1) Házím mincí dokud mi nepadne Hlava

$Pr[\text{Hlava}] = p \qquad Pr[\text{Orel}] = 1-p$

X ... počet hodů, než padne hlava

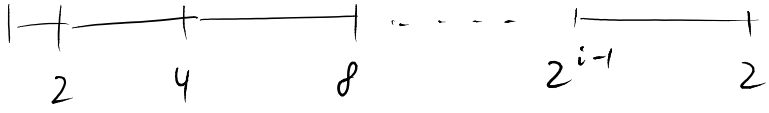
$\mathbb{E}[X] = ?$

$$\sum_{n=1}^{\infty} r^n = \frac{r}{1-r}$$

$$\sum_{n=1}^{\infty} n r^n = \frac{r}{(1-r)^2}$$

Př.: $\sum_{n=1}^{k} \frac{1}{n}$ $\sum_{n=1}^{\infty} \frac{1}{n^2}$ $\sum_{n=1}^{\infty} \frac{1}{n \cdot \lg^2 n} \approx \sum_{k} \frac{1}{k^2}$

$$\sum_{n=1}^{\infty} \frac{1}{n \cdot \lg n \cdot (\lg\lg n)^2} \approx \sum_{k} \frac{1}{k \lg^2 k}$$



$\frac{1}{2^{i-1}} < \quad < \frac{1}{2^i}$

$\frac{1}{2} < \quad < 1 \qquad \frac{1}{2} < \sum < 1$

$\frac{1}{2}\lg n < \quad < \lg n$

$$\frac{1}{k} - \frac{1}{k+1} = \frac{1}{k(k+1)}$$

$$\sum_{k=1}^{n} \frac{1}{k} - \frac{1}{k+1} = 1 - \frac{1}{n}$$

$\sum \frac{1}{n^2}$

2) X a) $Y = 2^X$ b) $Y = \cos X$

$H(X)$ vs $H(Y)$?

3) $Y = g(X)$ $\quad H(g(X)) \leq H(X)$ Dk: ?

4) $X_1, X_2, \ldots$ $\quad Pr[X_i] = \begin{cases} 0 & \text{pst } p \\ 1 & \text{pst } 1-p \end{cases}$

Nezávislé

chci: $g(X_1 \ldots X_n) = Z_1 \ldots Z_K$

$\forall k \quad Pr[Z_1 Z_2 \cdots Z_k = w \mid K = k] = 2^{-k}$
$\forall w \in \{0,1\}^k$

$E[K]$?

$H(X_1 \cdots X_n) = n \cdot H(p) \geq H(Z_1 \ldots Z_K, K)$
$= H(K) + H(Z_1 Z_2 \cdots Z_K \mid K)$
$\underbrace{\qquad\qquad}_{E[K]}$

$\geq E[K]$.

$E[K] \leq n \cdot H(p)$

Michal Koucky at 19. 4. 2016 12:05

- cvičení 11.4. 2016

R:

1) Existuje kód $[n, k, \frac{3}{4}n]_2$ pro $k > 1$?

$C_1 = \{0\ldots0, 1\ldots1\}$ $\quad k=1$ (NE)

2) Ex. kód $[n, k, \frac{2}{3}n]_2$ pro $k > 1$?

$\exists\ C_2 \ldots [9, 2, 6]_2$ kód

pro $k > 2$ žádný kód $[n, k, \frac{2}{3}n]$ neexistuje
- slabý argument jako v 1

3) (Plotkin) Pokud je kód $[n, k, (\frac{1}{2}+\varepsilon)n]_2$, pak $2^k \leq 1 + \frac{1}{2\varepsilon}$.

$C \subseteq \{-1, 1\}^n$ $\quad v_i, v_j \in C$

$\langle v_i, v_j \rangle \leq -2\varepsilon$

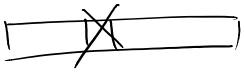
$\langle v_i, v_i \rangle = n$

$z = \sum_{v_i \in C} v_i \qquad \langle z, z \rangle = ? \Rightarrow |C| \leq 1 + \frac{1}{2\varepsilon}$.

