Tikimybių teorijos apžvalga

Diskrečioji tikimybinė erdvė

Apibrėžimas. *Tegu Ω yra baigtinė arba skaiti aibė, $\mathcal{P}(\Omega)$ visų jos poaibių sistema, $P(\omega),\ \omega \in \Omega$, neneigiami skaičiai, tenkinantys sąlygą*

$$\sum_{\omega \in \Omega} P(\omega) = 1. \tag{1}$$

Tikimybe vadinsime funkciją $P\ :\ \mathcal{P}(\Omega) \to [0,\ 1]$, kiekvienam $A \subset \Omega$ apibrėžiamą lygybe

$$P(A) = \sum_{\omega \in A} P(\omega).$$

Porą (Ω, P) vadinsime diskrečiąja tikimybine erdve, o Ω - elementariųjų įvykių aibe.

Klasikinė tikimybė

Tai yra baigtinė tikimybinė erdvė, kurioje visi elementarieji įvykiai vienodai galimi. Taigi, jei

$$\Omega = \{\omega_1, \omega_2, \ldots, \omega_n\},$$

tai

$$P(\omega_1) = P(\omega_2) = \cdots = P(\omega_n) = \frac{1}{n}.$$

Todėl pagal apibrėžimą įvykio $A = \{\omega_{i_1}, \omega_{i_2}, \ldots, \omega_{i_k}\} \subset \Omega$ tikimybė bus

$$P(A) = \sum_{j=1}^{k} P(\omega_{i_j}) = \frac{k}{n}.$$

Kitaip sakant, įvykio tikimybė yra lygi jam palankių elementariųjų baigčių skaičiaus ir visų elementariųjų baigčių skaičiaus santykiui.

Pavyzdys. Metamos trys simetriškos monetos. Raskime įvykio $A =${atsivertė bent vienas herbas} tikimybę. Šiuo atveju galime sudaryti tokią elementariųjų įvykių aibę

$$\Omega = \{\omega_0, \omega_1, \omega_2, \omega_3\},$$

čia $\omega_i =${atsivertė i herbų}. Tada $A = \{\omega_1, \omega_2, \omega_3\}$.
Atrodytų, kad $P(A) = \frac{3}{4}$.

Klasikinė tikimybė

Pavyzdys. Metamos trys simetriškos monetos. Raskime įvykio $A =$\{atsivertė bent vienas herbas\} tikimybę. Šiuo atveju galime sudaryti tokią elementariųjų įvykių aibę

$$\Omega = \{\omega_0, \omega_1, \omega_2, \omega_3\},$$

čia $\omega_i =$\{atsivertė i herbų\}. Tada $A = \{\omega_1, \omega_2, \omega_3\}$. Atrodytų, kad $P(A) = \frac{3}{4}$. Tačiau iš tikrųjų ne visi įvykiai ω_i yra vienodai galimi. Todėl

$$P(\omega_0) = P(\omega_3) = \frac{1}{8}, \quad P(\omega_1) = P(\omega_2) = \frac{3}{8}.$$

Taigi

$$P(A) = P(\omega_1) + P(\omega_2) + P(\omega_3) = \frac{7}{8}.$$

Apibrėžimas. *Įvykiai A ir B vadinami nesuderinamais, kai $P(A \cap B) = 0$. Jei $A \cap B = \emptyset$, tai A ir B vadinami nesutaikomais.*

Pavyzdys. Dėžėje yra k baltų ir m juodų rutulių. Atsitiktinai be grąžinimo traukiame du rutulius. Nagrinėsime įvykius $A =${pirmasis rutulys baltas} ir $B =${antrasis rutulys baltas}. Tegu

$$\Omega = \{\omega_{bb}, \omega_{bj}, \omega_{jb}, \omega_{jj}\} ,$$

čia elementariųjų įvykių ω indeksai žymi ištraukto rutulio spalvą. Pavyzdžiui, ω_{bj} = {pirmasis rutulys baltas, o antras - juodas}. Tada

$$A = \{\omega_{bb}, \omega_{bj}\} , \quad B = \{\omega_{bb}, \omega_{jb}\} , \quad A \cap B = \{\omega_{bb}\} \neq \emptyset.$$

Matome, kad įvykiai A ir B yra sutaikomi. Rasime jų tikimybes.

