3. mājasdarbs

Lietišķie algoritmi, 2019.g. rudens
Termiņš: 2019-12-02

1.uzdevums: Polinomu "dalīšana stabiņā".

(a) Doti divi polinomi ar vienu reālu mainīgo $x \in \mathbf{R}$:

$$A(x) = 3x^2 + 4x + 3, \quad B(x) = 5x + 6.$$

Dalīt $A(x)$ ar $B(x)$ ar atlikumu. T.i. izteikt $A(x) = Q(x)B(x) + R(x)$, kur polinoma $R(x)$ pakāpe ir mazāka par $B(x)$ pakāpi.

(b) Dalīt $A(x) = 3x^2+4x+3$ ar $B(x) = 5x+6$ ar atlikumu, ja polinoma mainīgie, koeficienti un vērtības ir nevis reāli skaitļi, bet elementi no galīga Galuā lauka $GF(7)$. Arī šajā gadījumā jāizsaka $A(x) = Q(x)B(x) + R(x)$, kur arī $Q(x), R(x)$ ir polinomi ar koeficientiem, kas pieder atlikumu kopai $GL(7) = \{0, 1, 2, 3, 4, 5, 6\}$.

2.uzdevums: Galuā lauks $GF(2^4)$. Galuā lauku $GF(2^4)$ veido visi kubiskie polinomi $a_3t^3 + a_2t^2 + a_1t + a_0$, kuru koeficienti $a_i \in \{0, 1\}$; turklāt visu saskaitīšanas un reizināšanas darbību rezultātus vienkāršo, dalot ar nereducējamo veidotājpolinomu $t^4 + t + 1$ (un, ja nepieciešams, darbību gaitā aizstājot nepāra koeficientus a_i ar 1, bet pāru koeficientus ar 0). Definējam divus $GF(2^4)$ elementus:

$$\alpha = t^2 + t + 1, \quad \beta = t + 1.$$

Aprēķināt izteiksmes: **(a)** $\alpha + \beta$, **(b)** $\alpha - \beta$, **(c)** $\beta - \alpha$, **(d)** $\alpha \cdot \beta$, **(e)** α/β, **(f)** β/α **(g)** β^4.

3.uzdevums: Difī-Helmana diskrēto logaritmu uzdevums. Alise un Bobs nodarbojas ar Difī-Helmana atslēgu apmaiņu. Viņi publiskojuši pirmskaitli $p = 41$ un primitīvo sakni pēc p moduļa: $\alpha = 6$. Pēc tam Alise iedomājusies savu privāto atslēgu $a = 5$ un Bobs iedomājies savu privāto atslēgu $b = 12$.

(a) Kādu publisko atslēgu Alise sūta Bobam?

(b) Kādu publisko atslēgu Bobs sūta Alisei?

(c) Kāds pēc publisko atslēgu apmaiņas ir viņiem abiem vienlaikus zināmais *kopīgais noslēpums* ("common secret")?

(d) Zināms, ka Difī-Helmana diskrēto logaritmu uzdevumā jāizvēlas tāds α, kurš ir *primitīvā sakne* pēc p moduļa - citādi diskrēto logaritmu uzdevumam daudzi atrisinājumi neder (un tātad uzbrucējs var vieglāk atminēt privātās atslēgas). Kura ir mazākā iespējamā primitīvās saknes α vērtība, ja Alisei un Bobam vairs nepatīk $\alpha = 6$?

4.uzdevums: LP uzdevuma sastādīšana. Rūpnīcas ceham pēc plāna ik dienas jāizgatavo ne mazāk 8 krēsli, 4 soli, 2 galdi un 8 ķebļi (ražošanas plānu drīkst arī pārsniegt). Ceham pieejamas trīs veidu finiera loksnes A, B un C, kuru izmaksas ir attiecīgi \$8.50, \$9.75, \$9.08. Katru no loksnēm var vienā noteiktā veidā sagriezt gabalos, iegūstot pa druskai no visu četru mēbeļu daļām, kā parādīts tabulā. (Piemēram, tabulas kolonnā zem A ir skaitļi 1/16, 1/4, 1/20, 1/4. Tas nozīmē, ka, sagriežot loksni A gabaliņos, radīsies 1/16 no nepieciešamā vienam krēslam, 1/4 no nepieciešamā vienam solam, 1/20 no nepieciešamā vienam galdam un 1/4 no nepieciešamā vienam ķeblītim.)

