110L

Artur Baxhaku, Ardi Benusi

Problema dhe Ushtrime për Teorinë e Kodimit

Tiranë, 2010

Problema dhe Ushtrime
për Teorinë e Kodimit

Prof. Artur Baxhaku
Departamenti i Matematikës
Fakulteti i Shkencave Natyrore,
Universiteti i Tiranës

Ardi Benusi
Departamenti i Teknologjisë së Informacionit
Banka Kombëtare Tregëtare

ISBN: 978-99956-34-57-5

Shtëpia botuse: "albPAPER"

Punuan dhe faqosën në kompjuter: Autorët

Kopertina: Orest Muça

Pasqyra e Lëndës

Hyrje

Claude Shannon me studimin "Teoria matematike e transmetimit", botuar më 1949 provoi se, në një kanal transmetimi me zhurma, duke përdorur teknikat e kodimit dhe të dekodimit mund të arriheshin komunikime me shkallë informacioni sado afër kapacitetit të kanalit. Kjo shënoi lindjen e teorisë së kodimit, një fushë që studion transmetimin e informacionit në një kanal me zhurma, zbulimin e gabimeve dhe ndreqjen e mesazheve të dëmtuara.

Teoria e kodimit ka njohur një zhvillim shumë të madh dhe aplikimet e saj janë të shumta. Ato shtrihen tashmë në shumë fusha të teknologjisë, që variojnë nga sistemet e komunikimit, tek lexuesit e disqeve të muzikës dhe tek tekonologjia pajisjeve të ruajtjes së informacionit.
Megjithëse problemet në teorinë e kodimit kanë lindur nga aplikimet inxhinierike, është e rëndësishme të theksohet aspekti matematik në zhvillimin dhe studimin e kodeve të ndryshme. Rëndësia e algjebrës, kombinatorikës dhe gjeometrisë në zhvillimin e teorisë së kodimit është një fakt i njohur me anë të shumë rezultateve që kanë ndihmuar ecjen dhe zhvillimin përpara të kësaj teorie.
Libri "Probleme dhe Ushtrime për Teorinë e Kodimit", ka shumë gjasë të jetë sprova e këtij tipi e botuar në Shqipëri. Përvoja në auditor e autorëve ka nxjerrë në pah rolin e madh e të pazëvendësueshëm të problemeve dhe ushtrimeve në procesin e përvetësimit të teorisë së kodimit nga studentët. Prej kohësh autorët, por dhe studentët e degës së informatikës, apo dhe ndjekësit e studimeve pasuniversitare në drejtimet e zbatuara të matem-

atikës apo të informatikës kanë ndjerë nevojën e një përmbledhje të tillë problemesh e ushtrimesh të teorisë së kodimit. Libri që po paraqesim synon plotësimin e kësaj mungese.
Duke pasur parasysh gamën e madhe të kodeve të ndërtuara deri tani, janë përzgjedhur ushtrime kryesisht të bazuara në kodet bllok lineare dhe ato ciklike. Libri është i organizuar në 7 krerë. Në kreun e parë trajtohen ushtrime të përgjithshme mbi llojet e kodeve dhe vetitë e tyre. Në kreun e dytë trajtohen ushtrime mbi teorinë e informacionit; burimin e informacionit, entropinë dhe ngjeshjen e informacionit. Në kreun e tretë fillon shkëputja nga burimi i informacionit dhe trajtohen ushtrime që mbulojnë aspekte të kodeve si; aftësitë zbuluese dhe ndreqëse të gabimeve, kodet e përsosura, ekuivalenca e kodeve etj. Në kreun e katërt, trajtohen kodet lineare. Gama e ushtrimeve në këtë kre është mjaft e gjerë duke pasur parasysh edhe strukuturën e pasur algjebrike të këtyre kodeve. Kreu i pestë ofron ushtrime për disa kode të veçanta lineare si kodet *Hamming*, kodet *Reed − Muller*, kodet *Golay* etj. Kreu i gjashtë, fokusohet në dekodimin e kodeve lineare me anë të tabelave standard. Kodet ciklike janë të trajtuara në kreun e shtatë së bashku me një grup ushtrimesh nga polimonet në fushat e fundme.
Libri përmban rreth 200 ushtrime, ku një pjesë e mirë e tyre janë të zgjidhura plotësisht. Disa prej tyre janë të shoqëruara me udhëzimet e nevojshme dhe pjesa tjetër u është lënë studentëve për punë të pavarur. Ky libër është shkruar për t'u ardhur në ndihmë studentëve të degëve informatikë dhe matematikë për të plotësuar njohuritë e tyre mbi teorinë e kodimit. Me gjithë kujdesin për të paraqitur një punë të arrirë, autorët janë të ndërgjegjshëm që në këtë sprovë të parë nuk mund të shmangen mungesat e pasaktësitë, apo dhe ndonjë mbivendosje; prandaj ata mirëpresin çdo vërejtje e sugjerim nga përdoruesit e këtij libri duke e inkuadruar në përpjekjet e tyre për përmirësimin e cilësisë së këtij libri dhe i falenderojnë ata paraprakisht.

Autorët
Tetor 2009

Kreu 1

Kodimi dhe Dekodimi

1.1 Përkufizime dhe veti

Për bashkësitë e dhëna $\mathcal{A}$ (alfabeti i burimit) dhe $\mathcal{B}$ (alfabeti i kodit), kodim quhet çdo funksion K i $\mathcal{A}$ në bashkësinë $\mathcal{B}^*$ të vargjeve të fundme me elemente në $\mathcal{B}$. Shëmbëllimet e elementëve të $\mathcal{A}$, quhen fjalë kode dhe bashkësia e të gjitha fjalëve kod quhet kod. Në qoftë se $|\mathcal{A}| = r$(alfabeti i kodit ka r simbole), kodi quhet $r - ar$ ose me rreze r.
Me këtë përkufizim, mesazhi $x_1, x_2, \ldots, x_n$ ku $x_i \in \mathcal{A}$ do të kodohej me anë të funksionit K^* si:

$$K^*(x_1 x_2 \ldots x_n) = K(x_1)K(x_2)\ldots K(x_n).$$

Kodimi (ose kodi) quhet i dekodueshëm në mënyrë të vetme, në qoftë se K^* është injektiv.
Kodimi që fjalët i ka të gjitha me gjatësi n, quhet kod bllok me gjatësi n.
Kodimi quhet instantan në qoftë se asnjë fjalë kod nuk ka si prefiks ndonjë fjalë kod tjetër.
Kodet instantane janë edhe të dekodueshëm në mënyrë të vetme, kurse e anasjellta nuk është e vërtetë.

1.2 Teorema Kraft

Dy pohimet e teoremës Kraft janë:

1. Për një kod instantan $r - ar$ me gjatësi të fjalëkodeve $d_1, d_2, \ldots, d_n$, ka vend mosbarazimi:

$$\sum_{i=1}^{n} \frac{1}{r^{d_i}} \leqslant 1.$$

2. Në qoftë se numrat $d_1, d_2, \ldots, d_k$ plotësojnë mosbarazimin e mësipërm, atëhere ekziston një kodim instantan $r-ar$ me gjatësi të fjalëve kod $d_1, d_2, \ldots, d_k$.

1.3 Teorema McMillan

Çdo kodim i dekodueshëm në mënyrë të vetme kënaq mosbarazimin Kraft.
Rrjedhim i kësaj teoreme është :
Për çdo kod të dekodueshëm në mënyrë të vetme ekziston një kod instantan me të njëjtat gjatësi të fjalëve kod.

1.4 Ushtrime dhe problema

1. Cila është gjatësia më e vogël e një kodi bllok me alfabet burimi $\{A, B, \ldots, Z\}$ e me të njëjtin alfabet kodi { . , − , hapësirë} si dhe kodi Mors?

2. Kontrolloni nëse të mëposhmit janë *ISBN*:

$$\begin{array}{lllll} 0 & - & 13165322 & - & 6 \\ 0 & - & 1392-4101 & - & 4 \\ 07 & - & 028761 & - & 4 \end{array}$$

3. *ISBN*-të e mëposhtme janë marrë me fshirje. Sa janë shifrat që mungojnë?

$$\begin{array}{lll} 0131x9139 & - & 9 \\ 0-02-32xx80 & - & 0 \end{array}$$

4. A është i aftë kodi *ISBN* të gjejë çdo gabim njësh (pra gabim në një shifër)?

5. A është i aftë kodi *ISBN* të gjejë çdo gabim dysh (pra kur gabohet në dy shifra)?

6. A është i aftë kodi *ISBN* të dallojë këmbime vendesh të dy prej shifrave (me vlera të ndryshme) të tij?

7. Konsiderojmë kodin C të të gjithë numrave me 10 shifra mbi alfabetin $\{0,1,2,3,4,5,6,7,8,9\}$, me vetinë që shuma e të dhjetë shifrave plotpjestohet nga 11, pra:

$$C = \left\{ x_1 x_2 x_3 \ldots x_{10} \;\middle|\; \sum_{i=1}^{10} x_i \equiv 0 \pmod{11} \right\}.$$

Tregoni që C mund të gjejë gabime njëshe. A ka të meta në krahasim me kodin *ISBN*?

8. Nëntë shifrat e para të numrit *ISBN* të një libri janë $0-13-869017$.

   (a) Të gjendet shifra e fundit e tij.

   (b) Të gjendet kodi *EAN* i këtij numri sipas vendimit të ISO (duke i shtuar prefiksin 978).

9. Është dhënë kodi më poshtë:

$$1 \to 01,\ 2 \to 011,\ 3 \to 10,\ 4 \to 1000,\ 5 \to 1100,\ 6 \to 0111.$$

   (a) A është instantan ky kod?

   (b) Në qoftë se jo, a mund të gjendet një kod instantan me të njëjtat gjatësi të fjalëve kod?

10. A është kodi i mëposhtëm i dekodueshëm në mënyrë të vetme?

$A \to 1010$, $B \to 001$, $C \to 101$, $D \to 0001$, $E \to 1101$, $F \to 1011$

11. A mund të përcaktohet nëse kodet e mëposhtëm:

a. $A \to 001$, $B \to 1001$, $C \to 0010$, $D \to 1110$, $E \to 1010$, $F \to 01110$, $G \to 0101$,
b. $A \to 00$, $B \to 10$, $C \to 011$, $D \to 101$, $E \to 111$, $F \to 110$, $G \to 010$

janë të dekodueshëm në mënyrë të vetme duke përdorur mosbarazimin Kraft?

12. Ndërtoni nëse ka, një kod instantan, me parametra si më poshtë:

(a) Kod binar me gjatësi të fjalëve kod:

$$1, 3, 3, 3, 4, 4$$

(b) Kod me alfabet $\{0, 1, 2, 3, 4\}$ dhe gjatësi të fjalëve kod:

$$1, 1, 1, 1, 1, 8, 9$$

DSH (c) Kod me alfabet $\{0, 1, 2, 3, 4\}$ dhe gjatësi të fjalëve kod:

$$1, 1, 1, 1, 2, 2, 3, 3, 4$$

13. Sa fjalë me gjatësi 5, mund t'i shtohen kodit instantan binar $\{0, 10, 110\}$, pa prishur vetinë e të qenit instantan?

14. Jepet burimi $S = \{A, B, C\}$ dhe kodi C që kodon këtë burim si më poshtë:

$$C = \{1, 01, 001\}$$

$$A \to 1,\ B \to 01,\ C \to 001$$

A është kodi instantan? Po i deshifrueshëm në mënyrë të vetme?

15. Të ndërtohet një kod instantan binar për alfabetin e mëposhtëm të burimit dhe gjatësitë përkatëse të fjalëve kod:

simboli	A	B	C	D	E	F	G	H	I	J	K	L
gjatësia	2	4	7	7	3	4	7	7	3	4	7	7

16. Të ndërtohet një kod instantan ternar (me tre simbole kodi) për alfabetin e mëposhtëm të burimit dhe gjatësitë përkatëse të fjalëve kod:

simboli	1	2	3	4	5	6	7	8	9	0
gjatësia	1	3	3	3	3	2	2	2	2	2

17. Ndërtoni një kod binar me vetinë që:

(a) Të jetë i deshifrueshëm në mënyrë të vetme, por jo instantan.

(b) Gjatësitë e fjalëve kod të plotësojnë mosbarazimin Kraft, por kodi të mos jetë instantan.

18. Sa simbole kodi nevojiten për të koduar burimin e mëposhtëm në një kod instantan me gjatësitë e dhëna të fjalëve kod:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	2	2	2	1	2	2	2	1	2	2	2	2	2	1	2

Kreu 2

Entropia dhe ngjeshja. Kodet Huffman

2.1 Përkufizime dhe veti

Një burim informacioni është një çift i renditur (S, P), ku $S = \{x_1, x_2, \ldots, x_n\}$ është një bashkësi (e fundme, e quajtur *bashkësi e simboleve të burimit*) dhe $P = \{p(x_1), p(x_2), \ldots, p(x_n)\}$ është një shpërndarja probabilitare mbi S.
Në qoftë se $P = \{p_1, p_2, \ldots, p_n\}$ është një shpërndarje probabilitare, madhësia

$$H_b(p_1, p_2, \ldots, p_n) = -\sum_{i=1}^{n} p_i \cdot \log_b p_i,$$

quhet entropi $b - are$ e shpërndarjes P.
Në qoftë se X është ndryshorja diskrete e rastit me vlera në P, entropia mund të shkruhet $H(X)$. Në qoftë se P është shpërndarje probabilitare mbi S, atëhere entropia mund të shkruhet $H(S)$. Nuk bëhet ndonjë dallim midis $H(P)$, $H(S)$ dhe $H(X)$.
Entropia ka këto veti:

1. $0 \leqslant H_b(P) \leqslant \log_b n$. $H_b(P)$ arrin vlerën maksimale për shpër-

ndarjen uniforme të probabiliteteve:

$$H_b(P) = 1 \iff p(x_i) = \frac{1}{n}, \ \forall i \in \{1, \ldots, n\}.$$

$H_b(P)$ arrin vlerën minimale kur ndonjë nga simbolet e burimit ka probabilitet 1:

$$H_b(P) = 0 \iff \exists i \in \{1, \ldots, n\} \ : p(x_i) = 0.$$

2. Në qoftë se X dhe Y, janë ndryshore rasti diskrete të pavarura, ka vend:

$$H(X,Y) \leqslant H(X) + H(Y).$$

Barazimi arrihet kur X dhe Y janë të pavarura.

