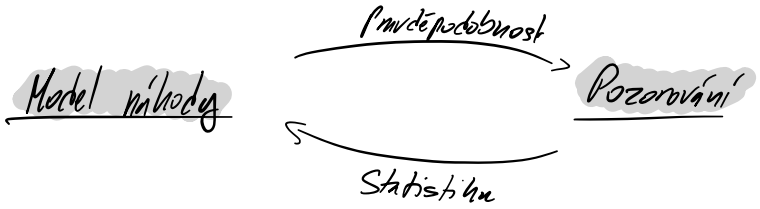


Aplikace násob. polyn.

f, g_1, g_2 → celočíselné polyn.

Test: $f(x) = g_1(x) \cdot g_2(x)$

$\deg = d$ $\quad$ $\deg = \frac{d}{2}$

alg 1: výpočet: $O(d^2)$ nebo $O(d \log d)$

alg 2: ověření: $O(d)$ $\quad$ $O(d)$ $\quad$ $O(d)$

$\forall x_i \in \mathbb{Z}$ $\quad$ $f(x_i) = g_1(x_i) \cdot g_2(x_i)$ $\quad$ } ✓ $O(d)$

pokud $\neq$ $\Rightarrow$ $f \neq g_1 \cdot g_2$

pokud $=$ $\Rightarrow$ x_i je kořen polyn. $f - g_1 \cdot g_2$

↳ nechť to x_i volíme náhodně z $\{1, \dots, 100d\}$ $\quad$ stupeň $\leq d$

Pokud $f \neq g_1 \cdot g_2$, $P(f(x) = g_1(x) \cdot g_2(x)) \leq \frac{d}{100d} = \frac{1}{100}$

Co to tedy je pst?

- Mějme nedeterministický jev → hod kostkou / doba běhu alg.

Def: Množina el. jevů (sample space) := Ω $\quad$ – pro hod kostkou: $\Omega = \{1, \dots, 6\} = [6]$

Def: Prostor jevů: $\mathcal{F} \subseteq \mathcal{P}(\Omega)$ $\quad$ → to jsou ty jevy, které zkoumáme

- pokud $\emptyset, \Omega \in \mathcal{F}$
- pokud $A \in \mathcal{F} \Rightarrow \Omega \setminus A \in \mathcal{F}$
- pokud $A_1, A_2 \in \mathcal{F} \Rightarrow A_1 \cup A_2 \in \mathcal{F}$

Def: $P : \mathcal{F} \to [0,1]$ je pravděpodobnost pokud:

1) $P(\Omega) = 1$
2) $P(\bigcup_{i=1}^{\infty} A_i) = \sum_{i=1}^{\infty} P(A_i)$ pro každou posl. disj. jevů $\in \mathcal{F}$

☼ $P(\emptyset) = 0$, $P(A_1 \cup A_2) = P(A_1) + P(A_2)$ $\Rightarrow$ opět můžou ostatní v nek. rozvoji $= \emptyset$

Def: Pravd. prostor:

je trojice $(\Omega, \mathcal{F}, P)$,

Def: Jistý jev: $P(A) = 1$

Nemožný jev: $P(A) = 0$

Thm: $(\Omega, \mathcal{F}, P)$, $A, B \in \mathcal{F}$

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

2) $A \subseteq B \Rightarrow P(A) \leq P(B)$

$\Rightarrow P(B \setminus A) = P(B) - P(A)$

3) $P(A \cup B) = P(A) + P(B) - P(A \cap B)$

4) $P(A_1 \cup A_2 \ldots) \leq \sum P(A_i)$

Dk:

$\boxed{A \mid A^c}$ Ω

1) $P(A \cup A^c) = P(A) + P(A^c) - \underbrace{P(A \cap A^c)}_{=\,\emptyset} = 1$

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

3) Intuitivní Vennův diagram

4) Najdu $B_1 \_ B_i$: $B_1 \cup B_2 \ldots = A_1 \cup A_2 \ldots$

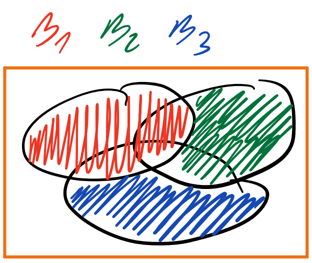
$B_i \subseteq A_i$

$B_1 = A_1$

$B_2 = A_2 \setminus B_1$

$\vdots$

$B_k = A_k \setminus (B_1 \cup B_2 \ldots \cup B_{k-1})$



Vždycky jsem buď nechal stejnou množinu, nebo ji trochu zmenšil. Zároveň jsem ale ve sjednocení B_i nic nevynechal.

Příklad:

1) Klasický pr. prost.

Ω konečný

$\mathcal{F} = \mathcal{P}(\Omega)$

$P(A) = \frac{|A|}{|\Omega|}$

2) Diskrétní pr. prostor

Ω konečný nebo spočetný

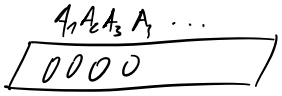
$\mathcal{F} = \mathcal{P}(\Omega)$

$p : \Omega \to [0,1] : \sum_{w \in \Omega} p(w) = 1$

$P(A) = \sum_{w \in A} p(w)$

1) $P(\Omega) = \sum_{w \in \Omega} p(w) = 1$

2) $P(\cup A) = \sum P(A)$

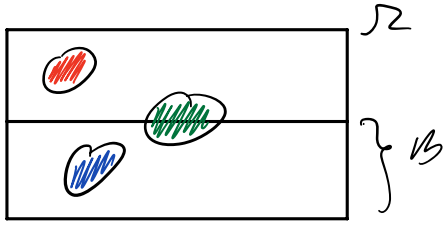


→ prostě posčítám

Def: Podmíněná pst:

$A, B \in \mathcal{F}, P(B) > 0 :$ $P(A|B) = \frac{P(A \cap B)}{P(B)}$:= pst A za podmínky B

Příklad:



A_1 A_2 A_3

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

$P(A_2|B) = \frac{P(A_2 \cap B)}{P(B)} = \frac{1}{2} \cdot \frac{P(A_3)}{P(B)}$

$P(A_3|B) = \frac{P(A_3 \cap B)}{P(B)} = \frac{P(A_3)}{P(B)}$

$P(B|A_3) = \frac{P(A_3 \cap B)}{P(A_3)} = \frac{P(A_3)}{P(A_3)} = 1$

↳ pokud nastalo A_3, jaká je pst B?