Verjetnostna metoda

Hugo Trebše (hugo.trebse@gmail.com)

24. september 2025

Zapiski sledijo avtorjevem predavanju na pripravah za mednarodna matematična tekmovanja, ki je bilo izvedeno 6. 12. 2024. Za vse napake ter netočnosti je odgovoren avtor sam. Če imate vprašanje ali popravek se obrnite na e-poštni naslov zgoraj.

Zahvaljujem se Luku Horjaku za nasvete ter pomoč pri urejanju.

Les esprits les plus grands sont capables des plus grands vices aussi bien que des plus grandes vertus; et ceux qui ne vont que fort lentement peuvent avancer beaucoup davantage, pourvu qu'ils suivent toujours le droit chemin, que ceux qui courent et s'en éloignent.

Največji umi so sposobni največjih izvrstnosti, pa tudi največjih zablod; in tisti, ki napredujejo zelo počasi, lahko dosežejo veliko večji napredek, če vedno sledijo pravi poti, kot tisti, ki tečejo, a jo zapustijo.

René Descartes - Razprava o metodi

1 Teoretično ozadje

V splošnem je verjetnostna metoda eksistenčna – uporabimo jo za dokaz obstoja objekta. Če pokažemo, da je verjetnost, da ima naključno izbran objekt neko želeno lastnost, pozitivna, potem takoj sledi, da tak objekt mora obstajati. Analogno lahko opišemo »slabe« objekte, ter pokažemo, da je verjetnost njihovega obstoja manjša od 1. Obstaja tudi verjetnostna oblika Dirichletovega principa, ki jo bomo povezali z novo količino: pričakovano vrednostjo.

Verjetnostnih prostorov ter povezanih pojmov ne bomo vpeljali v vsej njihovi splošnosti, marveč le do mere, ki je za nas potrebna.

Definicija 1.1 (Diskreten verjetnostni prostor)**.** Diskreten verjetnostni prostor *je trojica* $(\Omega, \mathcal{F}, \mathbb{P})$*, kjer je* Ω *množica vseh možnih izidov,* $\mathcal{F}$ *potenčna množica* Ω*, ki jo imenujemo množica dogodkov, ter* $\mathbb{P} : \mathcal{F} \to [0,1]$ *preslikava, ki je definirana na enojcih množice* Ω *za katero velja:*

$$\mathbb{P}(A) = \sum_{a \in A} \mathbb{P}(\{a\}).$$
$$\sum_{\omega \in \Omega} \mathbb{P}(\{\omega\}) = 1$$

Kanonični primer je met standardne kocke. Tedaj je $\Omega = \{1, 2, 3, 4, 5, 6\}$, $\mathcal{F}$ je potenčna množica slednje, $\mathbb{P}$ pa slika vsak element Ω v $\frac{1}{6}$, kar določi sliko poljubnega elementa $\mathcal{F}$.

Na podlagi zgornjih definicij lahko izpeljemo znane formule verjetnosti:

$$\mathbb{P}(A \cup B) = \mathbb{P}(A) + \mathbb{P}(B) - \mathbb{P}(A \cap B) \quad \text{ter} \quad \mathbb{P}(A) + \mathbb{P}(A^c) = 1.$$

Definicija 1.2 (Diskretna slučajna spremenljivka)**.** Diskretna slučajna spremenljivka *je funkcija* $X : \Omega \to \mathbb{R}$*, za katero velja, da je* $X^{-1}(\{c\})$ *dogodek (element* $\mathcal{F}$*) za vsak* $c \in \mathbb{R}$*. V primeru diskretne slučajne spremenljivke pišemo*

$$\mathbb{P}(X = x) = \mathbb{P}(X^{-1}(\{x\}))$$

V diskretnem verjetnostnem prostoru slučajne spremenljivke ter funkcije sovpadajo, a v splošnih verjetnostnih prostorih ni vsaka funkcija slučajna spremenljivka.

Trditev 1.3 (Načelo vključitev in izključitev)**.** *Naj bodo* $A_1, \ldots, A_n$ *dogodki v verjetnostnem prostoru. Velja:*

- $\mathbb{P}(A_1 \cup A_2) = \mathbb{P}(A_1) + \mathbb{P}(A_2) - \mathbb{P}(A_1 \cap A_2)$.
- *Če definiramo*

  $$S_k = \sum_{\substack{I \subseteq \{1,\ldots,n\} \\ |I| = k}} \mathbb{P}\left(\bigcap_{i \in I} A_i\right),$$

  potem je

  $$\mathbb{P}\left(\bigcup_{i=1}^{n} A_i\right) = \sum_{k=1}^{n} (-1)^{k-1} S_k.$$

Dokaz. Sledi po formuli o vključitvah in izključitvah, če izberemo za množico A celoten verjetnostni prostor ter za A_i podmnožico elementov verjetnostnega prostora. $\square$

Naslednja lema je pogosto uporabnejša od celotne trditve zgoraj.

