NMAI059 Pravděpodobnost a statistika 1
1. přednáška

Robert Šámal

Přehled

Organizace

Pravděpodobnost – úvod

Podmíněná pravděpodobnost

Bonus

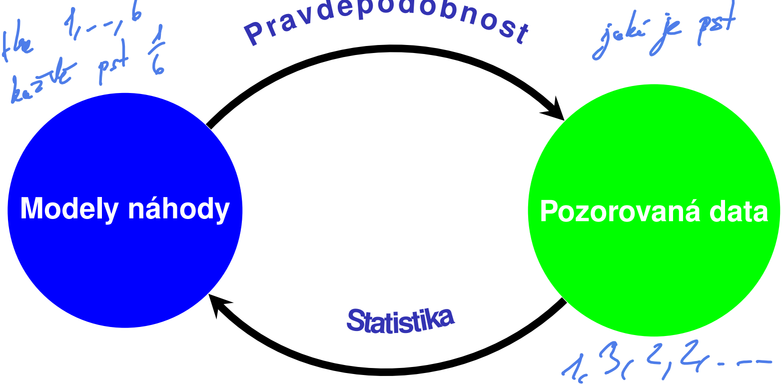
Organizace přednášky

- Přednášky v Zoomu, dokud to bude potřeba (patrně celý semestr). Přednáška má svoji stránku v Moodle (odkaz v SISu). Tam bude všechno.
- Nedojde-li k technickým komplikacím, bude video přednášky dostupné (po přihlášení do SISu).
- Kdyby vám vadilo být nahráni, můžete vypnout svoji kameru, případně dotazy klást v chatu.
- Budu ale rád, pokud si kameru zapnete, abych viděl, jak pomalu/rychle mluvím, co vás překvapilo, atd.
- Používejte též funkce Zoomu – přihlásit se, zpomalit-zrychlit, atd.
- Během přednášky budeme používat krátké ankety.
- Pdf verze „tabule“ bude též k dispozici – už před přednáškou.
- Zkouška bude v ideálním případě prezenční písemka s možností ústního dozkoušení.
- V Moodlu je také prostor pro diskuzi, jak (ne)funguje technologie. Případně se ozvěte emailem.

Organizace cvičení

- Detaily vám sdělí cvičící

Plán přednášky



kostka 1, ..., 6
každé pst $\frac{1}{6}$

1, 5, 4, 3, 3
jaká je pst

1, 3, 2, 2, . . . — — —

— — — — 6

hodně

Přehled

Aplikace na rozehřátí

$\frac{d}{4}$ pol. st. $\frac{d}{4}$

Schwartz–Zippel algo

NEZNÁME

$\frac{d}{2}$ kvadr. pol.

Příklad

Dány dva polynomy $f(x), g(x)$ stupně d. Chceme zjistit, zda jsou stejné, a to co nejrychleji.

$$f(x) = \sum_{i=0}^{d} a_i x^i \qquad g(x) = \boxed{\sum_{i=0}^{d} b_i x^i} = \underbrace{g_1(x)\, g_2(x)\, g_3(x) \dots}_{(x^2-x+1)(x^2+3x+2)\dots}$$

$f = g \iff a_0 = b_0,\ a_1 = b_1,\ \dots,\ a_d = b_d$ alg. s časem $O(d)$

Algo: zvolíme náhodné $x_1 \in \{1, 2, \dots, 100d\}$.

Ověříme zda $f(x_1) = g(x_1)$ — ano — $f = g$ ← ?

— ne — $f \neq g$ ← správně

Pokud $f(x_1) = g(x_1)$, tak x_1 je kořen pol. $f - g$

... takových x_1 je $\leq d$

$$P(f(x_1) = g(x_1) \mid f \neq g) \leq \frac{1}{100}$$

zvol. nák. $x_2, x_3 \in \{1, \dots, 100d\}$

$$P(\text{Pro } i = 1,2,3 \ f(x_i) = g(x_i) \mid f \neq g) \leq \left(\frac{1}{100}\right)^3 = 10^{-6}$$

Pravděpodobnost – intuice, definice

Některé jevy neumíme/nechceme popsat kauzálně:

- hod kostkou $\Omega = \{1, \dots, 6\} = [6]$
- tři hody kostkou, nekonečně mnoho hodů kostkou $[6]^3 = [6] \times [6] \times [6]$ $[6]^{\mathbb{N}}$
- hod šipkou na terč $\Omega =$ jednotk. kruh
- počet emailů za den $\Omega = \mathbb{N}$
- dobu běhu programu (v reálném počítači) $\mathbb{R}$

Důvody:

- fyzikální vlastnost přírody?
- komplikovaný proces (počasí, medicína, molekuly plynu)
- neznámé vlivy (působení dalších lidí, programů, ...)
- randomizované algoritmy (test prvočíselnosti, quicksort)
- náhodné grafy (odhady Ramseyových čísel)

Pro popis pomocí teorie pravděpodobnosti napřed vybereme *množinu elementárních jevů (sample space)* Ω.

