

Algebrai Kódelmélet

Tárgynév:	Algebrai kódelmélet				
Rövid név:	Algebrai kódelmélet		Kód:	GEMAN384M	
Angol név:	Algebraic Coding Theory				
Tanszék:	Analízis Tanszék				
Tárgyfelelős:	Rakaczki Csaba				
Előtanulmányok:	Lineáris Algebra, Diszkrét Matematika I, II		Kódja:	-	
Kredit:		Követelmény:	gyakorlati jegy		
Heti óraszámok:	Előadás:	2	Gyakorlat:	1	Labor: -
Oktatási cél:	A hibajavító kódolás alapjainak elsajátítása.				
Tárgy tartalom:	Matematikai háttér: Csoport, gyűrű, test, véges testek elemszáma, létezés és egyértelműség. véges testek konstrukciója, polinomok véges testek felett, számolás véges testekben. Vektortér, bázis, lineáris leképezések és mátrixuk. A kódolás alapfogalmai: zajos csatorna, bináris szimmetrikus csatorna; hibajelző, illetve hibajavító kód. Blokk-kódok. Hamming-távolság. Kód minimális távolsága, ennek kapcsolata a hibajavító képességgel. Korlátok a kódok hatásfokára: Singleton-korlát, Hamming-korlát. Bináris és nembináris Lineáris kódok , generátormátrix, paritás-ellenőrző mátrix. Hamming kódok. Ciklikus kódok, Polinomkódok. Generátorpolinom, ellenőrző polinom. Reed-Solomon-kódok, Perfekt kódok. Dekódolási algoritmusok, Kódkombinációk, Hibajavítás				
Irodalom:	Györfi László, Györi Sándor, Vajda István: Információ- és kódelmélet http://www.szt.bme.hu/~gyorfi/infkod.pdf Kiss Emil : Bevezetés az absztrakt algebrába (egyetemi tankönyv) http://people.inf.elte.hu/nebsabi/2011-2012-1/Algebra/Kiss%20Emil%20-%20Algebra.pdf Freud Róbert: Lináris Algebra Láng Csabáné: Testbővítés, véges testek, Hibajavító kódok http://compalg.inf.elte.hu/~zslang/TestbovitesVegestestekHibajavitokodokPeldatar.pdf Lakatos Piroska: Kódelmélet (egyetemi jegyzet) Horváth Gábor Véges testek http://math.unideb.hu/media/horvath-gabor/publications/VegesTestek.pdf Error-correcting codes and cryptology: http://www.win.tue.nl/~ruudp/courses/2WC11/2WC11-book.pdf				
Jellemző oktatási módok:					
Oktatási nyelv:	Magyar				
Előadás:	Minden hallgatónak előadás, tábla használatával				
Gyakorlat:	Minden hallgatónak előadás, tábla használatával				
Lezárási feltételek:	Az órákról való legfeljebb 3 hiányzás a félév során				

	A tárgy lezárásához a félév végén megírandó ZH-n megszerzett legalább elégséges gyakorlati jegy megszerzése szükséges. A ZH elméleti és gyakorlati feladatokból áll.
--	--

Ütemterv

- 1-3. hét **Matematikai háttér: Csoport, gyűrű, test, véges testek elemszáma, létezés és egyértelműség. véges testek konstrukciója. Polinomok véges testek felett, számolás véges testekben. Vektortér, bázis, lineáris leképezések és mátrixuk.**
4. hét **A kódolás alapfogalmai: zajos csatorna, bináris szimmetrikus csatorna; hibajelző, illetve hibajavító kód. Blokk-kódok. Hamming-távolság. Kód minimális távolsága, ennek kapcsolata a hibajavító képességgel.**
5. hét **Korlátok a kódok hatásfokára: Singleton-korlát, Hamming-korlát, feladatok**
6. hét **Lineáris kódok, generátormátrix, Duális kódok, paritás-ellenőrző mátrix.**
7. hét **Lineáris kódok kódolása. Lineáris kódok hibadetektálása, hibajavítása, Standard Elrendezési Tábla**
8. hét **Hamming-kódok. Hamming kódok hibajavító algoritmusai. Reed-Solomon kódok.**
- 9-10. hét **Ciklikus kódok és ideálokvaló kapcsolatuk, generátorpolinom, paritás-ellenőrző polinom.**
- 11-13. hét **Ciklikus kódok szisztematikus kódolása, ciklikus Reed-Solomon-kódok hibajelzése, hibajavítása, törléses hibák kezelése.**
14. hét **Kódkombinációk.**

Miskolc, 2018. február 13.