Zgjerimi i n-të i burimit (S,P) shënohet (S^n, P^n), ku S^n është bashkësia e fjalëve $\mathbf{x}$ me gjatësi n mbi S dhe P^n, probabiliteti i shpërndarjes i përcaktuar për $\mathbf{x}=x_1, x_2, \ldots, x_n$ si:

$$P^n(\mathbf{x}) = p(x_1) \cdot p(x_2) \ldots \cdot p(x_n)$$

Për shtrirjen e n-të të burimit (S,P) ka vend:

$$H(P^n) = n \cdot H(P)$$

2.2 Kodimi i burimit

$\mathcal{A}=\{a_1, \ldots, a_r\}$ është një bashkësi e fundme që quhet alfabet. Një varg (i fundmë) simbolesh nga $\mathcal{A}$ quhet fjalë. Gjatësia e një fjale është numri i simboleve të saj. $\mathcal{A}^*$ është bashkësia e të gjitha fjalëve me alfabet $\mathcal{A}$.

Kod mbi një burim (S,P), për alfabetin e zgjedhur $\mathcal{A}$, është quajtur çifti i renditur (C,f) i tillë që:

1. C është një bashkësi joboshe fjalësh nga $\mathcal{A}^*$. Elementët e C quhen fjalë kode. Bashkësia $\mathcal{A}$ quhet alfabet i kodit. Në qoftë se $|\mathcal{A}| = r$, kodi quhet $r-ar$.

2. f është një funksion(pasqyrim) injektiv i simboleve të burimit $\{x_1, x_2, \ldots, x_n\}$ tek fjalë kodet e $C = \{c_1, \ldots, c_n\}$:

$$\begin{aligned} f: S &\to C \\ x_i &\to \mathcal{A}^* \end{aligned} \tag{2.1}$$

Gjatësi mesatare e fjalëve kod të një kodi C, f që kodon burimin $S = \{x_1, \ldots, x_n\}$ me shpërndarje të probabiliteteve $P = \{p_1, \ldots, p_n\}$ quhet madhësia:

$$L(S) = \sum_{i=1}^{n} d_i \cdot P(x_i),$$

ku $d_i = |c_i|$ është gjatësia e fjalë kodit c_i që kodon x_i.

2.3 Teorema Shanon e kodimit pa zhurma

Për një burim (S,P) shënohet me $L_{min}(S)$ gjatësia mesatare më e vogël midis të gjithë kodeve instantane që kodojnë burimin S. Kanë vend:

1. $H(S) \leqslant L_{min}(S) \leqslant H(S) + 1$.

2. $\lim\limits_{k \to \infty} \frac{L_{min}(S^k)}{k} = H(S)$. Kjo njihet me emrin Teorema Shanon e kodimit pa zhurma, që tregon se me anë të një kodimi të përshtatshëm, informacioni i koduar mund të ngjeshet sa të duam afër entropisë së burimit.

2.4 Kodet Huffman

Kodet Huffman kodojnë një burimin (S,P) me gjatësinë mesatare më të vogël midis të gjitha kodimeve instantane të burimit S. Kodet Huffman janë kode instantane. Kodimi Huffman në shkencat kompjuterike është një algoritëm që përdoret për ngjeshjen (kompresimin) pa humbje të të dhënave. Algoritmi Huffman përdor tabelat e kodeve me gjatësi variabël për të koduar simbolet e burimit të informacionit. Secila tabelë përftohet nga paraardhësja nëpërmjet reduktimeve të shpërndarjes probabilitare P.

2.5 Ushtrime dhe problema

1. Të llogaritet $H_2(\frac{1}{8}, \frac{1}{8}, \frac{3}{4})$.

2. Të llogaritet $H_2(\frac{1}{3}, \frac{2}{3})$.

3. Tregoni që:

$$H(p_1, p_2, \dots, p_n) = H(p_1, p_2, \dots, p_n, 0)$$

Si shpjegohet rezultati i mësipërm?

4. Të gjendet entropia e burimit të mëposhtëm të informacionit:

Simboli	1	2	3	4	5	6
Probabiliteti	0.1	0.1	0.45	0.05	0.2	0.1

5. Burimi S përbëhet nga rezultatet e dy hedhjeve të pavarura të një zari dhe të një monedhe të rregullt. A është sasia e informacionit e S më e madhe se sasia e burimit që përftohet nga rezultatet e hedhjeve të pavaruara të tri monedhave të rregullta? Po sa hedhja e pavarur e katër monedhave të rregullta?

6. Burimi S përbëhet nga rezultatet e dy hedhjeve të njëpasnjëshme të një zari e të një monedhe. Herën e parë hidhet një zar i regullt, i cili ka dy faqe të shënuara me numër 1, dy faqe të tjera me numër 2 dhe dy të tjerat me numër 3. Herën e dytë, hidhet një monedhë e rregullt, aq herë sa është shënuar në faqen e sipërme të zarit në hedhjen e parë. Sa është entropia e këtij burimi?

7. Supozojmë hedhjen e pavarur të dy zareve të rregullta. Sa është sasia e informacionit kur:

   (a) Burimi i informacionit përbëhet nga shuma e pikëve të rezultatit të provës.

   (b) Burimi i informacionit përbëhet nga çiftet (a, b), ku a është numri i faqes së sipërme pas hedhjes së zarit të parë dhe b numri i faqes së sipërme pas hedhjes së zarit të dytë.

8. Cila garë ka papërcaktueshmërinë më të madhe, ajo në të cilën janë 7 garistë, 3 nga të cilët kanë probabilitet $\frac{1}{6}$ për të fituar dhe 4 të tjerët $\frac{1}{8}$, apo 8 garistë, dy prej të cilëve e kanë probablitetin e fitimit $\frac{1}{4}$ dhe 6 të tjerët $\frac{1}{12}$?

9. Një qitës që rrok shenjën me probabilitet $\frac{1}{2}$ shtin dy herë dhe një tjetër që rrok shenjën me probabilitet $\frac{1}{3}$ shtin 3 herë. Cila shenjë "merr më shumë informacion"(pra ka entropi më të madhe)?

10. Ndërtoni një kod Huffman binar, ternar dhe kuaternar për burimin me shpërndarje të probabiliteteve si më poshtë:

$$P = \{0.9,\ 0.02,\ 0.02,\ 0.02,\ 0.02,\ 0.02\}.$$

Në secilin rast të gjendet gjatësia mesatare e kodeve të ndërtuara.

11. Jepet burimi me shpërndarje të probabiliteteve si më poshtë:

$$P = \{0.3,\ 0.05,\ 0.03,\ 0.02,\ 0.3,\ 0.1,\ 0.15,\ 0.05\}$$

Të ndërtohet një kod Huffman dhe të gjendet gjatësia mesatare e tyre për:

   (a) Kodin ternar.

   (b) Kodin me alfabet $\{0, 1, 2, 3\}$.

   (c) Kodin me alfabet $\{0, 1, 2, 3, 4\}$.

12. Një burim S emeton simbolet A, B ku A shfaqet me probabilitet $\frac{1}{4}$ dhe B me probabilitet $\frac{3}{4}$.

(a) Të ndërtohet një kod binar Huffman për S.

(b) Të ndërtohet një kod binar Huffman për shtrirjen e dytë të S.

(c) Të gjenden gjatësitë mesatare të kodeve të ndërtuara.

13. Probabiliteti i shfaqjes së simboleve të burimit $S = \{a, b, c\}$ është $P = \{\frac{2}{3}, \frac{2}{9}, \frac{1}{9}\}$.

(a) Të ndërtohet një kod binar Huffman për S.

(b) Të ndërtohet një kod binar Huffman për shtrirjen e dytë të S.

(c) Të gjenden gjatësitë mesatare të kodeve të ndërtuara.

14. Një mesazh është shkruar me simbolet e burimit A, B, C, D ku A shfaqet 7 herë më shpesh se secili nga simbolet e tjerë. A ekziston një kodim binar që nuk kërkon mesatarisht më shumë se 1.4 bit për simbol? Në qoftë se po, të gjendet ai. (Të merret: $\log_2 7 = 2.807$, $\log_2 10 = 3.322$)

15. Përpiquni të gjeni tepricën në gjuhën shqipe me metodën e mëposhtëme: Kopjoni një paragraf nga një libër dhe, duke fshirë çdo gërmë të n-të, i kërkoni një shoku të lexojë paragrafin. Provoni $n = 2, 3, 4, 5, 6$.
Në qoftë se arrini në përfundimin se një paragraf me çdo gërmë të pestë mangut zakonisht mund të lexohet (kuptohet), atëherë do të quani që teprica e gjuhës (të paktën për leksikun e atij paragrafi) është të paktën 1/5, ose 20%.

16. Një kanal transmeton simbolet e barazmundëshme 0 e 1. Sa është probabiliteti i marrjes së mesazhit 01101? Sa është entropia e mesazheve prej 5 simbolesh?

17. Raporti i entropisë së një burimi informacioni S me gjatësinë mesatare të një kodi binar Huffman të tij quhet *Efektivitet* [$Ef(S)$] i atij burimi informacioni.

(a) Të provohet se efektiviteti ndodhet midis 0 e 1 dhe të studiohen vlerat ekstreme. Gjeni efektivitetin e burimeve të mëposhtëme:

	A	B	C	D	E	F	G	H
S1	$\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{8}$
S2	0.1	0.2	0.1	0.3	0.05	0.1	0.05	0.1
S3	0.15	0.15	0.15	0.15	0.1	0.1	0.1	0.1

(b) Të gjendet $\lim_{k\to\infty} Ef(S^k)$.

18. Le të jetë $X = \{a, b, c, d\}$ me shpërndarjen e probabiliteteve:

x	a	b	c	d	e
p(x)	0.05	0.1	0.12	0.13	0.6

Të gjenden gjatësia mesatare e një kodi Huffman, entropia dhe efektiviteti i tij.

19. Një burim emeton simbolet A, B, C, D, ku A shfaqet dy herë më shpesh se secili nga simbolet e tjera. A ekziston një kodim binar i tij që nuk kërkon më shumë se a) 1.99 bit për simbol, b) 1.92 bit? Në qoftë se po, të gjendet një i tillë.

20. Për burimin me simbole A, B, C, D ku A shfaqet dy herë më shpesh se secili nga simbolet e tjera, të gjendet:

(a) efektiviteti i tij;

(b) efektiviteti i shtrirjes së dytë të tij.

21. Për burimin me simbole A, B, C, D ku A shfaqet tri herë më shpesh se secili nga simbolet e tjera, të gjendet:

(a) efektiviteti i tij;

(b) efektiviteti i shtrirjes së dytë të tij.

22. Për burimin me simbole A, B, C, D ku A shfaqet katër herë më shpesh se secili nga simbolet e tjera, të gjendet:

    (a) efektiviteti i tij;

    (b) efektiviteti i shtrirjes së dytë të tij.

23. Për burimin me simbole A, B, C, D ku A shfaqet pesë herë më shpesh se secili nga simbolet e tjera, të gjendet:

    (a) efektiviteti i tij;

    (b) efektiviteti i shtrirjes së dytë të tij.

24. Për burimin me simbole A, B, C, D ku A shfaqet gjashtë herë më shpesh se secili nga simbolet e tjera, të gjendet:

    (a) efektiviteti i tij;

    (b) efektiviteti i shtrirjes së dytë të tij.

25. Gjej efektivitetin e një burimi binar S në të cilin 0 ka probabilitet 0.89. Të gjendet një shtrirje e S me efektivitet

    (a) të paktën 75%;

    (b) të paktën 90%.

Kreu 3

Kodet gabimndreqëse

3.1 Përkufizime dhe veti

Le të jetë $\mathcal{A}=\{a_1, a_2, \ldots, a_n\}$ një bashkësi e fundme me q elemente, të cilën e quajmë alfabet dhe elementet e saj simbole. Si alfabete të kodit zakonisht merren fushat e fundme $\mathbb{F}_q$.

1. Një fjalë $q-are$ me gjatësi n në $\mathcal{A}$ është një varg simbolesh $\omega_1, \omega_1, \ldots, \omega_n$, ku $\omega_i \in \mathcal{A}\ \forall i \in \{1, \ldots, n\}$.

2. Një kod bllok me gjatësi n mbi $\mathcal{A}$ është një bashkësi joboshe C e fjalëve $q-are$ me gjatësi n. Elementet e C quhen fjalë kode dhe kodi bllok, kod $q-ar$ me gjatësi n.

3. Numri i fjalë kodeve në C, shënohet me $|C|$ ose M dhe quhet madhësi e kodit.

4. Shkallë informacioni e kodit C me gjatësi n quhet madhësia $R = (\log_q |C|)/n$.

5. Një kod me gjatësi n dhe madhësi M shënohet kod (n, M).

Distanca *Hamming* $d(\mathbf{x}, \mathbf{y})$ e fjalëve $\mathbf{x}$ dhe $\mathbf{y}$ është e barabartë me numrin e pozicioneve në të cilat këto fjalë ndryshojnë. Për çdo tri fjalë $\mathbf{x}$, $\mathbf{y}$, $\mathbf{z}$ me gjatësi n nga i njëjti kod bllok kanë vend:

1. $0 \leq d(\mathbf{x}, \mathbf{y}) \leq n$.
2. $d(\mathbf{x}, \mathbf{y}) = 0 \iff \mathbf{x} = \mathbf{y}$.
3. $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{y}, \mathbf{x})$.
4. (Mosbarazimi i trekëndëshit). $d(\mathbf{x}, \mathbf{z}) \leq d(\mathbf{x} + \mathbf{y}) + d(\mathbf{y}, \mathbf{z})$.

Për një kod që ka të paktën dy fjalë kode, distanca(minimale) e C, që shënohet me d, është:

$$d(C) = min\{d(\mathbf{x}, \mathbf{y}) \colon \mathbf{x}, \mathbf{y} \in C, \mathbf{x} \neq \mathbf{y}\}.$$

Një kod (n, M) me distancë d, shënohet dhe (n, M, d). Numrat (n, M, d) njihen si parametra të kodit.
Një kod bllok, quhet që gjen (zbulon, dedekton) t gabime në qoftë se për çdo fjalë kod x dhe çdo fjalë y që merret nga x duke ndryshuar $1, 2, \ldots, t$ simbole, y nuk është fjalë kod.
Një kod gjen C t gabime vetëm kur $d(C) > t$.
Një kod ndreq t gabime vetëm kur $d(C) > 2t$.
Dy kode $q - are$ janë ekuivalente në qoftë se njëri mund të përftohet nga tjetri:

1. Duke përkëmbyer pozicionet e simboleve të fjalëve kod.
2. Duke përkëmbyer simbolet në pozicionet fikse të fjalëve kod.