Nesuderinami įvykiai

Kadangi

$$P(\omega_{bb}) = \frac{k(k-1)}{(k+m)(k+m-1)}, \quad P(\omega_{jj}) = \frac{m(m-1)}{(k+m)(k+m-1)},$$

$$P(\omega_{bj}) = P(\omega_{jb}) = \frac{k \cdot m}{(k+m)(k+m-1)},$$

tai

$$P(A) = P(\omega_{bb})+P(\omega_{bj}) = P(\omega_{bb})+P(\omega_{jb}) = P(B) = \frac{k}{k+m}.$$

Tačiau įvykiai A ir B ne visada bus suderinami, nes

$$P(A \cap B) = P(\omega_{bb}) = \frac{k(k-1)}{(k+m)(k+m-1)} = 0,$$

kai $k \leq 1$.

Tikimybių savybės

Tegu $A,\ B,\ B_1,\ A_1,\ A_2, \ldots$ yra atsitiktiniai įvykiai diskrečiojoje tikimybinėje erdvėje (Ω, P).

1. $P(\emptyset) = 0, \quad P(\Omega) = 1.$
2. Jei $A \subset B$, tai $P(A) \leq P(B)$.
3. Jei A ir B nesuderinami ir $A_1 \subset A,\ B_1 \subset B$, tai įvykiai A_1 ir B_1 taip pat bus nesuderinami.
4. Jeigu įvykiai $A_1, A_2, \ldots$ poromis nesuderinami, t.y. $P(A_i \cap A_j) = 0$ visiems natūraliesiems $i \neq j$, tai
$$P(\bigcup_i A_i) = \sum_i P(A_i)\,.$$
5. Jei $A \subset B$, tai $P(B \setminus A) = P(B) - P(A)\,.$
6. $P(\overline{A}) = 1 - P(A)\,.$
7. $P(A \cup B) = P(A) + P(B) - P(A \cap B)\,.$

Įvykių σ algebra

Atsitiktinių įvykių aibe laikoma tik tam tikra, pakankamai "turtinga" Ω paibių sistema $\mathcal{F}$, turinti tokias savybes:

i) $\Omega \in \mathcal{F}$,

ii) $A \in \mathcal{F} \Rightarrow \overline{A} \in \mathcal{F}$,

iii) $A_1, A_2, \ldots \in \mathcal{F} \Rightarrow A_1 \cup A_2 \cup \ldots \in \mathcal{F}$.

Paibių sistema $\mathcal{F}$ vadinama atsitiktinių įvykių σ (sigma) algebra.

Tada tikimybe vadinama funkcija $P : \mathcal{F} \to [0, 1]$, jei

i) $P(\Omega) = 1$;

ii) jei $A_i \in \mathcal{F}$ ir $A_i \cap A_j = \emptyset$ visiems natūraliesiems $i \neq j$, tai $P(A_1 \cup A_2 \cup \ldots) = P(A_1) + P(A_2) + \ldots$.

Sąlyginė tikimybė

Sąlyginė tikimybė žymima $P(A|B)$ (skaitoma "tikimybė, kad įvyks A su sąlyga, kad įvyko B" arba "įvyks A , jeigu įvyko B"). Jei $P(B) > 0$, tai

$$P(A|B) = \frac{P(A \cap B)}{P(B)} .$$

Iš sąlyginės tikimybės apibrėžimo išplaukia vadinamoji *tikimybių daugybos teorema* :

$$P(A \cap B) = P(B)P(A|B) = P(A)P(B|A). \qquad (2)$$

Apibrėžimas. *Įvykius A ir B vadinsime nepriklausomais, jeigu* $P(A \cap B) = P(A)P(B)$.

Didesnio įvykių skaičiaus nepriklausomumas apibrėžiamas sudėtingiau.