Prostor jevů

Dále vybereme *prostor jevů (event space)* $\mathcal{F} \subseteq \mathcal{P}(\Omega)$, u kterých budeme měřit jejich pravděpodobnost.
Často $\mathcal{F} = \mathcal{P}(\Omega)$, to je možné vždy, když Ω je spočetná. Ale např. pro $\Omega = \mathbb{R}$ to už nejde.

Definice

$\mathcal{F} \subseteq \mathcal{P}(\Omega)$ je prostor jevů (též σ-algebra), pokud

- $\emptyset \in \mathcal{F}$ a $\Omega \in \mathcal{F}$,
- $A \in \mathcal{F} \Rightarrow \Omega \setminus A \in \mathcal{F}$, a A^c
- $A_1, A_2, \ldots \in \mathcal{F} \Rightarrow \bigcup_{i=1}^{\infty} A_i \in \mathcal{F}$.

A_1, A_2 lib.; $A_3 = A_4 = \cdots = \emptyset$

$\Downarrow$ $A_1 \cup A_2 \in \mathcal{F}$

$A_1 \cap A_2 \in \mathcal{F}$

$A_1 \setminus A_2 \in \mathcal{F}$

Axiomy pravděpodobnosti

Definice

$P : \mathcal{F} \to [0, 1]$ se nazývá pravděpodobnost (probability), pokud

- $P(\emptyset) = 0$, $P(\Omega) = 1$, *a*
- $P(\bigcup_{i=1}^{\infty} A_i) = \sum_{i=1}^{\infty} P(A_i)$, *pro libovolnou posloupnost po dvou disjunktních jevů* $A_1, A_2, \ldots \in \mathcal{F}$.

$A_3 = A_4 = \ldots = \emptyset$, $P(\emptyset) = 0$

$P(A_1 \cup A_2) = P(A_1) + P(A_2)$

Definice

Pravděpodobnostní prostor (probability space) je trojice $(\Omega, \mathcal{F}, P)$ taková, že

- $\Omega \neq \emptyset$ *je libovolná množina,*
- $\mathcal{F} \subseteq \mathcal{P}(\Omega)$ *je prostor jevů, a*
- P *je pravděpodobnost.*

Názvosloví

- *Šance (odds)* jevu A je $O(A) = \frac{P(A)}{P(A^c)}$. Např. šance na výhru je 1 ku 2 znamená, že pravděpodobnost výhry je $1/3$; šance, že na kostce padne šestka je 1 ku 5.

- „A je *jistý jev*" znamená $P(A) = 1$. Také se říká, že A nastává *skoro jistě (almost surely)*, zkráceně s.j. (a.s.).
- „A je *nemožný jev*" znamená $P(A) = 0$.

$P(A) = 0 \overset{?}{\Longrightarrow} A = \emptyset$

$\Longleftarrow$ axiom

$\Longrightarrow$ platí často, ne vždy

$\Omega =$  kruh v rovině

$P(A) = \frac{\text{obsah } A}{\text{obsah } \Omega}$

$A = \{\text{střed kruhu}\}$

$P(A) = 0$

B spočetná množ.

$P(B) = 0 + 0 + \dots = 0$

B_i je i-tý bod

$B = B_1 \cup B_2 \cup \dots$

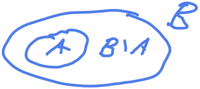
Základní vlastnosti

Věta

V pravděpodobnostním prostoru $(\Omega, \mathcal{F}, P)$ *platí pro* $A, B \in \mathcal{F}$

1. $P(A) + P(A^c) = 1 \qquad (A^c = \Omega \setminus A)$
2. $A \subseteq B \Rightarrow P(A) \le P(B)$
3. $P(A \cup B) = P(A) + P(B) - P(A \cap B)$
4. $P(A_1 \cup A_2 \cup \dots) \le \sum_i P(A_i)$ *(subaditivita, Booleova nerovnost)*

nevyžadujeme disj.



Dk ① $\Omega = A \cup A^c$; A, A^c disj.

$1 = P(\Omega) = P(A) + P(A^c)$

② $B = \underbrace{A \cup (B \setminus A)}$ → disj.

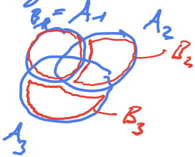
$P(B) = P(A) + \underbrace{P(B\setminus A)}_{\geq 0} \geq P(A)$

③ podobně, cvič.