Problemi kryesor i teorisë së kodimit është optimizimi i njërit nga parametrat n, M, d, kur jepen vlerat e dy parametrave të tjerë. Me $A_q(n, d)$ shënohet vlera më e madhe e M e tillë që ekziston një kod $q - ar$ (n, M, d). Kanë vend:

1. $A_q(n, 1) = q^n$.
2. $A_q(n, n) = q$.

3.2 Kodet e përsosura

$\mathbb{F}_q^n$ është bashkësia e fjalëve me gjatësi n mbi alfabetin $\{0, 1, \ldots, q-1\}$.
Për çdo fjalë $x \in \mathbb{F}_q^n$ dhe çdo $r \geq 0$, sfera me rreze r dhe qendër x përcaktohet si:

$$S_q(c, r) = \{x \in \mathbb{F}_q^n | d(x, c) \leq r\}.$$

Një sferë me rreze $0 \leq r \leq n$ në $\mathbb{F}_q^n$, përmban:

$$\sum_{h=0}^{r} C_h^n \cdot (q-1)^h$$

fjalë.

Kodi $C \subset \mathbb{F}_q^n$ që ndreq r gabime quhet i *përsosur* (për numrin e dhënë r) në qoftë se sferat me rreze r, $S_q(c, r)$, rreth secilës fjalë kod c janë jo vetëm prerëse, por edhe mbulojnë të gjithë $\mathbb{F}_q^n$.

Kusht i nevojshëm që një kod $q - ar$ me gjatësi n e që, ndreq r gabime të jetë i përsosur është

$$\sum_{h=0}^{r} C_n^h \cdot (q-1)^h \mid q^n.$$

3.3 Ushtrime dhe problema

1. Të llogariten distancat e mëposhtme Hamming:
   (a) $d(01001, 10110)$.
   (b) $d(12345, 54321)$.
   (c) $d(0010011, 0001111)$.
   (d) $d(111000, 000111)$.
2. Gjeni distancën minimale për kodet e mëposhtme:

(a) $\{0000, 1100, 1010, 1001, 0110, 0101, 0011, 1111\}$.

(b) $\{10000, 01010, 00001\}$.

(c) $\{000000, 101010, 010101\}$.

Në secilin rast gjeni numrin e gabimeve që zbulojnë dhe ndreqin kodet e mësipërme.

3. Cilëve nga kodet e ushtrimit 2 mund t'u shtohet një fjalë kod, pa ndryshuar distancën minimale.

4. Cilat nga fjalët e mëposhtme përmbajnë gabime të diktueshme, kur përdoret një $(3, 2)$ (gjatësia 3, dimensioni 2), kod i kontrollit të çiftësisë?
$$110, 010, 001, 111, 101, 000.$$

5. Të dekodohen fjalët e mëposhtme duke përdorur një $(3, 1)$ kod me përsëritje
$$111, 011, 101, 010, 000, 001.$$

6. Gjeni shkallën e informacionit për kodin $q-ar$ me përsëritje me gjatësi n.

7. Tregoni që distanca Hamming midis fjalëve binare x e y është
$$d(x, y) = \sum_{i=1}^{n} |x_i - y_i|.$$

8. Është shënuar $\omega(x)$ numri i koordinatave të ndryshme nga zero të fjalës x. Për fjalët binare $X = (x_1, x_2, \ldots, x_n)$ e $Y = (y_1, y_2, \ldots, y_n)$ shënojmë
$$X * Y = (x_1y_1, x_2y_2, \ldots, x_ny_n).$$
Pra $X * Y$ ka 1 në pozicionin e i-të vetëm kur X e Y kanë njëkohësisht 1 në vendin e i të.
Të provohet se për çdo $X, Y \in F_q^n$, $d(X, Y) = \omega(X - Y)$.
Të provohet se për çdo $X, Y \in F_2^n$ $d(X, Y) = \omega(X) + \omega(Y) - 2\omega(X * Y)$.

9. Sa është distanca Hamming minimale e kodit *ISBN*?

10. Sa gabime gjen dhe sa ndreq kodi *ISBN*?

11. A është kod linear kodi *ISBN*?

12. Paraqesim në vijim një metodë për kodimin e tabelave drejtkëndëshe me shifra. Në çdo rresht shtohet nga një shifër kontrolli çiftësie dhe pastaj në çdo shtyllë (duke përfshirë dhe shtyllën e shtuar) shtohet nga një shifër kontrolli çiftësie. Një parim i tillë përdoret në kontabilitet.

1	0	1	0
0	1	1	0
1	1	0	0

(a) Tregoni që kjo metodë mund të ndreqë një gabim, dhe tregoni si ndreqet ai.

(b) Mos është 2 numri i gabimeve që ndreq kjo metodë?

(c) Sa është numri maksimal i gabimeve që mund të gjejë ajo?

13. Quhet që një kod C zbulon ekzaktesisht t gabime, kur ai zbulon t gabime, por nuk zbulon $t+1$ gabime. Të vërtetohet që C, zbulon ekzaktesisht t gabime vetëm kur $d(C) = t + 1$.

14. Quhet që një kod C ndreq (korrigjon) ekzaktesisht t gabime, kur ai ndreq t gabime, por nuk ndreq $t+1$ gabime. Të vërtetohet që C ndreq ekzaktesisht t gabime vetëm kur $d(C) = 2t + 1$ ose $d(C) = 2t + 2$.

15. Le të jetë C një kod me $d(C) = d$ për të cilin shënojmë me g numrin në të madh të gabimeve që gjen ai dhe k numrin më të madh të gabimeve që ndreq ai. Të gjenden g e k në varësi të d.

16. C është një kod me distancë minimale $d = 2t + 2$ (çift) dhe përdoret njëkohësisht për zbulim dhe ndreqje gabimesh. Të vërtetohet se C ndreq ekzaktesisht t gabime dhe zbulon njëkohësisht $t+1$ gabime, por jo gjithmonë zbulon më shumë se $t+1$ gabime. Po nëse $d(C)$ është numër tek, çfarë mund të thuhet për numrin e gabimeve që C zbulon dhe ndreq njëkohësisht?

17. Në janar 1979, *Mariner 9* bëri fotografi bardh e zi të planetit Mars. Fotografitë u ndanë në një rrjet prej 600 x 600 *piksel*, secilit nga 360000 syresh, iu caktua një numër binar nga $0-63$, në varësi të nuancës (tonalitetit) së ngjyrës gri. Për të ndrequr gabimet u përdor një kod $(32, 64, 16)$.

    (a) Sa ishte numri i biteve që u përdorën për kodimin e informacionit?

    (b) Sa gabime ndreqte kodi? Sa gabime zbulonte?

    (c) Sa ishte shkalla e informacionit për kodin e ndërtuar?

18. Në periudhën midis viteve 1979 dhe 1981, *Voyager* bëri fotografi me ngyra të planeteve Jupiter dhe Saturn. Alafabeti i burimit kërkonte 4096 simbole për të shprehur nuancat e ngyrave të ndryshme. Informacioni u kodua me një kod binar $(24, 4096, 8)$ i njohur si kodi *Golay*.

    (a) Sa gabime ndeqte kodi? Sa zbulonte ai?

    (b) Sa ishte shkalla e informacionit e kodit të ndërtuar?

19. Jepet kodi ternar $C = \{00122, 12201, 20110, 22000\}$. Përdorni dekodimin me distancë minimale për dekodimin e fjalëve të mëposhtme:

    (a) 01122

    (b) 10021

    (c) 22022

    (d) 20120

20. Jepet kodi binar $C = \{01101, 00011, 10110, 11000\}$. Përdorni dekodimin me distancë minimale për dekodimin e fjalëve të mëposhtme:

    (a) 00000

    (b) 01111

    (c) 10110

    (d) 10011

    (e) 11011

21. Jepet kanali binar pa kujtesë me probabilitete të kanalit, $P(0|0) = 0.7$ dhe $P(1|1) = 0.8$. $P(0|0)$ është probabiliteti që të marrim simbolin zero me kusht që të kemi transmetuar simbolin zero në kanal. $P(1|1)$ është probabiliteti që të marrim simbolin 1 me kusht që të kemi transmetuar simbolin 1 në kanal. Fjalët kod të transmetuara në kanal janë: $\{000, 100, 111\}$. Të dekodohen:

    (a) 010 duke përdorur dekodimin me distancë minimale.

    (b) 011 duke përdorur dekodimin e ngjashmërisë maksimale.

    (c) 001 duke përdorur dekodimin me distancë minimale.

22. Fjalët nga kodi binar me gjatësi 5

$$C = \{01101, 00011, 10110, 11000\},$$

transmetohen në një kanal binar simetrik.

    (a) Të gjendet shkalla e kodit.

    (b) Sa gabime ndreq ky kod? Sa zbulon ai?

23. Fjalët nga kodi binar me gjatësi 5

$$C = \{00111, 10010, 01001, 11100\},$$

transmetohen në një kanal binar simetrik.

(a) Të gjendet shkalla e kodit.

(b) Sa gabime ndreq ky kod? Sa zbulon ai?

(c) Pas transmetimit në kanal merren në dalje fjalët $v = 01111$ dhe $\omega = 01100$. Të dekodohen v dhe ω duke përdorur dekodimin me distancë minimale.

24. Të provohet që $A_q(n, 1) = q^n$.

25. Të gjendet $A_q(n, n)$.

26. Të provohet që $A_2(3, 2) = 4$.

27. Të provohet që r-sfera $S_r(c)$ me qendër në vektorin c me n dimensione e koordinata në F_q (pra bashkësia e vektorëve me distancë jo më shumë se r nga c) përmban

$$1 + C_n^1(q-1) + \cdots + C_n^r(q-1)^r$$

vektorë.

28. Të provohet se ekziston një (n, M, d)-kod binar me d tek vetëm kur ekziston një $(n+1, M, d+1)$-kod binar.

29. Provoni që, në qoftë se d është numër tek, atëherë $A_2(n, d) = A_2(n+1, d+1)$.

30. Provoni që, në qoftë se d është numër çift, atëherë $A_2(n, d) = A_2(n-1, d-1)$.

31. Të ndërtohet një kod binar $(8, 4, 5)$.

32. A mund të ndërtohet (pra, a ekziston) një kod binar $(7, 3, 5)$?

33. M është madhësia e një kodi binar C me gjatësi 8 që ndreq dy gabime. Të provohet që $M \leqslant 6$.

34. Fjalët e kodit C me gjatësi 5, shkruhen si rreshta matrice si më poshtë:

$$C = \begin{pmatrix} 0 & 1 & 2 & 0 & 2 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 2 & 2 & 1 & 0 \\ 2 & 1 & 0 & 2 & 0 \end{pmatrix}$$

Të ndërtohet kodi ekuivalent me C, që merret kur aplikojmë përkëmbimin pozicional $\sigma = (2, 3, 4, 5, 1)$ dhe përkëmbimet sipas simboleve të alfabetit të kodit: $\pi_1 = (1, 2, 0)$, $\pi_2 = (2, 0, 1)$, $\pi_3 = \pi_4 = \pi_5 = (0, 1, 2)$.

35. Të tregohet se çdo (n, q, n) kod $q - ar$ është ekuivalent me një kod me përsëritje.

36. Sa është numri i kodeve binare joekuivalente $(n, 2)$?

37. Kodet C_1 dhe C_2 janë përkatësisht kode binare (n, M_1, d_1) dhe (n, M_2, d_2) mbi $\mathbb{F}_2$. Ndërtohet kodi i ri nga bashkimi i C_1 me $C_1 + C_2$:

$$C_1 \oplus C_2 = \{c|(c+d) : c \in C_1 \text{ dhe } d \in C_2\}$$

Të vërtetohet që $C_1 \oplus C_2$ është një kod $(2n, M_1 \cdot M_2, d')$, ku $d' = \min\{2d_1, d_2\}$.

Kreu 4

Kodet lineare

4.1 Perkufizime dhe veti

Një kod $L \subset \mathbb{F}_q^n$ është linear në qoftë se L është nënhapësirë lineare e $\mathbb{F}_q^n$. Në qoftë se L ka dimension k mbi $\mathbb{F}_q^n$, ai shënohet si kod $[n, k]$ dhe nëse ka distancë d, atëherë ai është kod $[n, k, d]$.
Për të vërtetuar që kodi L është linear kontrollohen kushtet e nënhapësirës:

1. $\forall x,\ y \in L,\ x + y \in L$;

2. $\forall x \in L,\ \alpha \in GF(q)\ \ \alpha \cdot x \in L$.

Madhësia M e një kodi linear $[n, k, d]$ mbi $\mathbb{F}_q^n$ është q^k, kurse shkalla R e kodit është $\frac{k}{n}$.
Për një kod linear L, pesha e tij përputhet me distancën minimale:

$$d(L) = \omega(L).$$

Matrica G me përmasa $k \times n$, rreshtat e së cilës formojnë bazë për kodin linear L, quhet matricë përftuese e L. Emrin matricë përftuese e përligj barazimi i mëposhtëm:

$$L = \{x \cdot G | x \in \mathbb{F}_q^k\},$$

ku k është dimensioni i kodit. Një matricë përftuese e formës $G = (I_k|A)$, ku I_k është matrica njësi e rendit k quhet matricë përftuese në formë standard. Një kod me matricë në këtë formë është sistematik në k pozicionet e para. Matrica H e kontrollit për kodin linear $L\,[n,k]$ quhet matrica me vetinë:

$$L = \left\{x \in F_q^n | x \cdot H^\top = 0\right\}.$$

Matrica e kontrollit për kodin linear L [n,k] është:

$$H = \left[-A^T | I_{n-k}\right],$$

ku $G = [I_k|A]$ është matrica përftuese në formë standard. Në qoftë se L është një $[n,k]$ kod linear, ekziston një kod linear ekuivalent me L që është sistematik në ato pozicione.

4.2 Ekuivalenca e kodeve lineare

Dy $k \times n$ matrica përftojnë kode lineare ekuivalente në $GF(q)$, në qoftë se njëra matricë mund të përftohet nga tjetra me veprimet e mëposhtme:

1. Përkëmbimi i rreshtave.
2. Shumëzimi i një rreshti me një skalar jozero nga fusha.
3. Mbledhja e një rreshti me një tjetër.
4. Përkëmbimi i shtyllave.
5. Shumëzimi i shtyllave me skalarë jozero nga fusha.

4.3 Kodet duale

Duali i një kodi linear L [n, k], përkufizohet si:

$$L^\perp = \{x \in \mathbb{F}_q^n | x \cdot c = 0\ \forall c \in L\}.$$

Kanë vend këto pohime në lidhje me kodet duale:

1. $L^\perp$ është $[n, n-k]$ kod linear.
2. Matrica përftuese G e kodit L, është matrica e kontrollit për $L^\perp$.
3. Për çdo kod linear L, $\left(L^\perp\right)^\perp = L$.