Sąlyginė tikimybė

Pavyzdžiui, įvykiai A, B ir C vadinami nepriklausomais, jei teisingos visos keturios lygybės

$$\begin{aligned} P(A \cap B) &= P(A)P(B), \quad P(A \cap C) = P(A)P(C), \\ P(B \cap C) &= P(B)P(C), \quad P(A \cap B \cap C) = P(A)P(B)P(C). \end{aligned}$$

Pilnosios tikimybės formulė

$$P(A) = \sum_{i \in I} P(H_i) P(A|H_i) \, , \tag{2}$$

čia $H_i, \ (i \in I)$ - baigtinė arba skaiti poromis nesuderinamų įvykių šeima, tenkinanti sąlygą

$$P(\bigcup_{i \in I} H_i) = 1.$$

Pilnosios tikimybės formulė teigia, kad *apriorinę* įvykio A tikimybę galima rasti, žinant *aposteriorines* (sąlygines) A tikimybes, esant sąlygoms H_i, ir tų sąlygų susidarymo tikimybes.

Bajeso formulė

Esant toms pačioms prielaidoms kaip ir pilnosios tikimybės formulėje, galime rasti ir hipotezių aposteriorines tikimybes $P(H_j|A)$:

$$P(H_j|A) = \frac{P(H_j)P(A|H_j)}{\sum\limits_{i\in I} P(H_i)P(A|H_i)} . \tag{3}$$

(3) lygybė vadinama Bajeso hipotezių tikrinimo formule.

Dešifravimo uždavinys

Tarkime, kad slaptas pranešimas užšifruotas raidėmis $a,\ b,\ c$ ir žinoma, kad paprastai pusę šifruoto teksto sudaro raidės a, o raidė b sutinkama dvigubai dažniau nei c. Be to, kol pasiekia adresatą, vidutiniškai 10% raidžių b bei 5% raidžių c iškraipomos ir virsta raidėmis a. Kokia tikimybė, kad tryliktas adresato gauto šifruoto teksto simbolis bus raidė a ? Parinksime hipotezes $H_1,\ H_2,\ H_3$:
H_1={tryliktas siunčiamo šifro simbolis buvo raidė a} ,
H_2={tryliktas siunčiamo šifro simbolis buvo raidė b} ,
H_3={tryliktas siunčiamo šifro simbolis buvo raidė c} ,
$P(H_1) = \frac{1}{2}$;$P(H_2) = \frac{1}{3}$;$P(H_3) = \frac{1}{6}$.
Tegul A={tryliktas gauto šifro simbolis yra raidė a} . Tuomet, pagal uždavinio sąlygas,

$$P(A|H_1) = 1\,, \quad P(A|H_2) = 0,1\,, \quad P(A|H_3) = 0,05\,.$$

Dešifravimo uždavinys

Pritaikę pilnosios tikimybės formulę, gauname

$$\begin{aligned} P(A) &= P(H_1)P(A|H_1) + P(H_2)P(A|H_2) + P(H_3)P(A|H_3) \\ &= \frac{1}{2}\cdot 1 + \frac{1}{3}\cdot\frac{1}{10} + \frac{1}{6}\cdot\frac{1}{20} = \frac{13}{24}\,. \end{aligned}$$

Galime formuluoti ir kitą, dažnai žymiai aktualesnį, klausimą. Tarkime, kad vienaip ar kitaip adresatas sugebėjo perskaityti tą nelemtą tryliktąjį gauto šifro simbolį - tai buvo raidė a. Kokia tikimybė, kad ji nėra iškraipyta? Kitaip sakant, mus dominanti tikimybė yra $P(H_1|A)$.

Dešifravimo uždavinys

Ją rasime, pasinaudoję Bajeso formule. Pastebėsime, kad trupmenos vardiklis (3) lygybėje, pagal pilnosios tikimybės formulę, yra lygus $P(A)$. Todėl

$$P(H_1|A) = \frac{P(H_1)P(A|H_1)}{P(A)} = \frac{\frac{1}{2}\cdot 1}{\frac{13}{24}} = \frac{12}{13}\,.$$

Bernulio eksperimentų schema nusakoma taip: eksperimentą atlikus vieną kartą, jo sėkmės tikimybė lygi p. Atliekame n nepriklausomų eksperimentų. Sėkmių skaičių pažymėkime S_n. Kokia tikimybė, kad eksperimentas pavyks k kartų, t.y. $S_n = k$? Atsakymas į šį klausimą toks:

$$P(S_n = k) = \binom{n}{k} p^k (1-p)^{n-k}, \quad k = 0, 1, \ldots, n. \tag{4}$$