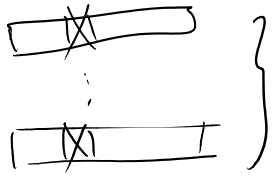
Michal Koucky at 26. 4. 2016 10:20

úpravy kódu:

- vynechání souřadnice $[n, k, d]_2 \longrightarrow [n-1, k, d-1]_2$

$C = \{$  $\}$

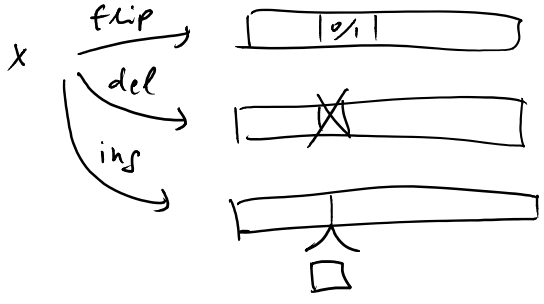
- restrikce souřadnice

$C = \{$  $\}$

vybere symboly, kterých se opakuje nejvíce krát v dané souřadnici, zahodím všechna slova, která mají na této souřadnici $\neq a$, souřadnici vyřízneme ze zbylých slov

$[n, k, d]_2 \rightarrow [n-1, k-1, d]_2$

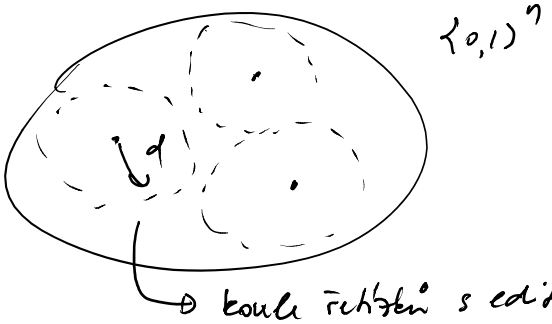
- editační vzdálenost



$d_{edit}(x, y)$ = #operací flip, insert, delete potřebných na převedení x na y.

- $d_{edit}(x,y) = d_{edit}(y,x)$
- $d_{edit}(x,y) \leq d_{edit}(x,z) + d_{edit}(z,y)$

kód pro editovací vzdálenost? Chci opravovat d chyb.



koule richtěných s editovací vzdáleností $\leq d$.

potřebujeme, aby byly objemy koulí

$Vol_{edit}(n, d)$ = objem koule $\leq 2^{\varepsilon n}$

= ?

$|C| \geq \frac{2^n}{Vol_{edit}(n,d)}$

pokud $d = \varepsilon n$ pro dostatečně malé ε.

Michal Koucky at 26. 5. 2016 9:39

Alenka $x \in \{0,1\}^n$ → g → Charlie $z \in \{0,1\}^n$ ← Bob $y \in \{0,1\}^n$

$f(x,y,z)$

- blackboard model

$EQ_n^k(x_1 \dots x_k) = [\forall i,j \;\; x_i = x_j]$

$NE_n^k(x_1 \dots x_n) = [\forall i \neq j, \; x_i \neq x_j]$

$D(EQ_n^k) = O(n)$ ... k hráčů, i-tý hráč x_i

$D(NE_n^k) = \Theta(kn)$ — " —

$(\underbrace{x_1 \dots x_k}_{\text{Alice}}, \underbrace{y_1, \dots y_k}_{\text{Bob}}) = [\forall i,\ x_i \neq y_i]$

NE_{kn} se dá efektivně spočítat správným protokolem pro NE^k_n (NIO)

$D(NE_{k,n}) = ?$ $\quad \Theta(kn) \Rightarrow D(NE^k_n) = \Omega(kn)$

- Number-on-the-forehead (NOF)

A $\quad$ B

x vidí (y,z) $\quad$ y vidí (x,z)

C

z vidí (x,y)

$D(EQ^k_n) \leq 2 \qquad D(NE^k_n) \leq 3$

- $DIS^k_n(x_1 \dots x_k) = [\overset{?}{\exists} i\ \forall j\ x_{j,i} = 1]$
- $MAJ^k_n(x_1 \dots x_k) = \sum_{i=1}^{n} MAJ(x_{1,i}, x_{2,i}, x_{3,i}) \bmod 2$
- $GIP^k_n(x_1, \dots x_k) = \sum_{i=1}^{n} x_{1,i}\, x_{2,i}\, x_{3,i} \dots x_{k,i} \bmod 2$

$D(DIS^k_n), D(MAJ^k_n), D(GIP^k_n) \leq O\left(\frac{n}{2^k}\right)$

$k = 3 \qquad D(DIS^3_n) \leq \frac{n}{2} + \text{pol} \log n$

$D(MAJ^3_n) \leq 3 \dots$

$MAJ(a,b,c) = ab + bc + ac \bmod 2$