

### Uporabne formule

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

### 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 pravilen odgovor ali "ne vem" in *P*("ne vem") < 1⁄2.

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

### Chernoff bound

*X*<sub>1</sub>, . . . , *X*<sub>*n*</sub> neodvisne slučajne spremenljivke, *X*<sub>*i*</sub> ∈ {0, 1}, *X* = ∑<sub>*i*=1</sub><sup>*n*</sup> *X*<sub>*i*</sub>, μ = *E*(*X*). Potem za vsak δ ∈ (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 (ϵ, δ)-aproksimacijo za *V*, če vrne *X* tako, da velja:

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

Naj bodo *X*<sub>1</sub>, . . . *X*<sub>*m*</sub> slučajne spremenljivke, μ = *E*(*X*<sub>*i*</sub>), *Y* = ∑*X*<sub>*i*</sub>. Če je *m* ≥ 3ln(2/δ)⁄ϵ<sup>2</sup>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*<sub>1</sub>, . . . , *x*<sub>*n*</sub>] je deg(*p*(*x*<sub>1</sub>, . . . , *x*<sub>*n*</sub>)) = deg(*p*(*x*, . . . , *x*))

#### Schwartz-Zippelov izrek

Naj bo *p* ∈ ℱ[*x*<sub>1</sub>, . . . , *x*<sub>*n*</sub>] in deg(*p*) = *d* ≥ 0. Naj bo *S* ⊆ ℱ<sup>*n*</sup> 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*<sub>*i*</sub>}<sup>∞</sup><sub>*i*=1</sub> 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*<sup>0</sup>) = 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*<sub>1</sub>, . . . , *X*<sub>*n*</sub> 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*<sup>2</sup>) in *E*(*Y*<sup>2</sup>), 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*<sup>2</sup>*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 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:

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

$$X, Y \; \mathrm{neodvisni} \implies X, Y \; \mathrm{nekorelirani}$$

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

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

#### Neenakost Markova

Če je *X* sl. sprem. z mat. up., potem je

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