## TODO

- Znani problemi (max/min cut, perfect matching, quicksort, ...)
- Porazdelitve

## Uporabne formule

$$H_n = \sum_{k=1}^{n} \frac{1}{k} \ \leq \ 1 + O(\log n)$$

$$\sum_{n=0}^{\infty} q^n = \frac{1}{1-q} \quad \sum_{n=0}^{b} q^n = \frac{1-q^{b+1}}{1-q}$$

$$\sum_{n=a}^{\infty} q^n = \frac{q^a}{1-q} \quad \sum_{n=a}^{b} q^n = \frac{q^a - q^{b+1}}{1-q}$$

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \ldots + ab^{n-2} + b^{n-1})$$

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$$

$$\frac{1}{(1-x)^n} = \sum_{k=0}^{n} \binom{n+k-1}{k} x^k$$

$$\binom{n}{k} = \frac{n^{\underline{k}}}{k!} = \frac{n!}{k!(n-k)!} = \binom{n}{n-k}$$

**Izbori**

Imamo $n$ oštevilčenih kroglic. Na koliko načinov lahko izberemo $k$ kroglic?

| | **s pon.** | **brez pon.** |
|---|---|---|
| **variacije** *vrstni red je pomemben* | $n^k$ | $n^{\underline{k}}$ |
| **kombinacije** *vrstni red ni pomemben* | $\binom{n+k-1}{k}$ | $\binom{n}{k}$ |

## Verjetnostni algoritmi za odločitvene probleme

Odgovarjamo na vprašanje $\omega \in \Pi$?
**Las Vegas** algoritmi vedno vrnejo pravilen odgovor
**Monte Carlo** algoritmi lahko vrnejo napačen odgovor

- tip 1: $P(\text{yes} \mid \omega \in \Pi) \geq \frac{1}{2}$ $P(\text{yes} \mid \omega \notin \Pi) = 0$
- tip 2: $P(\text{yes} \mid \omega \in \Pi) = 1$ $P(\text{yes} \mid \omega \notin \Pi) \leq \frac{1}{2}$
- tip 3: $P(\text{yes} \mid \omega \in \Pi) \geq \frac{3}{4}$ $P(\text{yes} \mid \omega \notin \Pi) \leq \frac{1}{4}$

**Razredi kompleksnosti odločitvenih problemov**

- RP (randomized polynomial time):
  $\exists$ Monte Carlo tipa 1, ki v najslabšem primeru deluje v polinomskem času.
- co-RP:
  $\exists$ Monte Carlo tipa 2, ki v najslabšem primeru deluje v polinomskem času.
- BPP (bounded-error probabilistic polynomial time): $\exists$ Monte Carlo tipa 3, ki v najslabšem primeru deluje v polinomskem času.
- ZPP (zero-error probabilistic polynomial time):
  $\exists$ Las Vegas algoritem, ki deluje v pričakovanem polinomskem času.
  Ali (ekvivalentna definicija): $\exists$ alg, ki v najslabšem primeru deluje v polinomskem času in vedno vrne pravilen odgovor ali "ne vem" in $P(\text{"ne vem"}) < \frac{1}{2}$.

$\text{ZPP} = \text{RP} \cap \text{co-RP}, \ \text{P} \subset \text{ZPP}, \ \text{RP} \cup \text{co-RP} \subset \text{BPP}$

## Chernoff bound

$X_1, \ldots, X_n$ neodvisne slučajne spremenljivke, $X_i \in \{0,1\}$, $X = \sum_{i=1}^{n} X_i$, $\mu = E(X)$. Potem za vsak $\delta \in (0,1)$ velja:

$$P(X - \mu \geq \delta\mu) \leq e^{-\frac{\delta^2\mu}{3}}$$

$$P(\mu - X \geq \delta\mu) \leq e^{-\frac{\delta^2\mu}{2}}$$

$$P(|X - \mu| \geq \delta\mu) \leq 2e^{-\frac{\delta^2\mu}{3}}$$

## Verjetnostni algoritmi za aproksimacijo

Verjetnostni algoritem izračuna $(\epsilon, \delta)$-aproksimacijo za $V$, če vrne $X$ tako, da velja:

$$P(|X - V| \leq \epsilon V) \geq 1 - \delta$$

Naj bodo $X_1, \ldots X_m$ slučajne spremenljivke, $\mu = E(X_i)$, $Y = \frac{\sum X_i}{m}$. Če je $m \geq \frac{3\ln(2/\delta)}{\epsilon^2\mu}$, potem velja:

$$P(|X - \mu| \geq \epsilon\mu) \leq \delta$$

in $Y$ je $(\epsilon, \delta)$-aproksimacija za $\mu$.

