

TODO

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

Uporabne formule

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

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

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

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

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

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

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

Izbori

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

	s pon.	brez pon.
variacije <i>vrstni red je pomemben</i>	<i>n</i> ^{<i>k</i>}	<i>n</i> ^{<i>k</i>}
kombinacije <i>vrstni red ni pomemben</i>	^(<i>n</i>+<i>k</i>−1) / _{<i>k</i>}	^(<i>n</i>) / _{<i>k</i>}

Verjetnostni algoritmi za odločitvene probleme

Odgovarjamo na vprašanje *ω* ∈ Π?

Las Vegas algoritmi vedno vrnejo pravilen odgovor

Monte Carlo algoritmi lahko vrnejo napačen odgovor

- tip 1: *P*(yes | *ω* ∈ Π) ≥ 1⁄2 *P*(yes | *ω* ∉ Π) = 0
- tip 2: *P*(yes | *ω* ∈ Π) = 1 *P*(yes | *ω* ∉ Π) ≤ 1⁄2
- tip 3: *P*(yes | *ω* ∈ Π) ≥ 3⁄4 *P*(yes | *ω* ∉ Π) ≤ 1⁄4

Razredi kompleksnosti odločitvenih problemov

- RP (randomized polynomial time):

∃ Monte Carlo tipa 1, ki v najslabšem primeru deluje v polinomskem času.

- co-RP:

∃ Monte Carlo tipa 2, ki v najslabšem primeru deluje v polinomskem času.

- BPP (bounded-error probabilistic polynomial time): ∃ Monte Carlo tipa 3, ki v najslabšem primeru deluje v polinomskem času.

- ZPP (zero-error probabilistic polynomial time):

∃ Las Vegas algoritem, ki deluje v pričakovanem polinomskem času.

Ali (ekvivalentna definicija): ∃ alg, ki v najslabšem primeru deluje v polinomskem času in vedno vrne pravi-len odgovor ali ”ne vem” in *P*(”ne vem”) < 1⁄2.

ZPP = RP ∩ co-RP, P ⊂ ZPP, RP ∪ co-RP ⊂ BPP

Neenakost Černoffa

*X*₁, ..., *X*_{*n*} neodvisne slučajne spremenljivke, *X*_{*i*} ∈ {0,1}, *X* = ∑_{*i*=1}^{*n*} *X*_{*i*}, *μ* = *E*(*X*). Potem za vsak *δ* ∈ (0,1) velja:

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

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

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

Verjetnostni algoritmi za aproksimacijo

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

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

Naj bodo *X*₁, ... *X*_{*m*} slučajne spremenljivke, *μ* = *E*(*X*_{*i*}), *Y* = ∑​*X*_{*i*}​_{*m*}. Če je *m* ≥ 3ln(2/δ)⁄ ϵ² μ, potem velja:

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

in *Y* je (ϵ,δ)-aproksimacija za *μ*.

Polinomi

Naj bo ℱ polje. Stopnja polinoma *p* ∈ ℱ[*x*₁, ..., *x*_{*n*}] je deg(*p*(*x*₁, ..., *x*_{*n*})) = deg(*p*(*x*, ..., *x*))

Schwartz-Zippelov izrek

Naj bo *p* ∈ ℱ[*x*₁, ..., *x*_{*n*}] in deg(*p*) = *d* ≥ 0. Naj bo *S* ⊆ ℱ^{*n*} poljubna končna podmnožica. Za naključno izbiro (enakomerno) *r* ∈ *S* velja:

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

Verjetnost

Verjetnost na (Ω, *F*) je preslikava *P* : *F* → ℝ z lastnostmi:

- P*(*A*) ≥ 0 za ∀*A* ∈ *F*
- P*(Ω) = 1

- Za paroma nezdružljive (disjunktne) dogodke {*A*_{*i*}}[∞]_{*i*=1} velja *šteвна aditivnost*

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

- P*(∅) = 0
- P* je končno aditivna.
- P* je *monotona*: *A* ⊆ *B* ⟹ *P*(*A*) ≤ *P*(*B*)
- P*(*A*^c) = 1 − *P*(*A*)
- P* je *zvezna*:

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

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

Matematično upanje

Za slučajno spremenljivko *X* : Ω → 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, ..., *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*) ≥ 0
- D*(*X*) = 0 ⟺ *P*(*X* = *E*(*X*)) = 1
- D*(*aX*) = *a*²*D*(*X*)

Standardna diviacija/odklon:

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

zanjo velja σ(*aX*) = |*a*|σ(*X*).

Neodvisnost

Diskretno porazdeljeni sl. sprem. *X* in *Y* sta neodvisni, 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 ε := *aσ*(*X*)

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

Pregled najpogostejših porazdelitev

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

Opomba: $q = 1 - p$.