UNIVERZA NA PRIMORSKEM
FAKULTETA ZA MATEMATIKO, NARAVOSLOVJE IN INFORMACIJSKE TEHNOLOGIJE KOPER
MATEMATIČNE ZNANOSTI, MAGISTRSKI ŠTUDIJSKI PROGRAM 2. STOPNJE

Aljaž Slivnik

Kode za popravljanje napak

Magistrska naloga

Mentor: doc. dr. Štefko Miklavič

Tržič, maj 2010

Ključna dokumentacijska informacija

Ime in priimek:	Aljaž Slivnik				
Naslov magistrske naloge:	Kode za popravljanje napak				
Kraj:	Tržič				
Leto:	2010				
Število listov:	63	Število slik:	1	Število tabel:	0
Število prilog:	0	Št. strani prilog:	0		
Število referenc:	5				
Mentor:	doc. dr. Štefko Miklavič				
UDK:	519.725(043.2)				
Ključne besede:	končni obseg, vektorski prostor, linearna koda, generatorska matrika, kontrolna matrika, ciklična koda, Reed-Solomonova koda				
Math. Subj. Class. (2000):	94B05, 94B15				

Izvleček

Informacijo lahko posredujemo na več načinov. Oblika same informacije je stvar dogovora med prejemnikom in pošiljateljem. Težava nastane, ko želimo poslati informacijo po komunikacijski poti, ki ni pod našim nadzorom in vsebuje veliko šumov. V tej magistrski nalogi so predstavljene tri linearne kode za popravljanje napak v komunikaciji:

- Hammingove kode,
- ciklične kode,
- Reed–Solomonove kode.

Key words documentation

Name and surname:	Aljaž Slivnik				
Title of Master's degree:	Kode za popravljanje napak				
Place:	Tržič				
Year:	2010				
Number of pages:	63	Number of figures:	1	Number of tables:	0
Number of additions:	0	Number of addition pages:	0		
Number of references:	5				
Mentor:	doc. dr. Štefko Miklavič				
UDK:	519.725(043.2)				
Key words:	finite fields, vector space, linear code, generator matrix, parity-check matrix, cyclic code, Reed-Solomon code				
Math. Subj. Class. (2000):	94B05, 94B15				

Abstract

We can provide information in many ways. Form of information is an agreement between sender and receiver. Problem appears when we want to send information over the communication channel with a lot of noise which is not under our control. In this work three linear codes for error correction over noise channel are presented:

- Hamming codes,
- Cyclic codes,
- Reed–Solomon codes.

Kazalo vsebine

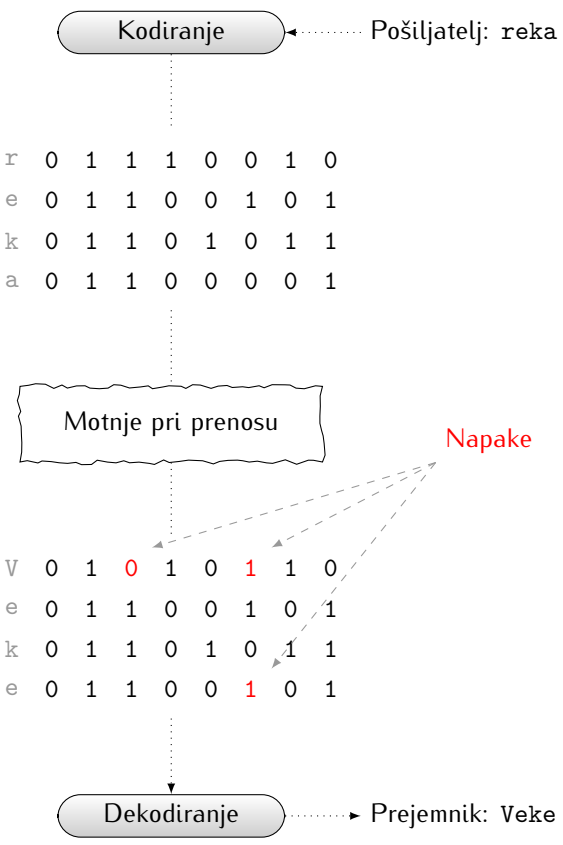
Kazalo slik

Poglavje 1

Uvod

Informacijo lahko posredujemo na več načinov. Oblika same informacije je stvar dogovora med prejemnikom in pošiljateljem. Do težave pa lahko pride, ko želimo poslati informacijo po komunikacijski poti, ki ni pod našim nadzorom.

To lahko prikažemo s primerom preproste otroške igre: Otroci sedijo v vrsti in so tiho. Prvi šepetaje pove besedo sosedu na uho. Ta pove naslednjemu in tako do konca. Zadnji pove na glas, kar je slišal. Najpogosteje je ta beseda na koncu popačena. Opisana otroška igra povzroči veliko zabave udeležencem.



Slika 1.1: Primer napake pri komunikaciji.

Toda predstavljajmo si sledečo, bolj resno situacijo. Dve angleški vojaški četi se odločita za sočasni napad s pomočjo odštevanja. Dogovorita se, da bo prva četa odštevanje prenašala preko radijskih valov, druga četa pa bo čakala na ukaz za napad. Sredi odštevanja druga četa začne izvajati napad. Po končanem spopadu z nasprotniki so se sestali poveljniki in so razglabljali, zakaj je druga četa predčasno napadla cilj. Prišli so do ugotovitve, da zaradi šumov v komunikaciji.

Besedi "five" (ang. pet) in "fire" (ang. streljaj) zvenita namreč zelo podobno. Zato so se odločili, da bodo od tistega trenutka naprej pri odštevanju izpustili število pet.

Podoben primer je prikazan tudi na sliki 1.1, kjer hoče Janez sporočiti Marjanu geslo "reka" v elektronski obliki. Janez pretvori geslo v dvojiški zapis in pošlje sporočilo. Zaradi kratkega stika v povezavi so se trije biti spremenili (iz 0 v 1 oziroma iz 1 v 0). Ko je spremenjeno/pokvarjeno sporočilo prišlo do Marjana, ga je ta pretvoril nazaj v napačno besedo, in sicer v "Veke". Ko je Marjan ugotovil, da je prišlo do napake, je Janeza prosil, naj mu še enkrat pošlje geslo.

Izpuščanje določenih besed oziroma nenehno ponavljanje le-teh ni najboljša rešitev. Zato se v takih primerih postavlja vprašanje: Ali je možna izmenjava sporočil po komunikacijski poti, ki vsebuje šum? Ena od rešitev je, da v izvirnem sporočilu vsak znak še dvakrat ponovimo; tako bi pri dekodiranju prejetega sporočila na vsake tri znake pogledali, kateri znak se največkrat pojavlja. S tem bi z veliko verjetnostjo ugotovili pravilni znak. Slabost tega načina ("napihovanja") je, da bi se velikost poslanega sporočila potrojila. Toda, ali obstaja način prenosa podatkov, ki bi s samo nekaj dodatnimi znaki omogočil normalno komuniciranje, ne da bi pri tem "prenapihnili" izvirno sporočilo?

Leta 1948 je C. Shannon dokazal obstoj takih kod, ki bi pod določenimi pogoji omogočale prenos podatkov brez napak in bi imele praktično uporabnost. Leta 1950 je R. W. Hamming (1915–1998) predstavil prvo uporabno kodo, ki je temeljila na linearni algebri. Seveda je splošna "evforija" povzročilo množično iskanje tehnik, s katerimi bi čim bolj učinkovito rešili problem odpravljanja napak pri prenosu podatkov.

Členjenost magistrske naloge

V prvem poglavju so postavljeni temelji za kasnejšo predstavitev kod. Poglavje vsebuje osnovne definicije teorije obsegov in vektorskih prostorov. Pri opisovanju obsegov je še posebej izpostavljen kolobar ostankov celih števil.

V drugem poglavju so najprej definirani osnovni pojmi teorije kodiranja. Nato so opisane linearne kode ter teža kodne besede. Sledi opis Hammingove razdalje in minimalne razdalje. S temi osnovami predstavimo generatorsko matriko ter definiramo, kdaj sta dve kodi ekvivalentni. Na koncu poglavja je definirana kontrolna matrika.

Proces kodiranja in dekodiranja ter definicija sindroma so opisani v tretjem poglavju.

V četrtem poglavju so predstavljene ciklične kode. Najprej so definirane same ciklične kode. Sledi opis postopka, kako s pomočjo generatorskega polinoma dobimo množico kodnih besed dane ciklične kode. Poglavje je zaključeno z opisom generatorske in kontrolne matrike.

V zadnjem poglavju so predstavljene Reed-Solomonove kode. Po definiciji Reed-Solomonovih kod

sledi dokaz trditve, da so Reed-Solomonove kode poseben razred linearnih kod.

Poglavje 2

Obsegi in vektorski prostori

Najprej bomo spoznali osnove algebraičnih struktur na dani množici. Te so podane z eno ali dvema binarnima operacijama, ki paru elementov dane množice priredi nek drugi element te iste množice. Nato bomo spoznali osnovne pojme teorije vektorskih prostorov, ki so potrebni za nadaljne delo.

2.1 Komutativni kolobar in obseg

Definicija 2.1 (Operacija). *Binarna operacija na množici G je preslikava*

$$\bigcirc : G \times G \to G.$$

Definicija 2.2 (Grupa). *Množica G z binarno operacijo $\bigcirc$ je grupa $(G, \bigcirc)$ natanko takrat, ko velja:*

- *asociativnost: $a \bigcirc (b \bigcirc c) = (a \bigcirc b) \bigcirc c$ za poljubne $a, b, c \in G$.*
- *nevtralni element: Obstaja tak element $e \in G$, za katerega velja*

  $$e \bigcirc a = a \bigcirc e = a$$

  za vsak $a \in G$. Elementu e pravimo nevtralni element grupe $(G, \bigcirc)$.
- *inverzni element: Za vsak $a \in G$ obstaja tak element $a' \in G$, da je*

  $$a \bigcirc a' = a' \bigcirc a = e.$$

  Elementu a' pravimo inverz elementa a.

Če je grupa $(G, \bigcirc)$ *komutativna, torej če velja*

$$a \bigcirc b = b \bigcirc a$$

za poljubna $a, b \in G$*, potem taki grupi rečemo Abelova grupa.*

Definicija 2.3 (Komutativni kolobar). *Naj bo množica* G *množica z dvema binarnima operacijama, in sicer* $\oplus : G \times G \to G$ *in* $\otimes : G \times G \to G$*.*
Trojica $(G, \oplus, \otimes)$ *je kolobar natanko takrat, ko veljajo naslednje lastnosti:*

- $(G, \oplus)$ *je Abelova grupa,*
- $\otimes$ *je asociativna operacija,*
- *binarni operaciji* $\oplus$ *in* $\otimes$ *povezuje zakon distributivnosti*

$$a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$$

za poljubne $a, b, c \in G$*.*

Če je $\otimes$ *komutativna operacija, torej, če velja*

$$a \otimes b = b \otimes a, \text{ kjer sta } a, b \in G,$$

potem je G *komutativni kolobar.*

Definicija 2.4 (Obseg). *Naj bo množica* G *množica z dvema binarnima operacijama, in sicer* $\oplus : G \times G \to G$ *in* $\otimes : G \times G \to G$*. Trojica* $(G, \oplus, \otimes)$ *je obseg natanko takrat, ko veljajo naslednje lastnosti:*

- $(G, \oplus)$ *je Abelova grupa (z enoto* e*),*
- $(G \setminus \{e\}, \otimes)$ *je grupa,*
- *binarni operaciji* $\oplus$ *in* $\otimes$ *povezuje zakon distributivnosti*

$$a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$$

za poljubne $a, b, c \in G$*.*

Primer 2.1 Naj bo $\mathbb{C} = \left\{a + bi; a, b \in \mathbb{R}, i^2 = -1\right\}$ množica vseh kompleksnih števil. Operaciji $\oplus$ in $\otimes$ na $\mathbb{C}$ lahko definiramo s predpisoma:

$$\begin{aligned}(a + bi) \oplus (c + di) &= (a + c) + (b + d)i \\ (a + bi) \otimes (c + di) &= (ac - bd) + (ad + bc)i\end{aligned}$$

za poljubne $a, b, c, d \in \mathbb{R}$. Množica $\mathbb{C}$ je za tako definirani binarni operaciji obseg.

Najprej pokažimo, da je $(\mathbb{C}, \oplus)$ abelova grupa:

- asociativnost: za poljubna kompleksna števila $c_1, c_2, c_3 \in \mathbb{C}$ pokažemo, da velja

$$(c_1 + c_2) + c_3 = c_1 + (c_2 + c_3)\,.$$

  Če zapišemo vsako kompleksno število c_j kot $a_j + b_j i$, potem je

$$\begin{aligned}(c_1 \oplus c_2) \oplus c_3 &= ((a_1 + b_1 i) \oplus (a_2 + b_2 i)) \oplus (a_3 + b_3 i) \\ &= ((a_1 + a_2) + (b_1 + b_2)\, i) \oplus (a_3 + b_3 i) \\ &= ((a_1 + a_2) + a_3) + ((b_1 + b_2) + b_3)\, i \\ &= (a_1 + (a_2 + a_3)) + (b_1 + (b_2 + b_3))\, i \\ &= (a_1 + b_1 i) \oplus ((a_2 + a_3) + (b_2 + b_3)\, i) \\ &= (a_1 + b_1 i) \oplus ((a_2 + b_2 i) \oplus (a_3 + b_3 i)) \\ &= c_1 \oplus (c_2 \oplus c_3)\,.\end{aligned}$$

- komutativnost: za poljubni kompleksni števili $c_1, c_2 \in \mathbb{C}$ velja

$$c_1 \oplus c_2 = c_2 \oplus c_1.$$

  Če zapišemo vsako kompleksno število c_j kot $a_j + b_j i$, potem je

$$\begin{aligned}c_1 \oplus c_2 &= (a_1 + b_1 i) \oplus (a_2 + b_2 i) \\ &= (a_1 + a_2) + (b_1 + b_2)\, i \\ &= (a_2 + a_1) + (b_2 + b_1)\, i \\ &= (a_2 + b_2 i) \oplus (a_1 + b_1 i) \\ &= c_2 \oplus c_1.\end{aligned}$$

- nevtralni element: nevtralni element za operacijo $\oplus$ je $e_s = 0 + 0i$. Pokazati moramo, da velja

$$c \oplus e_s = c.$$

  Torej, če je $c = a + bi$, potem je

$$\begin{aligned} c \oplus e_s &= (a + bi) \oplus (0 + 0i) \\ &= (a + 0) + (b + 0)\, i \\ &= (a) + (b)\, i \\ &= a + bi \\ &= c. \end{aligned}$$

- inverzni element: za poljubni element $c \in \mathbb{C}$ obstaja tak element $c_s \in \mathbb{C}$, da velja

$$c \oplus c_s = e_s.$$

  Če je $c = a + bi$, potem je inverz enak $c_s = (-a) + (-b)i$. Torej

$$\begin{aligned} c \oplus c_s &= (a + bi) \oplus ((-a) + (-b)i) \\ &= (a + (-a)) + (b + (-b))\, i \\ &= (0) + (0)\, i \\ &= 0 + 0i \\ &= e_s. \end{aligned}$$

Nato pokažemo, da za operacijo $\otimes$ velja:

- komutativnost: za poljubni kompleksni števili c_1, c_2 velja

$$c_1 \otimes c_2 = c_2 \otimes c_1.$$

Če zapišemo vsako kompleksno število c_j kot $a_j + b_j i$, potem je

$$\begin{aligned} c_1 \otimes c_2 &= (a_1 + b_1 i) \otimes (a_2 + b_2 i) \\ &= (a_1 a_2 - b_1 b_2) + (a_1 b_2 + b_1 a_2)\, i \\ &= (a_2 a_1 - b_2 b_1) + (a_2 b_1 + b_2 a_1)\, i \\ &= (a_2 + b_2 i) \otimes (a_1 + b_1 i) \\ &= c_2 \otimes c_1. \end{aligned}$$