## Polinomi

Naj bo $\mathbb{F}$ polje. Stopnja polinoma $p \in \mathbb{F}[x_1, \ldots, x_n]$ je $\deg(p(x_1, \ldots, x_n)) = \deg(p(x, \ldots, x))$

**Schwartz-Zippelov izrek**

Naj bo $p \in \mathbb{F}[x_1, \ldots, x_n]$ in $\deg(p) = d \geq 0$. Naj bo $S \subseteq \mathbb{F}^n$ poljubna končna podmnožica. Za naključno izbiro (enakomerno) $r \in S$ velja:

$$P(p(r) = 0) \leq \frac{d}{|S|}$$

## Verjetnost

**Verjetnost** na $(\Omega, \mathcal{F})$ je preslikava $P : \mathcal{F} \to \mathbb{R}$ z lastnostmi:

- $P(A) \geq 0$ za $\forall A \in \mathcal{F}$
- $P(\Omega) = 1$
- Za paroma nezdružljive (disjunktne) dogodke $\{A_i\}_{i=1}^{\infty}$ velja *števna aditivnost*

$$P(\bigcup_{i=1}^{\infty} A_i) = \sum_{i=1}^{\infty} P(A_i)$$

- $P(\emptyset) = 0$
- $P$ je končno aditivna.
- $P$ je *monotona*: $A \subseteq B \implies P(A) \leq P(B)$
- $P(A^{\complement}) = 1 - P(A)$
- $P$ je *zvezna*:

$$A_1 \subseteq A_2 \subseteq \cdots \implies P(\bigcup_{i=1}^{\infty}) = \lim_{i \to \infty} P(A_i)$$

$$B_1 \supseteq B_2 \supseteq \cdots \implies P(\bigcap_{i=1}^{\infty}) = \lim_{i \to \infty} P(B_i)$$

**Matematično upanje**

Za slučajno spremenljivko $X : \Omega \to \mathbb{Z}$

$$E(X) = \sum_{c \in \mathbb{Z}} cP(X = c)$$

**Lastnosti**

$$E(f(X)) = \sum_{c \in \mathbb{Z}} f(c)P(X = c)$$

*Linearnost*: za poljubne sl. sprem $X_1, \ldots, X_n$ velja:

$$E(a_1X_1 + \ldots a_nX_n) = a_1E(X_1) + \cdots + a_nE(X_n)$$

Če ima $|X|$ mat. up., ga ima tudi $X$ in velja

$$|E(X)| \leq E(|X|)$$

Če obstaja $E(X^2)$ in $E(Y^2)$, obstaja tudi $E(XY)$ in velja:

$$|E(XY)| \leq E(|XY|) \leq \sqrt{E(X^2)E(Y^2)}$$

**Disperzija (varianca)**

$$D(X) = E((X - E(X))^2) = E(X^2) - (E(X))^2$$

Lastnosti:

- $D(X) \geq 0$
- $D(X) = 0 \iff P(X = E(X)) = 1$
- $D(aX) = a^2D(X)$

Standardna diviacija/odklon:

$$\sigma(X) = \sqrt{D(X)}$$

zanjo velja $\sigma(aX) = |a|\sigma(X)$.

**Neodvisnost**

Diskretno porazdeljeni sl. sprem. $X$ in $Y$ sta noedvisni, če velja:

$$P(X = x_i, Y = y_j) = P(X = x_i)P(Y = y_j)$$

za vse $i, j$.

**Nekoreliranost**

Sl. sprem. $X$ in $Y$ sta nekorelirani, če velja:

$$E(XY) = E(X)E(Y)$$

$$X, Y \text{ neodvisni} \implies X, Y \text{ nekorelirani}$$

Če imata $X$ in $Y$, je nekoreliranost ekvivalentna zvezi:

$$D(X + Y) = D(X) + D(Y)$$

**Neenakost Markova**

Če je $X$ ne negativna sl. sprem. z mat. up., potem je

$$P(|X| \geq a) \leq \frac{E(|X|)}{a} \quad \forall a > 0$$

**Neenakost Čebiševa**

Če ima $X$ disperzijo, je

$$P(|X - E(X)| \geq a\sigma(X)) \leq \frac{1}{a^2} \quad \forall a > 0$$

oziroma za $\varepsilon := a\sigma(X)$

$$P(|X - E(X)| \geq \varepsilon) \leq \frac{D(X)}{\varepsilon^2}$$