Lema 1.4 (Razširjen union bound)**.** *Naj so $A_1, \ldots, A_n$ dogodki v verjetnostnem prostoru. Za lihe $k \leq n$ velja*

$$\mathbb{P}\left(\bigcup_{i=1}^{n} A_i\right) \leq \sum_{j=1}^{k} (-1)^{j-1} S_j,$$

za sode $k \leq n$ pa velja:

$$\mathbb{P}\left(\bigcup_{i=1}^{n} A_i\right) \geq \sum_{j=1}^{k} (-1)^{j-1} S_j.$$

Definicija 1.5: Pričakovana vrednost

Pričakovano vrednost diskretne slučajne spremenljivke definiramo kot sledečo vsoto, ki teče po vseh elementih verjetnostnega prostora:

$$\mathbb{E}[X] = \sum_{x} x \cdot \mathbb{P}(X = x).$$

Izrek 1.6: Linearnost pričakovane vrednosti

Če sta X in Y (morda odvisni) naključni spremenljivki velja

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

Dokaz. Izrek dokažimo za končne verjetnostne prostore (množica Ω je končna). Velja

$$\begin{aligned}
\mathbb{E}[X + Y] &= \sum_{x} \sum_{y} (x + y) \mathbb{P}(X = x,\ Y = y) \\
&= \sum_{x} \sum_{y} x \cdot \mathbb{P}(X = x,\ Y = y) + \sum_{x} \sum_{y} y \cdot \mathbb{P}(X = x,\ Y = y) \\
&= \sum_{x} x \cdot \sum_{y} \mathbb{P}(X = x,\ Y = y) + \sum_{y} y \cdot \sum_{x} \mathbb{P}(X = x,\ Y = y) \\
&= \sum_{x} x \cdot \mathbb{P}(X = x) + \sum_{y} y \cdot \mathbb{P}(X = x) \\
&= \mathbb{E}[X] + \mathbb{E}[Y].
\end{aligned}$$

$\square$

V primeru neskončnih verjetnostnih prostorov potrebujemo izreke Fubinijevega tipa.

Lema 1.7: Verjetnostni Dirichletov princip

Naj bo X slučajna spremenljivka, ki zavzame vrednosti iz množice celih števil. Denimo, da velja $\mathbb{E}x = c$. Tedaj je

$$\mathbb{P}(X \geq \lceil c \rceil) > 0 \quad \text{in} \quad \mathbb{P}(X \leq \lfloor c \rfloor) > 0.$$

Sledi, da naključna spremenljivka X zavzame vrednosti večje ali enake $\lceil c \rceil$ ter vrednosti manjše ali enake $\lfloor c \rfloor$.

Dokaz. Velja

$$c = \mathbb{E}X = \sum_x x \cdot \mathbb{P}(X = x) = \sum_{x \geq \lceil c \rceil} x \cdot \mathbb{P}(X = x) + \sum_{x \leq \lfloor c \rfloor} x \cdot \mathbb{P}(X = x).$$

Denimo, da slučajna spremenljivka X ne bi zavzela vrednosti večje ali enake $\lceil c \rceil$. Potem bi bila verjetnost tega, da X zavzame vrednost večjo ali enako $\lceil c \rceil$ enaka 0. Tako bi veljalo

$$c = \mathbb{E}X = \sum_{x < \lfloor c \rfloor} x \cdot \mathbb{P}(X = x) < \lfloor c \rfloor \cdot \sum_{x < \lfloor c \rfloor} \mathbb{P}(X = x) \leq \lfloor c \rfloor,$$

kjer zadnja enakost sledi iz dejstva, da je vsota verjetnosti disjunktnih elementov verjetnostnega prostora manjša ali enaka 1. Ker smo prispeli do protislovja sledi, da X gotovo zavzame vrednosti večje ali enake $\lceil c \rceil$; analogen dokaz pokaže tudi drugi del trditve. □

Definicija 1.8 (Konveksnost)**.** *Naj bo I interval. Funkcija $f\colon I \to \mathbb{R}$ je* konveksna*, če za vse $x, y \in I$ in $t \in [0,1]$ velja*

$$f(tx + (1-t)y) \leq tf(x) + (1-t)f(y).$$

Za dovolj lepe funkcije obstaja enostavnejša karakterizacija konveksnosti – dvakrat odvedljiva funkcija (karkoli to že pomeni) je konveksna natanko tedaj, ko je njen drugi odvod nenegativen na I.