④ trik zdisjunktnění

$B_1 = A_1$, $B_2 = A_2 \setminus A_1$

$B_i = A_i \setminus \bigcup_{j<i} A_j$



- $B_i \subseteq A_i \Rightarrow P(B_i) \le P(A_i)$
- $B_i \cap B_j = \emptyset$ kdykoli $j < i$ $\qquad B_i \cap B_j \subseteq B_i \cap A_j = \emptyset$
- $\bigcup_{i=1}^{\infty} B_i = \bigcup_{i=1}^{\infty} A_i$

$\subseteq$ ✓ $\qquad \supseteq$ $x \in \bigcup A_i \dots$ najdi i_0 aby $x \in A_{i_0}$ & i_0 min. $\quad x \in B_{i_0}$

$P(\bigcup A_i) = P(\bigcup B_i) = \sum P(B_i) \le \sum P(A_i)$ ∎

Příklady pravděpodobnostních prostorů 1

- **Konečný s uniformní pravděpodobností**
  Ω je libovolná konečná množina, $\mathcal{F} = \mathcal{P}(\Omega)$,
  $P(A) = |A|/|\Omega|$. $\frac{\#\text{příznivých}}{\#\text{všech}}$
- **Diskrétní**
  $\Omega = \{\omega_1, \omega_2, \dots\}$ je libovolná spočetná množina. Jsou dány $p_1, p_2, \dots \in [0, 1]$ se součtem 1.
  $$\boxed{P(A) = \sum_{i:\omega_i \in A} p_i}$$

$\sum p_i = 1$

$\sum_{i=1}^{N} p_i = 1$

$|\Omega| = N$

počet Ω nekon.

$\sum_{i=1}^{\infty} p_i = 1$

$P(\emptyset) = 0$

$P(\Omega) = 1$

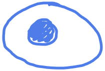
A_i disj.

$P(A_1 \cup A_2 \cup \dots) = \sum P(A_i)$

Příklady pravděpodobnostních prostorů 2

Ω určena nerovnostmi $\{x_1^2 + x_2^2 \leq 1\}$

- **Spojitý**
  $\Omega \subseteq R^d$ pro vhodné d (Ω např. uzavřená nebo otevřená)
  $\mathcal{F}$ vhodná (obsahuje např. všechny otevřené množiny)
  $f : \Omega \to [0, 1]$ je funkce taková, že $\int_\Omega f(x)dx = 1$.
  analogie $\sum p_i = 1$
  $P(A) = \int_A f(x)dx$



Ω

$\int_A f(x)\,dx = V_d(A) \cdot \frac{1}{V_d(\Omega)}$

  Spec. případ: $f(x) = 1/V_d(\Omega)$
  $P(A) = V_d(A)/V_d(\Omega)$,
  kde $V_d(A) = \int_A 1$ je d-rozměrný objem A.

$\int_0^1 f(x)\,dx = \int_{[0,1]} g(x)\,dx$

- **Bernoulliho krychle – nekonečné opakování**
  $\Omega = S^{\mathbb{N}}$, kde S je diskrétní s pstí Q,
  $\mathcal{F}$ vhodná (obsahuje např. všechny množiny tvaru
  $A = A_1 \times \cdots \times A_k \times S \times S \times \cdots$
  $P(A) = Q(A_1) \cdots Q(A_k)$

  P(na zač. prefix PPO) $= \frac{1}{8}$

  Př.: $\{0, 1\}^{\mathbb{N}}$ nekonečné házení mincí

$S = \{0, 1\}$ $Q(\{0\}) = Q(\{1\}) = \frac{1}{2}$

Nepříklady

Pokud $P(0) = P(1) = P(2) = \dots = p$ tak $P(\mathbb{N}) = p + p + \dots = \infty$ ($\neq 1$)

- **Náhodné přirozené číslo** můžeme vybrat mnoha způsoby. V přednášce poznáme geometrické a Poissonovo rozdělení. Nemůžeme ale požadovat, aby všechna přirozená čísla měla stejnou pravděpodobnost. (Proč?)
  „Náhodné přirozené číslo je sudé s pravd. $1/2$.“ ???
- **Náhodné reálné číslo** Opět není žádný preferovaný způsob, jak definovat pravděpodobnost pro $\Omega = \mathbb{R}$.
  Typicky bude každé reálné číslo mít pravděpodobnost 0!
  Navíc nejde definovat pravděpodobnost tak, aby nezáležela na posunu, tj. $P([0,1]) = P([1,2]) = \dots$
- **Náhodná tětiva kružnice – Bertrandův paradox**
  Vybereme náhodnou tětivu zadané kružnice. Jaká je pravděpodobnost, že její délka je větší, než strana vepsaného rovnostranného trojúhelníku?

