Typy pravdepodobnostných algoritmov

- **Las Vegas algoritmy:**
  vždy správny výstup
  čas závisí od náhodne generovaných bitov
  stredná hodnota času dobrá pre každý vstup

- **Monte Carlo algoritmy:**
  aj v najhoršom prípade dobrý čas
  občas môže dať nesprávnu odpoveď
  vysoká pravdepodobnosť správnej odpovede

Z Las Vegas do Monte Carlo

Majme Las Vegas algoritmus pre riešenie rozhodovacieho problému.
ELV(n): stredná hodnota počtu krokov

- Spusti K krokov Las Vegas algoritmu
- Ak Las Vegas algoritmus dovtedy skončil, vráť jeho výsledok (garantovaná správna odpoveď)
- V opačnom prípade vrát false (ak je správna odpoveď true, tak sme urobili chybu)

Ako nastaviť počet krokov K aby bola pravdepodobnosť chyby nízka? $\Rightarrow$ Monte Carlo algoritmus

Markovova nerovnosť

Veta: Nech X je náhodná premenná, $X \geq 0$
Ak $E[X] = \mu$ potom $\Pr(X \geq c\mu) \leq \frac{1}{c}$.

Dôkaz:

$$\begin{aligned}\mu = E[X] &= \textstyle\sum_x x.\Pr(X = x)\\ &\geq \textstyle\sum_{x<c\mu} 0.\Pr(X = x) + \sum_{x\geq c\mu} c\mu.\Pr(X = x)\\ &= c\mu \textstyle\sum_{x\geq c\mu} \Pr(X = x) = c\mu \Pr(X \geq c\mu)\end{aligned}$$

$\Pr(X \geq c\mu) \leq \frac{\mu}{c\mu} = \frac{1}{c}$ $\square$

Zvolíme $K = 2 \cdot ELV(n) \Rightarrow$ **pravdepodobnosť chyby** $\leq \frac{1}{2}$

SAT: Splniteľnosť logickej formuly

Daná formula v konjunktívnom normálnom tvare:

$(x_1 \vee x_2 \vee x_3) \wedge (x_1 \vee \neg x_2) \wedge (\neg x_1 \vee \neg x_2 \vee \neg x_3)$

Nájdite priradenie pravdivostných hodnôt tak, aby formula bola splnená.

3-SAT: všetky klauzuly majú 3 literály
2-SAT: všetky klauzuly majú 2 literály

3-SAT:

NP-ťažký problém
triviálne: $O(2^n \text{poly}(n, m))$
dá sa zlepšiť na $O(n^{1.465})$

2-SAT:

problém je v P
jednoduchý $O(n + m)$ algoritmus

```
RANDOMIZED-SAT-PAPADIMITRIOU (F):
  A := ľubovoľné ohodnotenie premenných
  repeat t times:
    if A spĺňa F return true
    C := ľubovoľná nesplnená klauzula
    a := náhodný literál v klauzule C
    zmeň v A hodnotu a
  return false
```

Ako zvoliť počet opakovaní t?

Uvažujme 2-SAT:

Nech S je ohodnotenie spĺňajúce F

t je počet zhodných ohodnotení v A a S

tzv. **náhodná prechádzka**

Označme e_t strednú hodnotu počtu krokov, za ktorý sa v náhodnej prechádzke dostaneme z hodnoty t na hodnotu n.

$e_n = 0$
$e_0 = 1 + e_1$
$e_i = 1 + \frac{1}{2}e_{i-1} + \frac{1}{2}e_{i+1}$

Potrebujeme vyriešiť rekurenciu!

Označme: $d_i := e_i - e_{i+1}$

$$e_i = 1 + \frac{1}{2}e_{i-1} + \frac{1}{2}e_{i+1}$$
$$2e_i = 2 + e_{i-1} + e_{i+1}$$
$$\underbrace{e_i - e_{i+1}}_{d_i} = 2 + \underbrace{e_{i-1} - e_i}_{d_{i-1}}$$

$$d_0 = e_0 - e_1 = 1$$

$$\Rightarrow d_i = 1 + 2i$$

Vráťme sa ku e_i:

$$e_i = e_{i+1} + d_i \qquad e_n = 0$$
$$\Rightarrow e_i = \sum_{j=i}^{n-1} d_j = \sum_{j=i}^{n-1}(1+2j) = (n-i) + 2\sum_{j=i}^{n-1} j$$
$$= n - i + n(n-1) - i(i-1) = n^2 - i^2$$

Stredná hodnota počtu krokov je zhora ohraničená n^2

```
RANDOMIZED-SAT-PAPADIMITRIOU (F):
  A := ľubovoľné ohodnotenie premenných
  repeat t times:
    if A spĺňa F return true
    C := ľubovoľná nesplnená klauzula
    a := náhodný literál v klauzule C
    zmeň v A hodnotu a
  return false
```

Ako zvoliť počet opakovaní t?