Atsitiktiniai dydžiai

Tarkime, kad (Ω, P) yra diskrečioji tikimybinė erdvė. *Atsitiktiniu dydžiu* šioje erdvėje vadinama realioji funkcija $X : \Omega \to \mathbb{R}$. *Diskretieji a.d.* dažniausiai nusakomi *reikšmių skirstiniu*, nurodant galimas reikšmes x_i ir jų tikimybes

$$p_i = P(X = x_i) = \sum_{\omega\in\Omega\,:\,X(\omega)=x_i} P(\omega)\,, \quad i = 1, 2, \ldots\,.$$

Apibrėžimas. *Atsitiktinis dydis X, kurio patekimo į intervalą $[a, b]$ tikimybė skaičiuojama pagal formulę*

$$P(a \le X \le b) = \int_a^b p(x)\,dx\,, \quad p(x) \ge 0\,,$$

vadinamas absoliučiai tolydžiuoju dydžiu, o funkcija $p(x)$ vadinama jo tankiu.

A.d. pasiskirstymo funkcija

Atsitiktinio dydžio X *pasiskirstymo funkcija* $F(x)$ yra

$$F(x) = P(X < x)\,, \quad x \in \mathbb{R}\,.$$

Absoliučiai tolydžiojo atsitiktinio dydžio pasiskirstymo funkciją ir tankį sieja lygybės:

$$\begin{aligned} F'(x) &= p(x)\,, \\ F(x) &= \int\limits_{-\infty}^{x} p(u)\,du\,. \end{aligned}$$

Nepriklausomi a.d.

Atsitiktinius dydžius X_1 ir X_2 vadiname nepriklausomais, kai su bet kuriais realiųjų skaičių poaibiais $B_1,\ B_2$ įvykiai $\{\omega\ :\ X_1(\omega) \in B_1\}$ ir $\{\omega\ :\ X_2(\omega) \in B_2\}$ yra nepriklausomi, kitaip sakant, jei

$$P(X_1 \in B_1,\, X_2 \in B_2) = P(X_1 \in B_1)P(X_2 \in B_2)\,.$$

Diskrečiųjų atsitiktinių dydžių atveju pakanka pareikalauti, kad visiems realiesiems $x,\ y$ būtų tenkinama lygybė

$$P(X_1 = x,\, X_2 = y) = P(X_1 = x)P(X_2 = y)\,.$$

A.d. vidurkis

X	x_1	x_2	x_3	$\ldots$
P	p_1	p_2	p_3	$\ldots$

Žinoma, $p_1 + p_2 + \cdots = 1\,,\quad p_i \geq 0$. Taip nusakyto atsitiktinio dydžio *vidurkiu* vadinama suma

$$\mathbf{E}X = x_1p_1 + x_2p_2 + x_3p_3 + \ldots\,.$$

Jeigu X turi tankį $p(x)$, tai vidurkis apibrėžiamas integralu

$$\mathbf{E}X = \int_{-\infty}^{\infty} xp(x)\,dx\,.$$

A.d. vidurkis

Dikrečiojo ir tolydžiojo dydžių atvejais funkcijos vidurkis atitinkamai yra

$$\mathbf{E}f(X) = f(x_1)p_1 + f(x_2)p_2 + f(x_3)p_3 + \dots$$

ir

$$\mathbf{E}f(X) = \int_{-\infty}^{\infty} f(x)p(x)\,dx\,.$$

A.d. vidurkis

Savybės

Tegu $X, X_1, X_2, \ldots, X_n$ yra atsitiktiniai dydžiai, turintys baigtinius vidurkius.

1. Su bet kokiomis konstantomis $c_1, c_2, \ldots, c_n$ teisinga lygybė

$$\mathbf{E}\Big(\sum_{i=1}^{n} c_i X_i\Big) = \sum_{i=1}^{n} c_i \mathbf{E} X_i\,.$$

2. Jei $X_1 \le X_2$, tai $\mathbf{E}X_1 \le \mathbf{E}X_2$.
3. $|\mathbf{E}X| \le \mathbf{E}|X|$.
4. Jei X_1, X_2 yra nepriklausomi, tai

$$\mathbf{E}(X_1 \cdot X_2) = \mathbf{E}(X_1) \cdot \mathbf{E}(X_2)\,.$$

A.d. dispersija

A.d. sklaidą apie vidurkį aprašo *dispersija*

$$\mathbf{D}X = \mathbf{E}(X - \mathbf{E}X)^2 \,.$$

Kvadratinė šaknis iš dispersijos vadinama *standartiniu nuokrypiu* $\sigma(X) = \sqrt{\mathbf{D}X}$.
Paminėsime keletą dispersijos savybių, laikydami, kad atsitiktiniai dydžiai $X, X_1, X_2, \ldots, X_n$ turi baigtines dispersijas.

