

---

# PAL: 10. cvičení

Tomáš Sieger

26. 11. 2020

---

# Opakování z minula

## Př. 9/1a: Hammingovsky blízka slova - dynamicky

---

Najděte v textu  $T$  všechny výskyty řetězců, které mají od vzorku  $P$  Hammingovu vzdálenost rovnou nejvýše  $k$ . Použijte metodu dynamického programování.

a)  $T = ccacbaabccaccbcabccc$ ,  $P = abcba$ ,  $k = 2$



## Př. 9/2a: Levenshteinovsky blízká slova - dynamicky

---

Najděte v textu  $T$  všechny výskyty řetězců, které mají od vzorku  $P$  Levenshteinovu vzdálenost rovnou nejvýše  $k$ . Použijte metodu dynamického programování.

a)  $T = aacacacbaabbbcbbcacc$ ,  $P = cbbba$ ,  $k = 3$



## Př. 8/13: generování podobných textů: Hamming

---

Navrhněte algoritmus pro vypsání všech slov nad abecedou  $A$ , která mají od daného vzorku  $p$  Hammingovu vzdálenost právě  $k > 0$ . Hodnota  $k$  je pevně dána. Jaká bude asymptotická složitost tohoto algoritmu?





## Př. 8/14: generování podobných textů: Levenshtein

---

Navrhněte algoritmus pro vypsání všech slov nad abecedou  $A$ , která mají od daného vzorku  $p$  Levenshteinovu vzdálenost nejvýše  $k > 0$ . Hodnota  $k$  je pevně dána. Jaká bude asymptotická složitost tohoto algoritmu?

## Př. 9/5a: bitový paralelizmus

---

Sestavte tabulky pro simulaci činnosti vyhledávacího automatu metodou bitového paralelizmu pro daný text  $T$ , vzorek  $P$  a Hammingovu vzdálenost  $k$ .

a)  $T = abcbcaaccbbaa$ ,  $P = bbac$ ,  $k = 2$ ,

b)  $T = accbbaaabcba$ ,  $P = acbb$ ,  $k = 2$ .



## Př. 9/3a: nedeterministické hledání slova z množiny

---

Sestrojte nedeterministický automat, který v textu nad abecedou  $A$  vyhledá právě každé slovo množiny  $M$ .

a)  $A = \{a, b, c\}$ ,  $M = \{a, b, ba, bc, aaa, bab, ccc, abbc, abcc\}$

## Př. 9/4a: deterministické hledání slova z množiny

---

Sestrojte deterministický automat, který v textu nad abecedou  $A$  vyhledá právě každé slovo množiny  $M$ .

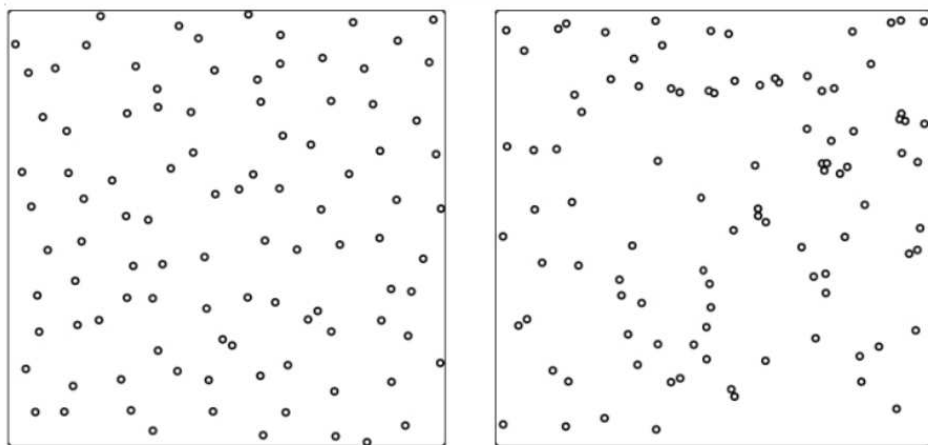
a)  $A = \{a, b, c\}$ ,  $M = \{a, b, ba, bc, aaa, bab, ccc, abbc, abcc\}$

---

Náhodná čísla. Prvočísla.  
Modulární umocňování.