4.4 Distanca minimale

-Distanca minimale e kodit linear $[n,k]$ me matricë kontrolli H është e barabartë me numrin e plotë d më të vogël, për të cilin, ekzistojnë d shtylla linearisht të varura në H. Pra H ka d shtylla linearisht të varura, por çdo $d-1$ shtylla janë linearisht të pavarura.

4.5 Kodimi me kode lineare

Kodimi i mesazhit $u = (u_1, \ldots, u_k)$ me anë të kodit linear $[n,k]$ me matricë përftuese G, kryhet me anë të shumëzimit vektor-matricë:

$$c = u \cdot G.$$

4.6 Numëruesi i peshave

Në qoftë se K është një kod bllok me A_i fjalë kod me pesha *Hamming* i $(i = 0, 1, \ldots, n)$, atëhere polinomi

$$A_K(x) = \sum_{i=0}^{n} A_i \cdot x^i$$

quhet numëruesi i peshave i kodit K.
Probabiliteti i një gabimi të padiktuar kur përdoret kodi K në një kanal binar simetrik me probabilitet gabimi p dhe $q = 1 - p$ është

$$P_{und} = q^n \cdot \left[A_k\left(\frac{p}{q}\right) - 1\right],$$

ku A_K është numëruesi i peshave për kodin linear K me gjatësi n.
Në qoftë se $A_C(z)$ dhe $A_{C^\perp}(z)$ janë shënuar përkatësisht numëruesit e peshave të $[n,k]$-kodit C dhe të dualit të tij $C^\perp$, atëhere

$$A_{C^\perp}(z) = \frac{1}{2^k}\cdot(1+z)^n\cdot A_C\left(\frac{1-z}{1+z}\right).$$

$$A_C(z) = \frac{1}{2^{n-k}}\cdot(1+z)^n\cdot A_{C^\perp}\left(\frac{1-z}{1+z}\right).$$

Barazimet e mësipërm njihet me emrin barazimet MacWilliams për kodet binare.

4.7 Ushtrime dhe problema

1. Cilët nga kodet e mëposhtme janë lineare? Për kodet lineare gjeni një matricë përftuese.
   (a) $\{21234, 42413, 13142, 34321, 00000\} \subset \mathbb{F}_5^5$.
   (b) $\{000, 201, 111, 021, 012, 120, 102, 222, 210\} \subset \mathbb{F}_3^3$.
   (c) $\{00000, 11111\} \subset \mathbb{F}_5^5$.
   (d) $\{11111, 11010, 11000, 00000\} \subset \mathbb{F}_2^5$.
2. A mundet që një kod me parametra $(11, 24, 5)$ të jetë linear?
3. Të gjenden dimensioni dhe distanca minimale për kodin linear $\{(00000), (11110), (10001), (01111)\} \subset \mathbb{F}_2^5$.
4. Ndërtoni një matricë përftuese për kodin $q-ar$ me përsëritje. Sa është numri i matricave përftuese që mund të ndërtohen për kodin $q-ar$?
5. Le të jetë n një numër çift i fiksuar. A është kodi binar i të gjithë palindromave me gjatësi n (pra fjalëve me gjatësi n që nuk ndryshojnë dhe po të lexohen mbrapsht) linear? Po kod Hamming? Përshkruajeni atë me ekuacione dhe përcaktoni numrin e gabimeve që gjen ai.

6. Le të jetë K kodi binar i të gjitha fjalëve me gjatësi 7 i tillë që
   (a) biti i tretë është kontroll çiftësie për dy bitet e para;
   (b) biti i gjashtë është kontroll çiftësie për të katërtin e të pestin;
   (c) biti i fundit është kontroll çiftësie i përgjithshëm.

   Përshkruajeni K me ekuacione dhe përcaktoni numrin e gabimeve që mund të ndreqë apo zbulojë ai.
7. Le të jetë d një numër pozitiv tek. Të provohet se ekziston një kod linear binar C me gjatësi n e distancë minimale d atëherë dhe vetëm atëherë kur ekziston një kod binar C' me gjatësi $n+1$, me distancë minimale $d+1$ e me të njëjtën sasi fjalësh. Për më tepër, kodi C' është linear.
8. Të provohet se çdo kod linear ose i ka të gjitha fjalët me peshë çift, ose gjysmën e fjalëve i ka me peshë çift, gjysmën me peshë tek.
9. Le të jetë L një kod binar linear me gjatësi n. Shënojmë me A_i bashkësinë e fjalëve kod me peshë i në L. Pra:

   $$A_i = \{l \in L | \omega(l) = i\}.$$

   Në qoftë se $|A_n| = 1$, të vërtetohet se $|A_i| = |A_{n-i}|\ \forall i \in \{0, 1, \ldots, n\}$.
10. Një vektor $x = x_1x_2\ldots x_n \in \mathbb{F}_q^n$ quhet *i ngjashëm me çift* në qoftë se

    $$\sum_{i=1}^{n} x_i = 0,$$

    përndryshe ai quhet *i ngjashëm me tek*. Le të jetë C një $[n,k]$ kod mbi $\mathbb{F}_q$ dhe C_e bashkësia e fjalëve të ngjashme me çift të tij. Të provohet se, ose

    1. $C = C_e$, ose

2. C_e është një $[n, k-1]$-nënkod i $\mathcal{C}$.

11. Në qoftë se C është kod binar me gjatësi n, *zgjatje me kontroll çiftësije* i tij quhet kodi me gjatësi $n+1$ i dhënë nga $C^{+}=$

$$\left\{(x_1, x_2, \ldots, x_n, x_{n+1}) \in \mathbb{F}_2^{n+1} \mid (x_1, x_2, \ldots, x_n) \in C, \sum_{i=1}^{n+1} x_i = 0\right\}.$$

Të provohet që, në qoftë se C është kod linear, atëherë dhe C^{+} është linear. Sa është $d(C^{+})$ në lidhje me $d(C)$?

12. Në qoftë se C është kod binar me gjatësi n, *shkurtim* i tij quhet kodi me gjatësi $n-1$ i dhënë nga

$$C^{-} = \left\{(x_1, x_2, \ldots, x_{n-1}) \in \mathbb{F}_2^{n-1} \mid \exists x_n \in \mathbb{F}_2 \ (x_1, x_2, \ldots, x_n) \in C\right\}.$$

Të provohet që, në qoftë se C është kod linear, atëherë dhe C^{-} është linear. Sa është $d(C^{-})$ në lidhje me $d(C)$?

13. Të provohet se një kod C ndreq e gabime atëherë dhe vetëm atëherë kur për çdo dy fjalë kod të ndryshme $\mathbf{x}$ e $\mathbf{y}$ të C, $S(\mathbf{x}, e) \cap S(\mathbf{y}, e) = \emptyset$.

14. Le të jenë C_1 e C_2 dy kode lineare. Me anë të tyre ndërtojmë kodin *shumë e drejtë* e tyre

$$C_1 \oplus C_2 = \{(\mathbf{x}|\mathbf{y}) \mid \mathbf{x} \in C_1, \mathbf{y} \in C_2\}.$$

(a) Provoni që dhe kodi $C_1 \oplus C_2$ është linear. A ka vend ky rezultat dhe për kode (lineare) C_1 e C_2 jobinare?

(b) Sa është $d(C_1 \oplus C_2)$ në lidhje me $d(C_1)$ e $d(C_2)$?

(c) Të gjenden matrica përftuese dhe ajo e kontrollit të kodit $C_1 \oplus C_2$ në varësi të matricave përftuese G_1, G_2 e atyre të kontrollit H_1, H_2 përkatësisht të kodeve C_1, C_2.

15. Le të jetë dhënë kodi $\mathcal{C}$ me matricë përftuese:

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

Të gjendet një tjetër matricë përftuese e $\mathcal{C}$ ku të duket që $\mathcal{C}$ është shumë e drejtë e dy kodeve binare.

16. Le të jenë C_1 e C_2 dy kode lineare me gjatësi n e të tillë që $C_2 \subset C_1$. Me anë të tyre ndërtojmë kodin me gjatësi $2n$ të dhënë nga

$$C_1|C_2 = \{(\mathbf{x}|\mathbf{x}+\mathbf{y}) \mid \mathbf{x} \in C_1, \mathbf{y} \in C_2\}.$$

(Me $\mathbf{a}|\mathbf{b}$ është shënuar "bashkimi" $a_1a_2\ldots a_nb_1b_2\ldots b_n$ i fjalëve $\mathbf{a} = a_1a_2\ldots a_n$ e $\mathbf{b} = b_1b_2\ldots b_n$).

Tregoni që $C_1|C_2$ është kod linear. Sa është dimensioni i tij në lidhje me $\dim(C_1)$ e $\dim(C_2)$? Sa është $d(C_1|C_2)$ në lidhje me $d(C_1)$ e $d(C_2)$?

17. Të gjenden matrica përftuese dhe ajo e kontrollit të kodit $C_1|C_2$ në varësi të matricave përftuese G_1, G_2 e atyre të kontrollit H_1, H_2 përkatësisht të kodeve C_1, C_2.

18. Le të jetë dhënë kodi $\mathcal{C}$ me matricë përftuese:

$$G = \left(\begin{array}{cccc|cccc} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right).$$

Të tregohet që $\mathcal{C}$ është bashkim i dy kodeve binare.

19. Kodi linear ternar C jepet me anë të matricës përftuese

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

Të kodohet fjala 102101210122 e dhënë nga burimi.

20. Të gjendet matrica e kontrollit e $(6,3)$-kodit ternar të dhënë me matricën përftuese

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

21. Kodi binar C përftohet nga vektorët $\mathbf{e}_1 = 1001$ dhe $\mathbf{e}_2 = 0110$:

$$C = \{\lambda_1 \mathbf{e}_1 + \lambda_2 \mathbf{e}_2 \in F_2^4 \mid \lambda_i \in F_2\}.$$

Për këtë kod të gjenden:

(a) matrica përftuese,

(b) matrica e kontrollit,

(c) të gjitha fjalët kod të C,

(d) të gjitha fjalët e kodit dual të C,

(e) distanca minimale,

(f) numri i gabimeve që gjen dhe ai që ndreq ky kod.

22. Të gjendet një matricë e anasjelltë e djathtë e matricës

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

23. Të gjendet një matricë e anasjelltë e djathtë e matricës

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

Me anë të saj të gjendet mesazhi $\mathbf{x}$ në qoftë se $\mathbf{x}G = 1000110$.

24. Pohimi i mëposhtëm jep një algoritëm për të thjeshtuar matricën përftuese të një kodi, duke ndërtuar matricën përftuese të një kodi ekuivalent me të.

Pohimi 4.7.1. *Matricat*

$$G,\ G' \in \mathcal{M}_{k\times n}(GF(q))$$

janë matrica përftuese të dy kodeve ekuivalente, në qoftë se njëra përftohet nga tjetra me anë të një vargu nga veprimet elementare të mëposhtëme:

(a) Këmbim vendesh të dy rreshtave;

(b) Shumëzim i elementeve të një rreshti me një element jozero të $GF(q)$;

(c) Shtim i një rreshti një rreshti tjetër të shumëzuar me një element të $GF(q)$;

(d) Përkëmbim i dy shtyllave;

(e) Shumëzim i elementeve të një shtylle me një element jozero të $GF(q)$.

Vërtetim. Tre veprimet e para japin të njëjtin kod, kurse dy të tjerët japin kode ekuivalente në bazë të përkufizimeve. □

Meqënëse rangu i matricës përftuese është sa numri i rreshtave, nga ky pohim kemi teoremën e mëposhtme.

Teorema 4.7.1. *Matrica G e një (n,k) kodi linear C mund të transformohet me anë të transformimeve të tipit të pohimit 4.7.1 në një matricë që ka në k shtyllat e para matricën njësi I_k, pra:*

$$G' = (I_k \mid A_{k\times n}).$$

Matrica G' është matricë përftuese e një kodi ekuivalent me kodin C. □

Matrica G' e përftuar në këtë mënyrë quhet *matricë në formë standard.*

25. A është e vetme forma standard e një matrice?

26. Kodi linear C jepet me anë të matricës përftuese

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

(a) Të kodohet fjala 100111.

(b) Të kthehet matrica G në formën standard.

(c) Të gjendet shkalla e informacionit dhe numri i fjalëve të tij $|C|$.

(d) Të ndërtohet matrica e kontrollit e tij H.

(e) Të ndërtohet matrica përftuese e kodit dual të tij.

(f) Të gjendet distanca minimale e kodit C. Sa gabime gjen dhe sa ndreq ky kod?

27. Përcaktoni se cilat nga çiftet e matricave të mëposhtme përftojnë kode ekuivalente.

(a)

$$G_1 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \quad G_2 = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

(b)

$$G_1 = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}, \quad G_2 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

(c)

$$G_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}, \quad G_2 = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

28. Gjeni matricën e kontrollit të kodit linear me matricë përftuese:

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

29. Shkruani të gjitha fjalët e kodit binar linear L me matricë kontrolli:

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

30. $[10, 8]$ - kodi C, i ndërtuar mbi $GF(11)$ ka matricë kontrolli

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{pmatrix}.$$

(a) Të gjendet matrica përftuese e tij;

(b) Të kodohet me të fjala 11000000.

31. Gjeni distancën e kodit linear ternar me matricë përftuese:

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

32. Jepet kodi linear binar L me matricë kontrolli:

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

(a) Të gjendet distanca minimale e kodit.

(b) Të gjendet distanca minimale e dualit të kodit.

(c) Të gjendet distanca minimale e kodit të zgjatur të kontrollit të çiftësisë, $\overline{L}$.

(d) A është L i përsosur?

33. Jepet kodi linear binar me matricë kontrolli:

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

(a) Të gjendet distanca minimale e kodit.

(b) Të gjendet distanca minimale e dualit të kodit.

(c) Të gjendet distanca minimale e kodit të zgjatur të kontrollit të çiftësisë, $\overline{L}$.

(d) A është L i përsosur?

34. Të gjendet një matricë në formë standard për kodin linear binar me matricë përftuese si më poshtë:

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

Të gjendet distanca minimale e kodit.

35. Jepet kodi lienar binar L me matricë përftuese:

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

(a) Të shkruhen të gjitha fjalët kod të L.

(b) Të gjendet një matricë përftuese për $L^\perp$.

(c) Të gjendet distanca e $L^\perp$.

36. Jepet kodi linear binar L me matricë përftuese:

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

(a) Të shkruhen të gjitha fjalët kod të L.

(b) A është i përsosur L?

