неповезаних клика. Вриједи напоменути да се сличне верзије ове теореме појављују у формулацијама о (не)постојању клика[5] у графовима дате величине, али оне се дају извести из нашег резултата посматрајући граф комплеметан оригиналном (тада сваки независтан скуп постаје клика). Такође, резултат добијен прије примјене Јенсенове неједнакости некада се назива теорема Каро-Вej[6].

[3] *Turán Pál* (1910-1976)

[4] *Noga Alon(1956-)* и *Joel Spencer(1946-)*

[5] клика представља супротно од независног скупа; скуп чворова у графу међу којима су свака два повезана

[6] независно су се појавили у радовима Yair, Caro (1971), V. K. Wei (1981)

4

Ловас[1] локална лема

До сада смо се бавили са двије врсте доказа. У једним смо постојање објеката задате величине оправдавали математичким очекивањем; уколико је очекивање датог вјероватносног простора довољно велико тада постоји и велики комбинаторни објекат.

Друга врста доказа служила се изоловањем „лоших" догађаја које желимо да избјегнемо, те рачунањем њихових вјероватноћа. Рецимо да смо жељели избјећи догађаје $E_1, E_2, \ldots, E_n$ који редом имају вјероватноће $\mathbb{P}(E_i) = p_i$.
Без неких напреднијих алата, ми смо опет могли изоловати два случаја у којима би доказ ове врсте могли завршити:

- Рецимо да су догађаји E_i по паровима независни. Тада можемо израчунати вјероватноћу да се ни један од њих не деси:

$$\mathbb{P}\left(\bigcap_i \overline{E_i}\right) = \prod_i (1 - p_i)$$

  одакле морамо захтијевати да је дати производ већи од нуле. Ово се врло лако може постићи; $0 \leq p_i \leq 1$ при чему подразумијевамо да је десна граница строга (уколико је вјероватноћа неког лошег догађаја 1, не можемо се надати да ћемо га избјећи).

- Са друге стране, уколико не знамо ништа о зависности догађаја E_i, можемо се искористити процјеном уније догађаја:

$$\mathbb{P}\left(\bigcap_i \overline{E_i}\right) = 1 - \mathbb{P}\left(\bigcup_i E_i\right) \geq 1 - \sum_i \mathbb{P}(E_i)$$

  Како желимо да постигнемо да је тражена вјероватноћа већа од нуле, то је сада довољно захтијевати $\sum_i \mathbb{P}(E_i) < 1$.

[1] Lovász László(1946-)

Ова метода може да донесе резултат у неким примјерима, али обазрив читалац ће примијетити да су процјене које користимо прилично лабаве. Штавише, можемо се надати да ће оне проћи само у случајевима када је вјероватноћа да је објекат добар и сама прилично велика. Шта радити када добрих објеката има релативно мало?

Уколико су лоши догађаји међусобно независни свакако их можемо избјећи; уколико зависе један од другог а малих су вјероватноћа можемо се послужити процјеном уније. Али шта радити ако се деси нешто треће, ако су лоши догађаји умјерено чести и имају мали број зависности између себе?

Локална лема која се појавила у раду Ловаса и Ердеша 1975. године бави се баш овим питањем. Она долази у више верзија, али ми ћемо показати ону најједноставнију, која се уједно појавила у изворном раду.

4.1 Тврђење теореме и доказ

Теорема 9. Нека су $E_1, E_2, \ldots, E_n$ догађаји такви да $\mathbb{P}(E_i) \leq p$ и сваки догађај је зависан са највише d осталих. Уколико $ep(d+1) \leq 1$ тада

$$\mathbb{P}\left(\overline{E_1} \cap \overline{E_2} \cap \cdots \cap \overline{E_n}\right) \geq \left(1 + \frac{1}{d+1}\right)^n > 0.$$

Овај резултат се повремено назива симетричном варијантом локалне леме; ово долази отуда што смо узели исте вриједности d и p за све догађаје E_i. Постоји и јача, асиметрична варијанта овог резултата, али ми се њоме нећемо бавити.

Доказ. Извођење које слиједи је прилично техничко, те нема неку комбинаторну интерпретацију. Можда га је најбоље на првом читању прескочити, погледати одјељак са примјенама теореме, те се после на њега вратити. Ипак, наводимо га ради комплетности.
Доказаћемо следећу лему, из које ће главни резултат врло брзо слиједити:

Лема. Нека имамо произвољан скуп $S \subset \{1, 2, \ldots, n\}$. Тада важи

$$\mathbb{P}\left(E_i \mid \bigcap_{k \in S} \overline{E_k}\right) \leq \frac{1}{d+1}.$$

Доказ вршимо индукцијом по $|S|$. За базни случај $|S| = 0$ теорема очигледно важи, јер се тада своди на $\mathbb{P}(E_i) \leq \frac{1}{d+1}$ што је тачно по процјени $ep(d+1) < 1$.