## Př. 10/1: náhodné body

Máme dva obrázky - pokaždé jde o čtverec se 100 body uvnitř. V jednom případě byly souřadnice každého bodu generovány nezávisle a pseudonáhodně, ve druhém případě byly generovány analogicky, ale navíc byly souřadnice systematicky modifikovány (nám neznámým) způsobem. Odhadněte, kterého obrázku se týkají dodatečné úpravy a zdůvodněte svůj odhad.



## Př. 10/2: náhodná čísla

---

Máte jednu hrací kostku. Popište, jak využijte házení kostkou tak, abyste měli generátor náhodných celých čísel v rozmezí  $0 \dots 10$ . Všechna čísla  $0, 1, 2, \dots, 10$  musí být generována se stejnou pravděpodobností.





## Př. 10/3: náhodné uspořádání

---

Vysvětlete, jak pomocí generátoru náhodných čísel zamícháte do náhodného pořadí seřazené pole čísel. Akce musí proběhnout v čase úměrném délce pole.



## Př. 10/4: lin. kongruenční generátor náh. čísel

---

Ověřte, zda lineární kongruenční generátor s danými parametry má maximální možnou délku periody.

a)  $x_{n+1} = (91x_n + 49) \pmod{600}$ ,

b)  $x_{n+1} = (8x_n + 80) \pmod{49}$ ,

c)  $x_{n+1} = (37x_n + 55) \pmod{144}$ ,

d)  $x_{n+1} = (99x_n + 81) \pmod{113}$ .



## Př. 10/5: perioda Lehmerova generátoru náh. čísel

---

Určete délku periody v Lehmerově generátoru, který je dán předpisem  $x_{n+1} = ((M - 1) \cdot x_n) \bmod M$ , kde  $M$  je prvočíslo.

## Př. 10/6: počet prvočísel

---

Určete, kolik přibližně prvočísel leží v intervalu:

a)  $\langle 0, 10^9 \rangle$ ,

b)  $\langle 10^9, 2 \cdot 10^9 \rangle$ ,

c)  $\langle 2 \cdot 10^9, 3 \cdot 10^9 \rangle$ .

## Př. 10/7: poloprvočísla

---

Řekneme, že přirozené číslo je poloprvočíslu, pokud je buď prvočíslem nebo celou mocninou prvočísla. Popište modifikaci Eratosthenova síta, která bude generovat právě poloprvočísla. Napište pseudokód.



## Př. 10/8: skoroprvočísla

---

Jako skoroprvočísla označíme právě ta přirozená čísla, která jsou součinem dvou různých prvočísel. Popište modifikaci Eratosthenova síta, která bude generovat skoroprvočísla. Napište pseudokód.

## Př. 10/10: prvočísla v intervalu

---

Určete, jaký je maximální možný počet prvočísel v kterémkoli z intervalů  $\langle 30k, 30k + 29 \rangle, k = 1, 2, 3, 4, \dots$

## Př. 10/11a: největší společný dělitel

---

Vypočtete největší společný dělitel

a)  $GCD(220, 284)$ ,

b)  $GCD\left(\binom{30}{10}, \binom{31}{9}\right)$ ,

c)  $GCD(2^{100}, 100!)$ .

## Př. 10/11b: největší společný dělitel

---

Vypočtete největší společný dělitel

a)  $GCD(220, 284)$ ,

**b)**  $GCD\left(\binom{30}{10}, \binom{31}{9}\right)$ ,

c)  $GCD(2^{100}, 100!)$ .

## Př. 10/11c: největší společný dělitel

---

Vypočtete největší společný dělitel

a)  $GCD(220, 284)$ ,

b)  $GCD\left(\binom{30}{10}, \binom{31}{9}\right)$ ,

c)  $GCD(2^{100}, 100!)$ .

## Př. 10/12: modulární umocňování

---

Vypočtete  $18^{89} \pmod{11}$ .

## Př. 10/14: modulární umocňování - kód

---

Uvedený kód počítá celočíselnou mocninu  $x^n$ . Popište, jak jej upravíte, aby počítal  $x^n \bmod m$ , pro kladné celé  $m$ . Minimalizujte riziko přetečení.

```
BinPower(int x, int n) {
    int r = 1, y = x;
    while (n > 1) {
        if (n % 2 == 1) r *= y;
        y *= y;
        n /= 2;
    }
    return r*y;
}
```

