Diszkrét matematika 2 - Minta ZH2

2015 tavasz

Polinomok

1. (Többszörös gyökök) Keressük meg a következő polinom *többszörös* gyökeit: $f = x^5 - 5x^3 + 5x + 2 \in \mathbb{C}[x]$.

   Megoldás: Polinomok Alapjai Példatár (Láng Zsuzsa honlapján) 2.5-18 feladat.

2. (Testbővítések) Legyen $f = x^3 - 2x^2 + 2 \in \mathbb{Z}_3[x]$, és végezzük el a következő műveleteket $\mathbb{Z}_3[x]/(f)$-ben: x^{-1} és $x^{-3} \cdot (x^8 + 2x^2)$. Igaz-e hogy $\mathbb{Z}_3[x]/(f)$ test?

   Megoldás: $\mathbb{Z}_3[x]/(f)$ elemei a $\mathbb{Z}_3[x]$ maradékosztályok $\bmod f$, azaz olyan polinomok, hogy az együtthatókat $\bmod 3$ kell venni, így $f = x^3 + x^2 + 2$. Tehát $x^3 + x^2 + 2 \equiv 0 \pmod f$, ezért $x^3 \equiv 2x^2 + 1 \pmod f$. Tudjuk, hogy minden $\mathbb{Z}_3[x]/(f)$-beli osztály reprezentálható egy legfeljebb másodfokú polinommal, így x inverze is, azaz tegyük fel hogy $x^{-1} = Ax^2 + Bx + C$ és oldjuk meg a következő kongruenciát A, B és C-re:

$$\begin{aligned} x \cdot x^{-1} = x \cdot (Ax^2 + Bx + C) &\equiv 1 \pmod f \\ Ax^3 + Bx^2 + Cx &\equiv 1 \pmod f \\ A(2x^2 + 1) + Bx^2 + Cx &\equiv 1 \pmod f \\ (2A + B)x^2 + Cx + A &\equiv 1 \pmod f \end{aligned}$$

   Innen $A = 1$, $C = 0$ és $B = 1$ mivel $2A + B = 0$, és így $x^{-1} = x^2 + x$.

   Vegyük észre, hogy $x^{-3} \cdot (x^8 + 2x^2) = x^5 + 2x^{-1}$ és így:

$$\begin{aligned} x^{-3} \cdot (x^8 + 2x^2) &= (2x^2 + 1) \cdot x^2 + 2 \cdot (x^2 + x) \\ &= 2x^4 + x^2 - x^2 - x \\ &= 4x^3 + 2x - x \\ &= x^3 + x \\ &= 2x^2 + x + 1 \end{aligned}$$

3. (Polinomok $\mathbb{Z}$ és $\mathbb{Q}$ felett)

   (a) Keressük meg az $f = x^3 - 6x^2 + 15x - 14$ polinom racionális gyökeit.

   (b) Az $f = 20x^4 + 26x^3 + 65x^2 + 91$ polinomot bontsuk fel irreducibilis polinomok szorzatára $\mathbb{Z}$ és $\mathbb{Q}$ fölött.

   Megoldás: Polinomok Alapjai Példatár. (Láng Zsuzsa honlapján) 2.6-24 és 2.6-32 feladat.

4. (Lagrange interpoláció, titokmegosztás): Mi a konstans tagja a legfeljebb negyedfokú $f \in \mathbb{Z}_{13}[x]$ polinomnak, ha $\hat{f}(1) = 2$, $\hat{f}(2) = 3$, $\hat{f}(3) = 5$, és $\hat{f}(4) = 7$?

   Megoldás:

   - $l_1 = \frac{x-2}{1-2} \cdot \frac{x-3}{1-3} \cdot \frac{x-4}{1-4} = 2x^3 + 8x^2 + 4$
   - $l_2 = \frac{x-1}{2-1} \cdot \frac{x-3}{2-3} \cdot \frac{x-4}{2-4} = 7x^3 + 9x^2 + 3x + 7$
   - $l_3 = \frac{x-1}{3-1} \cdot \frac{x-2}{3-2} \cdot \frac{x-4}{3-4} = 6x^3 + 10x^2 + 6x + 4$
   - $l_4 = \frac{x-1}{4-1} \cdot \frac{x-2}{4-2} \cdot \frac{x-3}{4-3} = 11x^3 + 12x^2 + 4x + 12$

   Végül $f = 2 \cdot l_1 + 3 \cdot l_2 + 5 \cdot l_3 + 7 \cdot l_4 = 2x^3 + 9x^2 + 2x + 3$, azaz f konstans tagja 3.