A.d. dispersija

Savybės

1. $\mathbf{D}X \geq 0$.
2. $\mathbf{D}X = \mathbf{E}X^2 - (\mathbf{E}X)^2$.
3. $\mathbf{D}(X_1 + X_2) = \mathbf{D}X_1 + \mathbf{D}X_2 + 2cov(X_1, X_2)$, čia

$$\begin{aligned} cov(X_1, X_2) &= \mathbf{E}(X_1 - \mathbf{E}X_1)(X_2 - \mathbf{E}X_2) \\ &= \mathbf{E}X_1X_2 - \mathbf{E}X_1\mathbf{E}X_2 \end{aligned}$$

   yra atsitiktinių dydžių X_1 ir X_2 *kovariacija*.
4. Jei $X_1, X_2, \ldots, X_n$ yra nepriklausomi atsitiktiniai dydžiai, tai su bet kokiomis konstantomis $c_1, c_2, \ldots, c_n$ teisinga lygybė

$$\mathbf{D}\Big(\sum_{i=1}^{n} c_i X_i\Big) = \sum_{i=1}^{n} c_i^2 \mathbf{D}X_i \, .$$

Pavyzdys. Rasime binominio skirstinio vidurkį ir dispersiją. Tegul $X_i = 1$, jei i-tasis Bernulio eksperimentas buvo sėkmingas, ir $X_i = 0$ - priešingu atveju. Tada sėkmių skaičius po n eksperimentų bus n nepriklausomų, vienodai pasiskirsčiusių atsitiktinių dydžių suma

$$S_n = X_1 + X_2 + \cdots + X_n \,.$$

Todėl

$$\begin{aligned} \mathbf{E}S_n &= \sum_{i=1}^{n} \mathbf{E}X_i = np \,, \\ \mathbf{D}S_n &= \sum_{i=1}^{n} \mathbf{D}X_i = np(1-p) \,. \end{aligned}$$

Įvykių sistemos

Tarkime $\mathcal{A} = \{A_i : i \in I\}$ yra diskrečiosios tikimybinės erdvės (Ω, P) įvykių šeima, I - baigtinė arba skaiti indeksų aibė.

Apibrėžimas. *Jei* $P(A_i \cap A_j) = 0$ *visiems* $i, j \in I$, $i \neq j$ *ir*

$$P\Big(\bigcup_{i \in I} A_i\Big) = 1\,,$$

tai $\mathcal{A}$ *vadinsime tikimybinės erdvės* (Ω, P) *įvykių sistema.*

Pastebėsime, kad poromis nesuderinamiems įvykiams A_i

$$P\Big(\bigcup_{i \in I} A_i\Big) = \sum_{i \in I} P(A_i)\,.$$

Todėl antrojoje apibrėžimo sąlygoje sąjungos tikimybę pakeitę atitinkamų tikimybių suma, gautume ekvivalentišką įvykių sistemos apibrėžimą.

Įvykių sistemos

Apibrėžimas. *Tarkime* $\mathcal{A} = \{A_i : i \in I\}$ *ir* $\mathcal{B} = \{B_j : j \in J\}$ *yra tikimybinės erdvės* (Ω, P) *įvykių sistemos.* $\mathcal{A}$ *yra sistemos* $\mathcal{B}$ *apvalkalas, jei kiekvienam* $j \in J$ *galima rasti tokį* $i \in I$ *, kad* $P(A_i \cap B_j) = P(B_j)$ *. Tokiu atveju sakysime, kad sistema* $\mathcal{B}$ *yra tikslesnė už sistemą* $\mathcal{A}$*.*

Kitaip sakant, kiekvienai tikslesnės sistemos aibei visada atsiras ją dengianti "grubesnės" sistemos aibė