(c) Të gjendet distanca e $L^\perp$.

(d) Të gjendet një matricë përftuese për $(\overline{L})^\perp$, ku $\overline{L}$ është kodi i zgjatur i kontrollit të çiftësisë.

37. Matrica G e mëposhtme është matricë përftues për kodin linear L. Të gjendet distanca minimale si edhe një fjalë kod me peshë minimale jozero për dualin e L.

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

38. Të gjendet numri i gabimeve që mund të ndreqë dhe i gabimeve që mund të gjejë kodi ternar me matricë kontrolli:

$$H = \begin{pmatrix} 2 & 0 & 0 & 1 & 1 \\ 0 & 2 & 0 & 0 & 2 \\ 0 & 0 & 1 & 2 & 0 \end{pmatrix}.$$

39. Një kod C quhet *vetë dual* në qoftë se përputhet me dualin e tij $C^\perp$.

(a) Duke i shtuar çdo rreshti të një matrice përftuese të kodit të *Hamming*-ut një koordinatë kontrolli çiftësie përftohet një $[4,8]$ matricë, që është matricë përftuese për kodin $\widehat{\mathcal{H}_3}$. Të provohet se $\widehat{\mathcal{H}_3}$ është kod vetë dual.

(b) $[4,2]$ kodi ternar $\mathcal{H}_{3,2}$, i quajtur dhe *tetrakodi*, ka matricë përftuese në formën standard

$$G = \left(\begin{array}{cc|cc} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & -1 \end{array}\right).$$

Të provohet se ky kod është vetë dual.

(c) Të provohet se gjatësia n e një kodi vetë dual është çift dhe dimensioni i tij është $\frac{n}{2}$.

40. A ka kode vetë duale me gjatësi 3. Po me gjatësi 4? Për kodet vetë duale, të gjendet një matricë përftuese.

41. Kodi C quhet *vetë ortogonal* në qoftë se $C \subset C^{\perp}$.

    (a) Të tregohet se, në qoftë se C është një kod binar vetëortogonal, atëherë çdo fjalë kod ka peshë çift.

    (b) Të tregohet se, në qoftë se C është një kod binar vetëortogonal, atëherë $C^{\perp}$ përmban fjalën $\mathbf{1} = 11\cdots 1$.

    (c) Të tregohet se, në qoftë se C është një kod ternar vetë ortogonal, atëherë pesha e çdo fjalë kod është shumëfish i plotë i numrit 3.

42. Le të jetë C një $[n, k, d]$ kod mbi $\mathbb{F}_q$ dhe S një bashkësi koordinatash të tij, pra $S \subset \{1, 2, \ldots, n\}$. Të provohet se

$$(C^{\perp})_S = (C^S)^{\perp} \text{ dhe } (C^{\perp})^S = (C_S)^{\perp}.$$

43. Të provohet që kodi binar me përsëritje

$$C = \{\mathbf{0} = 000\ldots 0, \mathbf{1} = 111\ldots 1\}$$

me gjatësi tek është i përsosur.

44. Le të jetë H matrica e kontrollit e (n, k)- kodit linear binar C. Të provohet se sindroma e një fjale të marrë është një matricë shtyllë që është shuma e shtyllave të H që u përkasin vendeve ku kanë ndodhur gabime.

45. Të provohet se një kod i përsosur për e gabime jep gjithnjë përgjigje të gabuar në qoftë se përdoret për të ndrequr $e + 1$ gabime.

46. Të gjendet numëruesi i peshave për kodin binar me matricë përftuese

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

47. Të gjendet numëruesi i peshave për kodin ternar me matricë përftuese

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

Të krahasohet rezultati me rezultatin e ushtrimit 46.

48. Le të jetë C një $[6, 3]$ kod binar me matricë përftuese

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

    (a) Të tregohet që C nuk është vetë ortogonal.

    (b) Gjej numëruesin e peshave të C.

    (c) A formojnë nënkod të C fjalët kod të C me pesha të plotpjesëtueshme me 4?

49. Të gjendet numëruesi i peshave të kodit $C = \{000, 011, 101, 110\}$ dhe i dualit $C^{\perp}$ të tij.

Kreu 5

Disa kode lineare

5.1 Kodet Hamming

Kodet *Hamming* janë kodet më të famshme gabimndreqëse.
Çdo kod *Hamming* binar është ekuivalent me ndonjë kod ciklik; nuk ndodh kështu për kodet *Hamming* jobinare, ka prej tyre që nuk janë ekuivalente me kode ciklike.
Parametrat e kodit Ham(m,q) janë:

$$\left[n = \frac{m^q - 1}{q - 1}, n - m, 3\right].$$

Shakalla e kodeve $Ham(m, q)$ është $R = \frac{m}{n}$.
Kodet $Ham(m, q)$ janë kode të përsosura për ndreqjen e një gabimi të vetëm.
Për të ndërtuar matricën e kontrollit për një kod $Ham(m, q)$ duhet që matrica të ketë çdo dy shtylla linearisht të pavarura dhe të ketë 3 shtylla linearisht të varura. Kjo mund të arrihet duke zgjedhur si shtyllë të parë një vektor të ndryshëm nga 0 në $\mathbb{F}_q^m$. Shtylla e dytë zgjidhet e tillë që të mos jetë proporcionale me shtyllën e parë. Shtyllat e tjera zgjidhen me radhë që të mos jenë proporcioanle me shtyllat e mëparshme. Në fund të këtij procesi kemi shkruar si shtylla $\frac{m^q-1}{q-1}$ fjalë nga $\mathbb{F}_q^m$. Në qoftë se shtyllat e matricës H të kontrollit zgjidhen në rendin rritës si numra në $\mathbb{F}_q$ dhe simboli i parë jozero

në çdo shtyllë është 1, atëherë një gabim i vetëm mund të zbulohet dhe ndreqet lehtësisht. Sindroma e gabimit është e formës

$$s = \alpha \cdot e_i \cdot H^{\top},$$

ku $\alpha \in \mathbb{F}_q$ dhe e_i paraqet një numër binar, i cili i konvertuar në numër dhjetor jep pozicionin e bitit të gabuar të fjalës kod.

5.2 Kodet e zgjatur Hamming

Në qoftë se kodit $Ham(m,2)$ i shtojmë një bit kontrolli të çiftësisë, përftohet kodi i zgjatur i kontrollit të çiftësisë $\overline{Ham(m,2)}$ me parametra $[2^m, 2^m - 1 - m, 4]$. Ky kod ndreq 1 gabim, por zbulon 2 të tillë. Në qoftë se H është matrica e kontrollit e kodit $Ham(m,2)$, atëherë matrica e kontrollit për kodin e zgjatur është

$$\overline{H} = \begin{pmatrix} & & & 0 \\ & H & & 0 \\ & & & \vdots \\ 1 & 1 & \dots & 1 \end{pmatrix},$$

duke shtuar te H, një shtyllë **0** dhe një rresht **1**. Dekodimi i fjalëve x me anë të kodit të zgjeruar bëhet si më poshtë:

1. Njehsohet sindroma $S(x) = \overline{H} \cdot x^{\top} = (s_1, s_2, s_3, s_4)$.
2. Në qoftë se $s_4 = 1$ dhe (s_1, s_2, s_3) është paraqitja binare e numrit $i \neq 0$, atëherë $S(x)$ është shtylla e i-të e matricës $\overline{H}$ dhe ndreqet biti i i-të.
3. Në qoftë se $(s_1, s_2, s_3) = \mathbf{0}$ dhe $s_4 = 1$, atëherë ka ndodhur gabim në bitin e fundit dhe e ndreqim atë.
4. Në qoftë se $(s_1, s_2, s_3) \neq 0$ dhe $s_4 = 0$, atëherë ka ndodhur një numër çift gabimesh(të paktën dy), prandaj kërkohet ritransmetim i x.

5.3 Kodet Reed-Muller

Reed – Muller janë kode lienare binare. Për çdo numër natyror m e për çdo numër $r = \{0, \dots, m\}$, kodi *Reed – Muller* $R(r,m)$ i rendit r ka parametra:

$$n = 2^m,$$

$$k = 1 + C_1^m + \dots + C_r^m,$$

$$d = 2^{m-r},$$

$$R = \frac{1 + C_1^m + \dots + C_r^m}{n}.$$

Kodi $R(0,m)$ është kodi me përsëritje me gjatësi 2^m, $\{\mathbf{0}, \mathbf{1}\}$. Për të ndërtuar një matricë përftuese për kodin $R(1,m)$, veprohet në këtë mënyrë:
Shënohet me v_0 vektori rresht me gjatësi n, me të gjithë kompnonentet njësha. Kurse me $v_1, v_2, \dots, v_m$ shënohen rreshtat e një matrice që ka për shtylla të gjithë vektorët e $\mathbb{F}^m$. Matrica përftuese e kodit $R(1,m)$ është:

$$G = \begin{pmatrix} v_0 \\ v_1 \\ \vdots \\ v_m \end{pmatrix}.$$

5.4 Kodet Golay

Ka në total 4 kode Galay, dy binare dhe dy ternare. Kodet binare Golay kanë këto parametra:

1. C_{24} ka parametra $(24, 12, 8)$ dhe është vetë dual.
2. C_{23} ka parametra $(23, 12, 7)$ dhe është i përsosur. C_{23} përftohet nga C_{24} duke e shpuar këtë të fundit në një nga bitet farëdo të tij.

Kodi Golay ternar C_{12} ka matricë përftuese $G = [I_6|B]$, ku I_6 është matrica njësi e rendit 6 dhe

$$B = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 & 2 & 1 \\ 1 & 1 & 0 & 1 & 2 & 2 \\ 1 & 2 & 1 & 0 & 1 & 2 \\ 1 & 2 & 2 & 1 & 0 & 1 \\ 1 & 1 & 2 & 2 & 1 & 0 \end{pmatrix}$$

Për kodin C_{12} kanë vend:

1. C_{12} është vetë dual.
2. $B = B^{\perp}$.
3. C_{12} është $(12, 6, 6)$ kod.
4. C_{11} me parametra $(11, 6, 5)$ është i përsosur. C_{11} përftohet nga c_{12} duke e shpuar këtë të fundit në simbolin e fundit.

Çdo kod ternar $(12, 3^6, 6)$ është ekuivalent me C_{12} dhe çdo kod $(11, 3^6, 5)$ është ekuivalent me C_{11}.

5.5 Ushtrime dhe problema

1. Provoni me detaje se kodi i Hamming është një $[7, 16, 2]$-kod (gjatësi 7, madhësi 16, binar) i përsosur.
2. Të shkruhen matrica e kontrollit, matrica përftuese dhe të gjitha fjalët kod të një kodi Hamming me gjatësi 3.
3. Të gjendet një fjalë me peshë tre në një kod Hamming të çfarëdoshëm.
4. Sa është $\dim(Ham(m, 2))$?
5. Sa vektorë ka $Ham(m, 2)$?

6. Të gjendet matrica përftuese e kodit të *Hamming*-ut.
7. Të dekodohen vektorët e mëposhtëm, të koduar me kodin binar Hamming me gjatësi 15:
   (a) 001000001100100,
   (b) 101001110101100,
   (c) 000100100011000,
   (d) 000010100011000,
   (e) 110011100011100,
   (f) 100001000011101.
8. Të tregohet me anë të teoremës që jep distancën minimale me anë të numrit minimal të shtyllave linearisht të varura, që kodi Hamming ka distancë 3.
9. Me kodin $Ham(3, 2)$ është marrë vektori $x = (1, 1, 0, 1, 0, 1, 1)$. Të njehsohet sindroma e tij e të dekodohet ai.
10. Të gjendet distanca minimale e dualit të kodit $Ham(3, 2)$.
11. Të ndërtohet matrica e kontrollit për kodin e zgjatur $Ham(3, 2)$.Të dekodohen fjalët $v = 01101110$ dhe $w = 11100111$.
12. Të ndërtohet një matricë kontrolli për kodin ternar $Ham(3, 3)$. Të dekodohen fjalët $\omega = (2222221111111)$ dhe $\gamma = (1101112211201)$.
13. Të provohet që kodet binare Hamming janë të përsosur.
14. Të provohet se kondité e nevojshme për ekzistencën e një kodi të përsosur në F_q me gjatësi n për një gabim është
$$(1 + n(q-1)) \mid q^n.$$
Që këtej të provohet që *nuk ekzistojnë kode binare të përsosur për një gabim me gjatësi çift.*

15. Njehsoni kufijtë e sipërm për $A_q(n,d)$ që rrjedhin nga kufiri i *Hamming*-ut për

    (a) $q=2,\ n=7,\ d=3$;

    (b) $q=2,\ n=7,\ d=4$;

    (c) $q=2,\ n=8,\ d=3$;

    (d) $q=2,\ n=15,\ d=3$;

    (e) $q=2,\ n=23,\ d=7$;

    (f) $q=3,\ n=12,\ d=5$.

16. Njehsoni probabilitetin e gabimit $P_{err}(K)$ të kodit Hamming me gjatësi 7 i përdorur në një kanal binar simetrik që gabon afërsisht 1 bit në njëqind.

17. Provoni që dekodimi i kodeve Hamming është gjithnjë i gabuar, në qoftë se në çdo fjalë kod gabohet në dy bit.

18. Një kod linear binar me gjatësi 8 përshkruhet nga ekuacionet e mëposhtme

$$\begin{array}{ccccccc} x_5 & = & x_2 & + & x_3 & + & x_4 \\ x_6 & = & x_1 & + & x_2 & + & x_3 \\ x_7 & = & x_1 & + & x_2 & + & x_4 \\ x_8 & = & x_1 & + & x_3 & + & x_4. \end{array}$$

    Të gjenden matrica e kontrollit, distanca minimale dhe numëruesi i peshave të këtij kodi.