Izrek 1.9 (Jensenova neenakost)**.** *Naj bo $f\colon I \to \mathbb{R}$ konveksna ter $n \in \mathbb{N}$. Če je $\sum_{i=1}^n t_i = 1$ in $t_i \geq 0$, potem za vse $\{x_i\}_{i=1}^n$ velja*

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

Oris dokaza. Upoštevajoč

$$\sum_{i=1}^n t_i y_i = (1 - t_{n-1}) \sum_{i=1}^{n-1} \frac{t_i}{1 - t_{n-1}} y_i + t_n y_n$$

izrek postane standardna vaja iz indukcije. □

Izrek 1.10: Erdős

Naj bo A množica neničelnih celih števil. Podmnožica B je *brez vsote*, če ne obstajajo $x, y, z \in B$, za katera velja

$$x + y = z.$$

Za vsako množico neničelnih celih števil A obstaja podmnožica B, ki je brez vsote, za katero velja

$$\frac{|A|}{3} < |B|\,.$$

Dokaz. Izberemo praštevilo $p = 3k + 2$, za katero velja, da je $A \subseteq [-k, k]$. Opazujemo A kot podmnožico $\mathbb{Z}_p$, ter ugotovimo, da je A brez vsote natanko tedaj, ko je brez vsote mod p.

Za naključno in enakomerno izbran $x \in \mathbb{Z}_p \setminus \{0\}$ tvorimo množico

$$B_x = \left\{a \in A \mid a \cdot x^{-1} \bmod p \in [k + 1, 2k + 1]\right\},$$

ki je brez vsote mod p, saj je množica $\{k+1, \ldots, 2k+1\}$ brez vsote v $\mathbb{Z}_p$. Želeli bi pokazati $\mathbb{E}[|B_x|] > \frac{|A|}{3}$. Definirajmo indikatorske spremenljivke

$$R_a = \begin{cases} 1; & a \in B_x \\ 0; & a \notin B_x \end{cases}$$

za katere velja

$$|B_x| = \sum_{a \in A} R_a$$

ter izračunajmo

$$\mathbb{E}[|B_x|] = \sum_{a \in A} \mathbb{P}(a \in B_x) = \sum_{a \in A} \mathbb{P}(x^{-1}a \in [k + 1, 2k + 1]).$$

Velja $|\{k + 1, \ldots, 2k + 1\}| > \frac{p-1}{3}$. Posledično je

$$\mathbb{E}[|B_x|] = \sum_{a \in A} \mathbb{P}(x^{-1}a \in [k + 1, 2k + 1]) > \sum_{a \in A} \frac{1}{3} = \frac{|A|}{3}.$$

□

2 Naloge

2.1 Kdaj uporabiti verjetnostno metodo

Verjetnostna metoda spada v sklop globalnih razmislekov. Globalni razmisliki so tisti, pri katerih obravnavamo celotno strukturo naenkrat, njihovo nasprotje pa so lokalni razmisleki, pri katerih obravnavamo samo del strukture. Primera lokalnih razmislekov sta požrešni algoritem ter princip ekstremnega elementa, ki pravi, da se je pogosto smoterno osredotočiti na elemente, ki so v nekem smislu najmanjši ali največji.

Seveda se pojavi vprašanje kdaj uporabiti verjetnostno metodo ter globalne metode na splošno. Eden izmed zelo dobrih indikatorjev za uporabo globalnih metod je, da imamo ob izbiri konkretnega objekta oz. elementa vedno lahko »nesrečo«. Poglejmo si to na primeru.