Претпоставимо сада да тврдња важи за све S такве да $|S| < t$. Докажимо да важи за $|S| = t$. Нека је D_i скуп свих догађаја E_j, $j \neq i$ са којима E_i није независан. Разликујемо два случаја:

- Претпоставимо да $S \cap D_i = \emptyset$. Одавде

$$\mathbb{P}\left(E_i \mid \bigcap_{k\in S} \overline{E_k}\right) = \mathbb{P}\left(E_i\right) < \frac{1}{e(d+1)} < \frac{1}{d+1}$$

  те је тврђење у овом случају тачно.

- Нека сада $S \cap D_i \neq \emptyset$. Према Бајесовој формули, ми имамо

$$\begin{aligned}
\mathbb{P}\left(E_i \mid \bigcap_{k\in S} \overline{E_k}\right) &= \mathbb{P}\left(E_i \mid \bigcap_{k\in S\cap D_i} \overline{E_k} \cap \bigcap_{k\in S\setminus D_i} \overline{E_k}\right) \\
&= \frac{\mathbb{P}\left(E_i \cap \bigcap\limits_{k\in S\cap D_i} \overline{E_k} \mid \bigcap\limits_{k\in S\setminus D_i} \overline{E_k}\right)}{\mathbb{P}\left(\bigcap\limits_{k\in S\cap D_i} \overline{E_k} \mid \bigcap\limits_{k\in S\setminus D_i} \overline{E_k}\right)} \\
&\leq \frac{\mathbb{P}\left(E_i \mid \bigcap\limits_{k\in S\setminus D_i} \overline{E_k}\right)}{\mathbb{P}\left(\bigcap\limits_{k\in S\cap D_i} \overline{E_k} \mid \bigcap\limits_{k\in S\setminus D_i} \overline{E_k}\right)} \\
&= \frac{\mathbb{P}\left(E_i\right)}{\mathbb{P}\left(\bigcap\limits_{k\in S\cap D_i} \overline{E_k} \mid \bigcap\limits_{k\in S\setminus D_i} \overline{E_k}\right)} \overset{?}{\leq} \frac{1}{d+1}
\end{aligned}$$

Сада је потребно да ограничимо именилац. Овдје ћемо употребити индуктивну претпоставку. Нека $S \cap D_i = \{i_1, \ldots, i_z\}$. Именилац постаје

$$\mathbb{P}\left(\bigcap_{k\in S\cap D_i} \overline{E_k} \mid \bigcap_{k\in S\setminus D_i} \overline{E_k}\right) =$$
$$= \mathbb{P}\left(\overline{E_{i_1}} \mid \bigcap_{l=2}^{z} \overline{E_k} \cap \bigcap_{k\in S\setminus D_i} \overline{E_k}\right) \cdot \mathbb{P}\left(\bigcap_{l=2}^{z} \overline{E_{i_l}} \mid \bigcap_{k\in S\setminus D_i} \overline{E_k}\right)$$
$$= \mathbb{P}\left(\overline{E_{i_1}} \mid \bigcap_{l=2}^{z} \overline{E_k} \cap \bigcap_{k\in S\setminus D_i} \overline{E_k}\right) \cdot \mathbb{P}\left(\overline{E_{i_2}} \mid \bigcap_{l=3}^{z} \overline{E_k} \cap \bigcap_{k\in S\setminus D_i} \overline{E_k}\right) \cdot \mathbb{P}\left(\bigcap_{l=3}^{z} \overline{E_{i_l}} \mid \bigcap_{k\in S\setminus D_i} \overline{E_k}\right)$$
$$\vdots$$
$$= \prod_{l=1}^{z} \mathbb{P}\left(\overline{E_{i_l}} \mid \bigcap_{k\in S\setminus D_i} \overline{E_k} \cap \bigcap_{k'=1}^{l-1} \overline{E'_k}\right) \overset{*}{\geq} \prod_{l=1}^{z} \left(1 - \frac{1}{d+1}\right) = (1 - \frac{1}{d+1})^z$$
$$\geq (1 - \frac{1}{d+1})^d \geq \frac{1}{e}$$