19. Të gjendet matrica e kontrollit e kodit $Ham(2,5)$.

20. Të ndërtohen matricat e kontrollit të kodeve
    a) $Ham(2,11)$ e b) $Ham(3,3)$.

21. Të gjendet $A_q(n,3)$ në qoftë se q është numër i thjeshtë dhe

$$\exists r \in \mathbb{N} \setminus \{1\} \text{ i tillë që } n = \frac{q^r - 1}{q-1}.$$

22. Të dekodohet fjala $x = (1\,1\,1\,1\,1\,0\,0\,0)$ e marrë me një $(8,4)$ kod të zgjeruar Hamming.

23. Të dekodohet fjala $x = (1\,0\,1\,1\,1\,0\,0\,0)$ e marrë me një $(8,4)$ kod të zgjeruar Hamming.

24. Të ndërtohet matrica përftuese dhe matrica e kontrollit e kodit $R(1,2)$.

25. Të provohet se $R(1,3)$ është ekuivalent me dualin e $(8,4)$-kodin e zgjeruar të Hamming.

26. Të provohet se $R(1,3)$ është ekuivalent me dualin e $(8,4)$-kodin e zgjeruar të Hamming.

27. Të ndërtohet një bazë për kodin $R(2,4)$.

28. Të vërtetohet se:
    Kodi binar i Golay-t C_{23} është i përsosur (për tre gabime).

29. Të vërtetohet se:
    Kodi ternar i Golay-t C_{11} është i përsosur (për dy gabime).

Kreu 6

Tabelat Standarde

Në qoftë se $L \subset \mathbb{F}_q^n$ është një $[n, k]$ kod linear me matricë kontrolli H, sindromë e fjalës $x \in \mathbb{F}_q^n$ quhet madhësia:

$$s(x) = H \cdot x^{\mathsf{T}}.$$

Klasë fqinje e kodit linear L për $x \in \mathbb{F}_q^n$ quhet bashkësia:

$$x + L = \{x + c \colon c \in L\}.$$

$x, y \in \mathbb{F}_q^n$ kanë të njëjtën sindromë vetëm kur ndodhen në të njëjtën klasë fqinje.
Për kodin linear me matricë kontrolli H, dekodimi me distancë minimale është ekuivalent me dekodimin e fjalës x si fjala $c = x - e$, ku e është fjala me peshë më të vogël në klasën fqinje të $x + L$. E thënë ndryshe e është fjala me peshë minimale me sindromë të njëjtë me x.

6.1 Ushtrime dhe problema

1. Le të jetë $C = \{(0000), (1011), (0101), (1110)\}$ një $(4, 2)$-kod linear binar. Të ndërtohet tabela standard e tij. Të dekodohet me anë të saj fjala (1111).

2. Gjeni një tabelë standard për kodin binar me përsëritje me gjatësi 7.

3. Përshkruani tabelën standard për kodin me përsëritje.

4. Të gjendet një tabelë standard për kodin Hamming me gjatësi 7 të përdorur në një kanal binar simetrik.

5. Le të jetë K_5 kodi linear me gjatësi 5 në të cilin biti i katërt kontrollon çiftësinë e dy biteve të parë, ndërsa biti i fundit kontrollon çiftësinë e përgjithshme. Të ndërtohet tabela standard e kodit K_5.

6. Të provohet që kodi binar me gjatësi 5 i përshkruar nga ekuacionet e mëposhtme

$$\begin{aligned} x_3 &= x_1 + x_2 \\ x_4 &= x_1 \\ x_5 &= x_1 + x_2 \end{aligned}$$

ndreq gabime të vetme. Të gjendet një tabelë standard dhe vëreni që dekodimi korrespondues ndreq më shumë se gabime të vetmuara.

7. Kodi linear binar K është dhënë me anë të matricës përftuese

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

(a) Të gjendet $\dim K$ dhe një bazë e tij.Të kodohet mesazhi 10011100 me anën e kodit linear K.

(b) Të gjendet një matricë kontrolli e tij .

(c) A është kod Hamming K-ja? Sa gabime ndreq e sa gjen ky kod? A është i përsosur ai?

(d) Sa gabime ndreq e sa gjen njëkohësisht C-ja?

(e) Sa është shkalla e informacionit e tij? Sa rreshta ka një tabelë standart e tij?

(f) Është marrë fjala $\mathbf{Y} = 1111$. Cila ka qenë fjala e dërguar?

(g) A mund të ndreqet më shumë se një gabim me anë të tabelave standart të këtij kodi?

8. Le të jetë C kodi linear i të gjithë shumave të mundshme të fjalëve të mëposhtme:

$$101011,\ 011101,\ 011010$$

(a) Të gjendet një matricë e kontrollit.

(b) Të gjendet një tabelë standard, e të dekodohet 111011.

9. Konsiderojmë $(6,3)$-kodin

$C = \{000000,\ 001110,\ 010101,\ 011011,\ 100011,\ 101101,\ 110110,$

$111000\}$.

Të dekodohen me tabela standard fjalët $\omega = 101011$ e $v = 011100$

10. L është një kod binar linear me matricë kontrolli H si më poshtë:

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

(a) Të shkruhet një matricë përftuese për L dhe të kodohen 101 dhe 110.

(b) Të dekodohet fjala $\omega = 011011$.

11. L është kodi linear binar i të gjithë shumave të fjalëve të mëposhtme:

$$101011, 011101, 011010$$

(a) Të gjenden të gjitha fjalët kod të L.

(b) Të gjendet një matricë përftuese në formë standard për L.

(c) Të dekodohet 111011.

Kreu 7

Kodet Ciklike

7.1 Përkufizime dhe veti

Kodi $C \subset \mathbb{F}_q^n$ është ciklik në qoftë se:

1. C është linear.

2. Çdo zhvendosje ciklike e fjalëve kod është përsëri fjalë kod.

Kodet ciklike janë polinome në $\mathbb{F}_q[x]$. Në qoftë se $c=(c_0, c_1 \dots, c_i, \dots, c_{n-2}, c_{n-1}) \in \mathbb{F}_q^n$, polinomi përkatës në $\mathbb{F}_q^n[x]$ është:

$$c(x) = c_0 + c_1 \cdot x + \cdots + c_i \cdot x^i + \cdots + c_{n-1} \cdot x^{n-1}.$$

Kodi C është ciklik në qoftë se ai është ideal i:

$$R_n = \mathbb{F}_q[x]/(x^n - 1) \ ,$$

ose

1. $a(x),\ b(x) \in C \implies a(x) + b(x) \in C.$

2. $a(x) \in C,\ r(x) \in R_n \implies a(x) \cdot r(x) \in C.$

Në R_n, veprimet kryhen sipas modulit $x^n - 1$, prandaj ka vend:

$$x^n - 1 \equiv 0.$$

7.2 Polinomi përftues

Për kodet ciklike kanë vend:

1. Në kod ekziston një polinom monik $g(x)$ me shkallë minimale. Ky polinom përfton kodin dhe ka vend:

$$C =< g(x) >= \{r(x) \cdot g(x) | sh(r(x) < n - r)\},$$

   ku $sh(g(x)) = r$.

2. $g(x) \mid x^n - 1$.
3. $dim(C) = n - r$, ku $sh(g(x)) = r$.
4. Në qoftë se $g(x) = g_0 + g_1 \cdot x + g_2 \cdot x^2 + \cdots + g_r \cdot x^r$, C ka matricë përftuese:

$$G = \begin{pmatrix} g_0 & g_1 & g_2 & \dots & g_r & 0 & 0 & 0 & \dots & 0 \\ 0 & g_0 & g_1 & g_2 & \dots & g_r & 0 & 0 & \dots & 0 \\ 0 & 0 & g_0 & g_1 & g_2 & \dots & g_r & 0 & \dots & 0 \\ \vdots & & & & & & & & & \\ \vdots & & & & & & & & & \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 & g_0 & \dots & g_r \end{pmatrix},$$

   ku çdo rresht është zhvendosje ciklike e paraardhësit.

5. Polinomi monik $p(x) \in \mathbb{R}_n$, është polinom përftues, vetëm kur $p(x) \mid x^n - 1$.

7.3 Polinomi i kontrollit

$x^n - 1 = g(x) \cdot h(x)$. Në qoftë se $sh(g(x)) = r$, polinomi $h(x)$ me shkallë $n - r$, quhet polinomi i kontrollit. Në lidhje me polinomin e kontrollit kanë vend këto:

1. $C = \{p(x) \in R_n | p(x) \cdot h(x) \equiv 0\}$.

2. Në qoftë se $h(x) = h_0 + h_1 \cdot x + h_2 \cdot x^2 + \cdots + h_{n-r} \cdot x^{n-r}$, matrica e kontrollit për kodin ciklik është:

$$H = \begin{pmatrix} h_{n-r} & h_{n-r-1} & \dots & h_0 & 0 & \dots & 0 \\ 0 & h_{n-r} & \dots & h_1 & h_0 & \dots & 0 \\ \vdots & & & & & & \\ \vdots & & & & & & \\ 0 & 0 & \dots & 0 & h_{n-r} & \dots & h_0 \end{pmatrix}.$$

7.4 Kodimi me kodet ciklike

Kodimi, duke përdorur kodet ciklike, bëhet duke shumëzuar dy polinome; polinomin-mesazh dhe polinomin përftues. Në qoftë se m është informacioni i shprehur me anë të polinomit $m(x)$ me shkallë k dhe polinom përftues $g(x) = g_0 + g_1 \cdot x + g_2 \cdot x^2 + \cdots + g_r \cdot x^r$, m kodohet si:

$$c = m \cdot G,$$

ose

$$c(x) \equiv m(x) \cdot g(x).$$

7.5 Dekodimi me kodet ciklike

C është kod ciklik me gjatësi n dhe polinom përftues $g(x)$. Fjala ω është fjala me gjatësi n pas transmetimit në kanal të një fjale kod të C . Mbetja $s(x)$ e pjesëtimit të polinomit $\omega(x)$ me $g(x)$, quhet sindromë e fjalës ω. Dekodimi i $\omega(x)$, për kodin ciklik me distancë d, kryhet si më poshtë:

1. Në qoftë se $s(x)$ ka peshë $\leqslant [\frac{d-1}{2}]$, $\omega(x)$ dekodohet si:

$$\omega(x) - s(x)$$

2. Në qoftë se $s(x)$ ka peshë $> [\frac{d-1}{2}]$, ω dekodohet si:

$$\omega(x) - s_1(x),$$

ku $s_1(x)$ është drejtuesi i klasës fqinje për klasën e ekuivalencës ku ndodhet $s(x)$. $s_1(x)$ llogaritet me anë të:

$$s_1(x) = \omega \cdot H^{\mathsf{T}},$$

ku H është matrica e kontrollit për C.

7.6 Ushtrime dhe problema

1. A është kodi i mëposhtëm ciklik?

   (a) Kodi binar $\{0000, 1100, 0110, 0011, 1001\}$.

   (b) Kodi binar $\{00000, 00110, 01101, 11011\}$.

   (c) Kodi ternar $\{0000, 1122, 2211\}$.

   (d) Kodi q-ar me përsëritje më gjatësi n.

   (e) Kodi binar i fjalëve me peshë çift.

   (f) Kodi ternar:

   $$\{x \in V(n,3) |\ \omega(x) \equiv 0 \pmod 3\}$$

   (g) Kodi ternar:

   $$\left\{(x_1 x_2 \cdots x_n) \in V(n,3) |\ \sum_{i=1}^{n} x_i \equiv 0 \pmod 3\right\}$$

2. Për kodet ciklike të ushtrimit **1**, të gjenden polinomet përftuese.

3. Të gjendet kodi binar ciklik më i vogël që përmban 0011010 si fjalë kod.

4. Të gjendet kodi binar ternar ciklik më i vogël që përmban 12002 si fjalë kod. Sa është disatanca minimale e tij?

5. Të gjendet kodi ciklik më i vogël në $\mathbb{F}_5$ që përmban 4203102 si fjalë kod.

6. Le të jetë

   $$C = \left\{(x_1 x_2 \cdots x_n) \in F_2^n |\ \sum_{i=1}^{n} x_i \equiv 0 \pmod 2\right\}.$$

   Të tregohet që C është kod ciklik. Të gjenden shkalla e informacionit, polinomi përftues, polinomi i kontrollit, matrica përftuese, matrica e kontrollit. A është kod Hamming ky kod? Po i përsosur?

7. Le të jetë

   $$C = \left\{(x_1 x_2 \cdots x_n) \in F_3^n |\ \sum_{i=1}^{n} x_i \equiv 0 \pmod 3\right\}.$$

   Të tregohet që C është kod ciklik. Të gjenden shkalla e informacionit, polinomi përftues, polinomi i kontrollit, matrica përftuese, matrica e kontrollit. A është kod Hamming ky kod? Po i përsosur?

8. C_1 dh C_2 janë kode ciklike në R_n me polinome përftuese përkatësisht $g_1(x)$ dhe $g_2(x)$. Të vërtetohet se $C_1 \cap C_2$ është gjithashtu ciklik. Të gjendet polinomi përftues i tij.

9. Le të jetë C një kod ciklik në $\mathbb{R}_n$. Kodi i kundërt i C, shënohet me $C^{[-1]}$ dhe merret duke shkruar në të kundërt fjalët kode të C:

   $$(c_0, c_1, \dots c_i, \dots, c_{n-1}) \in C \iff (c_{n-1}, \dots, c_{n-1-i}, \dots, c_1, c_0) \in C^{[-1]}$$

   Të vërtetohet që:

   (a) $C^{[-1]}$ është gjithashtu ciklik me të njëjtin dimension sa C.

(b) Në qoftë se $g(x)$ është polinomi përftues i kodit C, atëhere $g_0^{-1} \cdot g^{[-1]}(x)$ është polinomi përftues i kodit $C^{[-1]}$, ku $g^{[-1]}(x) = x^r \cdot g(x^{-1})$ dhe $r = sh(g(x))$.

10. A është ciklik, kodi ekuivalent i një kodi ciklik?

11. A ka fusha të fundme me?
    (a) 3 elemente.
    (b) 10 elemente.
    (c) 16 elemente.
    (d) 9 elemente.

12. Shkruani tabelën e shumëzimit për $F_2[x]/(x^2+1)$ e tregoni pse nuk është fushë.

13. Tregoni që polinomi i pazbërthyeshëm mbi $GF(2)$ me shkallë ≥ 2 ka një numër tek koeficientësh jozero.

14. Shkruani të gjithë polinomet e pazbërthyeshëm mbi $GF(2)$ me shkallë 1 deri në 4. Ndërtoni një fushë të fundme të rendit të 8.

15. $x^4 + x + 1$ është polinom me shkallë 4 në $\mathbb{F}_2[x]$.
    (a) Të vërtetohet që polinomi është i pazbërthyeshëm në $\mathbb{F}_2[x]$.
    (b) Duke u bazuar tek ky polinom, të ndërtohet $\mathbb{F}_{16}$.

16. Shkruani të gjithë polinomet monike të pazbërthyeshëm mbi $GF(3)$ të shkallës së dytë.

17. Të faktorizohen në $\mathbb{F}_2[x]$ polinomet e mëposhtme:
    (a) $x^9 - 1$.
    (b) $x^6 - 1$.
    (c) $x^8 - 1$.

18. Faktorizoni $x^5 - 1$ në polinome të pazbërthyeshëm dhe përcaktoni që këndej të gjithë kodet binare me gjatësi 5.

19. Le të jetë $g(x)$ polinomi përftues i një kodi binar ciklik që ka fjalë kod me peshë tek. A është bashkësia e fjalëve kod me peshë çift të $\langle g(x) \rangle$ kod ciklik? Në qoftë se po, cili është një polinom përftues i tij?