Denimo, da je na krožnici razporejenih 101 črnih točk ter 100 belih točk ter želimo pokazati, da obstajata dve sosednji točki črne barve. Če izberemo neko specifično točko gotovo obstaja konfiguracija, v kateri noben izmed njenih sosedov ni črne barve. Seveda bi lahko znotraj fiksne konfiguracije iskali črno točko z neko specifično lastnostjo, za katero bi pokazali, da ima črnega soseda, a taka lastnost se ne pojavi na dlani. Potreben je globalni razmislek, ki celotno strukturo krožnice ter točk obravnava sočasno.[1]

Opazimo, da ko želimo za izbran element pokazati kakšno lastnost, ki bi nam pomagala rešiti nalogo, naletimo na težavo, saj obstaja neka konfiguracija točk na krožnici, ki našo domnevo ovrže. To nas motivira, da poskusimo nadaljevati z nekim globalnim razmislekom.

2.2 Rešena naloga

Naloga 2.1: IMC 2002

30 dijakov in dijakinj se je udeležilo izbirnega testa, na katerem je 6 nalog. Vsako nalogo je rešilo vsaj 18 dijakov oziroma dijakinj. Dokaži, da obstajata dva tekmovalca, ki sta skupaj rešila vse naloge.

Rešitev. Naključno in enakomerno izberimo par tekmovalcev (a, b). Izračunali bomo pričakovano vrednost števila nalog, ki jih je rešil ta par, za katero upamo, da bo večja od 5, saj bi to po verjetnostnem Dirichletovem principu zaključilo dokaz.

Vpeljemo **indikatorske spremenljivke**

$$R_{j,(a,b)} = \begin{cases} 1; & \text{vsaj en član para } \ (a,b) \ \text{ je rešil nalogo } \ j \\ 0; & \text{sicer } \ . \end{cases}$$

Za vsak par (p, q) je število nalog, ki jih je rešil vsaj eden izmed njiju enako

$$N_{p,q} = \sum_{j=1}^{6} R_{j,(p,q)}.$$

[1] Na poljuben način oštevilčimo vse točke. Vsaka črna točka ima desnega soseda, obenem dve različni črni točki nimata soseda z isto številko. Če bi imele vse črne točke belega desnega soseda bi tako dobili injektivno preslikavo iz množice črnih točk v množico belih točk, kar ni mogoče zaradi velikosti množic.

Tako je

$$
\begin{aligned}
\mathbb{E}N_{p,q} &= \sum_{j=1}^{6} \mathbb{E}[R_{j,(a,b)}] \\
&= \sum_{j=1}^{6} \Big(1 \cdot \mathbb{P}(R_{j,(a,b)} = 1) + 0 \cdot \mathbb{P}(R_{j,(a,b)} = 0)\Big) \\
&= \sum_{j=1}^{6} \mathbb{P}\left(R_{j,(a,b)} = 1\right) \\
&= \sum_{j=1}^{6} \mathbb{P}\left(\text{par } (a,b) \text{ je rešil nalogo } j\right) \\
&= \sum_{j=1}^{6} \left(1 - \mathbb{P}\left(\text{par } (a,b) \text{ ni rešil naloge } j\right)\right).
\end{aligned}
$$

Verjetnost, da par (a, b) ne reši naloge j, pa je $\left(\frac{12}{30}\right)^2$. Tako sledi, da je

$$\mathbb{E}[N_{a,b}] = 6 \cdot \left(1 - \frac{144}{900}\right) = 5{,}04 > 5. \qquad \square$$

Komentar 2.2

Ideji zgornje naloge sta samo 2: uporaba probabilističnega Dirichletovega načela ter vpeljava indikatorskih spremenljivk, ki nam skupaj z linearnostjo pričakovane vrednosti problem štetja rešenih nalog prevede na določanje verjetnosti, da eden izmed tekmovalcev v paru reši dano nalogo.
Ideja z vpeljavo indikatorske spremenljivke je **zelo** standardna ter je vredna pomnenja.

2.3 Naloge za vajo

Naloga 2.3. *Naj bo n naravno število. Naključno in enakomerno izberemo permutacijo množice $\{1, 2, \dots, n\}$. Koliko je pričakovana vrednost števila fiksnih točk permutacije?*

Opomba: i je fiksna točka permutacije π, če je $\pi(i) = i$.