- asociativnost: za poljubna kompleksna števila $c_1, c_2, c_3 \in \mathbb{C}$ velja

$$(c_1 \otimes c_2) \otimes c_3 = c_1 \otimes (c_2 \otimes c_3).$$

Če zapišemo vsako kompleksno število c_j kot $a_j + b_j i$, potem je

$$\begin{aligned} (c_1 \otimes c_2) \otimes c_3 &= ((a_1 + b_1 i) \otimes (a_2 + b_2 i)) \otimes (a_3 + b_3 i) \\ &= ((a_1 a_2 - b_1 b_2) + (a_1 b_2 + b_1 a_2)\, i) \otimes (a_3 + b_3 i) \\ &= ((a_1 a_2 - b_1 b_2)\, a_3 - (a_1 b_2 + b_1 a_2)\, b_3) \\ &\quad + ((a_1 a_2 - b_1 b_2)\, b_3 + (a_1 b_2 + b_1 a_2)\, a_3)\, i \\ &= ((a_1 a_2 a_3 - b_1 b_2 a_3) - (a_1 b_2 b_3 + b_1 a_2 b_3)) \\ &\quad + ((a_1 a_2 b_3 - b_1 b_2 b_3) + (a_1 b_2 a_3 + b_1 a_2 a_3))\, i \\ &= (a_1 a_2 a_3 - b_1 b_2 a_3 - a_1 b_2 b_3 - b_1 a_2 b_3) \\ &\quad + (a_1 a_2 b_3 - b_1 b_2 b_3 + a_1 b_2 a_3 + b_1 a_2 a_3)\, i \\ &= (a_1 a_2 a_3 - a_1 b_2 b_3 - b_1 b_2 a_3 - b_1 a_2 b_3) \\ &\quad + (b_1 a_2 a_3 - b_1 b_2 b_3 + a_1 a_2 b_3 + a_1 b_2 a_3)\, i \\ &= (a_1\, (a_2 a_3 - b_2 b_3) - b_1\, (b_2 a_3 + a_2 b_3)) \\ &\quad + (b_1\, (a_2 a_3 - b_2 b_3) + a_1\, (a_2 b_3 + b_2 a_3))\, i \\ &= (a_1 + b_1 i) \otimes ((a_2 a_3 - b_2 b_3) + (a_2 b_3 + b_2 a_3)\, i) \\ &= (a_1 + b_1 i) \otimes ((a_2 + b_2 i) \otimes (a_3 + b_3 i)) \\ &= c_1 \otimes (c_2 \otimes c_3)\,. \end{aligned}$$

- nevtralni element: nevtralni element za operacijo $\otimes$ je $e_m = 1 + 0i$ in velja

$$c \otimes e_m = c$$

za vsak $c \in \mathbb{C}$. Torej, če je $c = a + bi$, potem je

$$\begin{aligned} c \otimes e_m &= (a + bi) \otimes (1 + 0i) \\ &= (a1 + b0) + (a0 + b1)\, i \\ &= (a) + (b)\, i \\ &= a + bi \\ &= c. \end{aligned}$$

- distributivnost: za poljubna kompleksna števila c_1, c_2, c_3 velja

$$(c_1 \oplus c_2) \otimes c_3 = (c_1 \otimes c_3) \oplus (c_2 \otimes c_3)\,.$$

Če zapišemo vsako kompleksno število c_j kot $a_j + b_j i$, potem je

$$\begin{aligned} (c_1 \oplus c_2) \otimes c_3 &= ((a_1 + b_1 i) \oplus (a_2 + b_2 i)) \otimes (a_3 + b_3 i) \\ &= ((a_1 + a_2) + (b_1 + b_2)\, i) \otimes (a_3 + b_3 i) \\ &= ((a_1 + a_2)\, a_3 - (b_1 + b_2)\, b_3) \\ &\quad + ((a_1 + a_2)\, b_3 + (b_1 + b_2)\, a_3)\, i \\ &= ((a_1 a_3 + a_2 a_3) - (b_1 b_3 + b_2 b_3)) \\ &\quad + ((a_1 b_3 + a_2 b_3) + (b_1 a_3 + b_2 a_3))\, i \\ &= (a_1 a_3 + a_2 a_3 - b_1 b_3 - b_2 b_3) \\ &\quad + (a_1 b_3 i + a_2 b_3 i + b_1 a_3 i + b_2 a_3 i) \\ &= a_1 a_3 + a_2 a_3 - b_1 b_3 - b_2 b_3 \\ &\quad + a_1 b_3 i + a_2 b_3 i + b_1 a_3 i + b_2 a_3 i \\ &= a_1 a_3 - b_1 b_3 + a_1 b_3 i + a_3 b_1 i \\ &\quad + a_2 a_3 - b_2 b_3 + a_2 b_3 i + a_3 b_2 i \\ &= ((a_1 a_3 - b_1 b_3) + (a_1 b_3 i + a_3 b_1 i)) \\ &\quad + ((a_2 a_3 - b_2 b_3) + (a_2 b_3 i + a_3 b_2 i)) \\ &= ((a_1 a_3 - b_1 b_3) + (a_1 b_3 + a_3 b_1)\, i) \\ &\quad \oplus ((a_2 a_3 - b_2 b_3) + (a_2 b_3 + a_3 b_2)\, i) \\ &= ((a_1 + b_1 i) \otimes (a_3 + b_3 i)) \oplus ((a_2 + b_2 i) \otimes (a_3 + b_3 i)) \\ &= (c_1 \otimes c_3) \oplus (c_2 \otimes c_3)\,. \end{aligned}$$

- inverzni element: za poljubni element $c \in \mathbb{C} \setminus \{e_s\}$ obstaja tak element $c_m \in \mathbb{C}$, da velja

$$c \otimes c_m = e_m.$$

Če je $c = a + bi$, potem je inverz enak $c_m = \frac{a}{a^2+b^2} + \frac{b}{a^2+b^2} i$ pri pogoju $a^2 + b^2 \neq 0$. Torej

$$\begin{aligned}
c \otimes c_m &= (a + bi) \otimes \left(\tfrac{a}{a^2+b^2} + \tfrac{b}{a^2+b^2} i \right) \\
&= \left(a \tfrac{a}{a^2+b^2} + b \tfrac{b}{a^2+b^2} \right) + \left(a \tfrac{b}{a^2+b^2} - b \tfrac{a}{a^2+b^2} \right) i \\
&= \left(\tfrac{a^2}{a^2+b^2} + \tfrac{b^2}{a^2+b^2} \right) + \left(\tfrac{ab}{a^2+b^2} - \tfrac{ba}{a^2+b^2} \right) i \\
&= \left(\tfrac{a^2+b^2}{a^2+b^2} \right) + \left(\tfrac{ab}{a^2+b^2} - \tfrac{ab}{a^2+b^2} \right) i \\
&= (1) + (0)\, i \\
&= 1 + 0i \\
&= e_m.
\end{aligned}$$

Kolobar ostankov celih števil

Naj bo $z \in \mathbb{Z}$ in naj bo $n \in \mathbb{N}$, kjer je $n \geq 2$. Ostanek pri deljenju števila z s številom n bomo označevali z

$$z \mod n.$$

V množico

$$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$$

vpeljemo operaciji

$$i \oplus j = (i + j) \mod n$$

in

$$i \otimes j = (i \cdot j) \mod n.$$

Operaciji $+$ in $\cdot$ tukaj predstavljata običajno seštevanje in množenje.

Povedano drugače: Vsota $i \oplus j$ je enaka ostanku pri deljenju $i + j$ z n in produkt $i \otimes j$ je enak ostanku

pri deljenju $i \cdot j$ z n.

Primer 2.2 Množenje in seštevanje za $\mathbb{Z}_n$, kjer je $n = 2, 3, 4, 9$. Množenje in seštevanje za $\mathbb{Z}_2$:

$\oplus$	0	1
0	0	1
1	1	0

$\otimes$	0	1
0	0	0
1	0	1

Množenje in seštevanje za $\mathbb{Z}_3$:

$\oplus$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\otimes$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Množenje in seštevanje za $\mathbb{Z}_4$:

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\otimes$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Množenje in seštevanje za $\mathbb{Z}_9$:

$\oplus$	0	1	2	3	4	5	6	7	8
0	0	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8	0
2	2	3	4	5	6	7	8	0	1
3	3	4	5	6	7	8	0	1	2
4	4	5	6	7	8	0	1	2	3
5	5	6	7	8	0	1	2	3	4
6	6	7	8	0	1	2	3	4	5
7	7	8	0	1	2	3	4	5	6
8	8	0	1	2	3	4	5	6	7

$\otimes$	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8
2	0	2	4	6	8	1	3	5	7
3	0	3	6	0	3	6	0	3	6
4	0	4	8	3	7	2	6	1	5
5	0	5	1	6	2	7	3	8	4
6	0	6	3	0	6	3	0	6	3
7	0	7	5	3	1	8	6	4	2
8	0	8	7	6	5	4	3	2	1

Trditev 2.1. $(\mathbb{Z}_n, \oplus, \otimes)$ *je komutativni kolobar.*

Dokaz. Najprej pokažemo, da za $\oplus$ velja:

- asociativnost: Za poljubna števila $a, b, c \in \mathbb{Z}_n$ velja

$$\begin{aligned}
(a \oplus b) \oplus c &= ((a + b) \mod n) \oplus c \\
&= (((a + b) \mod n) + c) \mod n \\
&= ((a + b) + c) \mod n \\
&= (a + b + c) \mod n \\
&= (a + (b + c)) \mod n \\
&= (a + ((b + c) \mod n)) \mod n \\
&= a \oplus ((b + c) \mod n) \\
&= a \oplus (b \oplus c).
\end{aligned}$$

- komutativnost: Za poljubni števili $a, b \in \mathbb{Z}_n$ velja

$$\begin{aligned}
a \oplus b &= (a + b) \mod n \\
&= (b + a) \mod n \\
&= b \oplus a.
\end{aligned}$$

- nevtralni element: Nevtralni element za seštevanje je 0.

- inverzni element: Inverzni element za število $a \in \mathbb{Z}_n$ je $n - a \in \mathbb{Z}_n$.

Nato pokažemo še za $\otimes$:

- asociativnost: Za poljubna števila $a, b, c \in \mathbb{Z}_n$ velja asociativnost.

$$\begin{aligned}
(a \otimes b) \otimes c &= ((a \cdot b) \mod n) \otimes c \\
&= (((a \cdot b) \mod n) \cdot c) \mod n \\
&= ((a \cdot b) \cdot c) \mod n \\
&= (a \cdot b \cdot c) \mod n \\
&= (a \cdot (b \cdot c)) \mod n \\
&= (a \cdot ((b \cdot c) \mod n)) \mod n \\
&= a \otimes ((b \cdot c) \mod n) \\
&= a \otimes (b \otimes c)
\end{aligned}$$

- komutativnost: Za poljubni števili $a, b \in \mathbb{Z}_n$ velja komutativnost.

$$\begin{aligned} a \otimes b &= (a \cdot b) \mod n \\ &= (b \cdot a) \mod n \\ &= b \otimes a \end{aligned}$$

- distributivnost: Za poljubna števila $a, b, c \in \mathbb{Z}_n$ velja distributivnost.

$$\begin{aligned} (a \oplus b) \otimes c &= ((a \oplus b) \cdot c) \mod n \\ &= (((a + b) \mod n) \cdot c) \mod n \\ &= ((a + b) \cdot c) \mod n \\ &= ((a \cdot c) + (b \cdot c)) \mod n \\ &= (((a \cdot c) \mod n) + ((b \cdot c) \mod n)) \mod n \\ &= ((a \otimes c) + (b \otimes c)) \mod n \\ &= (a \otimes c) \oplus (b \otimes c) \end{aligned}$$

- nevtralni element: Enota za množenje je 1.

□

Trditev 2.2. *Kolobar $\mathbb{Z}_n$ je obseg natanko takrat, ko je n praštevilo.*

Dokaz. Če n ni praštevilo, potem je $n = q \otimes r$ za dve naravni števili q in r iz množice $\{2, 3, \ldots, n-1\}$. Zato je $q \otimes r = 0$ v $\mathbb{Z}_n$. Množenje v $\mathbb{Z}_n \backslash \{0\}$ ni notranja operacija in $\mathbb{Z}_n$ ni obseg.

Predpostavimo, da je n praštevilo. Izberemo $i \in \{2, 3, \ldots, n-1\}$ (1 ima inverz, namreč kar samega sebe). Ker je n praštevilo, sta števili i in n tuji. Zato obstajata taki celi števili p in q, da je $p \cdot n + q \cdot i = 1$. Pri tem lahko izberemo $1 \leq q \leq n-1$. Če to ne velja, q delimo z n in dobimo $q = sn + q'$, kjer je $1 \leq q' \leq n-1$. Potem je

$$(p + si)n + q' \cdot i = 1 \quad \text{in} \quad 1 \leq q' \leq n-1.$$

Privzemimo, da je $pn + qi = 1$ in $1 \leq q \leq n-1$. Potem v $\mathbb{Z}_n$ velja $q \cdot i = 1$ in q je inverz za i. Ker je i poljuben neničeln element, je $\mathbb{Z}_n$ obseg.

□

2.2 Vektorski prostor

Zaradi boljše preglednosti bomo znaka za operaciji $\otimes$ in $\oplus$ zamenjali z $\cdot$ in $+$.

Definicija 2.5 (Vektorski prostor). *Naj bo $\mathcal{O}$ komutativen obseg z enoto $e_{(\cdot)}$ za operacijo $\cdot$. Potem rečemo, da je množica V, na kateri sta dani operaciji $+ : V \times V \to V$ in $\cdot : \mathcal{O} \times V \to V$, vektorski prostor nad $\mathcal{O}$, če velja:*

- $(V, +)$ *je abelova grupa,*
- $(\alpha + \beta) \cdot v = \alpha \cdot v + \beta \cdot v$ *za vse* $\alpha, \beta \in \mathcal{O}$ *in za vse* $v \in V$,
- $\alpha \cdot (u + v) = \alpha \cdot u + \alpha \cdot v$ *za vse* $\alpha \in \mathcal{O}$ *in za vse* $v, u \in V$,
- $\alpha \cdot (\beta \cdot v) = (\alpha \cdot \beta) \cdot v$ *za vse* $\alpha, \beta \in \mathcal{O}$ *in za vse* $v \in V$,
- $e_{(\cdot)} \cdot v = v$ *za vse* $v \in V$.

Elementom iz vektorskega prostora V bomo običajno rekli vektorji, elementom iz obsega $\mathcal{O}$ pa skalarji. Operaciji $+ : V \times V \to V$ bomo rekli seštevanje vektorjev, operaciji $\cdot : \mathcal{O} \times V \to V$ pa množenje skalarja z vektorjem. Znaka $+$ in $\cdot$ bomo uporabili tudi za seštevanje/množenje skalarja s skalarjem oz. vektorja z vektorjem, zato mora biti bralec bolj pazljiv pri branju nadaljnjega besedila.

Definicija 2.6 (Vektorski podprostor). *Naj bo V vektorski prostor nad obsegom $\mathcal{O}$. Potem je podmnožica $U \subseteq V$ vektorski podprostor, če je zaprta za obe operaciji:*

- $u + v \in U$ *za poljubna* $u, v \in U$,
- $\alpha \cdot u \in U$ *za vse* $\alpha \in \mathcal{O}$ *in za vse* $u \in U$.