При чему процјена $(*)$ важи по индуктивној претпоставци, пошто сваки члан једначине има мање од t догађаја.
Сада када смо процијенили именилац, можемо доказати лему.

$$\begin{aligned}\mathbb{P}\left(E_i \mid \bigcap_{k\in S} \overline{E_k}\right) &\leq \frac{\mathbb{P}(E_i)}{\mathbb{P}\left(\bigcap_{k\in S\cap D_i} \overline{E_k} \mid \bigcap_{k\in S\setminus D_i} \overline{E_k}\right)} \\ &\leq \mathbb{P}(E_i) \cdot e \\ &\leq \frac{1}{d+1}\end{aligned}$$

Гдје задња процјена важи по условима из теореме.
Користећи доказану лему, нашу првобитну теорему је лако доказати. Сличним развијањем као малопријe добијамо

$$\begin{aligned}\mathbb{P}\left(\bigcap_{i=1}^{n} \overline{E_i}\right) &= \prod_{i=1}^{n} \mathbb{P}\left(\overline{E_i} \mid \bigcap_{k<i} \overline{E_k}\right) \\ &\geq \prod_{i=1}^{n} \left(1 - \frac{1}{d+1}\right) = \left(1 - \frac{1}{d+1}\right)^n > 0\end{aligned}$$

што завршава доказ.

□

4.2 Неке примјене

Започнимо са једним класичним примјером.

Задатак. Претпоставимо да $11n$ куглица стоје на кругу, и да су све обојене у једну од n боја, тако да за сваку боју постоје тачно 11 куглица те боје. Доказати да се у свакој таквој конфигурацији може одабрати n куглица, свака од по једне боје, али тако да никоје двије одабране нису сусједне на кругу.

Рјешење. Рецимо да бирамо по једну куглицу од сваке боје насумично, и да је сваки избор независан од осталих. Тада сваку од n куглица бирамо са вјероватноћом $\frac{1}{11}$.
Наши „лоши" догађаји ће представљати бирање двије сусједне куглице на кругу, рецимо a и b. Вјероватноћа да смо изабрали и a и b износи највише $p = \frac{1}{121}$, наиме она је једнака овој вјероватноћи када су a и b различитих боја, а једнака је нули када су исте боје.
Испитајмо сада за два лоша пара, рецимо a, b и c, d гдје су a и b, а c и d сусједне на кругу, када ова два догађаја зависе један од другога. Уколико су куглице a и b различитих боја од c и d тада смо их по конструкцији бирали независно једне од других, те су ови лоши догађаји независни. Дакле да би они били зависни, барем нека од a, b мора дијелити боју са неком од c, d.
Избројимо сада колико пута се ово дешава за сваки пар a, b. Ако фиксирамо боју од a и наметнемо да нека од c, d такође има ову боју, можемо ту једну од c, d изабрати на једанаест начина. За сваку од тих једанаест куглица имамо по два сусједа, те је лоших парова у овом случају 21, ако уклонимо онај који одговара изворном пару a, b. Ако урадимо исту ствар за b добијамо још 21 лош пар зависан од пара a, b, па можемо посматрати најгори случај када су обје групе од по 21 парова дисјунктне и узети $d = 42$.
Сада важи

$$ep(d+1) = e \cdot \frac{1}{121} \cdot 43 \leq 0.967 < 1$$

те је по локалној леми могуће избјећи све лоше догађаје, па постоји избор несусједних куглица, што је и требало доказати. □

Следећи задатак појавио се на средњошколском такмичењу у Русији.

Задатак. *(Русија 2006)* На кампу математичара, свака особа има између 50 и 100 пријатеља. Показати да је могуће подијелити мајице свакој особи на кампу, тако да мајице имају највише 1331 различитих боја и свака особа има барем 20 пријатеља који сви носе мајице различитих боја.

Рјешење. Дајмо свакој особи мајицу насумичне боје. За сваку особу P, нека $E(P)$ означава догађај да пријатељи од P носе највише 19 боја мајица. Послужићемо се локалном лемом да покажемо да постоји ненулта вјероватноћа да се ни један од догађаја $E(P)$ не деси.

Догађај $E(P)$ зависи само од особе P и њених пријатеља, зато важи да ако су догађаји $E(A)$ и $E(B)$ зависни, тада су A и B или пријатељи или имају неког заједничког пријатеља. Како свака особа P има максимално 100 пријатеља, и сваки од њених пријатеља има максимално 99 пријатеља различитих од P, $E(P)$ зависи од максимално $d = 100 + 100 \cdot 99 = 100^2$ других догађаја.