Přehled

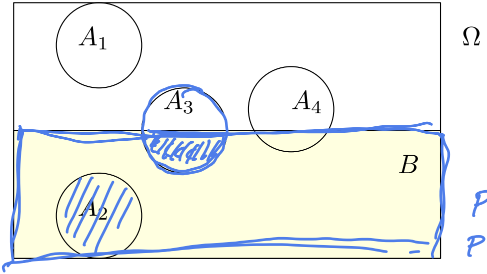
Podmíněná pravděpodobnost

Definice

Pokud $A, B \in \mathcal{F}$ a $P(B) > 0$, pak definujeme podmíněnou pravděpodobnost A při B (probability of A given B) jako

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

$$P(A_1 \mid B) = \frac{P(A_1 \cap B)}{P(B)} = 0$$



$$P(A_2 \mid B) = \frac{P(A_2)}{P(B)} \doteq 0.1$$

$$P(B \mid A_2) = 1$$

$$P(A_3 \mid B) = 0.05$$

$$P(B \mid A_3) = \frac{1}{2}$$

$\underline{Q(A)} := \underline{P(A \mid B)}$. Pak $(\Omega, \mathcal{F}, Q)$ je pravděpodobnostní prostor.

$(B, \mathcal{F}', Q)$

Zřetězené podmiňování

- $\boxed{P(A \cap B) = P(B)P(A \mid B)}$

Věta

Pokud $A_1, \dots, A_n \in \mathcal{F}$ *a* $P(A_1 \cap \dots \cap A_n) > 0$, *tak*

$$P(A_1 \cap A_2 \cap \dots \cap A_n) = P(A_1)P(A_2 \mid A_1)P(A_3 \mid A_1 \cap A_2) \dots P(A_n \mid \bigcap_{i=1}^{n-1} A_i)$$

Rozbor všech možností

Definice

Spočetný systém množin $B_1, B_2, \ldots \in \mathcal{F}$ je rozklad (partition) Ω, pokud

- $B_i \cap B_j = \emptyset$ *pro* $i \neq j$ *a*
- $\bigcup_i B_i = \Omega$.

Věta

Pokud $B_1, B_2, \ldots$ je rozklad Ω a $A \in \mathcal{F}$, tak

$$P(A) = \sum_i P(A \mid B_i)P(B_i)$$

(sčítance s $P(B_i) = 0$ považujeme za 0).

Rozbor všech možností

Bayesova věta

Věta

Pokud $B_1, B_2, \dots$ *je rozklad* Ω*,* $A \in \mathcal{F}$ *a* $P(A), P(B_j) > 0$*, tak*

$$P(B_j \mid A) = \frac{P(A \mid B_j)P(B_j)}{\sum_i P(A \mid B_i)P(B_i)}.$$

(sčítance s $P(B_i) = 0$ *považujeme za 0).*

Bayesova věta

Nezávislost jevů

Definice

Jevy $A, B \in \mathcal{F}$ *jsou nezávislé (independent) pokud* $P(A \cap B) = P(A)P(B)$.

- Pak také $P(A \mid B) = P(A)$, pokud $P(B) > 0$.

Nezávislost více jevů

Definice

Jevy $\{A_i : i \in I\}$ *jsou (vzájemně) nezávislé, pokud pro každou konečnou množinu* $J \subseteq I$

$$P(\bigcap_{i \in J} A_i) = \prod_{i \in J} P(A_i).$$

Pokud podmínka platí jen pro dvouprvkové množiny J*, nazýváme jevy* $\{A_i\}$ *po dvou nezávislé (pairwise independent).*

Spojitost pravděpodobnosti

Věta

Nechť pro množiny z prostoru jevů platí

$$A_1 \subseteq A_2 \subseteq A_3 \subseteq \cdots$$

a $A = \cup_{i=1}^{\infty} A_i$*. Pak platí*

$$P(A) = \lim_{i \to \infty} P(A_i).$$

- $A_n \subset \{P, O\}^{\mathbb{N}}$, $A_n =$ mezi prvními n hody padl aspoň jednou orel.

Přehled

Borel-Cantelliho lemma

Věta

Nechť jevy $A_1, A_2, \ldots$ *splňují* $P(A_i) = p_i > 0$ *pro každé* i*.* *Označme Nic jev „nenastal žádný z jevů* $\{A_i\}$*" a Inf jev „nastalo nekonečně mnoho z jevů* $\{A_i\}$*".*

1. *Pokud* $\sum_i p_i < \infty$*, tak* $P(Inf) = 0$*.*
2. *Pokud jsou jevy* $A_1, A_2, \ldots$ *nezávislé a* $\sum_i p_i = \infty$*, tak* $P(Nic) = 0$*,* $P(Inf) = 1$*.*