TODO

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

Uporabne formule

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

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

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

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

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

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

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

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

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 $P(\text{"ne vem"}) < \frac{1}{2}$.

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

Neenakost Černoffa

$X_1, \ldots, X_n$ 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:

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

Verjetnostni algoritmi za aproksimacijo

Verjetnostni algoritem izračuna (ϵ, δ)-aproksimacijo za V, če vrne X tako, da velja:

$$P(|X - V| \le \epsilon V) \ge 1 - \delta$$

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

$$P(|X - \mu| \ge \epsilon\mu) \le \delta$$

in Y je (ϵ, δ)-aproksimacija za μ.

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 $\deg(p) = d \ge 0$. Naj bo $S \subseteq \mathbb{F}^n$ poljubna končna podmnožica. Za naključno izbiro (enakomerno) $r \in S$ velja:

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

Verjetnost

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

- $P(A) \ge 0$ 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*: $A \subseteq B \implies P(A) \le P(B)$
- $P(A^{\complement}) = 1 - P(A)$
- 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:

$$E(a_1 X_1 + \ldots a_n X_n) = a_1 E(X_1) + \cdots + a_n E(X_n)$$

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

$$|E(X)| \le E(|X|)$$

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

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

Disperzija (varianca)

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

Lastnosti:

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

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

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

Neenakost Čebiševa

Če ima X disperzijo, je

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

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

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

Pregled najpogostejših porazdelitev

Porazdelitev	Oznaka	Opis	$E(X)$	$D(X)$	Izvor
Bernoullijeva	$\mathrm{Ber}(p)$	$P(X=0)=1-p$ $P(X=1)=p$	p	pq	Indikator dogodka
Binomska	$\mathrm{Bin}(n,p)$	$P(X=k)=\binom{n}{k}p^k q^{n-k}$	np	npq	Število uspešnih izidov v n neodvisnih poskusih; vsota n neodv. Bernoullijevih sl. spr.
Geometrijska	$\mathrm{Geo}(p)$	$P(X=k)=pq^{k-1}$ $k=1,2,\ldots$	$\frac{1}{p}$	$\frac{q}{p^2}$	Število poskusov do prvega uspešnega izida
Negativna binomska	$\mathrm{NegBin}(n,p)$	$P(X=k)=\binom{k-1}{n-1}p^n q^{k-n}$ $k=n,\,n+1,\ldots$	$\frac{n}{p}$	$\frac{nq}{p^2}$	Število poskusov do n-tega uspešnega izida; vsota n neodv. geom. sl. spr.
Poissonova	$\mathrm{Poi}(\lambda)$	$P(X=k)=\frac{\lambda^k e^{-\lambda}}{k!}$ $k=0,1,\ldots$	λ	λ	Število telefonskih klicev, nesreč ipd. v določenem času
Hipergeometrijska	$\mathrm{Hip}(s;r,n)$ $\mathrm{Hip}(r;s,n)$	$P(X=k)=\frac{\binom{s}{k}\binom{n-s}{r-k}}{\binom{n}{r}}$	$\frac{rs}{n}$	$\frac{rs(n-r)(n-s)}{n^2(n-1)}$	Število rdečih kroglic v vzorcu velikosti s, če je v škatli skupaj n kroglic, od tega r rdečih
Diskretna enakomerna na množici $M=\{x_1,\ldots x_n\}$	$\mathrm{Enak_d}(M)$	$P(X=x_k)=\frac{1}{n}$ $P(X\in A)=\frac{\lvert A\cap M\rvert}{\lvert M\rvert}$	$\bar{x}:=\frac{\sum_{k=1}^{n} x_k}{n}$	$\frac{1}{n}\sum_{k=1}^{n}(x_k-\bar{x})^2=$ $=\frac{\sum_{k=1}^{n} x_k^2-n\bar{x}^2}{n}$	Slepi izbor
Enakomerna na intervalu	$\mathrm{Enak_c}[a,b]$	$p_X(x)=\frac{1}{b-a},\ a\le x\le b$	$\frac{a+b}{2}$	$\frac{(b-a)^2}{12}$	Slepi izbor
Normalna	$\mathrm{N}(\mu,\sigma)$	$p_X(x)=\frac{1}{\sigma\sqrt{2\pi}}e^{-\frac{1}{2}\left(\frac{x-\mu}{\sigma}\right)^2}$	μ	σ^2	Če je X vsota veliko (vsaj 30) neodvisnih sl. spr., je približno $X\sim\mathrm{N}(\mu,\sigma)$, kjer je $\mu=E(X)$ in $\sigma=\sqrt{D(X)}$.
Standardizirana normalna	$\mathrm{N}(0,1)$	$p_X(x)=\frac{1}{\sqrt{2\pi}}e^{-x^2/2}$ $P(a<X<b)=\Phi(b)-\Phi(a)$	0	1	$X\sim\mathrm{N}(\mu,\sigma)\Rightarrow\frac{X-\mu}{\sigma}\sim\mathrm{N}(0,1)$
Eksponentna	$\mathrm{Exp}(\lambda)$	$p_X(x)=\lambda e^{-\lambda x},\ x>0$	$\frac{1}{\lambda}$	$\frac{1}{\lambda^2}$	Čas čakanja na dogodek
Gama	$\mathrm{Gama}(n,\lambda)$	$p_X(x)=\frac{\lambda^n x^{n-1}e^{-\lambda x}}{\Gamma(n)}$ $x>0$	$\frac{n}{\lambda}$	$\frac{n}{\lambda^2}$	Za $n\in\mathbb{N}$: čas n-te pojavitve dogodka
Hi kvadrat	$\chi^2(n)=$ $\mathrm{Gama}(\frac{n}{2},\frac{1}{2})$	$p_X(x)=\frac{x^{n/2-1}e^{-x/2}}{2^{n/2}\Gamma(n/2)}$ $x>0$	n	$2n$	Vsota kvadratov n neodvisnih stand. normalnih slučajnih spremenljivk

Opomba: $q=1-p$.