За произвољну особу, посматрајмо њених $50 \leq k \leq 100$ пријатеља. Вјероватноћа да сви они имају највише 19 боја међу мајицама износи максимално

$$\binom{1331}{19} \cdot \left(\frac{19}{1331}\right)^k < \binom{1331}{19} \cdot \left(\frac{19}{1331}\right)^{50}.$$

Ако убацимо ове вриједности у локалну лему, остаје да се докаже

$$e\binom{1331}{19}\left(\frac{19}{1331}\right)^{50}(100^2+1) < 1$$

Ово представља врло слабу процјену која би се могла извести и на такмичењу без коришћења дигитрона; очигледно је да је фактор $\frac{1}{1331^{50}}$ много већи од свих осталих.

Овдје се види и особина неких руских задатака да се константе које треба доказати бирају прилично произвољно те да су често много слабије од најбољих могућих константи; са пажљивијим процјенама локалном лемом би се константа 1331 могла поправити на чак 48. □

Показаћемо још један интересантан резултат из теорије графова. Да ли постоји минималан степен графа δ који обезбјеђује постојање циклуса парне дужине? Примијетимо да ово не ради за непарне циклусе; наиме бипартитни графови могу имати произвољно велике степене а да имају само парне циклусе. Испоставља се да можемо обезбиједити постојање циклуса дужине дјељиве са k за сваки природан број k.

Теорема 10. (Алон и Линиал[2] 1987, поједностављено) Нека је дат усмјерен граф најмањег излазног степена δ и највећег улазног степена Δ. Тада он има циклус дужине дјељиве са k за свако $k \in \mathbb{N}$ за које важи

$$k \leq \frac{\delta}{1 + \ln(1 + \Delta + \delta\Delta)}.$$

[2]Nathan Linial (1953-)

Доказ. Учинићемо прво малу оптимизацију. За сваки чвор, бришимо гране које излазе из њега све док његов излазни степен не постане тачно δ. Ово нам очигледно одржава услове теореме али отежава њен доказ; довољно је показати да она важи у овом случају.

Означимо са V скуп свих чворова графа. Узмимо произвољно бојење графа $f : V \to \{0, 1, \ldots, k-1\}$, такво да сваком чвору v додјељујемо насумичну боју $f(v)$ по униформној расподјели. Потом бришемо све гране из графа, сем оних за које важи $v \to u$ и $f(u) \equiv f(v) + 1 \pmod{k}$.

Ако у овом графу сваки чвор има излазни степен барем један, загарантовано је да ћемо добити циклус дужине дјељиве са k; наиме можемо кренути из произвољног чвора и увијек путовати неком граном која излази из њега; како чворова има коначно много некада током овог путовања десиће се да смо исти чвор посјетили двапута; тада тај чвор мора бити дио циклуса дужине дјељиве са k по конструкцији.

За свако $v \in V$, нека је A_v догађај да v нема излазну грану (ово желимо да избјегнемо). За сваког комшију u чвора v знамо да грана $v \to u$ бива избачена са вјероватноћом $(1 - \frac{1}{k})$. Одатле $\mathbb{P}(A_v) = (1 - \frac{1}{k})^{\delta} \leq e^{-\frac{\delta}{k}}$.

Остаје да продискутујемо максималан број догађаја са којима је A_v у зависном односу. A_v зависи од оних догађаја A_u онда када важи једно од следећег:

1. $u \to v$ у оригиналном графу, има највише Δ таквих;
2. $v \to u$ у оригиналном графу, даје највише δ чворова;
3. u и v оба имају грану која излази ка неком чвору w, што даје највише $\delta(\Delta - 1)$ могућности.

Свеукупно, бројимо највише $\Delta + \delta\Delta$ зависних догађаја, те можемо у локалној леми узети $d = \Delta + \delta\Delta$, што даје

$$ep(d+1) \leq e^{1-\frac{\delta}{k}}(1 + \Delta + \delta\Delta) \overset{?}{<} 1$$
$$\iff k \leq \frac{\delta}{1 + \ln(1 + \Delta + \delta\Delta)}$$

што је еквивалентно процјени датој у теореми. □

Локална лема нашла је примјену чак и на најтежем задатку са Међународне математичке олимпијаде.

