

## Lietiškie algoritmi – 4. mājas darbs

**Termiņš:** 2019. gada 9. decembris. Laiks 23:59:59 (UTC+2).

**Lasāmviela:** <http://linen-tracer-682.appspot.com/algorithms/references.html>, tēmas 4,5,6.

**1.uzdevums: RSA algoritms.** Bobs vēlas izveidot savu privātās/publiskās atslēgas pāri  $(n, e)$ , kur  $n = p \cdot q$  ir reizinājums diviem mazākajiem 17-ciparu pirmskaitļiem (un  $p < q$ ), bet kā publisko kāpinātāju viņš grib izvēlēties skaitli  $e = 2^{16} + 1$ .

- Kādi ir pirmskaitļi  $p$  un  $q$  un to reizinājums  $n$ ? (Lielu pirmskaitļu pārbaudīšanai var izmantot esošas bibliotēkas, kas implementē Rabina-Millera varbūtisko pirmskaitļu pārbaudi, piemēram Python funkciju `sympy.isprime`.)
- Alise grib nosūtīt ziņojumu  $m = 100$ , izmantojot publisko RSA kriptatslēgu - pāri  $(n, e)$ . Kāds ir viņas iešifrētais ziņojums?
- Cik reizināšanas darbības pēc  $n$  moduļa Alisei jāveic, lai iešifrētu  $m$ ?
- Kāda ir Boba izmantotā privātā kriptatslēga  $d$ , kurai ir spēkā  $e \cdot d \equiv 1$  pēc  $\varphi(n)$  moduļa?
- Cik reizināšanas darbības pēc  $n$  moduļa Bobam jāveic, lai atšifrētu Alises iešifrēto ziņojumu?

**2.uzdevums: Afīnās mērogošanas metode LP uzdevumā.** Dots LP uzdevums: Maksimizēt  $2x_1 + 3x_2$ , kur

$$\begin{cases} x_1 - 2x_2 \leq 4, \\ x_1 + x_2 \leq 18, \\ x_2 \leq 10, \\ x_1, x_2 \geq 0. \end{cases}$$

Aprēķināt un attēlot koordinātu plaknē šī LP uzdevuma pirmos 2 tuvinājumus  $X(1)$  un  $X(2)$  kā 2-dimensionālus vektorus, izmantojot afīnās skalēšanas metodi.

Izvēlētais sākumpunkts  $X(0) = (5, 5)$  (t.i. sākumpunkta koordinātes ir  $x_1 = 5$  un  $x_2 = 5$ ). Gan  $X(1)$ , gan  $X(2)$  abas koordinātes atbildē noapaļot līdz 5 cipariem aiz komata. Soļa garums abos gadījumos:  $\beta = 0.96$ . (Vektoru un matricu operācijām var izmantot Python bibliotēkas.)

**3.uzdevums: KMP un BM algoritmi.** Virknē 947892879487 meklējam apakšstringu 9487.

- Atrast Knuta-Morisa-Prata algoritmam vajadzīgo prefiksu funkciju  $\pi$ .
- Atrast Bojera-Mūra algoritmam vajadzīgo labo sufiksu tabulu un sliktā simbola tabulu.

**4.uzdevums: Bojera-Mūra algoritms.** Dots teksts  $T = \text{abcabbcabcbcababababcbcab}$  un meklējamais paraugs  $P = \text{abcbcab}$ .

- Uzrakstīt Bojera-Mūra algoritmā lietotās tabulas apakšstringam  $P$ .
- Nodemonstrēt Bojera-Mūra darbību pa soļiem, meklējot paraugu  $P$  dotajā tekstā  $T$ .

**5.uzdevums: I-iespēja (atzīmei 10).** Vispārināt Rabina-Karpa algoritmu, lai atrastu kvadrātveida paraugu  $m \times m$  divdimensionālā simbolu masīvā ar izmēru  $n \times n$ , kur  $n > m$ . (Meklējamo paraugu var bīdīt pa horizontāli un vertikāli, bet to nedrīkst pagriezt.)

- Aprakstīt algoritmu (ar skaidri definētiem soļiem), kas atrod visas parauga atrašanās vietas divdimensionālajā  $n \times n$  masīvā kā pozīciju pārus  $(s_x, s_y)$ , kur  $s_x$  ir nobīde pa horizontāli un  $s_y$  ir nobīde pa vertikāli.
- Pamatot, ka Jūsu algoritms atrod izvada visas vietas, kur paraugs atrodams.
- Atrast mazāko laika sarežģītību visu atrašanās vietu izvadei.