Naloga 2.4 (IMO 1987)**.** *Naj bo $p_n(k)$ število permutacij množice $\{1, \dots, n\}$, ki imajo natanko k fiksnih točk. Pokaži, da je*

$$\sum_{k=0}^{n} k \cdot p_n(k) = n!.$$

Naloga 2.5 (NIMO)**.** *Tekač in skakač se znajdeta na neskončni šahovnici, katero zadane roj meteorjev, ki v vsako celico neodvisno z verjetnostjo p postavi meteor. Niti tekač, niti skakač nista bila zadeta, a meteorji lahko omejijo njune možne premike. Prav tako tekač in skakač ne blokirata morebitnih potez drug drugemu. Določi vrednosti p, za katere je pričakovana vrednost števila potez, ki jih lahko naredita na obstreljeni šahovnici, enaka za tekača in skakača.*

Naloga 2.6 (HMMT 2006)**.** *V krogu sedi n dijakov, nakar vsak izmed njih poda svoj svinčnik bodisi svojemu levemu, bodisi svojemu desnemu sosedu, vsakemu z enako verjetnostjo ter neodvisno od dejanj drugih dijakov. Kolikšna je pričakovana vrednost števila dijakov, ki niso prejeli nobenega svinčnika?*

Naloga 2.7 (Engel)**.** *V krogu z radijem 16 imamo 650 točk. Dan je kolobar z notranjim radijem 2 ter zunanjim radijem 3. Pokaži, da lahko kolobar postavimo tako, da pokrije vsaj 10 točk.*

Naloga 2.8 (Engel)**.** 12 % *površine krogle je bilo pobarvane s črno barvo, preostanek je bele barve. Pokaži, da lahko krogli vrišemo kvader, ki ima vsa oglišča bela.*

Naloga 2.9 (ISL 1987)**.** *Pokaži, da lahko pobarvamo elemente množice $\{1, \dots, 1987\}$ s štirimi barvami tako, da nobeno aritmetično zaporedje desetih elementov nima vseh elementov iste barve.*

Naloga 2.10 (IMO 1998)**.** *Na izbirnem testu je a tekmovalcev in b ocenjevalcev, kjer je $b > 3$ liho število. Vsak ocenjevalec vsakemu tekmovalcu dodeli točko, ali pa mu je ne. Vemo, da sta poljubna ocenjevalca dodelila točko največ k istim tekmovalcem. Pokaži, da je*

$$\frac{k}{a} \geq \frac{b-1}{2b}.$$

Naloga 2.11 (ISL 2006)**.** *Naj bo S končna množica točk v ravnini, nobene tri izmed katerih niso kolinearne. Za vsak konveksen večkotnik $\mathcal{P}$, čigar oglišča ležijo v S, označimo število njegovih oglišč z $a(\mathcal{P})$ ter število točk S, ki ležijo izven $\mathcal{P}$, z $b(\mathcal{P})$. Daljica, točka ter prazna množica so vsi konveksni mnogokotniki, zaporedoma z 2, 1 ter 0 oglišči. Pokaži, da za vse $x \in \mathbb{R}$ velja*

$$\sum_{\mathcal{P}} x^{a(\mathcal{P})} \cdot (1-x)^{b(\mathcal{P})} = 1,$$

kjer vsota teče po vseh konveksnih večkotnikih $\mathcal{P}$ z oglišči v S.

Naloga 2.12 (Inaba)**.** *Pokaži, da lahko poljubnih* 10 *točk v ravnini pokrijemo z disjunktnimi enotskimi diski.*

Naloga 2.13 (ISL 1991)**.** *Naj bo A množica n ostankov po modulu n^2. Pokaži, da obstaja množica B, ki je prav tako množica n ostankov mod n^2, tako, da lahko vsaj $\frac{1}{2}$ ostankov mod n^2 zapišemo kot vsoto elementa A ter elementa B.*

Naloga 2.14 (Rusija 1996)**.** *V parlamentu je* 1600 *poslancev, ki tvorijo* 16000 *komitejev po* 80 *poslancev. Pokaži, da obstajata dva komiteja, ki imata vsaj* 4 *skupne člane.*

Naloga 2.15 (Engel)**.** *Potepuh ima plašč s površino* 1*, na katerem je* 5 *zaplat, vsaka ima površino vsaj $\frac{1}{2}$. Pokaži, da obstaja par zaplat, ki ima skupno površino $\frac{1}{5}$.*

Literatura

[1] Ravi Boppana. *Unexpected Uses of Probability*. 2004. URL: https://cdn.artofproblemsolving.com/attachments/6/0/ddd43ddb390a02614796b60a0081020445c532.pdf (pridobljeno 22. 10. 2024).

[2] Evan Chen. *Expected Uses of Probability*. 2014. URL: https://web.evanchen.cc/handouts/ProbabilisticMethod/ProbabilisticMethod.pdf (pridobljeno 16. 9. 2024).

[3] Arthur Engel. *Problem Solving Strategies*. 1997.