Dr. Rakaczki Csaba

- 1) Egy $\mathbb{Z}_7$ feletti C ciklikus Reed-Solomon kód generátorpolinomja $g(x) = (x-3)(x-2)$.
A csatornán keresztül érkezett vett jelből két karakter törlődött

$$\bar{v} = (6 \ * \ 5 \ 1 \ * \ 2).$$

Javítsuk ki a törléses hibákat a fenti kód felhasználásával! A javítás után kapott kódszóról ellenőrizzük le, hogy valóban kódszó! [16p]

- 2) Mondja ki a Hamming korlátot és bizonyítsa is be! [16p]
- 3) A tanult algoritmussal határozzon meg primitív elemet a $\mathbb{Z}_p$ testben, ha $p = 19$! Ellenőrzésként adja meg a test nullától különböző elemeit a keresett primitív elem hatványaiként! [16p]
- 4) Hogyan készítsünk egy Q véges test feletti $[n, k]$ paraméterű Reed-Solomon kódot? Adjuk meg egy ilyen kód egy generátormátrixát! [16p]
- 5) Egy $\mathbb{Z}_7$ feletti C lineáris kód egy generátormátrixa:

$$\begin{pmatrix} 1 & 3 & 2 & 6 & 4 & 5 \\ 1 & 2 & 4 & 1 & 2 & 4 \\ 1 & 6 & 1 & 6 & 1 & 6 \\ 1 & 4 & 2 & 1 & 4 & 2 \end{pmatrix}$$

Határozza meg a kód egy paritásmátrixát! Mennyi a kód Hamming-távolsága? [16p]

- 6) Egy $\mathbb{Z}_{19}$ feletti C ciklikus Reed-Solomon kód generátorpolinomja $g(x) = (x-4)(x-16)$.
A csatornán keresztül érkezett vett jel

$$\bar{v} = (13, 1, 2, 2, 8, 1, 0, 8, 0).$$

Történt-e hiba? Ha igen, akkor javítsuk a fenti kóddal! Mi volt a csatornán átküldött kódszó? [16p]

Értékelés: 0p-47p elégtelen; 48p-59p elégséges; 60p-71p közepes; 72p-84p jó; 85p-96p jeles

(1)

$$g(x) = x^2 - 5x + 6 = x^2 + 2x + 6$$

$$\alpha = 3$$

$$\alpha^2 = 2$$

$$\alpha^3 = 6$$

$$\alpha^4 = 4$$

$$\alpha^5 = 5$$

$$\alpha^6 = 1$$

$$\bar{r} = (6 \ a \ 5 \ 1 \ b \ 2)$$

$$\bar{r}(x) = 6 + ax + 5x^2 + x^3 + bx^4 + 2x^5 \quad (3)$$

$$\begin{aligned} \bar{r}(\alpha) &= 6 + 3a + 10 + 6 + 4b + 10 \\ &= 4 + 3a + 4b \end{aligned} \quad (2)$$

$$\bar{r}(\alpha^2) = 6 + 2a + 20 + 1 + 2b + 1 = 2a + 2b + 0 \quad (2)$$

$$2a + 2b = 0$$

$$3a + 4b = 3 \quad (2_1)$$

$$4a + 4b = 0$$

$$3a + 4b = 3$$

$$\boxed{a = 4} \quad (2_2)$$

$$\boxed{b = 3} \quad (2_3)$$

$$\bar{C} = (6 \ 4 \ 5 \ 1 \ 3 \ 2) \quad (1_1)$$

$$H = \begin{pmatrix} 1 & 3 & 2 & 6 & 4 & 5 \\ 1 & 2 & 4 & 1 & 2 & 4 \end{pmatrix} \quad (1)$$

$$\bar{C} H^T = (0 \ 0) \quad (2)$$

(2)

$$q^{n-2} \geq \sum_{i=0}^t \binom{n}{i} (q-1)^i \quad t \in \text{höchste Potenz}$$

(48)

! $\bar{c} \in C$

$$X_\epsilon(\bar{c}) = \{ \bar{x} \in \mathbb{Q}^n \mid d(\bar{x}, \bar{c}) \leq \epsilon \}$$

(20)