   Megjegyzés: az "osztás" itt moduláris inverzzel való szorzást jelent.

Kódolás

5. (Huffmann kód) A gyakorlaton megoldott feladat, valahogy úgy hangzott, hogy adott a következő relatív gyakoriságok $0.34, 0.18, 0.17, 0.16, 0.15$. Konstruáljuk a megfelelő bináris Huffmann kódot és hasonlítsuk az átlagos szóhosszt az entrópiával.

6. (Lineáris kód):

   (a) Határozzuk meg egy a

$$G = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix} \in \mathbb{Z}_2$$

generátor mátrixhoz tartozó hibaellenőrző H mátrixot. Hány elemű a kód? Mi a kód távolsága, hibajelző és hibajavító képessége? Mi a `110` üzenet kódja? Mire fogjuk dekódolni a `1011100` kódszót?

Megoldás: Megengedett műveletek

- Sorcserék, melynek inverzét utólag végre kell hajtani H oszlopain.
- Oszlopműveletek.

Először végezzük el a $(4\,3\,2)$ sorcserét (4. sort a 3. helyére, 3. a 2. helyére és 2. a 4. helyére).

$$G_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

Az így kapott mátrix már $G_1 = \left(\begin{smallmatrix} \mathbb{I} \\ P \end{smallmatrix}\right)$ alakú, innen kiolvasható a hibaellenőrző $H_1 = \left(\begin{smallmatrix} -P & \mathbb{I} \end{smallmatrix}\right)$ mátrix (egyenlőre permutált oszlopokkal).

$$H_1 = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Majd végrehajtva H_1 oszlopain az G-n végrehajtott oszlopcsere inverzét, vagyis a $(2\,3\,4)$ permutációt, megkapjuk a G-hez tartozó

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Ha sorerével nem oldható meg a G ilyen előállítása, akkor oszlop műveletek is megengedettek, ld következő feladat.

A kód az 8 elemű, ugyan is $k = 3$ (az üzenetek hossza), $n = 7$ (az kódszavak hossza), $q = 2$ (az ábécé elemszáma), és a kódszavak száma mindig $q^k = 2^3 = 8$.

A kód távolság H oszlopaiból olvasható ki. H első három oszlopa független (a maradék 4 oszlop egységmátrixot alkot, így azok is függetlenek), de mondjuk az 1. a 3. az 5. oszlop összege már nulla, így ezek összefüggnek, azaz van három összefüggő oszlop, de kevesebb nincs így $d = 3$. Ebből közvetlenül adódik, hogy a kód pontosan $d - 1 = 2$ hibajelző és pontosan $\lfloor (d-1)/2 \rfloor = 1$ hiba javító.

Az $u = 110$ üzenet kódja $Gu = 1010101$. A $v = 1011100$ üzenetet le kell ellenőrizni, ha $Hv = 0$ akkor az üzenet első, harmadik és negyedik bitje (ebben a sorrendben) adja vissza az üzenetet. Viszont $s = Hv = 1011$ ami nem nulla. Ebben az esetben szindróma dekódolást alkalmazhatunk, azaz az $s = 1011$ a H mátrix 3. oszlopával egyezik meg, így a 3. bit sérült, azaz 1011100 helyett az 1001100 üzenet lett elküldve, melyből kiolvasva az első, harmadik és negyedik bitet megkapjuk az eredeti 101 üzenetet!

   (b) Határozzuk meg a

$$G = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

generátor mátrixhoz tartozó hibaellenőrző H mátrixot.

Megoldás: Hasonlóan mint az előző feladatnál végezzük el először a $(1\,3\,2\,4)$ permutációt G sorain:

$$G_1 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

Majd adjuk a második oszlophoz az elsőt.

$$G_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

Innen

$$H_2 = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

A sor permutációk $(4\,2\,3\,1)$ inverzét alkalmazva az oszlopokra kapjuk, hogy

$$H_1 = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Mivel a G_2 ellőállításához alkalmazott oszlop transzformáció miatt G_1 és G_2 által generált altér megegyezik, ezért $H_1 = H$ egy ellenőrző mátrixa G-nek.

Megjegyzés: most $d = 2$ ugyanis H 3. és 7. megegyezik, így összegük 0, azaz összefüggőek.