Za naše primere bomo uporabljali vektorje iz vektorskega prostora $\mathcal{O}^n$, kjer je $\mathcal{O}$ poljuben obseg in n neko naravno število. Vektorji iz vektorskega prostora $\mathcal{O}^n$ imajo obliko

$$\begin{bmatrix} o_1 & o_2 & \cdots & o_n \end{bmatrix} \text{ ali } \begin{bmatrix} o_1 \\ o_2 \\ \vdots \\ o_n \end{bmatrix},$$

kjer so $o_1, o_2, \ldots, o_n \in \mathcal{O}$. Seštevanje vektorjev bo definirano kot

$$\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} + \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} x_1 + y_1 \\ x_2 + y_2 \\ \vdots \\ x_n + y_n \end{bmatrix}$$

ter množenje skalarja z vektorjem kot

$$\alpha \cdot \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} \alpha \cdot x_1 \\ \alpha \cdot x_2 \\ \vdots \\ \alpha \cdot x_n \end{bmatrix}.$$

Primer 2.3 Naj bo $\mathbb{R}^2$ vektorski prostor. Za

$$U = \left\{ \begin{bmatrix} x \\ -x \end{bmatrix}, x \in \mathbb{R} \right\}$$

velja, da je vektorski podprostor vektorskega prostora $\mathbb{R}^2$. Kar pomeni, da za poljubna $\alpha, \beta \in \mathcal{O}$ in poljubna vektorja

$$\begin{bmatrix} x \\ -x \end{bmatrix}, \begin{bmatrix} y \\ -y \end{bmatrix} \in U$$

velja

$$\alpha \begin{bmatrix} x \\ -x \end{bmatrix} + \beta \begin{bmatrix} y \\ -y \end{bmatrix} = \begin{bmatrix} \alpha x \\ -\alpha x \end{bmatrix} + \begin{bmatrix} \beta y \\ -\beta y \end{bmatrix} = \begin{bmatrix} \alpha x + \beta y \\ -\alpha x - \beta y \end{bmatrix} \in U.$$

Definicija 2.7 (Linearna kombinacija vektorjev)**.** *Naj bo V vektorski prostor nad obsegom $\mathcal{O}$. Naj bodo $v_1, v_2, \ldots, v_k$ poljubni vektorji iz V in $\alpha_1, \alpha_2, \ldots, \alpha_k$ poljubni skalarji iz $\mathcal{O}$. Vsoto*

$$\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_k v_k = \sum_{i=1}^{k} \alpha_i v_i$$

imenujemo linearna kombinacija vektorjev $v_1, v_2, \ldots, v_k$.

Primer 2.4 Naj bo $\mathbb{R}^3$ vektorski prostor. Ali je vektor v_3 linearna kombinacija vektorjev v_2 in v_1, kjer so

$$v_3 = \begin{bmatrix} 2 \\ 0 \\ 1 \end{bmatrix}, v_2 = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}, v_1 = \begin{bmatrix} 0 \\ 2 \\ -1 \end{bmatrix}?$$

Poiskati moramo dva skalarja $\alpha, \beta \in \mathcal{O}$, da bo veljalo

$$\alpha \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 2 \\ -1 \end{bmatrix} = \begin{bmatrix} 2 \\ 0 \\ 1 \end{bmatrix}.$$

Na ta način dobimo sistem enačb

$$\begin{aligned} \alpha &= 2 \\ \alpha + 2\beta &= 0 \\ -\beta &= 1, \end{aligned}$$

kjer je rešitev $\alpha = 2$ in $\beta = -1$.

Primer 2.5 Naj bo $\mathbb{R}^3$ vektorski prostor. Vektor v_3 ni linearna kombinacija vektorjev v_2 in v_1, kjer so

$$v_3 = \begin{bmatrix} 2 \\ 0 \\ -1 \end{bmatrix}, v_2 = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}, v_1 = \begin{bmatrix} 0 \\ 2 \\ -1 \end{bmatrix},$$

saj sistem enačb

$$\begin{aligned} \alpha &= 2 \\ \alpha + 2\beta &= 0 \\ -\beta &= -1 \end{aligned}$$

nima rešitve.

Trditev 2.3. *Naj bodo vektorji $v_1, \ldots, v_k$ elementi vektorskega prostora V nad obsegom $\mathcal{O}$. Potem je množica vseh linearnih kombinacij vektorjev $v_1, \ldots, v_k$ vektorski podprostor v V.*

Dokaz. Naj bo V vektorski prostor na obsegom $\mathcal{O}$. Naj bosta $\sum_{i=1}^{k} \alpha_i v_i$ in $\sum_{i=1}^{k} \beta_i v_i$ dve linearni kombinaciji vektorjev $v_1, v_2, \ldots, v_k$ in γ, δ dva skalarja. Potem je

$$\gamma \left(\sum_{i=1}^{k} \alpha_i v_i \right) + \delta \left(\sum_{i=1}^{k} \beta_i v_i \right) = \sum_{i=1}^{k} (\gamma \alpha_i + \delta \beta_i) v_i$$

spet linearna kombinacija vektorjev $v_1, v_2, \ldots, v_k$. Zato je množica vseh linearnih kombinacij vektorski podprostor v V.

□

Definicija 2.8 (Linearna ogrinjača vektorjev). *Množico vseh linearnih kombinacij vektorjev $v_1, \ldots, v_k \in V$*

imenujemo linearna ogrinjača vektorjev $v_1, \ldots, v_k$. *Označimo jo z* $\mathscr{L}(v_1, \ldots, v_k)$.

Če je $\mathscr{M} = \{v_1, \ldots, v_k\}$ *neka končna podmnožica vektorjev iz* V, *potem z* $\mathscr{L}(\mathscr{M})$ *označimo linearno ogrinjačo* $\mathscr{L}(v_1, \ldots, v_k)$.

Definicija 2.9. *Naj bo* $\mathcal{O}$ *poljuben obseg. Potem z* $\mathcal{O}[x]$ *označimo množico vseh polinomov v spremenljivki* x *in s koeficienti iz obsega* $\mathcal{O}$. *Hitro se lahko prepričamo, da je* $\mathcal{O}[x]$ *vektorski prostor za običajno seštevanje polinomov ter množenje polinoma s skalarjem.*

Baza vektorskega prostora

Definicija 2.10 (Linearna neodvisnost vektorjev). *Naj bodo* $v_1, v_2, \ldots, v_k$ *vektorji iz vektorskega prostora* V *nad obsegom* $\mathcal{O}$. *Vektorji* $v_1, v_2, \ldots, v_k$ *so linearno odvisni, če obstajo taki skalarji* $\alpha_1, \alpha_2, \ldots, \alpha_k$ *iz obsega* $\mathcal{O}$, *da je vsaj eden od njih neničeln, in da velja* $\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_k v_k = 0$.

Če vektorji $v_1, v_2, \ldots, v_k$ *niso linearno odvisni, potem rečemo, da so linearno neodvisni.*

Primer 2.6 Ali so vektorji

$$v_1 = \begin{bmatrix} 1 \\ 1 \\ 3 \end{bmatrix}, v_2 = \begin{bmatrix} 4 \\ 2 \\ 0 \end{bmatrix}, v_3 = \begin{bmatrix} 0 \\ 1 \\ 6 \end{bmatrix},$$

kjer so $v_1, v_2, v_3 \in \mathbb{R}^3$, linearno neodvisni?

Iz zveze

$$\alpha \begin{bmatrix} 1 \\ 1 \\ 3 \end{bmatrix} + \beta \begin{bmatrix} 4 \\ 2 \\ 0 \end{bmatrix} + \gamma \begin{bmatrix} 0 \\ 1 \\ 6 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

dobimo sistem linearnih enačb

$$\begin{aligned} \alpha &+ 4\beta &&= 0 \\ \alpha &+ 2\beta + \gamma &= 0 \\ 3\alpha &+ 6\gamma &= 0. \end{aligned}$$

Ta sistem ima več neničelnih rešitev (npr: $\alpha = -4$, $\beta = 1$ in $\gamma = 2$), zato so vektorji v_1, v_2, v_3 linearno odvisni.

Definicija 2.11 (Baza vektorskega prostora). *Množico vektorjev* $\{v_1, v_2, \ldots, v_k\}$ *imenujemo baza vektorskega prostora* V, *če velja:*

- $V = \mathscr{L}(v_1, v_2, \ldots, v_k)$,
- *vektorji* $v_1, v_2, \ldots, v_k$ *so linearno neodvisni.*

Trditev 2.4. *Naj bosta* $\mathscr{B}_1 = \{v_1, v_2, \ldots, v_n\}$ *in* $\mathscr{B}_2 = \{u_1, u_2, \ldots, u_m\}$ *dve bazi vektorskega prostora* V. *Potem je* $n = m$.

Dokaz. Razvijmo vektorje iz baze $\mathscr{B}_2$ po bazi $\mathscr{B}_1$. Potem je

$$u_j = \sum_{i=1}^{n} \alpha_{ij} v_i, \quad \text{za } j = 1, 2, \ldots m,$$

za neke skalarje α_{ij}. Naj bo

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nm} \end{bmatrix} \text{ in } b = \begin{bmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_m \end{bmatrix} \in \mathcal{O}^m$$

tak vektor, da je $Ab = 0$. Potem je

$$0 = \sum_{i=1}^{n} \left(\sum_{j=1}^{m} \alpha_{ij} \beta_j \right) v_i = \sum_{j=1}^{m} \beta_j \sum_{i=1}^{n} \alpha_{ij} v_i = \sum_{j=1}^{m} \beta_j u_j.$$

Ker je $\mathscr{B}_2$ baza, so $u_1, u_2, \ldots, u_m$ linearno neodvisni, zato je

$$\beta_1 = \beta_2 = \ldots = \beta_m = 0.$$

Torej ima sistem $Ab = 0$ samo trivialno rešitev $b = 0$. Od tod sklepamo, da je $m \leq n$. Če zamenjamo vlogi $\mathscr{B}_1$ in $\mathscr{B}_2$, dobimo $n \leq m$. Zato je $m = n$.

□

Definicija 2.12 (Dimenzija vektorskega prostora). *Naj bo* $\mathscr{B} = \{v_1, v_2, \ldots, v_k\}$ *baza vektorskega prostora* V. *Potem število vektorjev v bazi imenujemo dimenzija (ali razsežnost) vektorskega prostora* V. *Pišemo*

$$\dim V = k.$$

Definicija 2.13 (Odsek). *Naj bo* L *vektorski podprostor vektorskega prostora* V *in naj bo* $v \in V$. *Potem je množica vektorjev*

$$v + L = \{v + y; y \in L\}$$

odsek vektorskega prostora L *glede na vektor* v.

Poglavje 3

Linearne kode

V tem poglavju bomo definirali osnovne pojme iz teorije kodiranja, ki so pomembni za nadaljne delo. Definirali bomo, kaj so linearne kode in kako lahko te linearne kode predstavimo s pomočjo generatorske oziroma kontrolne matrike.

Definicija 3.1. *Naj bo $n \in \mathbb{N}$ in naj bo $\mathcal{O}^n$ vektorski prostor na obsegu $\mathcal{O}$:*

- *Koda – Koda C dolžine n je podmnožica v $\mathcal{O}^n$.*
- *Velikost kode – Število elementov kode C se imenuje velikost kode C.*
- *Beseda – Elementi množice $\mathcal{O}^n$ se imenujejo besede.*
- *Kodne besede – Elementi kode C se imenujejo kodne besede.*

Definicija 3.2 (Linearna koda). *Naj bo C koda v $\mathcal{O}^n$. Koda C je linearna, če je vektorski podprostor v $\mathcal{O}^n$.*

Definicija 3.3 (Teža). *Naj bo $\mathcal{O}$ obseg, n naravno število ter x element vektorskega prostora $\mathcal{O}^n$. Teža vektorja x je število njegovih neničelnih koordinat. Težo vektorja x bomo označevali z $w(x)$.*

Skozi primere bomo nekatere vektorje iz $\mathcal{O}^n$ zaradi preglednosti poenostavili iz

$$\begin{bmatrix} o_1 \\ o_2 \\ \vdots \\ o_n \end{bmatrix} \in \mathcal{O}^n$$

v

$$o_1 o_2 \ldots o_n.$$

Tako bi na primer vektorji iz $\mathbb{Z}_2^2$ bili poenostavljeni takole:

$$\begin{bmatrix} 0 \\ 0 \end{bmatrix} \leftrightarrow 00,$$

$$\begin{bmatrix} 0 \\ 1 \end{bmatrix} \leftrightarrow 01,$$

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} \leftrightarrow 10,$$

$$\begin{bmatrix} 1 \\ 1 \end{bmatrix} \leftrightarrow 11.$$

Primer 3.1 Tabela nam prikazuje težo elementov v $\mathbb{Z}_3^2$.

Vektor	Teža
00	0
01	1
02	1

Vektor	Teža
10	1
11	2
12	2

Vektor	Teža
20	1
21	2
22	2

Primer 3.2 Tabela nam prikazuje težo elementov v $\mathbb{Z}_2^3$.

Vektor	Teža
000	0
001	1
010	1
011	2

Vektor	Teža
100	1
101	2
110	2
111	3

Definicija 3.4 (Hammingova razdalja). *Naj bosta $x, y \in \mathcal{O}^n$. Hammingova razdalja vektorjev x in y je število koordinat, na katerih se x in y razlikujeta. Hammingovo razdaljo vektorjev x in y bomo označevali z $d_H(x, y)$.*

Primer 3.3 Tabela prikazuje Hammingovo razdaljo med paroma elementov v $\mathbb{Z}_3^2$.

	00	01	02	10	11	12	20	21	22
00	0	1	1	1	2	2	1	2	2
01	1	0	1	2	1	2	2	1	2
02	1	1	0	2	2	1	2	2	1
10	1	2	2	0	1	1	1	2	2
11	2	1	2	1	0	1	2	1	2
12	2	2	1	1	1	0	2	2	1
20	1	2	2	1	2	2	0	1	1
21	2	1	2	2	1	2	1	0	1
22	2	2	1	2	2	1	1	1	0

Primer 3.4 Tabela prikazuje Hammingovo razdaljo med paroma elementov v $\mathbb{Z}_2^3$.

	000	001	010	011	100	101	110	111
000	0	1	1	2	1	2	2	3
001	1	0	2	1	2	1	3	2
010	1	2	0	1	2	3	1	2
011	2	1	1	0	3	2	2	1
100	1	2	2	3	0	1	1	2
101	2	1	3	2	1	0	2	1
110	2	3	1	2	1	2	0	1
111	3	2	2	1	2	1	1	0

Definicija 3.5 (Minimalna razdalja). *Minimalna razdalja kode C je najmanjše izmed števil $d_H(x, y)$, kjer sta x in y različni kodni besedi kode C.*

Primer 3.5 Oglejmo si linearne kode iz $\mathbb{Z}_3^2$. Linearni kodi $\{00, 01, 02\}$ in $\{00, 10, 20\}$ imata minimalno razdaljo 1, medtem ko ima linearna koda $\{00, 22, 11\}$ minimalno razdaljo 2.

Primer 3.6 Naslednje linearne kode v $\mathbb{Z}_2^3$ imajo minimalno razdaljo 1:

$$\{000, 001, 010, 011\}, \{000, 001, 100, 101\},$$

$$\{000, 010, 100, 110\}, \{000, 010, 101, 111\},$$

$$\{000, 100, 011, 111\}.$$

Koda $\{000, 011, 101, 110\}$ ima minimalno razdaljo 2.

Trditev 3.1. *Naj bo C linearna koda v $\mathcal{O}^n$. Potem je njena minimalna razdalja enaka*

$$w_{\min} = \min\{w(x); x \in C \wedge x \neq 0\}.$$

Dokaz. Ker je Hammingova razdalja translacijska invarianta, potem v splošnem velja

$$d_H(x, y) = d_H(x - z, y - z)$$

za x, y, z iz $\mathcal{O}^n$. Če za z vzamemo kar y, potem dobimo

$$d_H(x, y) = d_H(x - y, y - y) = d_H(x - y, 0) = w(x - y)$$

za vsak $x, y \in \mathcal{O}^n$. Torej

$$\begin{aligned} & \min\{d_H(x, y); x, y \in C, x \neq y\} = \\ = \quad & \min\{w(x - y); x, y \in C, x \neq y\} \\ = \quad & \min\{w(z); z \in C \wedge z \neq 0\}. \end{aligned}$$

□

Naj bo C linearna koda. Če je C k-dimenzionalen podprostor v $\mathcal{O}^n$, potem lahko najdemo bazo za C, ki jo sestavlja k kodnih besed $x_1, x_2, \ldots, x_k \in \mathcal{O}^n$. Vsaka kodna beseda v C je torej linearna kombinacija kodnih besed iz te baze.