Hc $\bar{c}_1, \bar{c}_2 \in C \quad \bar{c}_1 \neq \bar{c}_2$ dann

$$X_\epsilon(\bar{c}_1) \cap X_\epsilon(\bar{c}_2) = \emptyset$$

(49)

$$\text{Daher wenn } d(\bar{x}, \bar{c}_1) \leq \epsilon \quad d(\bar{x}, \bar{c}_2) \leq \epsilon$$

$\downarrow$ C ist höchstens

$$|X_\epsilon(\bar{c})| = \binom{n}{0}(q-1)^0 + \binom{n}{1}(q-1)^1 + \binom{n}{2}(q-1)^2 + \dots + \binom{n}{t}(q-1)^t = \sum_{i=0}^t \binom{n}{i}(q-1)^i$$

$$|C| \leq q^n \quad \text{"ganzheit" von}$$

(21)

$$\text{d.h. } q^n \left(\sum_{i=0}^t \binom{n}{i} (q-1)^i \right) \leq q^n$$

$\downarrow$
ganzheit (21) $\mathbb{Q}$ d.h.

(3)

$$\mathbb{Z}_{18}$$

$$h = 18 = 2 \cdot 3^2 \quad (2r)$$

$$f_1(x) = x^9 - 1 \quad (2r)$$

$$-1 + 2^9 = 17$$

$$p_1 = 2 \quad (2r)$$

$$\alpha_1 = 2^9 = 18 \quad (1r)$$

$$f_2(x) = x^6 - 1 \quad (2r)$$

$$2^6 = 64 = 7$$

$$f_2(x) = 6$$

$$p_2 = 2 \quad (2r)$$

$$\alpha_2 = 2^2 = 4 \quad (1r)$$

$$\alpha = \alpha_1 \alpha_2 = 15 \quad (2r)$$

$$2 \quad 2^2 = 4 \quad 2^3 = 8 \quad 2^4 = 16$$

$$2^5 = 17 \quad 2^6 = 7 \quad 2^7 = 14 \quad 2^8 = 9$$

$$2^9 = 18$$

$$19, 38, 57, 76$$

$$\alpha = 15 = -4$$

$$\alpha^{10} = 4$$

$$\alpha^2 = 16 = -3$$

$$\alpha^4 = 3$$

$$\alpha^3 = 12 = -7$$

$$\alpha^{12} = 7$$

$$\alpha^4 = 9$$

$$\alpha^{13} = 10$$

$$\alpha^5 = 2$$

$$\alpha^{14} = 17$$

$$\alpha^6 = 11$$

$$\alpha^{15} = 8$$

$$\alpha^7 = 13$$

$$\alpha^{16} = 6$$

$$\alpha^8 = 5$$

$$\alpha^{17} = 14$$

$$\alpha^9 = 18$$

$$\alpha^{18} = 1$$

(2r)

(4)

$$! \quad |Q| = q \quad n \leq q$$

$\alpha_0, \alpha_1, \dots, \alpha_{n-1}$ ndb gewählt $\alpha_{n-1} \in Q$ (20)

$$\bar{u} = (u_0, u_1, \dots, u_{n-1}) \text{ so } \bar{u} \in K^n$$

$\downarrow$

$$\bar{u}(x) = u_0 + u_1 x + u_2 x^2 + \dots + u_{n-1} x^{n-1} \text{ Interpolation} \quad (41)$$

$$\bar{u} \rightarrow \bar{c} = (c_0, c_1, \dots, c_{n-1}) \text{ amix} \quad (42)$$

$$c_i = \bar{u}(d_i) \quad i = 0, \dots, n-1$$

$$G = \begin{pmatrix} 1 & 1 & \dots & 1 \\ d_0 & d_1 & \dots & d_{n-1} \\ d_0^2 & d_1^2 & \dots & d_{n-1}^2 \\ \vdots & \vdots & \ddots & \vdots \\ d_0^{n-1} & d_1^{n-1} & \dots & d_{n-1}^{n-1} \end{pmatrix} \quad (68)$$

5

	$\bar{g}_1$	$\bar{g}_2$	$\bar{g}_3$	$\bar{g}_4$	$\bar{g}_5$	$\bar{g}_6$
$\bar{e}_1$	<u>1</u>	3	2	6	4	5
$\bar{e}_2$	1	2	4	1	2	4
$\bar{e}_3$	1	6	1	6	1	6
$\bar{e}_4$	1	4	2	1	4	2

(2)