20. Supozojmë se $x^n - 1$ është prodhim i t polinomeve të ndryshëm të pazbërthyeshëm mbi $GF(q)$. Sa kode ciklike me gjatësi n mbi $GF(q)$ ka?

21. Faktorizimi i $x^7 - 1$ në polinome të pazbërthyeshëm është $(x-1)(x^3+x+1)(x^3+x+1)$. Përcaktoni të gjithë kodet lineare ciklike me gjatësi 7.

22. Faktorizoni polinomin $x^8 - 1$ mbi $GF(3)$. Sa kode ternare ciklike me gjatësi 8 ka?

23. Shkruani një polinom kontrolli dhe një matricë kontrolli për secilin nga kodet ternare ciklike me gjatësi 4.

24. Për kodin ciklik me gjatësi 15 me polinom përftues $1 + x + x^4$ të gjendet një matricë përftuese e një matricë kontrolli. A është kod Hamming ai? A është fjala $x = (101011000000001)$ fjalë kod e tij? Në qoftë se jo, a mund të ndreqet ajo? Në qoftë se po, të ndreqet ajo.

25. Të vërtetohet se duali i një kodi ciklik është kod ciklik.

26. Le të jetë C një kod ciklik me polinom kontrolli $h(x)$. Cila është lidhja midis C dhe $\langle h(x) \rangle$ (A janë të njëjtë? A janë ekuivalente?)?

27. Le të jenë C_1 dhe C_2 kode ciklike në $\mathbb{R}_n$ me polinome përftuese përkatësisht $g_1(x)$ dhe $g_2(x)$. Të vërtetohet që $C_1 \subset C_2 \iff g_2(x) \mid g_1(x)$.

28. Le të jetë $\mathbb{E}_n$, bashkësia e kodeve binare ciklike, që i kanë të gjitha fjalë kodet me pesha çift. Të vërtetohet se $\langle g(x)\rangle \in \mathbb{E}_n \iff (x-1) \mid g(x)$.

29. Le të jetë C një kod binar ciklik me gjatësi tek dhe polinom përftues $g(x)$. Të vërtetohet që $1 \in C \iff (x-1) \nmid g(x)$.

30. Le të jetë C një kod binar ciklik me gjatësi tek dhe polinom përftues $g(x)$. Të vërtetohet që $1 \in C \iff g(1) \neq 0$.

31. Le të jetë C një kod binar ciklik me gjatësi tek. Të vërtetohet që C përmban një fjalë kod me peshë tek vetëm kur 1 është fjalë kod e C.

32. Të gjendet polinomi përftues i dualit të kodit binar ciklik me gjatësi 7 dhe polinom përftues x^3+x+1.

33. C është kod binar ciklik me gjatsi 7 dhe polinom kontrolli $h(x) = x^3+x^2+1$. Të gjendet polinomi i kontrollit për $C^{\perp}$.

34. Të provohet se nuk ka asnjë kod ciklik ekuivalent me kodin e zgjatur Hamming $[8,4]$.

35. Le të jetë C $[15,11]$ kodi binar ciklik me polinom përftues x^4+x+1.

    (a) Të shkruhet një matricë përftuese në formë standard e C.

    (b) Të vërtetohet që C është kod Hamming.

36. Le të jetë L kod binar linear me matricë përftuese si më poshtë:

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

    (a) Të shkruhen fjalët e kodit $L_1 = \{x \in L | \omega(x) \equiv 2\}$. Të vërtetohet që L_1 është kod ciklik.

    (b) Të gjendet polinomi përftues dhe polinomi i kontrollit i kodit L_1.

37. Jepet kodi binar ciklik me polinom përftues $g(x) = 1+x+x^3$. Të dekodohen fjalët e mëposhtme:

    (a) 1101011.

    (b) 0101111.

    (c) 0100011.

Kreu 8

Përgjigje, udhëzime, zgjidhje

8.1 Entropia dhe ngjeshja

7b Udhëzim. Për dy burime me shpërndarje të probabiliteteve, ndryshoret e pavarura të rastit X dhe Y, ka vend barazimi: $H(X,Y) = H(X) + H(Y)$.

14 Zgjidhje. Meqë $H(S) = -0.7 \cdot \log_2 0.7 - 3 \cdot 0.1 \cdot \log_2 0.1 \approx 1.357$, prandaj, në bazë të teoremës Shanon, ekziston një kodim binar me gjatësi më pak se 1.4 $b/simb$. Gjejmë një kodim Huffman për atë burim:

Simboli	A	B	C	D
kodimi	0	11	100	101
Probabiliteti	0.7	0.1	0.1	0.1

Gjatësia mesatare e këtij kodi është

$$L_{min}(S) = 0.7 \cdot 1 + 0.1 \cdot (2 + 3 + 3) = 1.5 > 1.4$$

Prandaj nuk është ky kodimi **i** kërkuar. Shohim shtrirjen e dytë të tij:

Simb	AA	AB	AC	AD	BA	BB	BC	BD
kod	1	0000	0001	0010	0011	011001	0110100	0110101
gjat	1	4	4	4	4	6	7	7
Prob	0.49	0.07	0.07	0.07	0.07	0.01	0.01	0.01
Simb	CA	CB	CC	CD	DA	DB	DC	DD
kod	0100	011100	011101	0110100	0101	0110101	0110000	0110001
gjat	4	6	6	7	4	7	7	7
Prob	0.07	0.01	0.01	0.01	0.07	0.01	0.01	0.01

Gjatësia mesatare e simboleve të tij është

$$L_{min}(S^2) = 0.49 + 0.07 \cdot (6 \cdot 4) + 0.01 * (6 \cdot 3 + 7 \cdot 6) = 2.77$$

që nga gjatësia për simbol do të jetë $\frac{2.77}{2} = 1.385 < 1.4$

18 Përgjigje. Një kod Hufmann për burimin është

x	a	b	c	d	e
f(x)	000	001	010	011	1

me gjatësi mesatare $L_{\text{min}}(f) = 1.8$, entropi $H(X) = 1.7402$ dhe efektivitet $Ef(X) = 0.9668$.

19 Përgjigje. Meqë burimi është me probabilitete $\frac{2}{5}, \frac{1}{5}, \frac{1}{5}, \frac{1}{5}$, njehsojmë

$$H(S) = \frac{2}{5}\log_2\frac{5}{2} + 3\frac{1}{5}\log_2 5$$

$$H(S) = \log_2 5 - \frac{2}{5} = 2.3219 - \frac{2}{5} = 1.9219$$

rrjedhimisht, nga teorema Shannon e kodimit pa zhurma ka një kodim të këtij burimi me më pak se 1.99 bit për simbol, por nga marrëdhënia e gjatësisë mesatare me entropinë, nuk ka ndonjë kodim me gjatësi

mesatare më të shkurtër se entropia 1.9219.

20 Përgjigje. a) Meqë burimi është me probabilitete $\frac{2}{5}, \frac{1}{5}, \frac{1}{5}, \frac{1}{5}$, njehsojmë

$$H(S) = \frac{2}{5}\log_2\frac{5}{2} + 3\frac{1}{5}\log_2 5$$

$$H(S) = \log_2 5 - \frac{2}{5} = 2.3219 - \frac{2}{5} = 1.9219$$

Një kod Huffman për këtë burim është 1, 01, 000, 010, me gjatësi mesatare $\frac{2}{5} + 2\frac{1}{5} + 3 \cdot 2\frac{1}{5} = (2+2+6)/5 = 2$. Efektiviteti është $\frac{H}{2} = \frac{1.9219}{2} = 0.9609640475$.

21 Zgjidhje. Një kod Huffman binar për burimin

A	B	C	D
$\frac{1}{2}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$

është

A	B	C	D
0	10	110	111

Gjatësia mesatare e tij është

$$L_{\text{min}} = 1 \cdot \frac{1}{2} + 2 \cdot \frac{1}{6} + 2 \cdot 3 \cdot \frac{1}{6} = \frac{11}{6} = 1,8\overline{3}.$$

Ndërsa entropia e tij është

$$H(S) = \sum_{i=1}^{4} p_i \log_2\frac{1}{p_i} = \frac{1}{2} + 3\frac{1}{6}\log_2 6 = 1,79$$

Prandaj

$$Ef(S) = 97,8\%$$

22 Zgjidhje. Një kod Huffman binar për burimin

A	B	C	D
$\frac{4}{7}$	$\frac{1}{7}$	$\frac{1}{7}$	$\frac{1}{7}$

është

A	B	C	D
0	10	110	111

Gjatësia mesatare e tij është

$$L_{\min} = 1 \cdot \frac{4}{7} + 2 \cdot \frac{1}{7} + 2 \cdot 3 \cdot \frac{1}{7} = \frac{12}{7} = 1,714.$$

Ndërsa entropia e tij është

$$H(S) = \sum_{i=1}^{4} p_i \log_2 \frac{1}{p_i} = \frac{4}{7} \log_2 \frac{7}{4} + 3\frac{1}{7} \log_2 7 = 1,66$$

Prandaj

$$Ef(S) = 97,1\%$$

8.2 Kodimi dhe Dekodimi, Kodet Huffman

4 Zgjidhje. Po. Në qoftë se në shifrën $i_0 \in \mathbb{N}_{10}$, a_{i_0} ka ndodhur gabimi $e \in \mathbb{N}_{10}$, atëherë në prodhimin

$$\sum_{i=1}^{10} i \cdot a_{11-i} = 11 \cdot M$$

është ndryshuar termi i i_0 duke u bërë $a_{i_0} + e$ dhe është marrë:

$$11 \cdot M + i_0 \cdot e.$$

Ky numër nuk mund të plotëpjesëtohet nga 11 meqë i mbledhshmi i dytë i tij $i_0 \cdot e$ nuk është i tillë, si prodhim dy numrash më të vegjël se numri i thjeshtë 11.

5 Zgjidhje. Jo. Për shembull, në qoftë se në numrin $ISBN$ $0-521-78280-5$ gabohet në shifrën e tretë (në vend të numrit 2 shkruhet numri 1) e në shifrën e tetë (në vend të numrit 8 shkruhet numri 7) merret numri i mëposhtëm:

$$0-511-78270-5$$

i cili kontrollohet lehtë që nuk është $ISBN$.

6 Përgjigje. Po. Supozojmë se në numrin $ISBN$ (me dhjetë shifra a janë ndërruar shifra e i-të p me shifrën e j-të q. Vërejmë që numrat i, j, p, q janë më të vegjël se 11 dhe $i - j \neq 0$, e $p - q \neq 0$. Në qoftë se numri i ri a' do të ishte një numër $ISBN$, atëherë prodhimi i tij me vektorin $V = (10,9,8,7,6,5,4,3,2,1)$ do të jetë shumëfish i 11, ashtu si dhe prodhimi $a' \cdot V$. Diferenca e këtyre prodhimeve do të jetë

$$i \cdot p + j \cdot q - i \cdot q - j \cdot p = (p-q)(i-j),$$

gjithashtu do të jetë shumëfish i 11, si diferencë e dy shumëfishave të tillë. Por kjo gjë nuk mund të ndodhë, meqë numri i thjeshtë 11 nuk mund të jetë prodhim dy numrash më të vegjël se ai.

8a Përgjigje. Shifra e fundit duhet të jetë 0, meqë prodhimi i (0 1 3 8 6 9 0 1 7 0) me (10 9 8 7 6 5 4 3 2 1) është $187 = 11 \cdot 17$.

8b Përgjigje. Numri i kërkuar është (9 7 8 0 1 3 8 6 9 0 1 7 5), meqë prodhimi i tij me vektorin $(1,3,1,3,1,3,1,3,1,3,1,3,1)$ është 110, pra shumëfish i 10.

10 Zgjidhje. $1010001 = (1010)(001) = AB = (101)(0001) = CD$.

18 Përgjigje. Numri i kërkuar është më i vogli numër natyror x që plotëson mosbarazimin Kraft $12x^{-2} + 4x^{-1} \leq 1$. Duke zgjidhur inekuacionin përkatës $x^2 - 4x - 12 \geq 0$ marrim vlerën më të vogël të x të barabartë me 6.

8.3 Kodet gabimndreqëse

2. Përgjigje.

a. d = 2. Zbulon 1, nuk ndreq asnjë.
b. d = 2.
c. d = 3. Ndreq 1 e zbulon 2.

9. Përgjigje. 2, 1 nuk mund të jetë se 11 është numër prim.

10. Përgjigje. Gjen 1 dhe nuk ndreq asgjë.

11. Përgjigje. Jo. Alfabeti i tij nuk është fushë.

12a Përgjigje. Në qoftë se ndodh një gabim, ndryshon çiftësia në 1 rresht e një shtyllë, atëherë ndreqet biti në prerjen e tyre.
12b Jo. Në qoftë se janë në një rresht apo një shtyllë, atij i shpëton.
12c $min(r,s)$.

13 Zgjidhje. Supozojmë që C zbulon ekzaktësisht t gabime. Pra ai zbulon t gabime, prandaj $d(C) \geqslant t+1$. $d(C)$ nuk mund të jetë $t+2$, sepse C do zbulonte $t+1$ gabime, pra $d(C) = t+1$. Anasjelltas, në qoftë se $d(C) = t+1$, atëhere meqë $d(C) > t$, C zbulon t gabime. C nuk mund të zbulojë $t+1$ gabime, sepse përndryshe $d(C) \geqslant t+2$. (!)

14 Udhëzim. Të ndiqet e njëjta rrugë e vërtetimit si tek ushtrimi **13**.

15 Përgjigje. $g = d-1$, $k = \left[\frac{d-1}{2}\right]$.

16 Zgjidhje. Në qoftë se C do përdoret vetëm për gjetje gabimesh, atëhere ai do të zbulojë $d-1$ gabime ose $2t+1$.
Supozojmë se C përdoret njëkohësisht për gjetje dhe ndreqje gabimesh. Meqë $d = 2t+2$, C ndreq ekzaktësisht t gabime (*Ushtrimi 14*). Pra në qoftë se pas transmetimit në kanal merret fjala x dhe në qoftë se ekziston c për të cilën $d(c,x) \leqslant t$, atëhere kanë ndodhur të shumtën t gabime dhe ndreqet x si c.
Tani supozojmë se kanë ndodhur $t+1$ gabime gjatë transmetimit të c duke marrë në dalje fjalën x. Të provojmë që nuk ekziston ndonjë $d \in C$ të tillë që $d(x,d) \leqslant t$.
Sikur të ndodhte kjo, do kishim absurditet si më poshtë:

$$d(c,d) \leqslant d(c,x) + d(x,d) \leqslant t+1+t = 2t+1 < d.$$

Pra x nuk mund të ndreqet si ndonjë fjalë kod c i vetëm nga C, por ekziston ndonjë $d \in C$ i tillë që $d(c,x) = d(d,x) = t+1$ dhe C zbulon $t+1$ gabime.
Në qoftë se ndodhin $t+2$ gabime, meqë $d = 2t+2$, në të paktën një rast, ekziston $d \in C$ me distancë nga x të barabartë me $d(d,x) = t$. Pra në këtë rast fjala x do të dekodohej gabimisht si d dhe jo si c.
C jo gjithmonë zbulon $t+2$ gabime.
Pë rastin e distancës tek mund të tregohet në të njëjtën mënyrë se C

nuk arrin të zbulojë dhe ndreqë më shumë se t gabime.

