

Valik ülesandeid aines “Sissejuhatus andmeturbesse”

2. aprill, 2004

1 Ülesanded

Ülesanne 1. Leia neljandat järku I-liiki nihkeregistrid (ja vastavad algolekud), mille väljundjadad (nullise sisendjada korral) sisaldavad lõike:

a) 1 0 0 1 1 0 1 0

b) 1 0 0 0 0 1 0 1.

Ülesanne 2. Kas leiduvad polünoomid $\alpha(x)$ ja $\beta(x)$ (üle \mathbb{Z}_2), nii et kehtiks (polünoomide) võrdus

$$\alpha(x) \cdot (x^2 + 1) + \beta(x) \cdot (x^5 + 1) = 1.$$

Ülesanne 3. Leia polünoom $a(x)$ (üle \mathbb{Z}_2), nii et

$$a(x) \cdot (x^2 + 1) \equiv 1 \pmod{x^4 + x + 1}.$$

$$a(x) \cdot (x^2 + 1) \equiv 1 \pmod{x^4 + x + 1}.$$

Ülesanne 4. Leia neljanda astme polünoom $f(x)$ (üle \mathbb{Z}_2), millel puuduvad juured hulgas \mathbb{Z}_2 ja mis on taanduv, s.t. leiduvad madalama astme mittekonstantsed polünoomid $f_1(x), f_2(x) \in \mathbb{Z}_2[x]$, nii et $f(x) = f_1(x) \cdot f_2(x)$.

Ülesanne 5. Olgu $\vartheta \in \mathbb{R}$ polünoomi $f(x) = x^3 + x + 1 \in \mathbb{R}[x]$ üks juurtest. Avalda kaks ülejäänud (kompleksarvulist) juurt ϑ kaudu.

2 Lahendused

Ülesanne 1. Analüüsid esimese nelja taktilise registreerimise käitumist esimese nelja taktilise registreerimise jooksul, saame juhul a), et algolek $S^0 = S_0^0 S_1^0 S_2^0 S_3^0$ oli 1 0 0 1. Ülejäänud kolm olekut S^1 , S^2 ja S^3 avalduvad järgmiselt:

$$S^1 = 0011, \quad S^2 = 0110, \quad S^3 = 1101.$$

Jada viimane bitt 0 vastab olekubitile S_0^4 . Kasutades esimest liiki nihkeregistrit iseloomustavat rekurrentset seost

$$S_0^{i+1} = r_0 S_3^i + r_1 S_2^i + r_2 S_1^i + r_3 S_0^i,$$

saame olemasolevate andmete põhjal ($i = 0 \dots 3$) järgmise võrrandisüsteemi:

$$\begin{aligned} 1r_0 + 0r_1 + 0r_2 + 1r_3 &= 1 \\ 0r_0 + 0r_1 + 1r_2 + 1r_3 &= 0 \\ 0r_0 + 1r_1 + 1r_2 + 0r_3 &= 1 \\ 1r_0 + 1r_1 + 0r_2 + 1r_3 &= 0, \end{aligned}$$

mida lehendades saame, et $r_0 = r_1 = 1$ ja $r_2 = r_3 = 0$.

Talitledes analoogiliselt juhul b), saame teiseks võrrandiks

$$0r_0 + 0r_1 + 0r_2 + 0r_3 = 1,$$

mis ei ole muidugi lahenduv. Seetõttu ei leidu ka vastava väljundjada lõiguga I-liiki nihkeregistrit.

Ülesanne 2. Nimetatud omadustega polünoome ei leidu, sest siis peaks polünoom $f(x) = \alpha(x) \cdot (x^2 + 1) + \beta(x) \cdot (x^5 + 1)$ võrduma konstantse polünoomiga 1, mistõttu peaks olema $f(0) = f(1) = 1$. Kontroll näitab aga, et

$$f(1) = \alpha(1) \cdot (1^2 + 1) + \beta(1) \cdot (1^5 + 1) = \alpha(1) \cdot 0 + \beta(1) \cdot 0 = 0 \neq 1.$$