$e_i \leq n^2$; nech $t = 2n^2$
z Markovovej nerovnosti: pravdepodobnosť, že by náhodná pochôdzka trvala viac ako t krokov $\leq \frac{1}{2}$
$\Rightarrow$ Monte Carlo algoritmus s jednostrannou chybou

Ako postupovať, ak chceme menšiu chybu?

```
RANDOMIZED-SAT-SCHONING (F):
* repeat s times:
*   A := náhodné ohodnotenie premenných
    repeat t times:
      if A spĺňa F return true
      C := ľubovoľná nesplnená klauzula
      a := náhodný literál v klauzule C
      zmeň v A hodnotu a
  return false
```

Analýza pre 3-SAT

$e_n = 0$

$e_0 = 1 + e_1$

$e_i = 1 + \frac{2}{3}e_{i-1} + \frac{1}{3}e_{i+1}$

Náhodná prechádzka tohto typu by mala očakávaný počet krokov

$e_0 \approx 2^n$

```
RANDOMIZED-SAT-SCHONING (F):
* repeat s times:
*   A := náhodné ohodnotenie premenných
    repeat t times:
      if A spĺňa F return true
      C := ľubovoľná nesplnená klauzula
      a := náhodný literál v klauzule C
      zmeň v A hodnotu a
  return false
```

Ak vnútorný cyklus má pravdepodobnosť úspechu p
vonkajší cyklus má pravdepodobnosť chyby $(1-p)^s \leq e^{-ps}$
(ak chceme pravdepodobnosť chyby $< 1\%$, tak stačí $s \geq 5/p$)

Zvoľme radšej menšie $t = 3n$.

Aká je pravdepodobnosť p úspechu vnútorného cyklu?

Aká je pravdepodobnosť p úspechu vnútorného cyklu?

Začneme vo vzdialenosti u od spĺňajúceho priradenia
(v náhodnej prechádzke: začíname na $n-u$, chceme dôjsť na n)

Uvažujme $3u$ krokov, ak sa pohneme $2u$ krát doprava a u krát doľava, určite sa do pozície n dostaneme.

$$\begin{aligned}\Pr(\mathsf{OK} \mid n-u) &\geq \binom{3u}{2u}\left(\frac{1}{3}\right)^{2u}\left(\frac{2}{3}\right)^{u} = \binom{3u}{u}\left(\frac{1}{3}\right)^{2u}\left(\frac{2}{3}\right)^{u} \\ &\geq \frac{1}{\sqrt{5n}}\frac{3^{3u}}{2^{2u}}\frac{2^u}{3^{3u}} = \frac{1}{\sqrt{5n}}\left(\frac{1}{2}\right)^{u}\end{aligned}$$

Ako ďaleko začneme závisí od náhodnej voľby priradenia:

$$\begin{aligned}\Pr(\mathsf{OK}) &= \sum_u \binom{n}{u}\frac{1}{2^n}\Pr(\mathsf{OK} \mid n-u) \\ &\geq \sum_u \binom{n}{u}\frac{1}{2^n}\frac{1}{\sqrt{5n}}\left(\frac{1}{2}\right)^{u} = \frac{1}{\sqrt{5n}}\frac{1}{2^n}\sum_u \binom{n}{u}\left(\frac{1}{2}\right)^{u} \\ &= \frac{1}{\sqrt{5n}}\frac{1}{2^n}\left(1+\frac{1}{2}\right)^n = \frac{1}{\sqrt{5n}}\left(\frac{3}{4}\right)^{n}\end{aligned}$$

Pravdepodobnosť úspechu vnútorného cyklu je $p = \frac{1}{\sqrt{5n}}\left(\frac{3}{4}\right)^{n}$

Potrebujeme ho bežať $s = 5\sqrt{5n}\left(\frac{4}{3}\right)^{n}$ krát

Zhrnutie

- Ukázali sme si Markovovu nerovnosť, ktorá nám umožňuje jednoducho prerábať Las Vegas algoritmy na Monte Carlo algoritmy
- Pojem náhodnej pochôdzky; očakávaný počet krokov, kým sa dostaneme v symetrickej náhodnej pochôdzke z 0 na n je n^2
- Monte Carlo algoritmus s jednostrannou chybou môžeme bežať viac krát, čím znižujeme pravdepodobnosť chyby (exponenciálne s počtom behov)
- Monte Carlo algoritmus na riešenie problému 3-SAT v čase $O\left(\left(\frac{4}{3}\right)^n poly(m,n)\right)$