Задатак. *(ИМО 2014/6)* За скуп правих у равни кажемо да су у општем положају ако никоје двије нису паралелне и никоје три не пролазе кроз исту тачку. Скуп правих у општем положају дијели раван на области; оне области које имају коначну површину називамо *ограниченим* областима. Доказати да за свако довољно велико n важи следеће тврђење: у сваком скупу од n правих у општем положају можемо обојити у плаво бар $\sqrt{n}$ правих тако да ниједна од ограничених области нема потпуно праву границу.

Напомена: Докази тврђења у којима је $\sqrt{n}$ замијењено са $c\sqrt{n}$ биће бодовани у зависности од вриједности константе c.

Рјешење. Доказаћемо тврдњу у којој је $\sqrt{n}$ замијењено са $c\sqrt{n}$ гдје је $c = (6e)^{-\frac{1}{2}}$.
Подијелимо n правих у $\lfloor c\sqrt{n} \rfloor$ група, гдје свака група има $\lceil \frac{\sqrt{n}}{c} \rceil$ правих. Из сваке групе, одаберимо по једну праву и обојимо је у плаво.
Означимо све ограничене области равни са $R_1, R_2, \ldots, R_m$ и за сваку ограничену област изаберимо неке три праве са њене границе. Дефинишимо сада догађаје A_k да важе ако су оне три праве са границе R_k плаве. Докажимо да постоји ненулта вјероватноћа да се ни један од ових догађаја не деси, тада ће важити да постоји бојење такво да са сваке ограничене области барем једна права са границе није плава.
Вјероватноћа да се догађај A_k деси износи највише $(\frac{c}{\sqrt{n}})^3$ (она је једнака овоме ако три изабране праве припадају различитим групама, у супротном она је једнака нули).
За свако A_k три изабране праве означавају три групе. У свакој од ових група има највише $\frac{\sqrt{n}}{c}$ правих, а свака права је граница највише $2n-2$ ограничених области. Одатле, догађај A_k зависи од највише $3 \cdot \frac{\sqrt{n}}{c} \cdot (2n-2)$ других догађаја. Сада како

$$e\left(\frac{c}{\sqrt{n}}\right)^3 \left(3 \cdot \frac{\sqrt{n}}{c} \cdot (2n-2)\right) < 6ec^2 = 1$$

тврдња је одмах доказана помоћу Ловас локалне леме.

5

Повратак алгоритмици и завршна ријеч

За крај, издвојићемо пар ријечи о алгоритамском аспекту вјероватносне методе и њеној вези са рачунарским наукама. Као што смо видјели, једно је доказати да ли нека комбинаторна структура постоји, док је проблем за себе конструисати примјер такве структуре. Сродно питање које занима алгоритмичаре јесте да ли се он може генерисати ефикасним алгоритмом. Дискусија је посебно интересантна онда када се доказ постојања објеката о којим говоримо извео вјероватносном методом. Ове идеје налазе своју примјену у модерној криптографији, те теоријама кодирања и информација.

Интересантни су алгоритми који користе насумичне величине током извршавања. Најпознатији примјер је свакако *Quicksort* алгоритам за сортирање. Са њима неријетко долазе и нове идеје или посебни осврти на структуру са којом радимо. Ипак, ми често желимо да жртвујемо мало ефикасности да би алгоритам учинили ригорознијим. Коришћење пробабилистичких хеуристика при креирању детерминистичких алгоритама називамо дерандомизација. Примјери ове методе јесу CAT проблем (проблем задовољивости), пресјеци графова, налажење независног скупа у графу те алгоритамска верзија Ловасове локалне леме.

Коришћење других напредних алата, попут алгебарских и аналитичких техника, спектралних метода, и тополошких доказа такође у многим случајевима доводи до неконструктивних доказа. Њихово превођење у алгоритамске аргументе чини се као један од главних будућих подухвата комбинаторике као области.

Ови изазови, естетска привлачност комбинаторике као дисциплине, њена повезаност са другим областима и разни фасцинантни отворени проблеми осигуравају да ће она наставити да игра значајну улогу у развоју математике у будућности.

Библиографија

[1] Noga Alon, Joel Spencer *The Probabilistic Method*, Wiley and Sons, New York, NY, 2nd edition 2000.

[2] Martin Aigner, Günter M. Ziegler *Proofs from the book*, Springer, 1998.

[3] Evan Chen, `https://web.evanchen.cc/handouts/ProbabilisticMethod/ProbabilisticMethod.pdf`

[4] Jiří Matoušek, Jan Vondrák `https://www.cs.cmu.edu/~15850/handouts/matousek-vondrak-prob-ln.pdf`, Department of Applied Mathematics, Charles University