Ülesanne 3. Et mooduli võtmine (antud juhul polünoomi $x^4 + x + 1$ järgi) säilitab polünoomide korrutamise, siis juhul kui kongruents

$$a(x) \cdot (x^2 + 1) \equiv 1 \pmod{x^4 + x + 1}.$$

on üldse lahenduv, peab leiduma ka lahend $a(x)$, mille aste ei ületa kolme, s.t. kui $A(x)$ on suvaline lahend, siis on lahend ka $a(x) = A(x) \bmod(x^4 + x + 1)$. Seega otsime lahendit kujul

$$a(x) = a_3x^3 + a_2x^2 + a_1x + a_0.$$

Arvutame kõigepealt $a(x) \cdot (x^2 + 1) \bmod(x^4 + x + 1)$. Kõigepealt leiame, et

$$x^2a(x) \bmod(x^4 + x + 1) = a_1x^3 + (a_0 + a_3)x^2 + (a_2 + a_3)x + a_2.$$

Seega taandub ülesanne järgmise polünoomide võrduse lahendamisele:

$$(a_1 + a_3)x^3 + (a_0 + a_2 + a_3)x^2 + (a_1 + a_2 + a_3)x + a_0 + a_2 = 1,$$

mis omakorda taandub võrrandisüsteemile (üle \mathbb{Z}_2):

$$\begin{aligned} 0 &= a_1 + a_3 \\ 0 &= a_0 + a_2 + a_3 \\ 0 &= a_1 + a_2 + a_3 \\ 1 &= a_0 + a_2. \end{aligned}$$

Lahendades saame, et $a_0 = a_1 = a_3 = 1$ ja $a_2 = 0$. Seega on otsitav polünoom $a(x) = x^3 + x + 1$, mille sobivust lahendina kinnitab ka otsene kontroll.

Ülesanne 4. Et igal lineaarpolünoomil $g(x) \in \mathbb{Z}_2[x]$ on juur korpuses $\mathbb{Z}_2 = \{0, 1\}$, siis lineaarpolünoomid teguriteks $f_1(x)$ ja $f_2(x)$ ei sobi. Jääb seega üle, et mõlemad $f(x)$ tegurid $f_1(x)$ ja $f_2(x)$ on ruutpolünoomid. Et polünoomil $f(x)$ ei tohtinud olla juurt hulgas \mathbb{Z}_2 , siis sellest järeldub, et mõlema teguri vabaliikmed on võrdsed 1-ga, kuna vastasel korral jaguks $f(x)$ lineaarpolünoomiga x ja omaks juurt $0 \in \mathbb{Z}_2$. Seega sobiksid teguriteks ainult polünoomid kujul:

$$x^2 + \varphi x + 1,$$

kus $\varphi \in \{0, 1\}$. Et aga $\varphi = 0$ ei sobi teguriteks lahtuse $x^2 + 1 = (x+1)(x+1)$ tõttu, siis ainus võimalus tegurina on polünoom $f_1(x) = f_2(x) = x^2 + x + 1$. Tõepoolest, sellel polünoomil puuduvad juured hulgas $\mathbb{Z}_2 = \{0, 1\}$, sest $f_1(1) = f_2(1) = 1$. Seega on sobilik neljanda astme polünoom

$$f(x) = (x^2 + x + 1)^2 = x^4 + x^2 + 1.$$

Ülesanne 5. Kui ϑ on polünoomi $f(x) = x^3 + x + 1$ juur, siis järelikult $f(x)$ jagub lineaarpolünoomiga $(x - \vartheta)$. Teostades otsese jagamistehte (arvestades seost $\vartheta^3 + \vartheta + 1$), saame et

$$x^3 + x + 1 = (x - \vartheta) \cdot (x^2 + \vartheta x + \vartheta^2 + 1).$$

Ülejäänud juured ϑ_1, ϑ_2 annab seega ruutvõrrandi

$$x^2 + \vartheta x + \vartheta^2 + 1 = 0$$

lahendamise, millest saame, et

$$\vartheta_{1,2} = -\frac{\vartheta}{2} \pm \sqrt{\frac{\vartheta^2}{4} - \vartheta^2 - 1}.$$