Iznākums	**Loksne** A	**Loksne** B	**Loksne** C
Krēsli	1/16	1/14	1/18
Soli	1/4	1/4	1/6
Galdi	1/20	1/25	1/30
Ķebļi	1/4	1/3	1/6

(a) Sastādīt LP uzdevumu lineāru vienādību/nevienādību sistēmas veidā, izmantojot iespējami nelielu skaitu mainīgo $x_1, x_2, \ldots$. Katram mainīgajam uzrakstīt tā interpretāciju (ko tas saturīgi nozīmē šajā teksta uzdevumā).

(b) Pārveidot LP uzdevumu simpleksalgoritma standartformā. Cik tajā ir brīvo mainīgo, cik pamatmainīgo? (Nav nepieciešams šo LP uzdevumu risināt.)

(c) Uzrakstīt pirmajā punktā izveidotajam LP uzdevumam duālo uzdevumu, izmantojot mainīgos $y_1, y_2, \ldots$.

(d) Duālā LP uzdevuma mainīgajiem $y_1, y_2, \ldots$ formulējiet tā interpretāciju: ko tas saturīgi nozīmē teksta uzdevumā. Interpretācija, kas pasaka, ko vajag maksimizēt (vai minimizēt?) duālajā uzdevumā, reizēm sarežģīti izsakāma cilvēku valodā, bet šoreiz to jācenšas definēt.

5.uzdevums: Simpleksalgoritms. Dots LP uzdevums: Maksimizēt $2x_1 + 3x_2 + 4x_3$, kur

$$\begin{cases} 2x_1 + x_2 + 4x_3 \leq 100 \\ x_1 + 3x_2 + x_3 \leq 80 \\ x_1, x_2, x_3 \geq 0. \end{cases}$$

(a) Pārveidot šo LP uzdevumu simpleksalgoritma standartformā.

(b) Izveidot simpleksalgoritma sākotnējo tabulu; apzīmēt, kuri ir brīvie mainīgie, kuri - pamatmainīgie.

(c) Veikt simpleksalgoritma soļus.

(d) Uzrakstīt atrisinājumu formā $(x_1, x_2, x_3) = \ldots$ un atrast, kāda ir izteiksmes maksimālā vērtība.

(e) Uzrakstīt dotajam LP uzdevumam duālo uzdevumu.

6.uzdevums: I-iespēja (atzīmei 10). Apskatām uzdevumu par maksimālo sapārojumu. Šajā uzdevumā doti n cilvēki un n uzdevumi ar nosacījumiem, kuri cilvēki drīkst pildīt kurus uzdevumus. Jānosaka maksimālais uzdevumu skaits, ko var izpildīt vienlaikus, ja viens cilvēks drīkst pildīt ne vairāk kā vienu uzdevumu (un vienu uzdevumu drīkst pildīt ne vairāk kā viens cilvēks). Šo uzdevumu var modelēt ar lineāru programmu ar mainīgajiem x_{ij} katram i, j, kur i ir cilvēks, kas drīkst pildīt uzdevumu j:

$$\text{Maksimizēt} \quad \sum_{i,j=1}^{n} x_{ij}$$

ar nosacījumiem

$$\begin{array}{l} \sum\limits_{j=1}^{n} x_{ij} \leq 1 \ \text{ katram } \ i, \\ \sum\limits_{i=1}^{n} x_{ij} \leq 1 \ \text{ katram } \ j, \\ 0 \leq x_{ij}, \ \ x_{ij} \leq 1 \ \text{ katram } \ i, j. \end{array} .$$

(a) Pierādīt, ka šīs programmas maksimums reālos skaitļos sakrīt ar tās maksimumu veselos skaitļos (tas ir, katram atrisinājumam reālos skaitļos, kas sasniedz summu S, ir atrisinājums veselos skaitļos, kas sasniedz summu, kas ir vismaz S).

(b) Interpretēt (aprakstīt cilvēku valodā) šai problēmai duālajā uzdevumā minimizējamo izteiksmi un tās mainīgos.