Definicija 3.6 (Generatorska matrika). *Naj bo C linearna koda v $\mathcal{O}^n$. Generatorska matrika kode C je matrika, katere vrstice sestavljajo bazo za C.*

Generatorska matrika za k-dimenzionalno linearno kodo v $\mathcal{O}^n$ je $k \times n$ matrika, katere rang je k. Obratno, katera koli $k \times n$ matrika z rangom k je generatorska matrika za neko kodo. Da bi poiskali vse kodne besede linearne kode, katere generatorska matrika je G, moramo z matriko pomnožiti vse vektorje iz $\mathcal{O}^k$.

Primer 3.7 Oglejmo si linearno kodo v $\mathbb{Z}_3^4$, katere baza je množica $\{0002, 1001, 0100\}$. Ta baza nam porodi generatorsko matriko

$$G = \begin{bmatrix} 0 & 0 & 0 & 2 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix}.$$

Da bi poiskali vse kodne besede linearne kode, katere generatorska matrika je G, moramo z matriko

pomnožiti vse vektorje iz $\mathbb{Z}_3^3$. Tako nam množenja

$$\begin{bmatrix} 0 & 0 & 0 \end{bmatrix} G = \begin{bmatrix} 0 & 0 & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 & 1 \end{bmatrix} G = \begin{bmatrix} 0 & 1 & 0 & 0 \end{bmatrix},$$

$$\begin{bmatrix} 0 & 0 & 2 \end{bmatrix} G = \begin{bmatrix} 0 & 2 & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 & 0 \end{bmatrix} G = \begin{bmatrix} 1 & 0 & 0 & 1 \end{bmatrix},$$

$$\begin{bmatrix} 0 & 1 & 1 \end{bmatrix} G = \begin{bmatrix} 1 & 1 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 & 2 \end{bmatrix} G = \begin{bmatrix} 1 & 2 & 0 & 1 \end{bmatrix},$$

$$\begin{bmatrix} 0 & 2 & 0 \end{bmatrix} G = \begin{bmatrix} 2 & 0 & 0 & 2 \end{bmatrix}, \quad \begin{bmatrix} 0 & 2 & 1 \end{bmatrix} G = \begin{bmatrix} 2 & 1 & 0 & 2 \end{bmatrix},$$

$$\begin{bmatrix} 0 & 2 & 2 \end{bmatrix} G = \begin{bmatrix} 2 & 2 & 0 & 2 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 0 \end{bmatrix} G = \begin{bmatrix} 0 & 0 & 0 & 2 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 0 & 1 \end{bmatrix} G = \begin{bmatrix} 0 & 1 & 0 & 2 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 2 \end{bmatrix} G = \begin{bmatrix} 0 & 2 & 0 & 2 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 1 & 0 \end{bmatrix} G = \begin{bmatrix} 1 & 0 & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 & 1 \end{bmatrix} G = \begin{bmatrix} 1 & 1 & 0 & 0 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 1 & 2 \end{bmatrix} G = \begin{bmatrix} 1 & 2 & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 1 & 2 & 0 \end{bmatrix} G = \begin{bmatrix} 2 & 0 & 0 & 1 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 2 & 1 \end{bmatrix} G = \begin{bmatrix} 2 & 1 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 2 & 2 \end{bmatrix} G = \begin{bmatrix} 2 & 2 & 0 & 1 \end{bmatrix},$$

$$\begin{bmatrix} 2 & 0 & 0 \end{bmatrix} G = \begin{bmatrix} 0 & 0 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 2 & 0 & 1 \end{bmatrix} G = \begin{bmatrix} 0 & 1 & 0 & 1 \end{bmatrix},$$

$$\begin{bmatrix} 2 & 0 & 2 \end{bmatrix} G = \begin{bmatrix} 0 & 2 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 2 & 1 & 0 \end{bmatrix} G = \begin{bmatrix} 1 & 0 & 0 & 2 \end{bmatrix},$$

$$\begin{bmatrix} 2 & 1 & 1 \end{bmatrix} G = \begin{bmatrix} 1 & 1 & 0 & 2 \end{bmatrix}, \quad \begin{bmatrix} 2 & 1 & 2 \end{bmatrix} G = \begin{bmatrix} 1 & 2 & 0 & 2 \end{bmatrix},$$

$$\begin{bmatrix} 2 & 2 & 0 \end{bmatrix} G = \begin{bmatrix} 2 & 0 & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 2 & 2 & 1 \end{bmatrix} G = \begin{bmatrix} 2 & 1 & 0 & 0 \end{bmatrix},$$

$$\begin{bmatrix} 2 & 2 & 2 \end{bmatrix} G = \begin{bmatrix} 2 & 2 & 0 & 0 \end{bmatrix}$$

dajo kodne besede

$$\begin{array}{cccccccccc} 0000, & 0100, & 0200, & 1001, & 1101, & 1201, & 2002, & 2102, & 2202, \\ 0002, & 0102, & 0202, & 1000, & 1100, & 1200, & 2001, & 2101, & 2201, \\ 0001, & 0101, & 0201, & 1002, & 1102, & 1202, & 2000, & 2100, & 2200. \end{array}$$

Primer 3.8 Oglejmo si linearno kodo v $\mathbb{Z}_2^5$, katere baza je množica $\{00011, 01110, 11100\}$. Ta baza nam porodi generatorsko matriko:

$$G = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 \end{bmatrix}.$$

Da bi poiskali vse kodne besede linearne kode, katere generatorska matrika je G, moramo z matriko pomnožiti vse vektorje iz $\mathbb{Z}_2^3$.

$$\begin{bmatrix} 0 & 0 & 0 \end{bmatrix} G = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

$$\begin{bmatrix} 0 & 0 & 1 \end{bmatrix} G = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \end{bmatrix},$$

$$\begin{bmatrix} 0 & 1 & 0 \end{bmatrix} G = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 \end{bmatrix},$$

$$\begin{bmatrix} 0 & 1 & 1 \end{bmatrix} G = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 0 & 0 \end{bmatrix} G = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 0 & 1 \end{bmatrix} G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 1 & 0 \end{bmatrix} G = \begin{bmatrix} 0 & 1 & 1 & 0 & 1 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 1 & 1 \end{bmatrix} G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Tudi množica $\{10001, 01101, 10010\}$ je baza te iste linearne kode. Kodne besede zapišemo v vrsticah generatorske matrike G'.

$$G' = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

Kodne besede lahko najdemo tudi s pomočjo generatorske matrike G', ampak v drugačnem vrstnem redu.

$$\begin{bmatrix} 0 & 0 & 0 \end{bmatrix} G' = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

$$\begin{bmatrix} 0 & 0 & 1 \end{bmatrix} G' = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \end{bmatrix},$$

$$\begin{bmatrix} 0 & 1 & 0 \end{bmatrix} G' = \begin{bmatrix} 0 & 1 & 1 & 0 & 1 \end{bmatrix},$$

$$\begin{bmatrix} 0 & 1 & 1 \end{bmatrix} G' = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 0 & 0 \end{bmatrix} G' = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 0 & 1 \end{bmatrix} G' = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 1 & 0 \end{bmatrix} G' = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 1 & 1 \end{bmatrix} G' = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 \end{bmatrix}.$$

Primer 3.9 Poglejmo si linearno kodo v $\mathbb{Z}_5^3$, katere baza je množica $\{143, 212\}$. Ta baza nam porodi generatorsko matriko:

$$G = \begin{bmatrix} 1 & 4 & 3 \\ 2 & 1 & 2 \end{bmatrix}.$$

Da bi poiskali vse kodne besede linearne kode, katere generatorska matrika je G, moramo z matriko

pomnožiti vse vektorje iz $\mathbb{Z}_5^2$:

$$\begin{array}{lllll} 00\ G = 000, & 10\ G = 143, & 20\ G = 231, & 30\ G = 324, & 40\ G = 412, \\ 01\ G = 212, & 11\ G = 300, & 21\ G = 443, & 31\ G = 031, & 41\ G = 124, \\ 02\ G = 424, & 12\ G = 012, & 22\ G = 100, & 32\ G = 243, & 42\ G = 331, \\ 03\ G = 131, & 13\ G = 224, & 23\ G = 312, & 33\ G = 400, & 43\ G = 043, \\ 04\ G = 434, & 14\ G = 431, & 24\ G = 024, & 34\ G = 112, & 44\ G = 200. \end{array}$$

Kodne besede so

$$\begin{array}{llllllllll} 000, & 212, & 424, & 131, & 434, & 143, & 300, & 012, & 224, & 431, \\ 231, & 443, & 100, & 312, & 024, & 324, & 031, & 243, & 400, & 112, \\ 412, & 124, & 331, & 043, & 200. & & & & & \end{array}$$

Definicija 3.7 (Osnovne vrstične operacije). *Osnovne vrstične operacije na matrikah naredimo tako, da zamenjamo poljubno vrstico te matrike z vsoto te vrstice in večkratnikom neke druge.*

Če imamo generatorsko matriko G za linearno kodo C, potem vse ostale generatorske matrike za C dobimo iz matrike G z uporabo osnovnih vrstičnih operacij.

Primer 3.10 V primeru 3.8 smo videli, da ima linearna koda naslednji generatorski matriki:

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

in

$$G' = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

Matriko G' lahko dobimo iz matrike G z osnovnimi vrstičnimi operacijami:

1. zamenjaj drugo vrstico z vsoto prve in druge vrstice:

$$G_1 = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 \end{bmatrix};$$

2. zamenjaj tretjo vrstico z vsoto prve in tretje vrstice:

$$G_2 = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix};$$

3. zamenjaj tretjo vrstico z vsoto druge in tretje vrstice:

$$G_3 = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix};$$

4. zamenjaj prvo vrstico z vsoto prve in tretje vrstice:

$$G' = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

Definicija 3.8 (Ekvivalentni kodi). *Naj bosta C_1 in C_2 linearni kodi v $\mathcal{O}^n$. Naj bo G_1 generatorska matrika kode C_1 in naj bo G_2 generatorska matrika kode C_2. Kodi C_1 in C_2 sta ekvivalentni, če lahko G_2 dobimo iz G_1 z uporabo osnovnih vrstičnih operacij in z zamenjavo stolpcev.*

Primer 3.11 Oglejmo si linearni kodi v $\mathbb{Z}_3^4$. Matrika

$$G' = \begin{bmatrix} 1 & 2 & 0 & 1 \\ 2 & 0 & 1 & 0 \end{bmatrix}$$

je generatorska matrika linearne kode $\{0000, 2010, 1020, 1201, 0211, 2221, 2102, 1112, 0122\}$. Matrika

$$G = \begin{bmatrix} 2 & 1 & 2 & 0 \\ 1 & 1 & 2 & 1 \end{bmatrix}$$

je generatorska matrika linearne kode $\{0000, 1121, 2212, 2120, 0211, 1002, 1210, 2001, 0122\}$. Linearni kodi sta ekvivalentni, ker matriko G dobimo iz matrike G', če izvedemo sledeče operacije:

1. prvo vrstico nadomestimo z dvakratnikom prve vrstice:

$$G_1 = \begin{bmatrix} 2 & 1 & 0 & 2 \\ 2 & 0 & 1 & 0 \end{bmatrix};$$

2. drugo vrstico nadomestimo z vsoto prve in druge vrstice:

$$G_2 = \begin{bmatrix} 2 & 1 & 0 & 2 \\ 1 & 1 & 1 & 2 \end{bmatrix};$$

3. zamenjamo tretji in četrti stolpec:

$$G = \begin{bmatrix} 2 & 1 & 2 & 0 \\ 1 & 1 & 2 & 1 \end{bmatrix}.$$

Definicija 3.9 (Kanonična forma). *Generatorska matrika G $k-$dimenzionalne linearne kode v $\mathcal{O}^n$ je v kanonični formi, če velja*

$$G = [I : A],$$

kjer je I identična matrika velikosti $k \times k$, A pa matrika velikosti $k \times (n-k)$. Generatorsko matriko G lahko preoblikujemo v kanonično formo z osnovnimi vrstičnimi operacijami in z zamenjavo stolpcev. Torej sta kodi, ki jih generirata generatorska matrika in njena kanonična forma ekvivalentni.

Primer 3.12 Naj bo

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

generatorska matrika linearne kode $\{0000, 0001, 1000, 1001\}$ v $\mathbb{Z}_2^4$. Da pretvorimo G v kanonično formo, najprej zamenjamo prvi in drugi stolpec. Dobimo

$$G_1 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix}.$$

Potem zamenjamo prvi in zadnji stolpec in dobimo

$$G_2 = \left[\begin{array}{cc:cc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{array}\right].$$

Vidimo, da je sedaj G_2 v kanonični formi, kjer je

$$A = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Generatorska matrika G_2, ki je v kanonični formi, nam da štiri kodne besede:

$$0000, 1000, 0100, 1100.$$

Primer 3.13 Dana je generatorska matrika

$$G = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 2 & 0 \\ 1 & 3 & 0 & 0 \end{bmatrix}$$

linearne kode v $\mathbb{Z}_4^4$. Da spremenimo G v kanonično formo, bomo najprej uporabili osnovne vrstične operacije. Najprej zamenjamo drugo vrstico, tako da seštejemo dvakratnik prve in druge vrstice. Dobimo

$$G_1 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 2 \\ 1 & 3 & 0 & 0 \end{bmatrix}.$$

Potem zamenjamo tretjo vrstico tako, da seštejemo drugo in tretjo vrstico. Dobimo

$$G_2 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 2 \\ 1 & 0 & 0 & 2 \end{bmatrix}.$$

Na koncu zamenjamo prvi in tretji stolpec. Dobimo

$$G_3 = \left[\begin{array}{ccc:c} 1 & 0 & 0 & 2 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 1 \end{array}\right].$$

Vidimo, da je G_3 v kanonični formi, kjer je

$$A = \begin{bmatrix} 2 \\ 2 \\ 1 \end{bmatrix}.$$

Linearna koda generatorske matrike G je ekvivalentna linearni kodi generatorske matrike G_3, ki je v kanonični formi.

Primer 3.14 Dana je generatorska matrika

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

iz katere dobimo linearno kodo $\{00000, 00001, 00110, 00111, 11000, 11001, 11110, 11111\}$ v $\mathbb{Z}_2^5$.

Da spremenimo G v kanonično formo, bomo najprej uporabili osnovne vrstične operacije. Najprej zamenjamo tretjo vrstico, tako da seštejemo drugo in tretjo vrstico. Dobimo

$$G_1 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 \end{bmatrix}.$$

Potem zamenjamo drugo vrstico tako, da seštejemo prvo in drugo vrstico. Dobimo

$$G_2 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 \end{bmatrix}.$$

Zamenjamo prvi in zadnji stolpec. Dobimo

$$G_3 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

Na koncu zamenjamo drugi in tretji stolpec. Dobimo

$$G_4 = \left[\begin{array}{ccc:cc} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{array}\right].$$

Vidimo, da je sedaj G_4 v kanonični formi, kjer je

$$A = \left[\begin{array}{cc} 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{array}\right].$$

Linearna koda, ki smo jih dobili iz generatorske matrike G_4, ki je v kanonični formi, je

$$\{00000, 10000, 01010, 00101, 11010, 10101, 01111, 11111\}.$$

Definicija 3.10 (Kontrolna matrika). *Naj bo G generatorska matrika velikosti $k \times n$. Kontrolna matrika generatorske matrike G je matrika H velikosti $n - k \times n$, za katero velja*

$$GH^T = 0.$$

Izrek 3.1. *Naj bo $G = [I_G : A]$ generatorska matrika v kanonični formi velikosti $k \times n$, kjer je I_G identična matrika velikosti $k \times k$. Potem je kontrolna matrika kode C*

$$H = \left[-A^T : I_H\right],$$

kjer je I_H identična matrika velikosti $(n - k) \times (n - k)$.