Įvykių sistemos

Teorema. *Jei $\mathcal{B}$ yra tikslesnė už sistemą $\mathcal{A}$, tai visiems* $i \in I,\ j \in J$

$$P(A_i \cap B_j) = P(B_j) \quad arba \quad P(A_i \cap B_j) = 0.$$

Įvykių sistemos

Įrodymas. Kai $P(B_j) = 0$, šis teiginys akivaizdus. Tarkime, kad $P(B_j) \neq 0$ ir $P(A_i \cap B_j) \neq P(B_j)$. Lieka įsitikinti, kad tokiu atveju būtinai $P(A_i \cap B_j) = 0$. Pagal apvalkalo apibrėžimą, aibėje I galima rasti tokį $i_0 \neq i$, kad

$$P(A_{i_0} \cap B_j) = P(B_j).$$

Vadinasi

$$B_j = A_{i_0} \cap B_j \cup N\,, \quad P(N) = 0.$$

Taigi

$$\begin{aligned} P(A_i \cap B_j) &= P(A_i \cap (A_{i_0} \cap B_j) \cup (A_i \cap N)) \\ &\leq P(A_i \cap A_{i_0}) + P(N) = 0. \end{aligned}$$

$\square$

Jungtinė įvykių sistema

Tarkime $\mathcal{A} = \{A_i : i \in I\}$ ir $\mathcal{B} = \{B_j : j \in J\}$ yra tikimybinės erdvės (Ω, P) įvykių sistemos. Jų *jungtinė sistema* $\mathcal{A} \wedge \mathcal{B}$ nusakoma lygybe

$$\mathcal{A} \wedge \mathcal{B} = \{A_i \cap B_j : (i, j) \in I \times J\}.$$

Akivaizdu, kad $\mathcal{A} \wedge \mathcal{B}$ tikslesnė ir už $\mathcal{A}$ ir už $\mathcal{B}$. Bet pasirodo, kad ji yra pati "grubiausia" iš visų tikslesnių už $\mathcal{A}$ ir $\mathcal{B}$.

Jungtinė įvykių sistema

Teorema. *Jei sistema $\mathcal{C}$ yra tikslesnė už $\mathcal{A}$ ir $\mathcal{B}$, tai ji tikslesnė ir už $\mathcal{A} \wedge \mathcal{B}$.*

Įrodymas. Iš tikrųjų, iš teiginio prielaidos išplaukia, kad kiekvienam $C \in \mathcal{C}$ galima rasti tokius A_i ir B_j kad $P(A_i \cap C) = P(B_j \cap C) = P(C)$.
Todėl

$$B_j \cap C = C \setminus N\,,\;\; N \subset C\,,\;\; P(N) = 0.$$

Dabar gauname

$$\begin{aligned} P(A_i \cap B_j \cap C) &= P(A_i \cap (C \setminus N)) \\ &= P((A_i \cap C) \setminus (A_i \cap N)) \\ &= P(A_i \cap C) - P(A_i \cap N) = P(C). \end{aligned}$$

□

Nepriklausomos įvykių sistemos

Tikimybinės erdvės (Ω, P) įvykių sistemos $\mathcal{A} = \{A_i : i \in I\}$ ir $\mathcal{B} = \{B_j : j \in J\}$ vadinamos *nepriklausomomis*, jei

$$P(A_i \cap B_j) = P(A_i)P(B_j)$$

visiems $(i, j) \in I \times J$.

Pavyzdys. Tarkime X ir Y diskretieji atsitiktiniai dydžiai erdvėje (Ω, P), o $\{x_i \in \mathbb{R} : i \in I\}$ ir $\{y_j \in \mathbb{R} : j \in J\}$ - jų galimų reikšmių aibės. Apibrėžkime įvykius $A_i = \{X = x_i\}$ ir $B_j = \{Y = y_j\}$. Nesunku pastebėti, kad $\mathcal{A} = \{A_i : i \in I\}$ ir $\mathcal{B} = \{B_j : j \in J\}$ yra tikimybinės erdvės (Ω, P) įvykių sistemos. Jos bus nepriklausomos tada ir tik tada, kai nepriklausomi yra jas generuojantys atsitiktiniai dydžiai X ir Y.