

Aplikace násob. polyn.

$f, g_1, g_2 \rightarrow$ celoč. polyn.

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

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

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

alg 2: ověření:

$\forall x_i \in \mathbb{Z} \quad f(x_i) = g_1(x_i) \cdot g_2(x_i) \quad \left. \vphantom{\forall x_i \in \mathbb{Z}} \right\} \sim O(d)$

polyn. $\neq \Rightarrow f \neq g_1 \cdot g_2$

polyn. $= \Rightarrow x_i$ je vhodn. polyn. $f = g_1 \cdot g_2$

\hookrightarrow vybrat to x_i volíme

množině \mathbb{Z} $\{1, \dots, 100d\}$

stepeni $\leq d$

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

Co to tedy je pst?

- Mějme nedeterministický jev \rightarrow hod. losování / dobrá věta alg.

Def: Množin. d. jeví (sample space) $:= \Omega$

- pro hod. losování: $\Omega = \{1, \dots, 6\} = [6]$

Def: Prostor jeví: $\mathcal{F} \subseteq \mathcal{P}(\Omega)$

\rightarrow to jsou imp. jevy, které chceme

- polyn. $\emptyset, \Omega \in \mathcal{F}$

- polyn. $A \in \mathcal{F} \Rightarrow \Omega \setminus A \in \mathcal{F}$

- polyn. $A_1, A_2 \in \mathcal{F} \Rightarrow A_1 \cup A_2 \in \mathcal{F}$

Def: $P: \mathcal{F} \rightarrow [0, 1]$ je praviděpodobnost polyn.:

1) $P(\Omega) = 1$

2) $P\left(\bigcup_{i=1}^{\infty} A_i\right) = \sum_{i=1}^{\infty} P(A_i)$ pro konečn. posl. disj. jeví $\in \mathcal{F}$

☀ $P(\emptyset) = 0$, $P(A_1 \cup A_2) = P(A_1) + P(A_2)$ \rightarrow opět měřan ostatní v rel. vzájemnosti = \emptyset

Def: Prvd. prostor:

je trojice (Ω, \mathcal{F}, P) ,

Def: Jistý jev: $P(A) = 1$

Nemožný jev: $P(A) = 0$

Thm: (Ω, \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) $P(A_1 \cup A_2 \dots) \leq \sum P(A_i)$

Důk:

1) $P(A \cup A^c) = P(A) + P(A^c) - P(A \cap A^c) = 1$ $\boxed{A \mid A^c}^{\Omega}$

2) $B = A \cup B \setminus A$, $P(B) = P(A) + P(B \setminus A) \geq P(A)$

3) Intuitivní Vennův diagram

4) Najdu B_1, \dots, B_n : $B_1 \cup B_2 \dots = A_1 \cup A_2 \dots$

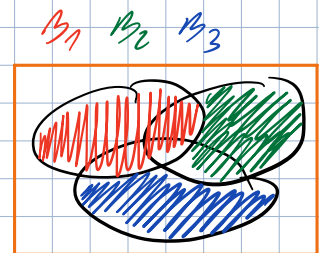
$B_i \subseteq A_i$

$B_1 = A_1$

$B_2 = A_2 \setminus B_1$

\vdots

$B_n = A_n \setminus (B_1 \cup B_2 \dots \cup B_{n-1})$



Vždycky jsem

buď nechtal stejnan
množinu, nebo ji trochu

zmenšil. Zároveň jsem

ale ve sjednocení B_i nic nevynechal.

Příklad:

1) Ukončený prv. prostor

Ω konečný

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

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

2) Diskrétní prv. prostor

Ω konečný nebo spočetný

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

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

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

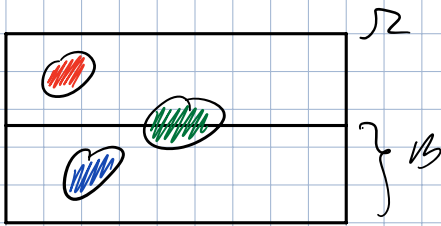
$$1) P(\Omega) = \sum_{\omega \in \Omega} p(\omega) = 1$$

$$2) P(\cup A) = \sum P(A) \quad \begin{array}{|c|} \hline A_1 A_2 A_3 A_4 \dots \\ \hline 0000 \\ \hline \end{array} \quad \Omega \rightarrow \text{prostě počítám}$$

Def: Podmíněný pst:

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

Příklad:



$A_1 A_2 A_3$

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

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

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

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

\hookrightarrow pokud nastalo A_3 , jistě je pst B ?