Dokaz. Pokazati moramo, da je vsak element zmnožka $(GH^T)_{ij} = 0$. Torej

$$\begin{aligned} GH^T &= \left[\begin{array}{c:c} I_G & A \end{array}\right] \cdot \left[\begin{array}{c:c} -A^T & I_H \end{array}\right]^T \\ &= \left[\begin{array}{c:c} I_G & A \end{array}\right] \cdot \left[\begin{array}{c} -A \\ \hdashline I_H \end{array}\right] \end{aligned}$$

$$\begin{aligned} &= I_G \cdot (-A) + A \cdot I_H \\ &= -A + A \\ &= \begin{bmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{bmatrix}. \end{aligned}$$

□

Če G ni v kanonični formi, lahko najdemo matriko H tako, da spremenimo matriko G v kanonično formo. Potem izračunamo H_C. S pomočjo obratnega vrstnega reda operacij na stolpcih pretvorimo H_C v H.

Primer 3.15 Dana je generatorska matrika za linearno kodo v $\mathbb{Z}_2^5$

$$G = \left[\begin{array}{ccc:cc} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{array}\right],$$

ki je v kanonični formi. Potem je

$$A = \begin{bmatrix} 0 & 1 \\ 1 & 1 \\ 1 & 0 \end{bmatrix}.$$

Matriko H dobimo tako, da transponiramo matriko $-A$ in dodamo 2×2 identično matriko

$$H = \left[-A^T : I\right] = \left[A^T : I\right] = \left[\begin{array}{ccc:cc} 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{array}\right].$$

Kot smo pričakovali, smo dobili

$$GH^T = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 1 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Primer 3.16 Naj bo

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

generatorska matrika za linearno kodo

$$\{00000, 00001, 00110, 00111, 11000, 11001, 11110, 11111\} \subseteq \mathbb{Z}_2^5.$$

Generatorsko matriko G spremenimo v matriko G_C, ki je v kanonični formi

$$G_C = \left[\begin{array}{ccc:cc} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{array}\right]$$

z naslednjimi operacijami:

1. Tretjo vrstico zamenjamo z vsoto druge in tretje vrstice.
2. Drugo vrstico zamenjamo z vsoto prve in druge vrstice.
3. Zamenjamo prvi in peti stolpec.
4. Zamenjamo drugi in tretji stolpec.

S pomočjo izreka 3.1 poiščemo kontrolno matriko H_C:

$$H_C = \left[\begin{array}{ccc:cc} 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{array}\right].$$

Da najdemo kontrolno matriko matrike G, moramo upoštevati zamenjavo stolcev, ki smo jih uporabljali, ko smo spremenili matriko G v kanonično formo G_C, iste zamenjave stolpcev naredimo v sedanji matriki H_C, vendar v obratnem vrstnem redu.

Najprej zamenjamo drugi in tretji stolpec. Dobimo

$$H_1 = \begin{bmatrix} 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

Potem zamenjamo prvi in peti stolpec. Dobimo

$$H = \begin{bmatrix} 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 \end{bmatrix}.$$

Preverimo

$$GH^T = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 1 \\ 1 & 0 \\ 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Primer 3.17 Dana je generatorska matrika

$$G = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix},$$

iz katere dobimo linearno kodo $\{000, 101, 011, 110\} \subseteq \mathbb{Z}_2^3$. Matrika G je v kanonični formi. Kontrolna matrika je

$$H = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix}.$$

Preverimo, kaj se zgodi, če elemente v $\mathbb{Z}_2^3$ pomnožimo s H^T:

$$\begin{aligned} 000\ H^T &= 0, \\ 001\ H^T &= 1, \\ 010\ H^T &= 1, \\ 011\ H^T &= 0, \\ 100\ H^T &= 1, \\ 101\ H^T &= 0, \\ 110\ H^T &= 0, \\ 111\ H^T &= 1. \end{aligned}$$

Produkt matrike H^T in kateri koli kodne besede, ki smo jih zgenerirali iz matrike G, so nič, ostali produkti

so različni od nič.

Primer 3.18 Dana je generatorska matrika iz $\mathbb{Z}_3^3$ v kanonični formi

$$G = \begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 1 \end{bmatrix}.$$

Ker je G v kanonični formi, je njena kontrolna matrika

$$H = \begin{bmatrix} -2 & -1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 1 \end{bmatrix}.$$

Pomnožimo z matriko H^T vse vektorje iz $\mathbb{Z}_3^3$:

$$\begin{array}{llllllll}
000\,H^T = 0, & 100\,H^T = 1, & 200\,H^T = 2, \\
001\,H^T = 1, & 101\,H^T = 2, & 201\,H^T = 0, \\
002\,H^T = 2, & 102\,H^T = 0, & 202\,H^T = 1, \\
010\,H^T = 2, & 110\,H^T = 0, & 210\,H^T = 1, \\
011\,H^T = 0, & 111\,H^T = 1, & 211\,H^T = 2, \\
012\,H^T = 1, & 112\,H^T = 2, & 212\,H^T = 0, \\
020\,H^T = 1, & 120\,H^T = 2, & 220\,H^T = 0, \\
021\,H^T = 1, & 121\,H^T = 0, & 221\,H^T = 1, \\
022\,H^T = 0, & 122\,H^T = 1, & 222\,H^T = 2.
\end{array}$$

Zopet opazimo, da je produkt vektorjev z matriko H^T enak nič. Naslednja trditev nam pove, da to ni slučaj.

Trditev 3.2. *Naj bo G generatorska matrika linearne kode C ter naj bo H njena kontrolna matrika. Za poljuben vektor $x \in \mathcal{O}^n$ velja*

$$xH^T = 0 \Leftrightarrow x \in C.$$

Dokaz.

($\Leftarrow$) Če je $x \in C$, potem je $x = yG$ za nek vektor y dimenzije k. Torej je $xH^T = yGH^T$. Ker pa je $GH^T = 0$, je torej tudi $xH^T = 0$.

($\Rightarrow$) Rang matrike H (in zato tudi matrike H^T) je $(n-k)$, saj vsebuje identično matriko dimenzije $(n-k) \times (n-k)$ kot podmatriko. Če iščemo vse vektorje iz $\mathcal{O}^n$, ki so pravokotni na vsako vrstico matrike H, dobimo $n-(n-k) = k$ dimenzionalno rešitev. Podprostor vseh vektorjev, ki so pravokotni

na vsako vrstico matrike H, je ravno podprostor, ki ga generirajo vrstice matrike G, torej ravno linearna koda C. Če je torej nek vektor x pravokoten na vsako vrstico matrike H, potem mora x pripadati linearni kodi C.

□

Poglavje 4

Kodiranje in dekodiranje

Naj bo G generatorska matrika linearne kode C vektorskega prostora $\mathcal{O}^n$. Torej je G matrika dimenzije $k \times n$, kjer je k dimenzija kode C.

Naj bo v vektor iz vektorskega prostora $\mathcal{O}^k$. V procesu kodiranja vektor v pomnožimo z matriko G. Dobljeno kodno besedo označimo z b, kjer je $b = v \cdot G$. Prvim k bitom kodne besede b pravimo sporočilo, zadnjim n-k bitom pa pravimo kontrolni biti. Če je G v kanonični formi, potem je sporočilo kodne besede b (torej prvih k bitov) kar enako vektorju v.

Vektor b sedaj po nekem komunikacijskem kanalu (radijski valovi, telefon, internet ...) prenesemo do drugega uporabnika. Med prenosom se vektor b lahko "pokvari" in se nekateri biti vektorja b spremenijo. Uporabnik tako prejme vektor b_1, ki ni nujno enak vektorju b. V tem primeru se pojavi vprašanje, v kateri vektor kode C naj dekodiramo vektor b_1? Za pojasnitev procesa dekodiranja potrebujemo še naslednjo definicijo.

Definicija 4.1 (Sindrom). *Naj bo C linearna koda s pripadajočo generatorsko matriko G dimenzije $k \times n$ in kontrolno matriko H. Naj bo b poljubna beseda iz $\mathcal{O}^n$. Sindrom za besedo b je podan kot $s = bH^T$.*

Algoritem za dekodiranje je dokaj preprost. Za poljubno besedo b izračunamo sindrom s. Iz odseka $\{b + C\}$ izberemo vektor e z najmanjšo težo in s pomočjo njega dekodiramo kodno besedo b v kodno besedo $b - e$.

Primer 4.1 Naj bo matrika

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

generatorska matrika linearne kode C v $\mathbb{Z}_2^4$ in

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

njena kontrolna matrika.

Da sestavimo tabelo sindromov, bomo začeli z elementi v C, kateri imajo sindrom 00. Prva vrstica tabele sindroma izgleda takole:

Sindrom	Odsek				Minimalni
00	0000	0011	1100	1111	0000

kjer je sindrom na levi strani, kodne besede iz C so v sredini in vektor z minimalno težo je na desni strani.

Sedaj bomo izbrali vektor, ki ne pripada C-ju in izračunamo njegov sindrom. Pri računanju sindroma ne smemo pozabiti, da je seštevanje v $\mathbb{Z}_2$ isto kot odštevanje. Izberemo 0001, kateremu pripada sindrom 10. Da dobimo odsek, kateremu pripada beseda 0001, besedi 0001 prištejemo vse kodne besede kode C. V tem primeru imamo dva vektorja z minimalno razdaljo v tem odseku, vendar si izberemo samo en (poljuben) vektor.

Sindrom	Odsek				Minimalni
00	0000	0011	1100	1111	0000
10	0001	0010	1101	1110	0001

Nato izberemo drug vektor, in izračunamo njego sindrom. Če izberemo 0110, je sindrom 11 in lahko dodamo novo vrstico tabeli sindroma:

Sindrom	Odsek				Minimalni
00	0000	0011	1100	1111	0000
10	0001	0010	1101	1110	0001
11	0110	0101	1010	1001	0101

Ponovno izberemo poljubni vektor z minimalno razdaljo.

Izberemo še en vektor in izračunamo njegov sindrom. Če izberemo 0100, je sindrom 01. Uporabimo

to, da zaključimo tabelo:

Sindrom	Odsek				Minimalni
00	0000	0011	1100	1111	0000
01	0100	0111	1000	1011	0100
10	0001	0010	1101	1110	0001
11	0110	0101	1010	1001	0101

Sedaj uporabimo tabelo za popravljanje napak. Predpostavimo, da moramo vektor 1010 popraviti. Izračunamo njegov sindrom, ki je 11. Dodamo ga vektorju z minimalno težo v odseku s sindromom 11 za 1010:

$$1010 + 0101 = 1111.$$

Popravljena kodna beseda je 1111.

Če želimo popraviti vektor 0111, najprej izračunamo njegov sindrom, ki je 01. Vektorju 0111 prištejemo vektor iz njegovega odseka, ki ima minimalno težo:

$$0111 + 0100 = 0011.$$

Popravljena kodna beseda je 0011.

Če želimo popraviti vektor 1110, najprej izračunamo njegov sindrom, ki je 10. Vektorju 1110 prištejemo vektor iz njegovega odseka, ki ima minimalno težo:

$$1110 + 0001 = 1111.$$

Popravljena kodna beseda je 1111.

Če želimo popraviti vektor 1100, je njegov sindrom 00, kar pomeni, da je kodna beseda, zato popravek ni potreben.

Poglavje 5

Ciklične kode

V tem poglavju bomo spoznali posebni razred kod, ki imajo lepo matematično lastnost.

Definicija 5.1. *Naj bo $\mathcal{O}$ poljuben obseg in $n \in \mathbb{N}$. Za vektor $c = (c_0, c_1, \ldots, c_{n-1})$ iz vektorskega prostora $\mathcal{O}^n$ naj bo $c' \in \mathcal{O}^n$ vektor podan s*

$$c' = (c_{n-1}, c_0, c_1, \ldots, c_{n-2}).$$

Definicija 5.2. *Linearna koda C v $\mathcal{O}^n$ je ciklična, kadar za vsak $c \in \mathcal{O}^n$ velja*

$$c \in C \Longrightarrow c' \in C.$$

Primer 5.1 Primer ciklične kode na $\mathbb{Z}_2^7$, sestavljene iz kodnih besed:

$$\begin{array}{llll} 0000000, & 1011100, & 0101110, & 0010111, \\ 1001011, & 1100101, & 1110010, & 0111001. \end{array}$$

Za lažje razumevanje cikličnih kod, bomo vsakemu vektorju $c \in \mathcal{O}^n$ priredili ustrezen polinom iz $\mathcal{O}[x]$.

Definicija 5.3. *Naj bo $\mathcal{O}$ poljuben obseg in n naravno število. Za vektor $c = (c_0, c_1, \ldots, c_{n-1})$ iz vektorskega prostora $\mathcal{O}^n$ naj bo $c(x) = c_{n-1}x^{n-1} + \ldots + c_1 x + c_0$.*

Nadalje v tekstu ne bomo razlikovali med kodnimi besedami in njim prirejenimi polinomi.

O veljavnosti naslednje leme se bralec lahko prepriča sam.

Lema 5.1. *Naj bo C ciklična koda v $\mathcal{O}^n$ in naj bo $c = (c_0, c_1, \ldots, c_{n-1}) \in C$. Potem velja*

$$c'(x) = xc(x) - c_{n-1}(x^n - 1).$$

Lema 5.2. *Naj bo $\mathcal{O}$ poljuben obseg ter n poljubno naravno število. Naj bo C ciklična koda v $\mathcal{O}^n$ in naj bo $c(x) \in C$. Potem velja:*

i) $x^i c(x) \in C$ *za* $0 \leq i \leq n - 1 - deg(c(x))$*;*

ii) $x^i c(x) \in C, 0 \leq i \leq n - 1 - deg(c(x))$*, so linearno neodvisne kodne besede;*

iii) $a(x)c(x) \in C$ *za vsak* $a(x) \in \mathcal{O}[x]$ *z* $deg(a(x)) \leq n - 1 - deg(c(x))$.

Dokaz.

i) Očitno trditev velja za $i = 0$. Privzemimo sedaj, da trditev velja za nek i, $0 \leq i \leq n - 2 - deg(c(x))$. Pokazali bomo, da potem trditev velja tudi za $i + 1$. Ker je $i \leq n - 2 - deg(c(x))$, je stopnja polinoma $x^i c(x)$ manjša od $n - 1$. Po lemi 5.1 je torej $(x^i c(x))' = x(x^i c(x)) = x^{i+1} c(x) \in C$. Torej trditev res velja za vsak i, $0 \leq i \leq n - 1 - deg(c(x))$.

ii) Med kodnimi besedami $x^i c(x)$, $0 \leq i \leq n - 1 - deg(c(x))$ je natanko ena kodna beseda stopnje j za $deg(c(x)) \leq j \leq n - 1$. Torej so kodne besede res linearno neodvisne.

iii) Sledi neposredno iz točke i) zgoraj, ker je koda C linearna.

□

Izrek 5.1. *Naj bo $\mathcal{O}$ poljuben obseg ter n poljubno naravno število. Naj bo C ciklična koda v $\mathcal{O}^n$ in naj bo $g(x) \in C$ neničelni polinom z vodilnim koeficientom* 1*, ki ima najmanjšo stopnjo med vsemi neničelnimi polinomi v C. Potem velja:*

i) $g(x)$ *je enolično določen;*

ii) $g(x)$ *deli* $c(x)$ *za vsak* $c \in C$*;*

iii) $g(x)$ *deli* $x^n - 1$ *v* $\mathcal{O}[x]$*;*

iv) dimenzija kode C je enaka $n - \deg(g(x))$.