$\bar{g}_1$	1	3	2	6	4	5
$\bar{e}_1$	0	6	2	2	5	6
$\bar{e}_3$	0	3	6	0	4	1
$\bar{e}_4$	0	<u>1</u>	0	2	0	4

(2)

$\bar{g}_1$	1	0	2	0	4	0
$\bar{e}_1$	0	0	2	4	5	3
$\bar{e}_3$	0	0	6	<u>1</u>	4	3
$\bar{g}_2$	0	1	0	2	0	4

3

(2)

$\bar{g}_1$	1	0	2	0	4	0
$\bar{e}_1$	0	0	6	0	3	<u>5</u>
$\bar{g}_3$	0	0	6	1	4	3
$\bar{g}_2$	0	1	2	0	6	5

(2)

$\bar{g}_1$	1	0	2	0	4	0
$\bar{g}_6$	0	0	4	0	2	1
$\bar{g}_4$	0	0	1	1	5	0
$\bar{g}_2$	0	1	3	0	3	0

(1)

$\bar{g}_3$	0	0	6	0	0	0
$\bar{g}_5$	0	0	0	0	6	0

$\bar{g}_1 \bar{g}_2 \bar{g}_3 \bar{g}_4 \bar{g}_5 \bar{g}_6$

$\bar{g}_1$	1	0	2	0	4	0
$\bar{g}_2$	0	1	3	0	3	0
$\bar{g}_3$	0	0	6	0	0	0
$\bar{g}_4$	0	0	1	1	5	0
$\bar{g}_5$	0	0	0	0	6	0
$\bar{g}_6$	0	0	4	0	2	1

(1)

$$H = \begin{pmatrix} 2 & 3 & 6 & 1 & 0 & 4 \\ 4 & 3 & 0 & 5 & 6 & 2 \end{pmatrix}$$

(2)

nincs $\bar{e}$ $\rightarrow d(c) > 1$ (1)

egyetlen költségvetési c melyre $d(c) > 2$

$$\frac{1}{5} = 3$$

$$-\frac{2}{5} = -9 = 5$$

Sinfiter blik

(1)

$$n-2 < 1 \geq d(c) \quad (1)$$

$$3 \geq d(c) > 2$$

$$\Rightarrow d(c) = 3$$

(1)

⑥

$\mathbb{Z}_{15}$

$$g(x) = (x-4)(x-10)$$

$$\begin{array}{cccccc} h & h^2=16 & h^3=7 & h^4=9 & h^5=17 \\ h^6=11 & h^7=6 & h^8=5 & h^9=1 & \end{array}$$

$$\alpha = 4 \quad (18)$$

$$O(4) =$$

$$19, 38, 57, 76$$

$$N(x) = 13 + x + 2x^2 + 2x^3 + 8x^4 + x^5 + 8x^7 \quad (11)$$

$$N(4) = 13 + 4 + 6 + 14 + 15 + 17 + 10 = 10$$

$$N(h^2) = 13 + 16 + 18 + 22 + 40 + 4 + 3 = 2 \quad (21)$$

$$8 \cdot h^{14} = 8 \cdot h^5 = 8 \cdot (-1) = -8 = 7$$

$$\text{Total } h_i \quad (11)$$

$$\begin{aligned} (11) \quad N(\alpha) &= e_i \alpha^{i-1} \\ N(\alpha^2) &= e_i \alpha^{2(i-1)} \end{aligned}$$

$$\frac{N(\alpha^2)}{N(\alpha)} = \alpha^{i-1} \quad (11)$$

$$\frac{2}{10} = 4^{i-1} \quad (11)$$

$$\frac{2}{10} = \frac{15^5}{15^{15}} = \frac{1}{15^8} = \frac{1}{5} = \frac{15^{18}}{15^8} = 15^{10} = 4$$

$$4 = 4^{i-1} \quad (11)$$

$$i=2 \quad (11)$$

$$N(\alpha) = e_i \cdot \alpha^{i-1} = e_i \cdot \alpha$$

$$10 = e_i \cdot 4 \quad (11)$$

$$e_i = \frac{10}{4} = 10 \cdot 5 = 50 = 12$$

$$(11)$$

$$\bar{C} = \bar{r} - \bar{e} = (13 \ 1 \ 2 \ 2 \ 8 \ 1 \ 0 \ 8 \ 0) - (0 \ 12 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0)$$

$$\bar{C} = (13 \ 8 \ 2 \ 2 \ 8 \ 1 \ 0 \ 8 \ 0) \quad (11)$$