Dokaz.

i) Naj bosta $g_1(x) \in C$ in $g_2(x) \in C$ dva neničelna polinoma z vodilnim koeficientom 1 ter najmanjšo možno stopnjo. Potem ima polinom $p(x) = g_1(x) - g_2(x) \in C$ stopnjo manjšo od stopnje polinomov $g_1(x)$ in $g_2(x)$. Če je $p(x)$ neničeln polinom, potem naj bo $a (a \in \mathcal{O})$ njegov vodilni koeficient. Polinom $a^{-1}p(x) \in C$ je potem neničeln polinom z vodilnim koeficientom 1 ter stopnjo manjšo od stopnje polinomov $g_1(x)$ in $g_2(x)$, kar pa je protislovje. Torej je $p(x)$ ničeln polinom, kar pa pomeni, da je $g_1(x) = g_2(x)$.

ii) Izberimo si $c(x) \in C$ in naj bosta $a(x)$ in $r(x)$ taka polinoma, da velja $c(x) = a(x)g(x) + r(x)$, kjer je $\deg(r(x)) < \deg(g(x))$. Ker je $\deg(a(x)) + \deg(g(x)) = \deg(c(x)) \leq n-1$, je $\deg(a(x)) \leq n - 1 - \deg(g(x))$. Po iii) točki leme 5.2 je torej $a(x)g(x) \in C$. Ker je koda C linearna, je tudi $r(x) = c(x) - a(x)g(x) \in C$. Če je $r(x)$ neničelni polinom, potem podobno kot v dokazu točke i) zgoraj konstruiramo neničelni polinom iz C, ki ima vodilni koeficient 1 ter stopnjo manjšo od $\deg(g(x))$, torej je protislovje. Torej je $r(x)$ ničeln polinom, kar pa pomeni, da $g(x)$ deli $c(x)$.

iii) Naj bo $c(x) \in C$ poljuben polinom stopnje $n-1$ in z vodilnim koeficientom 1 (tak polinom vedno obstaja po točki i) leme 5.2 in ker je koda C linearna). Po lemi 5.1 dobimo, da je $x^n - 1 = xc(x) - c'(x)$. Ker polinom $g(x)$ deli vsak polinom kode C, deli tako polinom $xc(x)$ kot tudi polinom $c'(x)$. Torej deli tudi njuno razliko, to pa je ravno polinom $x^n - 1$.

iv) Naj bo $c(x)$ poljuben polinom kode C. Po točki ii) zgoraj je $c(x) = a(x)g(x)$. Pri tem velja $\deg(a(x)) = \deg(c(x)) - \deg(g(x)) \leq n - 1 - deg(g(x))$. Torej je $c(x)$ linearna kombinacija polinomov $x^i g(x), 0 \leq i \leq n - 1 - \deg(g(x))$. Ker so ti polinomi tudi linearno neodvisni po točki ii) leme 5.2, je dimenzija kode C ravno $n - \deg(g(x))$.

□

Polinomu $g(x)$ iz izreka 5.1 rečemo tudi generatorski polinom ciklične kode C.

Primer 5.2 V primeru 5.1 je generatorski polinom $g(x) = x^4 + x^3 + x^2 + 1$. Vse kodne besede so torej oblike $(a_2x^2 + a_1x + a_0)g(x)$, kjer je $a_i \in \mathbb{Z}_2$. Prav tako se lahko prepričamo tudi, da $g(x)$ deli $x^7 - 1$, saj je $x^7 - 1 = (x^4 + x^3 + x^2 + 1)(x^3 + x^2 + 1)$.

Temu sledi vprašanje: Ali so vsi delitelji $x^n - 1$ generatorski polinomi kakšne ciklične kode? To lahko dokažemo z naslednjim izrekom.

Izrek 5.2. *Naj bo $\mathcal{O}$ poljuben obseg ter n poljubno naravno število. Naj bo $g(x) \in \mathcal{O}[x]$ delitelj polinoma $x^n - 1$. Potem je*

$$C = \{i(x)g(x) | i(x) \in \mathcal{O}[x], \deg(i(x)) < n - \deg(g(x))\}$$

ciklična koda z generatorskim polinomom $g(x)$.

Dokaz. Očitno je C linearna koda. Če je ciklična, potem je $g(x)$ njen generatorski polinom, saj ima vodilni koeficient 1 ter najnižjo možno stopnjo med neničelnimi polinomi množice C. Pokazati moramo torej samo še to, da je C ciklična koda. Naj bo $g(x) = x^s + g_{s-1}x^{s-1} + \cdots + g_0$ in naj bo $h(x) = \frac{x^n-1}{g(x)} = x^{n-s} + h_{n-s-1}x^{n-s-1} + \cdots + h_1x + h_0$. Izberimo si poljubni polinom $c(x) = i(x)g(x)$ iz kode C (torej je

$\deg(i(x)) < n - s$). Po lemi 5.1 dobimo:

$$\begin{aligned} c'(x) &= xc(x) - c_{n-1}(x^n - 1) \\ &= xi(x)g(x) - c_{n-1}h(x)g(x) \\ &= (xi(x) - c_{n-1}h(x))\, g(x). \end{aligned}$$

Če je $c_{n-1} = 0$, potem je $\deg(i(x)) < n - s - 1$. Torej je stopnja polinoma $xi(x) - c_{n-1}h(x) = xi(x)$ manjša od $n - s$. Če pa je $c_{n-1} \neq 0$, potem imata polinoma $xi(x)$ in $c_{n-1}h(x)$ stopnjo $n - s$ ter vodilni koeficient c_{n-1}. Zato je polinom $xi(x) - c_{n-1}h(x)$ zopet stopnjo manjši od $n - s$. Torej je v vsakem primeru c' zopet element kode C. To pa pomeni, da je C ciklična koda.

□

Ta dva izreka nam povesta, da lahko preučujemo ciklične kode tako, da preučujemo delitelje polinoma $x^n - 1$.

Primer 5.3 Naj bo $n = 7$ in $\mathcal{O} = Z_2$. Polinom $x^7 - 1$ lahko faktoriziramo kot

$$x^7 - 1 = (x - 1)(x^3 + x + 1)(x^3 + x^2 + 1).$$

Ker so koeficienti polinomov iz obsega $\mathbb{Z}_2$, lahko minuse nadomestimo s plusi:

$$x^7 + 1 = (x + 1)(x^3 + x + 1)(x^3 + x^2 + 1).$$

Na voljo imamo 8 generatorskih polinomov:

- $1 = 1$,
- $x + 1 = x + 1$,
- $x^3 + x + 1 = x^3 + x + 1$,
- $x^3 + x^2 + 1 = x^3 + x^2 + 1$,
- $(x + 1)(x^3 + x + 1) = x^4 + x^3 + x^2 + 1$,
- $(x + 1)(x^3 + x^2 + 1) = x^4 + x^2 + x + 1$,
- $(x^3 + x + 1)(x^3 + x^2 + 1) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$,
- $(x + 1)(x^3 + x + 1)(x^3 + x^2 + 1) = x^7 + 1$.

Za naš primer si izberimo generatorski polinom $g(x) = x^3+x^2+1$. Ciklična koda, ki jo porodi generatorski polinom $g(x)$, je množica vseh polinomov oblike

$$C = \left\{ i(x)(x^3 + x^2 + 1) | i(x) \in \mathbb{Z}_2[x], \deg(i(x)) < 7 - 3 \right\}.$$

Če pomnožimo generatorski polinom z vsemi polinomi, ki ustrezaju pogoju, dobimo:

$$\begin{aligned}
0 \cdot g(x) &= 0, \\
1 \cdot g(x) &= x^3 + x^2 + 1, \\
x \cdot g(x) &= x^4 + x^3 + x, \\
(x+1) \cdot g(x) &= x^4 + x^2 + x + 1, \\
x^2 \cdot g(x) &= x^5 + x^4 + x^2, \\
(x^2+1) \cdot g(x) &= x^5 + x^4 + x^3 + 1, \\
(x^2+x) \cdot g(x) &= x^5 + x^3 + x^2 + x, \\
(x^2+x+1) \cdot g(x) &= x^5 + x + 1, \\
x^3 \cdot g(x) &= x^6 + x^5 + x^3, \\
(x^3+1) \cdot g(x) &= x^6 + x^5 + x^2 + 1, \\
(x^3+x) \cdot g(x) &= x^6 + x^5 + x^4 + x, \\
(x^3+x+1) \cdot g(x) &= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, \\
(x^3+x^2) \cdot g(x) &= x^6 + x^4 + x^3 + x^2, \\
(x^3+x^2+1) \cdot g(x) &= x^6 + x^4 + 1, \\
(x^3+x^2+x) \cdot g(x) &= x^6 + x^2 + x, \\
(x^3+x^2+x+1) \cdot g(x) &= x^6 + x^3 + x + 1.
\end{aligned}$$

Ciklična koda, ki jo porodi generatorski polinom $g(x) = x^3 + x^2 + 1$, je torej:

$$\begin{array}{llll}
0000000, & 0001011, & 0010110, & 0011101, \\
0101100, & 0100111, & 0111010, & 0110001, \\
1011000, & 1010011, & 1001110, & 1000101, \\
1110100, & 1111111, & 1100010, & 1101001.
\end{array}$$

5.1 Generatorska in kontrolna matrika cikličnih kod

Naj bo C ciklična koda dimenzije k v $\mathcal{O}^n$. Pokazali smo, da ima koda C generatorski polinom $g(x)$ stopnje $n-k$, tj. $g(x) = x^{n-k} + g_{n-k-1}x^{n-k-1} + \cdots + g_1 x + g_0$, kot tudi, da so $x^j g(x), j = 0, 1, \ldots, k-1$ linearno neodvisne kodne besede. To pomeni, da je generatorska matrika kode C enaka

$$G = \begin{bmatrix} g_0 & g_1 & \cdots & \cdots & g_{n-k-1} & 1 & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & \cdots & g_{n-k-1} & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & g_0 & g_1 & \cdots & \cdots & g_{n-k-1} & 1 & 0 \\ 0 & \cdots & \cdots & 0 & g_0 & g_1 & \cdots & \cdots & g_{n-k-1} & 1 \end{bmatrix}.$$

Tako ima G v prvi vrstici koeficiente polinoma $g(x)$, preostalih $k-1$ vrstic so dobljene z "zamikanjem" elementov prve vrstice in predstavljajo koeficiente polinomov $x^i g(x)$ za $1 \leq i \leq n - deg(g(x))$.

Primer 5.4 Naj bo $\mathcal{O} = \mathbb{Z}_2$. Če polinom $x^{15} - 1 \in \mathcal{O}[x]$ faktoriziramo, dobimo

$$x^{15} - 1 = (x-1)(x^2 + x + 1)(x^4 + x^3 + x^2 + x + 1)(x^8 - x^7 + x^5 - x^4 + x^3 - x + 1).$$

Ker delamo nad obsegom $\mathbb{Z}_2$, je to isto kot

$$x^{15} + 1 = (x+1)(x^2 + x + 1)(x^4 + x^3 + x^2 + x + 1)(x^8 + x^7 + x^5 + x^4 + x^3 + x + 1).$$

Iz množice možnih generatorskih polinomov izberimo $g(x) = x^8 + x^7 + x^5 + x^4 + x^3 + x + 1$. Seveda bi lahko izbrali za generatorski polinom tudi kakšen drug delitelj polinoma $x^{15} - 1$. Generatorska matrika kode C, ki jo porodi generatorski polinom $g(x)$, je

$$G = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

Da bi dobili vse kodne besede ciklične kode C , moramo generatorsko matriko G pomnožiti z vsemi vektorji iz $\mathbb{Z}_2^6$:

Beseda	Kodna beseda	Beseda	Kodna beseda	Beseda	Kodna beseda
[0000000]	[000000000000000]	[0000001]	[000000110111011]	[0000010]	[000001101110110]
[0000011]	[000001011001101]	[0000100]	[000011011101100]	[0000101]	[000011101010111]
[0000110]	[000010110011010]	[0000111]	[000010000100001]	[0001000]	[000110111011000]
[0001001]	[000110001100011]	[0001010]	[000111010101110]	[0001011]	[000111100010101]
[0001100]	[000101100110100]	[0001101]	[000101010001111]	[0001110]	[000100001000010]
[0001111]	[000100111111001]	[0010000]	[001101110110000]	[0010001]	[001101000001011]
[0010010]	[001100011000110]	[0010011]	[001100101111101]	[0010100]	[001110101011100]
[0010101]	[001110011100111]	[0010110]	[001111000101010]	[0010111]	[001111110010001]
[0011000]	[001011001101000]	[0011001]	[001011111010011]	[0011010]	[001010100011110]
[0011011]	[001010010100101]	[0011100]	[001000010000100]	[0011101]	[001000100111111]
[0011110]	[001001111110010]	[0011111]	[001001001001001]	[0100000]	[011011101100000]
[0100001]	[011011011011011]	[0100010]	[011010000010110]	[0100011]	[011010110101101]
[0100100]	[011000110001100]	[0100101]	[011000000110111]	[0100110]	[011001011111010]
[0100111]	[011001101000001]	[0101000]	[011101010111000]	[0101001]	[011101100000011]
[0101010]	[011100111001110]	[0101011]	[011100001110101]	[0101100]	[011110001010100]
[0101101]	[011110111101111]	[0101110]	[011111100100010]	[0101111]	[011111010011001]
[0110000]	[010110011010000]	[0110001]	[010110101101011]	[0110010]	[010111110100110]
[0110011]	[010111000011101]	[0110100]	[010101000111100]	[0110101]	[010101110000111]
[0110110]	[010100101001010]	[0110111]	[010100011110001]	[0111000]	[010000100001000]
[0111001]	[010000010110011]	[0111010]	[010001001111110]	[0111011]	[010001111000101]
[0111100]	[010011111100100]	[0111101]	[010011001011111]	[0111110]	[010010010010010]
[0111111]	[010010100101001]	[1000000]	[110111011000000]	[1000001]	[110111101111011]
[1000010]	[110110110110110]	[1000011]	[110110000001101]	[1000100]	[110100000101100]
[1000101]	[110100110010111]	[1000110]	[110101101011010]	[1000111]	[110101011100001]
[1001000]	[110001100011000]	[1001001]	[110001010100011]	[1001010]	[110000001101110]
[1001011]	[110000111010101]	[1001100]	[110010111110100]	[1001101]	[110010001001111]
[1001110]	[110011010000010]	[1001111]	[110011100111001]	[1010000]	[111010101110000]
[1010001]	[111010011001011]	[1010010]	[111011000000110]	[1010011]	[111011110111101]

Beseda	Kodna beseda	Beseda	Kodna beseda	Beseda	Kodna beseda
[1010100]	[111001110011100]	[1010101]	[111001000100111]	[1010110]	[111000011101010]
[1010111]	[111000101010001]	[1011000]	[111100010101000]	[1011001]	[111100100010011]
[1011010]	[111101111011110]	[1011011]	[111101001100101]	[1011100]	[111111001000100]
[1011101]	[111111111111111]	[1011110]	[111110100110010]	[1011111]	[111110010001001]
[1100000]	[101100110100000]	[1100001]	[101100000011011]	[1100010]	[101101011010110]
[1100011]	[101101101101101]	[1100100]	[101111101001100]	[1100101]	[101111011110111]
[1100110]	[101110000111010]	[1100111]	[101110110000001]	[1101000]	[101010001111000]
[1101001]	[101010111000011]	[1101010]	[101011100001110]	[1101011]	[101011010110101]
[1101100]	[101001010010100]	[1101101]	[101001100101111]	[1101110]	[101000111100010]
[1101111]	[101000001011001]	[1110000]	[100001000010000]	[1110001]	[100001110101011]
[1110010]	[100000101100110]	[1110011]	[100000011011101]	[1110100]	[100010011111100]
[1110101]	[100010101000111]	[1110110]	[100011110001010]	[1110111]	[100011000110001]
[1111000]	[100111111001000]	[1111001]	[100111001110011]	[1111010]	[100110010111110]
[1111011]	[100110100000101]	[1111100]	[100100100100100]	[1111101]	[100100010011111]
[1111110]	[100101001010010]	[1111111]	[100101111101001]		

Ciklična koda C z generatorskim polinomom $g(x)$ oziroma z generatorsko matriko G je

$$
\begin{aligned}
C = \{&000000000000000,\ 000000110111011,\ 000001101110110,\ 000001011001101,\\
&000011011101100,\ 000011101010111,\ 000010110011010,\ 000010000100001,\\
&000110111011000,\ 000110001100011,\ 000111010101110,\ 000111100010101,\\
&000101100110100,\ 000101010001111,\ 000100001000010,\ 000100111111001,\\
&001101110110000,\ 001101000001011,\ 001100011000110,\ 001100101111101,\\
&001110101011100,\ 001110011100111,\ 001111000101010,\ 001111110010001,\\
&001011001101000,\ 001011111010011,\ 001010100011110,\ 001010010100101,\\
&001000010000100,\ 001000100111111,\ 001001111110010,\ 001001001001001,\\
&011011101100000,\ 011011011011011,\ 011010000010110,\ 011010110101101,\\
&011000110001100,\ 011000000110111,\ 011001011111010,\ 011001101000001,\\
&011101010111000,\ 011101100000011,\ 011100111001110,\ 011100001110101,\\
&011110001010100,\ 011110111101111,\ 011111100100010,\ 011111010011001,\\
&010110011010000,\ 010110101101011,\ 010111110100110,\ 010111000011101,\\
&010101000111100,\ 010101110000111,\ 010100101001010,\ 010100011110001,
\end{aligned}
$$

010000100001000, 010000010110011, 010001001111110, 010001111000101,
010011111100100, 010011001011111, 010010010010010, 010010100101001,
110111011000000, 110111101111011, 110110110110110, 110110000001101,
110100000101100, 110100110010111, 110101101011010, 110101011100001,
110001100011000, 110001010100011, 110000001101110, 110000111010101,
110010111110100, 110010001001111, 110011010000010, 110011100111001,
111010101110000, 111010011001011, 111011000000110, 111011110111101,
111001110011100, 111001000100111, 111000011101010, 111000101010001,
111100010101000, 111100100010011, 111101111011110, 111101001100101,
111111001000100, 111111111111111, 111110100110010, 111110010001001,
101100110100000, 101100000011011, 101101011010110, 101101101101101,
101111101001100, 101111011110111, 101110000111010, 101110110000001,
101010001111000, 101010111000011, 101011100001110, 101011010110101,
101001010010100, 101001100101111, 101000111100010, 101000001011001,
100001000010000, 100001110101011, 100000101100110, 100000011011101,
100010011111100, 100010101000111, 100011110001010, 100011000110001,
100111111001000, 100111001110011, 100110010111110, 100110100000101,
100100100100100, 100100010011111, 100101001010010, 100101111101001}.

Izrek 5.3. *Naj bo $\mathcal{O}$ poljuben obseg ter n poljubno naravno število. Naj bo C ciklična koda dimenzije k v $\mathcal{O}^n$ in naj bo $g(x) \in C$ generatorski polinom kode C. Naj bo $h(x) = \frac{x^n-1}{g(x)} = x^k + h_{k-1}x^{k-1} + \cdots + h_1 x + h_0$ in naj bo $g^\perp(x) = x^k h(x^{-1}) = h_0 x^k + h_1 x^{k-1} + \cdots + h_{k-1}x + 1$. Potem je kontrolna matrika kode C matrika dimenzije $n - k \times n$, ki je podana z*

$$H = \begin{bmatrix} 1 & h_{k-1} & \cdots & \cdots & h_1 & h_0 & 0 & \cdots & \cdots & 0 \\ 0 & 1 & h_{k-1} & \cdots & \cdots & h_1 & h_0 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & h_{k-1} & \cdots & \cdots & h_1 & h_0 & 0 \\ 0 & \cdots & \cdots & 0 & 1 & h_{k-1} & \cdots & \cdots & h_1 & h_0 \end{bmatrix}.$$

V prvi vrstici matrike H so torej koeficienti polinoma $g^\perp(x)$, preostale $n - k - 1$ vrstice pa dobimo z "zamikanjem" prve vrstice v desno.

Dokaz. Pokazati moramo, da je matrika GH^T ničelna matrika. Vzemimo i-to ($1 \leq i \leq k$) vrstico matrike

G ter j-ti ($1 \leq j \leq n-k$) stolpec matrike H^T (torej j-to vrstico matrike H). i-ta vrstica matrike G je

$$\begin{bmatrix} 0 & \cdots & 0 & g_0 & g_1 & \cdots & g_{n-k-1} & 1 & 0 & \cdots & 0 \end{bmatrix}.$$

j-ta vrstica matrike H pa je

$$\begin{bmatrix} 0 & \cdots & 0 & 1 & h_{k-1} & \cdots & h_1 & h_0 & 0 & \cdots & 0 \end{bmatrix}.$$

Če je $i \leq j$, potem je skalarni produkt teh dveh vrstic enak

$$g_{j-i} + g_{j-i+1}h_{k-1} + g_{j-i+2}h_{k-2} + \ldots$$

Če pa je $i > j$, potem je skalarni produkt teh dveh vrstic enak

$$g_0 h_{k-i+j} + g_1 h_{k-i+j+1} + g_2 h_{k-i+j+2} + \ldots$$

V obeh dveh primerih je to število natanko koeficient polinoma $g(x)h(x)$ pri potenci x^{k-i+j}. Potenca $k-i+j$ je lahko največ $n-1$ (v primeru, ko je $i = 1$ in $j = n-k$), najmanj pa 1 (v primeru, ko je $i = k$ in $j = 1$). Ker je $g(x)h(x) = x^n + 1$, so torej koeficienti pri potencah x^{k-i+j} enaki 0. Torej je skalarni produkt i-te vrstice matrike G in j-tega stolpca matrike H^T enak 0 za vsak i in vsak j. Produkt GH^T je torej res ničelna matrika.

□

Primer 5.5 Naj bo C ciklična koda v Z_2^7, ki jo porodi generatorski polinom

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

Pripadajoča polinoma $h(x)$ in $g^\perp(x)$ za generatorski polinom $g(x)$ sta

$$\begin{aligned} h(x) &= \tfrac{x^7+1}{g(x)} \\ &= \tfrac{x^7+1}{x^4+x^2+x+1} \\ &= x^3 + x + 1 \end{aligned}$$

in

$$g^\perp(x) = 1 + x^2 + x^3.$$

Pripadajoča generatorska matrika G za generatorski polinom $g(x)$ je

$$G = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix},$$

kontrolna matrika pa

$$H = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

Poglavje 6

Reed–Solomonove kode

Leta 1960 sta Irving Reed in Gus Solomon objavila članek "Polynomial Codes over Certain Finite Fields"[3]. V njem sta predstavila nov razred kod, ki so sedaj znane kot Reed–Solomonove kode. V današnjih časih so te kode splošno uporabljenje/zastopane na različnih področjih. Srečamo jih pri predvajanju CD– in DVD–ploščkov, v telekomunikaciji, pa tudi pri komunikaciji s sateliti.

V tem poglavju bodo Reed–Solomonove kode predstavljene v obsegu $\mathcal{O} = Z_p$, kjer je p poljubno praštevilo. V splošnem lahko te kode definiramo v poljubnem končnem obsegu.

Definicija 6.1 (Reed–Solomonove kode). *Naj bo $m, n \in \mathbb{N}$ in naj velja $m \leq n \leq p$. Definicija Reed–Solomonove kode v $\mathcal{O}$ z m sporočilnimi in n kodnimi simboli je podana na sledeči način. Za dani vektor $[x_0\ x_1\ \ldots\ x_{m-1}] \in \mathcal{O}^m$, naj bo $P(t) \in \mathcal{O}[t]$ polinom oblike*

$$P(t) = x_{m-1}t^{m-1} + x_{m-2}t^{m-2} + \cdots + x_1 t + x_0,$$

kjer so koeficienti sporočilni simboli. Potem je kodni vektor a vektor, katerega koordinate so vrednosti polinoma $P(t)$ v številih $0, 1, \ldots, n-1$:

$$a = [a_0\ a_1\ \ldots\ a_{n-1}] = [P(0)\ P(1)\ \ldots\ P(n-1)].$$

Primer 6.1 Primer Reed–Solomonove kode v $\mathbb{Z}_3^3$ je $\{000, 012, 021, 111, 120, 102, 222, 201, 210\}$ za besede

iz $\mathbb{Z}_3^2$. Sledi tabelarni prikaz navedenega:

Beseda	$P(0)$	$P(1)$	$P(2)$	Kodna beseda
[0 0]	$0\cdot 0+0 = 0$	$0\cdot 1+0 = 0$	$0\cdot 2+0 = 0$	[0 0 0]
[0 1]	$1\cdot 0+0 = 0$	$1\cdot 1+0 = 1$	$1\cdot 2+0 = 2$	[0 1 2]
[0 2]	$2\cdot 0+0 = 0$	$2\cdot 1+0 = 2$	$2\cdot 2+0 = 1$	[0 2 1]
[1 0]	$0\cdot 0+1 = 1$	$0\cdot 1+1 = 1$	$0\cdot 2+1 = 1$	[1 1 1]
[1 1]	$1\cdot 0+1 = 1$	$1\cdot 1+1 = 2$	$1\cdot 2+1 = 0$	[1 2 0]
[1 2]	$2\cdot 0+1 = 1$	$2\cdot 1+1 = 0$	$2\cdot 2+1 = 2$	[1 0 2]
[2 0]	$0\cdot 0+2 = 2$	$0\cdot 1+2 = 2$	$0\cdot 2+2 = 2$	[2 2 2]
[2 1]	$1\cdot 0+2 = 2$	$1\cdot 1+2 = 0$	$1\cdot 2+2 = 1$	[2 0 1]
[2 2]	$2\cdot 0+2 = 2$	$2\cdot 1+2 = 1$	$2\cdot 2+2 = 0$	[2 1 0]

Da bo definicija 6.1 smiselna, moramo še pokazati, da se dva različna vektorja iz $\mathcal{O}^m$ zakodirata v dve različni kodni besedi iz $\mathcal{O}^n$. Pokazati torej moramo, da če je $P_1(t) = P_2(t)$ za $t = 0, 1, \ldots, n-1$, potem sta polinoma P_1 in P_2 enaka. Če hočemo to pokazati, se moramo spomniti nekaterih dejstev o polinomih.

Lema 6.1. *Naj bo $P(t) \in \mathcal{O}[t]$ neničeln polinom. Če je a ničla polinoma $P(t)$, tj. $P(a) = 0$, potem lahko $P(t)$ faktoriziramo kot $P(t) = (t-a)Q(t)$, kjer je $Q(t) \in \mathcal{O}[t]$. Seveda je stopnja $Q(t)$ natanko za ena manjša od stopnje $P(t)$.*

Dokaz. Ne glede na to, ali je a ničla ali ne, lahko $P(t)$ delimo z $(t-a)$ in dobim kvocient $Q(t)$ in ostanek c oziroma

$$P(t) = (t-a)Q(t) + c.$$

Če je $t = a$, potem je $P(a) = c$. Kar pomeni, če je a ničla, potem je $c = 0$.

□

Izrek 6.1. *Naj bo $P(t) \in \mathcal{O}[t]$ neničeln polinom, ki ima d ničel. Potem je stopnja $P(t)$ vsaj d.*

Dokaz. Naj bodo $a_1, \ldots, a_d$ ničle polinoma $P(t)$. V lemi 6.1 smo videli, da $P(t)$ zapišemo kot $(t-a_1)Q_1(t)$. Če nadomestimo t z a_i, kjer je $i \neq 1$, potem vidimo, da so $a_2, \ldots, a_d$ ničle polinoma $Q_1(t)$. V naslednjem koraku faktoriziramo $Q_1(t)$, in sicer kot $(t-a_2)Q_2(t)$, kjer so $a_3, \ldots, a_d$ ničle polinoma $Q_2(t)$. S ponavljanjem postopka dobimo $P(t) = (t-a_1)(t-a_2)\cdots(t-a_d)Q_d(t)$, kar pomeni, da je $P(t)$ vsaj stopnje d.

□

Privzemimo, da je $P_1(t) = P_2(t)$ za $t = 0, 1, ..., n-1$. Potem ima polinom $P(t) = P_1(t) - P_2(t)$ vsaj n ničel v $\mathcal{O}$. Ker je polinom P stopnje največ $m-1$, mora biti po izreku 6.1 ničeln polinom. Torej je $P_1 = P_2$.

Iz definicije 6.1 še ni razvidno, da imamo opravka z linearnimi kodami.

Izrek 6.2. *Reed–Solomonova koda v $\mathcal{O}$ z m sporočilnimi in n kodnimi simboli je linearna koda.*

Dokaz. Naj bo $a \in \mathcal{O}$ in naj bo $f(t), g(t) \in \mathcal{O}[t]$, kjer je $\deg f(t), \deg g(t) \leq m-1$. Dokaz temelji na dejstvu, da če sta polinoma $f(t)$ in $g(t)$ stopnje manjše ali enake $m-1$, potem sta polinoma $af(t)$ in $g(t) + f(t)$ tudi polinoma stopnje manjše ali enake $m-1$.

Naj bosta sporočili $s_1, s_2 \in \mathcal{O}^m$ kodirani v $P_{s_1}(t)$ in $P_{s_2}(t)$, kjer sta polinoma $P_{s_1}(t), P_{s_2}(t) \in \mathcal{O}[t]$ stopnje manjše ali enake $m-1$. Ker velja

$$\begin{aligned}
P_{s_1}(t) + P_{s_2}(t) &= \left(s_{1_{m-1}} t^{m-1} + s_{1_{m-2}} t^{m-2} + \cdots + s_{1_1} t + s_{1_0}\right) + \\
&\quad \left(s_{2_{m-1}} t^{m-1} + s_{2_{m-2}} t^{m-2} + \cdots + s_{2_1} t + s_{2_0}\right) \\
&= s_{1_{m-1}} t^{m-1} + s_{1_{m-2}} t^{m-2} + \cdots + s_{1_1} t + s_{1_0} + s_{2_{m-1}} t^{m-1} + s_{2_{m-2}} t^{m-2} + \cdots + s_{2_1} t + s_{2_0} \\
&= s_{1_{m-1}} t^{m-1} + s_{2_{m-1}} t^{m-1} + s_{1_{m-2}} t^{m-2} + s_{2_{m-2}} t^{m-2} + \cdots + s_{1_1} t + s_{2_1} t + s_{1_0} + s_{2_0} \\
&= \left(s_{1_{m-1}} + s_{2_{m-1}}\right) t^{m-1} + \left(s_{1_{m-2}} + s_{2_{m-2}}\right) t^{m-2} + \cdots + \left(s_{1_1} + s_{2_1}\right) t + \left(s_{1_0} + s_{2_0}\right) \\
&= P_{s_1+s_2}(t)
\end{aligned}$$

in

$$\begin{aligned}
aP_{s_1}(t) &= a\left(s_{1_{m-1}} t^{m-1} + s_{1_{m-2}} t^{m-2} + \cdots + s_{1_1} t + s_{1_0}\right) \\
&= a\left(s_{1_{m-1}} t^{m-1}\right) + a\left(s_{1_{m-2}} t^{m-2}\right) + \cdots + a\left(s_{1_1} t\right) + a\left(s_{1_0}\right) \\
&= \left(as_{1_{m-1}}\right) t^{m-1} + \left(as_{1_{m-2}}\right) t^{m-2} + \cdots + \left(as_{1_1}\right) t + \left(as_{1_0}\right) \\
&= P_{as_1}(t),
\end{aligned}$$

je Reed–Solomonova koda linearna koda.

□

Sedaj lahko izračunamo težo Reed–Solomonove kode.

Izrek 6.3. *Teža Reed–Solomonove kode v $\mathcal{O}$ z m sporočilnimi in n kodnimi simboli je enaka $n - m + 1$.*

Dokaz. Najprej bomo pokazali, da je teža vsaj $n - m + 1$. Glede na definicijo 6.1 moramo pokazati, da je za vsak neničelni polinom $P(t) \in \mathcal{O}[t]$, kjer je $\deg(P(t)) \leq m-1$, izmed števil $P(0), P(1), ..., P(n-1)$ vsaj $n-m+1$ neničelnih. Predpostavimo, da to ne drži. Predpostavimo torej, da obstaja polinom $P(t) \in \mathcal{O}[t]$ z $\deg(P(t)) \leq m-1$, za katerega velja, da je izmed števil $P(0), P(1), \ldots, P(n-1)$ kvečjemu $n-m$ neničelnih. Potem ima $P(t)$ vsaj m ničel med elementi iz $\mathcal{O}$. Po izreku 6.1 je $P(t)$ ničeln polinom. Zaključimo torej

lahko, da ima za vsak neničeln polinom $P(t) \in \mathcal{O}[t]$, vektor $[P(0)\ P(1)\ \cdots\ P(n-1)]$ težo vsaj $n-m+1$. Da pokažemo, da je teža enaka $n-m+1$ in zaključimo dokaz, moramo najti kodni vektor, ki ima težo točno $n-m+1$. Po definiciji 6.1 je to enako obstoju vektorja $P(t) \in \mathcal{O}[t]$ stopnje največ $m-1$, za katerega velja, da je med števili $P(0), P(1), \ldots, P(n-1)$ natanko $m-1$ ničelnih. Tak polinom je recimo polinom $P(t) = (t-a_1)(t-a_2)\cdots(t-a_{m-1})$, kjer so $a_1, a_2, \ldots, a_{m-1}$ poljubni različni elementi obsega $\mathcal{O}$, ki pripadajo množici $\{0, 1, 2, ..., n-1\}$.

□

Kar naredi Reed–Solomonove kode resnično uporabne, je obstoj preprostega algoritma za popravljanje napak in dekodiranja. Algoritem, o katerem bomo govorili, sta leta 1983 patentirala Berlekamp in Welch.

Od sedaj naprej bodo sledeče vrednosti predstavljale:

- m - število sporočilnih simbolov,
- $n = m + 2e$ - število kodnih simbolov,
- e - število napak, ki jih lahko koda popravi.

Proces dekodiranja se zanaša na dve lemi, kateri lahko dokažemo s pomočjo izreka 6.1.

Lema 6.2. *Naj bo poslana kodna beseda* $[P(0)\ P(1)\ \cdots\ P(n-1)]$ *in naj bo prejeti vektor* $[R_0\ R_1\ \cdots\ R_{n-1}]$. *Predpostavimo, da se je zgodilo največ* e *napak, tj. za največ* e *vrednosti velja* $R_i \neq P(i)$. *Potem obstajata taka neničelna polinoma* $E(t)$ *in* $Q(t)$, *da velja*

$$Q(i) = R_i E(i) \text{ za } i = 0, 1, \ldots n-1. \tag{6.1}$$

Pri tem je stopnja polinoma $E(t)$ *manjša ali enaka* e *in stopnja* $Q(t)$ *manjša ali enaka* $m+e-1$. *Vodilni koeficient polinoma* $E(t)$ *je enak* 1.

Dokaz. Naj bo $\{i_0, i_1, \ldots, i_{k-1}\}$ množica pozicij pojavitve napak. Torej, ko velja, da je $R_i \neq P(i)$. Naj bo

$$\begin{aligned} E(t) &= (t-i_0)(t-i_1)\cdots(t-i_{k-1}), \\ Q(t) &= P(t)E(t). \end{aligned}$$

Očitno je $E(t)$ stopnje k, kar je manjše ali enako od e po predpostavki. Ker je stopnja $P(t)$ manjša ali enaka od $m-1$, sledi, da je stopnja $Q(t)$ manjša ali enaka $m+e-1$. Da pokažemo, da enačba 6.1 velja za vsak i, morem pogledati, ko:

- i ni mesto napake. Potem je $R_i = P(i)$, torej je $Q(i) = P(i)E(i) = R_i E(i)$.

- i je mesto napake. V tem primeru i pripada množici $\{i_0, i_1, \ldots, i_{k-1}\}$. Po definiciji polinoma $E(t)$ je v tem primeru $E(i) = 0$ in je $Q(i) = P(i)E(i) = 0 = R_i E(i)$.

S tem smo pokazali, da enačba 6.1 drži.

□

Enačba 6.1 je ključna enačba za dekodiranje. Lema 6.2 nam pove, da ima enačba neničelne rešitve. Rešitev, ki je opisana pri dokazovanju leme, je koristna le v primeru, ko poznamo mesta napak. V praksi moramo rešiti sistem linearnih enačb za neznane koeficiente polinomov $E(t)$ in $Q(t)$. Lema nam zagotavlja, da obstaja neničelna rešitev za sistem linearnih enačb.

Lema 6.3. *Če $E(t)$ in $Q(t)$ zadovoljita enačbo 6.1 v lemi 6.2 in je število napak največ e, potem velja $Q(t) = P(t)E(t)$. Sledi, da $P(t)$ enak $Q(t)/E(t)$.*

Dokaz. Pri dokazovanju leme 6.2 smo pokazali, da obstaja rešitev za enačbo 6.1 s $Q(t) = P(t)E(t)$. Pokazati moramo, da to velja za vsako rešitev.

Ker je stopnja polinoma $Q(t)$ in polinoma $P(t)E(t)$ manjša ali enaka od $m + e - 1$, je prav tako tudi stopnja razlike polinomov $Q(t) - P(t)E(t)$ manjša ali enaka od $m + e - 1$. Če i ni mesto napake, potem je $P(i) = R_i$ in je $Q(i) - P(i)E(i) = 0$. Ker je takih mest po predpostavki vsaj $n - e$, ima polinom $Q(t) = P(t)E(t)$ vsaj $n - e = m + e$ ničel. Ker je stopnja polinoma $Q(t) - P(t)E(t)$ manjša od $m + e$, mora biti po izreku 6.1 $Q(t) - P(t)E(t) = 0$.

□

Glede na na zadnji dve lemi, lahko opišemo algoritem za dekodiranje.

Algoritem za dekodiranje

Naj bo poslana kodna beseda

$$[P_0\ P_1\ \cdots\ P_{n-1}],$$

prejeti vektor pa

$$[R_0\ R_1\ \cdots\ R_{n-1}].$$

Naj bosta $Q(t), E(t) \in \mathcal{O}[t]$ polinoma stopnje $m + e - 1$ in e:

$$\begin{aligned} Q(t) &= u_{m+e-1}t^{m+e-1} + u_{m+e-2}t^{m+e-2} + \cdots + u_1 t + u_0, \\ E(t) &= t^e + v_{e-1}t^{e-1} + \cdots + v_1 t + v_0. \end{aligned}$$

Koeficiente polinomov $Q(t)$ in $E(t)$ določimo tako, da bo veljalo $Q(i) = R_i E(i)$ za $i = 0, 1, \ldots, n-1$. Teh n enačb da sistem n linearnih enačb za n neznank (koeficientov polinomov $Q(t)$ in $E(t)$). Poiščemo neničelno rešitev tega sistema enačb ter tako dobimo $Q(t)$ in $E(t)$. Definirajmo sedaj polinom $P(t)$ kot $P(t) = Q(t)/E(t)$. Prejeti vektor $[R_0\ R_1\ \cdots\ R_{n-1}]$ dekodiramo v vektor $[x_0\ x_1\ \cdots\ x_{m-1}]$, kjer je $P(t) = x_{m-1}t^{m-1} + \cdots + x_1 t + x_0$.

Seveda se pojavi vprašanje, kaj se zgodi, če je več kot e napak v prejetem vektorju? Zgodi se lahko, da je sistem enačb nerešljiv. Lema 6.2 zagotavlja, da je v tem primeru pri prenosu prišlo do več kot e napak. Zgodi se tudi, da pri deljenju $Q(t)$ z $E(t)$ dobimo neničeln ostanek. V tem primeru nam lema 6.3 zagotavlja, da je pri prenosu prišlo do več kot e napak. Teh napak ni mogoče popraviti, vendar smo jih zaznali. Ni nujno, da bomo vsako napako odkrili, kar ima za posledico napačno dekodiranje sporočila.

Primer 6.2 Naj bo C koda v $\mathbb{Z}_5^4$ za besede iz $\mathbb{Z}_5^2$, ki zna popraviti eno napako.

Beseda	$P(0)$	$P(1)$	$P(2)$	$P(3)$	Kodna beseda
00	$0\cdot 0+0$	$0\cdot 1+0$	$0\cdot 2+0$	$0\cdot 3+0$	0000
01	$1\cdot 0+0$	$1\cdot 1+0$	$1\cdot 2+0$	$1\cdot 3+0$	0123
02	$2\cdot 0+0$	$2\cdot 1+0$	$2\cdot 2+0$	$2\cdot 3+0$	0241
03	$3\cdot 0+0$	$3\cdot 1+0$	$3\cdot 2+0$	$3\cdot 3+0$	0314
04	$4\cdot 0+0$	$4\cdot 1+0$	$4\cdot 2+0$	$4\cdot 3+0$	0432
10	$0\cdot 0+1$	$0\cdot 1+1$	$0\cdot 2+1$	$0\cdot 3+1$	1111
11	$1\cdot 0+1$	$1\cdot 1+1$	$1\cdot 2+1$	$1\cdot 3+1$	1234
12	$2\cdot 0+1$	$2\cdot 1+1$	$2\cdot 2+1$	$2\cdot 3+1$	1302
13	$3\cdot 0+1$	$3\cdot 1+1$	$3\cdot 2+1$	$3\cdot 3+1$	1420
14	$4\cdot 0+1$	$4\cdot 1+1$	$4\cdot 2+1$	$4\cdot 3+1$	1043
20	$0\cdot 0+2$	$0\cdot 1+2$	$0\cdot 2+2$	$0\cdot 3+2$	2222
21	$1\cdot 0+2$	$1\cdot 1+2$	$1\cdot 2+2$	$1\cdot 3+2$	2340
22	$2\cdot 0+2$	$2\cdot 1+2$	$2\cdot 2+2$	$2\cdot 3+2$	2413
23	$3\cdot 0+2$	$3\cdot 1+2$	$3\cdot 2+2$	$3\cdot 3+2$	2031
24	$4\cdot 0+2$	$4\cdot 1+2$	$4\cdot 2+2$	$4\cdot 3+2$	2104
30	$0\cdot 0+3$	$0\cdot 1+3$	$0\cdot 2+3$	$0\cdot 3+3$	3333
31	$1\cdot 0+3$	$1\cdot 1+3$	$1\cdot 2+3$	$1\cdot 3+3$	3401

Beseda	$P(0)$	$P(1)$	$P(2)$	$P(3)$	Kodna beseda
32	$2\cdot 0+3$	$2\cdot 1+3$	$2\cdot 2+3$	$2\cdot 3+3$	3024
33	$3\cdot 0+3$	$3\cdot 1+3$	$3\cdot 2+3$	$3\cdot 3+3$	3142
34	$4\cdot 0+3$	$4\cdot 1+3$	$4\cdot 2+3$	$4\cdot 3+3$	3210
40	$0\cdot 0+4$	$0\cdot 1+4$	$0\cdot 2+4$	$0\cdot 3+4$	4444
41	$1\cdot 0+4$	$1\cdot 1+4$	$1\cdot 2+4$	$1\cdot 3+4$	4012
42	$2\cdot 0+4$	$2\cdot 1+4$	$2\cdot 2+4$	$2\cdot 3+4$	4130
43	$3\cdot 0+4$	$3\cdot 1+4$	$3\cdot 2+4$	$3\cdot 3+4$	4203
44	$4\cdot 0+4$	$4\cdot 1+4$	$4\cdot 2+4$	$4\cdot 3+4$	4321

V tem primeru bomo pokazali postopek dekodiranja za prejeti vektor 3124, pri katerem je prišlo do napake pri prenosu.

Najprej določimo polinoma $Q(t)$ in $E(t)$ tako, da bo veljalo $Q(i) = R_i E(i)$ za $i = 0, 1, 2, 3$. Polinom $Q(t)$ je stopnje $m + e - 1 = 2 + 1 - 1 = 2$, torej $Q(t) = u_2 t^2 + u_1 t + u_0$. Polinom $E(t)$ pa je stopnje $e = 1$ in ima vodilni koeficient 1. Torej je $E(t) = t + v_0$. Za $i = 0, 1, 2, 3$ tako dobimo štiri linearne enačbe s štirimi neznankami:

$$u_2 i^2 \;+\; u_1 i \;+\; u_0 \;=\; R_i \;(\; i \;+\; v_0 \;).$$

Če vstavimo vrednosti v enačbe, dobimo:

$$\begin{aligned}
u_2\cdot 0^2 \;+\; u_1\cdot 0 \;+\; u_0 \;&=\; 3 \;\cdot\; (0 \;+\; v_0),\\
u_2\cdot 1^2 \;+\; u_1\cdot 1 \;+\; u_0 \;&=\; 1 \;\cdot\; (1 \;+\; v_0),\\
u_2\cdot 2^2 \;+\; u_1\cdot 2 \;+\; u_0 \;&=\; 2 \;\cdot\; (2 \;+\; v_0),\\
u_2\cdot 3^2 \;+\; u_1\cdot 3 \;+\; u_0 \;&=\; 4 \;\cdot\; (3 \;+\; v_0).
\end{aligned}$$

Ker je obseg $\mathbb{Z}_5$, dobimo:

$$\begin{aligned}
u_0 \;+\; v_0\cdot 2 \;&=\; 0,\\
u_2 \;+\; u_1 \;+\; u_0 \;+\; v_0\cdot 4 \;&=\; 1,\\
u_2\cdot 4 \;+\; u_1\cdot 2 \;+\; u_0 \;+\; v_0\cdot 3 \;&=\; 4,\\
u_2\cdot 4 \;+\; u_1\cdot 3 \;+\; u_0 \;+\; v_0\cdot 1 \;&=\; 2.
\end{aligned}$$

Rešitev sistema je $u_2 = 2$, $u_1 = 1$, $u_0 = 2$ in $v_0 = 4$, kar pomeni, da sta polinoma $Q(t)$ in $E(t)$ enaka:

$$\begin{aligned} Q(t) &= 2t^2 + t + 2, \\ E(t) &= t + 4. \end{aligned}$$

Nato izračunamo polinom $P(t)$, ki je enak kvocientu

$$P(t) = \frac{2t^2 + t + 2}{t + 4} = 2t + 3.$$

Iz tega sledi, da je izvirno sporočilo beseda 32.

Literatura

[1] J. Justesen, T. Høholdt, *A Course in Error-Correcting Codes (EMS Textbooks in Mathematics)*, European Mathematical Society, February 2004.

[2] F. MacWilliams, N. Sloane, *Theory of Error-correcting Codes*, Elsevier, 1977.

[3] I. S. Reed, G. Solomon, Polynomial codes over certain finite fields, *Journal of the Society for Industrial and Applied Mathematics* **8** (1960), 300–304.

[4] C. Shannon, A mathematical theory of communication, *Bell Labs Technical Journal* **27** (1948), 300–304,623–656.

[5] J. H. V. Van Lint, *Introduction to Coding Theory (Graduate Texts in Mathematics)*, Springer, 1999.