24 Zgjidhje. Barazimi $d(C) = 1$ do të thotë që janë të gjitha fjalët kod të ndryshme nga njëra-tjetra. Pra C mund të përmbajë të gjitha fjalët e F_q^n, rrjedhimisht

$$M = |F_q^n| = q^n.$$

25 Zgjidhje. Le të jetë $C \subseteq F_q^n$ një $(n, M, n) - kod$. Atëherë distanca $d(x, y)$ midis dy fjalëve është maksimalja e mundshme, pra fjalët x e y ndryshojnë nga të gjitha pozicionet. Kjo do të thotë që në çdo pozicion shfaqen jo më shumë se të gjithë simbolet e mundshme, pra $M \leq q$.
Nga ana tjetër, kodi q- ar me përsëritje ka q fjalë dhe distancë minimale n. Rrjedhimisht $A_q(n, n) = q$.

28 Zgjidhje. Le të jetë C një (n, M, d)-kod binar me d tek. Me anë të tij ndërtojmë kodin $\overline{C}$ që ka të gjitha fjalët e C të zgjatura me një bit të kontrollit të çiftësisë. Pra, për çdo fjalë $x = x_1x_2 \ldots x_n \in C$ ndërtojmë fjalën $\overline{x} \in \overline{C}$:

$$\overline{x} = \begin{cases} x_1x_2 \ldots x_n0, & \text{në qoftë se } \omega(x) = 0 \pmod 2 \\ x_1x_2 \ldots x_n1, & \text{në qoftë se } \omega(x) = 1 \pmod 2. \end{cases}$$

Është e qartë që $\overline{C}$ ka gjatësi $n + 1$ dhe madhësi M. Përveç kësaj, të gjitha fjalët e tij kanë peshë çift.
Distanca e çdo dy fjalëve $\overline{x}, \overline{y} \in \overline{C}$:

$$d(\overline{x}, \overline{y}) = \omega(\overline{x}) + \omega(\overline{y}) - 2\omega(\overline{x} * \overline{y})$$

do të jetë numër çift, si shumë numrash çift.
Atëherë dhe distanca minimale e kodit $\overline{C}$ do të jetë çift.
Nga ana tjetër, $d(\overline{C}) \leq d + 1$, dhe meqënëse d është tek, marrin $d(\overline{C}) = d + 1$.

Anasjelltas, le të jetë D një $(n + 1, M, d + 1)$ kod binar dhe le të jenë $x, y \in D$ të tillë që $d(x, y) = d + 1$.
Gjejmë një koordinatë ku fjalët x e y ndryshojnë dhe e fshijmë në të, të gjithë fjalët kod të D. Kodi i përftuar në këtë mënyrë do të jetë një (n, M, d) kod.

29 Zgjidhje. Rrjedhim i ushtrimit 28.

30 Zgjidhje. Rrjedhim i ushtrimit 28.

32 Përgjigje. Jo.

33 Udhëzim. Numri i fjalëve që përftohen nga ndonjë fjalë kod x i C duke ndryshuar të shumtën 2 simbole, është sa $|S_2(x, 2)|$. Të shfrytëzohet edhe fakti që sferat $S_2(x, 2)$ $\forall x \in C$ duhet të jenë joprerëse në mënyrë që C të ndreqë dy gabime.

36 Përgjigje dhe udhëzim. Të tregohet fillimisht që për një distancë d të fiksuar, çdo dy $(n, 2, d)$-kode janë ekuivalente. Nga ana tjetër, dy $(n, 2)$-kode me distanca të ndryshme, nuk mund të jenë ekuivalente.
Që këtej rrjedh se numri i kodeve binare joekuivalente është sa numri i distancave të ndryshme, pra n.

37 Zgjidhje. Duket që gjatësia e kodit $C_1 \oplus C_2$, është $2 \cdot n$ dhe madhësia e tij është $M_1 \cdot M_2$.

Njehsojmë distancën e kodit. Marrim dy fjalë kode të ndryshme $u_1 = c_1|(c_1 + d_1)$ dhe $u_2 = c_2|(c_2 + d_2)$ ku $c_1 \in C_1$ dhe $c_2 \in C_2$.
Supozojmë fillimisht se $d_1 = d_2$. Kemi:

$$d(u_1, u_2) = 2 \cdot d(c_1, c_2) \geqslant 2 \cdot d_1.$$

Shqyrtojmë $d_1 \neq d_2$. Kemi:

$$d(u_1, u_2) = \omega(u_1 - u_2) = \omega(c_1 - c_2) + \omega(c_1 - c_2 + d_1 - d_2).$$

Shfrytëzojmë mosbarazimin e trekëndëshit dhe kemi:

$$d(u_1, u_2 \geqslant \omega(d_1 - d_2) = d(d_1, d_2) \geqslant d_2.$$

Kemi vërtetuar kësisoj që:

$$d(C_1 \oplus C_2) \geqslant min\{2 \cdot d_1, d_2\}.$$

8.4 Kodet lineare

2 Përgjigje. Jo.

4 Përgjigje. $G = [11\ldots1]$. Numri i matricave përftuese është $q-1$.

8 Zgjidhje. Supozojmë se kodi linear C përbëhet nga fjalët

$$v_1, v_2, v_3, \ldots, v_n,$$

ku fjala kod v_1 është me peshë çift. Atëherë fjalët

$$v_1 + v_1, v_2 + v_1, v_3 + v_1, \ldots, v_n + v_1,$$

nga lineariteti i C janë përsëri fjalë kod. Për më tepër janë të ndryshme, meqë nga

$$v_i + v_1 = v_j + v_1$$

do të rridhte

$$v_i = v_j.$$

Pra

$$K = \{v_1 + v_1, v_2 + v_1, v_3 + v_1, \ldots, v_n + v_1\}.$$

Kuptohet që, sa herë që një fjalë kod v_i ka peshë tek, fjala $v_i + v_1$ ka peshë çift, dhe anasjelltas. Pra pasqyrimi

$$v_i \rightarrow v_i + v_1$$

është një përkëmbim i C që kalon fjalët me peshë tek te ato me peshë çift dhe anasjelltas. Kjo tregon se sasia e atyre fjalëve është e njëjtë.

9 Zgjidhje. Ka vetëm një fjalë kod me peshë n. Ajo është $x = 11\ldots1$. Pra $A_n = \{x\}$.

Meqë L është kod linear, ai është i mbyllur në lidhje me veprimin e mbledhjes. Atëherë,

$$\forall l \in L,\ l + x \in L.$$

Duket qartë që:

$$\omega(l+x) = n - \omega(l)$$

ose

$$l \in A_i \implies l + x \in A_{n-i}.$$

Duhet treguar lidhja bijektive midis A_i dhe A_{n-i} $\forall i \in \{0,1,\dots,n\}$. Ndërtohen pasqyrimet e mëposhtme:

$$f_i : A_1 \to A_{n-i} : f_i(l) = l + x$$

$$k_i : A_{n-i} \to A_i : k_i(d) = d + x$$

Këto pasqyrime janë bijektive sepse:

$$f_i \circ k_i = id = k_i \circ f_i.$$

Kjo tregon që $|A_i| = |A_{n-i}|$ $\forall i \in \{0,1,\dots,n\}$.

14 Përgjigje. $d(C_1 \oplus C_2) = \min\{d(C_1), d(C_2)\}$.

$$G_1 \oplus G_2 = \begin{pmatrix} G_1 & 0 \\ 0 & G_2 \end{pmatrix}$$

$$H_1 \oplus H_2 = \begin{pmatrix} H_1 & 0 \\ 0 & H_2 \end{pmatrix}.$$

16 Udhëzim dhe përgjigje. Në qoftë se

$$e_1, e_2, \dots, e_{k_1}, \quad \text{dhe } f_1, f_2, \dots f_{k_2}$$

janë përkatësisht baza të hapësirave C_1 e C_2, atëherë vërtetohet lehtë se sistemi i vektorëve të $C_1|C_2$:

$$(e_1|e_1), (e_2|e_2), \dots, (e_{k_1}|e_{k_1}), (0|f_1), (0|f_2) \dots, (0|f_{k_2})$$

është jo vetëm linearisht i pavarur, por dhe sistem përftuesish për atë hapësirë, prandaj do të jetë dhe bazë e saj. Rrjedhimisht,

$$dim(C_1|C_2) = dim(C_1) + dim(C_2).$$

Nga ana tjetër, shënojmë $u = (x_1, x_1 + y_1)$ dhe $v = (x_2, x_2 + y_2)$ dy vektorë të çfarëdoshëm të $C_1|C_2$. Në qoftë se $y_1 = y_2$, atëherë

$$d(u,v) = 2d(x_1, x_2) \geq 2d(C_1).$$

Në qoftë se $y_1 \neq y_2$, atëherë

$$\begin{aligned} d(u,v) &= wt(x_1 - x_2) + wt(x_1 - x_2 + y_1 - y_2) \geq wt(y_1 - y_2) = \\ &= d(y_1, y_2) \geq d(C_2). \end{aligned}$$

(Nga mosbarazimi i trekëndëshit

$$wt(-a) + wt(a+b) \geq wt(b),$$

meqë $wt(x) + wt(y) \geq wt(x+y)$.)
Barazimet arrihen në të dy rastet, prandaj, përfundimisht,

$$d(C_1|C_2) = \min\{2d(C_1), d(C_2)\}.$$

17 Përgjigje.

$$G_1|G_2 = \begin{pmatrix} G_1 & G_2 \\ 0 & G_2 \end{pmatrix}$$

$$H_1|H_2 = \begin{pmatrix} H_1 & 0 \\ -H_2 & H_2 \end{pmatrix}.$$

18 Zgjidhje. Mund të përftohet si bashkim dy kodesh, njëri $[4,3,2]$ kod e tjetri $[4,1,4]$ kod. Ata kode kanë matrica përftuese përkatësisht

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

dhe

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

Shënojmë që vetë C_1 mund të përftohet si bashkim dy kodesh, njëri $[2,2,1]$ kod e tjetri $[2,1,2]$ kod. Ata kode kanë matrica përftuese përkatësisht

$$G_3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ dhe } G_4 = \begin{pmatrix} 1 & 1 \end{pmatrix}.$$

20 Zgjidhje. Ndërrojmë shtyllën e tretë me të katërtën:

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

Ndërrojmë rreshtin e parë me të tretin, duke marrë formën standarde:

$$\overline{\overline{G}} = \begin{pmatrix} 1 & 0 & 0 & 2 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 2 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} = (I_k|A).$$

Matrica e kontrollit $\overline{\overline{H}} = (-A^{\mathsf{T}}|I_{n-k})$ do të jetë

$$\overline{\overline{H}} = \begin{pmatrix} -2 & -1 & 0 & 1 & 0 & 0 \\ -1 & -1 & -1 & 0 & 1 & 0 \\ -1 & -2 & -1 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 0 & 1 & 0 & 0 \\ 2 & 2 & 2 & 0 & 1 & 0 \\ 2 & 1 & 2 & 0 & 0 & 1 \end{pmatrix}.$$

Ndërrojmë shtyllën e tretë me të katërtën e marrim matricën e kontrollit:

$$\overline{H} = \begin{pmatrix} 1 & 2 & 1 & 0 & 0 & 0 \\ 2 & 2 & 0 & 2 & 1 & 0 \\ 2 & 1 & 0 & 2 & 0 & 1 \end{pmatrix}.$$

21 Përgjigje.

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

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

3. $C = \{(0000), (1001), (0110), (1111)\}$,

4. $C^{\perp} = \{(0000), (1001), (0110), (1111)\}$,

5. $d(C) = 2$, gjen 1 gabim e nuk ndreq gjë.

22 Përgjigje.

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

23 Zgjidhje. Në shtyllat e matricës G nuk janë të gjitha shtyllat e matricës njësi I_3, prandaj ndërtojmë një matricë përftuese për të njëjtin kod, që ka për shtylla të gjitha shtyllat e I_3. Kjo arrihet duke i shtuar rreshtit të parë rreshtin e dytë të saj:

$$G = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} \begin{matrix} (+II) \\ \\ \\ \\ \end{matrix} \sim G' = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}.$$

E anasjellta e djathtë e G' është

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

Duke i shtuar rreshtit të parë të K' rreshtin e dytë të saj marrim një matricë të anasjelltë të djathtë të matricës G:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{matrix} (+II) \\ \\ \\ \\ \\ \\ \\ \end{matrix} \sim K = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Për të dekoduar, njehsojmë

$$\mathbf{x} = \mathbf{x}G \cdot K = (1000110)$$

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

29 Zgjidhje. Fjalët e kodit L janë zgjidhje të ekuacionit matricor $H \cdot x^\top = 0^\top$, ku $x = (x_1, x_2, x_3, x_4, x_5, x_6, x_7)$. Ky sistem ekuacionesh mund të shkruhet duke shprehur x_2, x_3, x_5, x_6 në varësi të x_1, x_4, x_7 (kjo rrjedh nga fakti se shtyllat $2, 3, 5, 6$ janë shtyllat e matricës njësi I_7). Rreshtat e matricës përcaktojnë ekuacionet e mëposhtme:

$$\begin{cases} x_2 = x_1 + x_4 + x_7 \\ x_5 = x_4 + x_7 \\ x_3 = x_1 + x_4 + x_7 \\ x_6 = x_7 \end{cases}$$

Ka tetë vlera të ndryshme te x_1, x_4, x_7, të cilat përcaktojnë fjalët kod:

$$\begin{pmatrix} 0000000 & 1110000 \\ 0110111 & 1000111 \\ 0111100 & 1001100 \\ 0001011 & 1111011 \end{pmatrix}$$

30 Zgjidhje.

1. E kthejmë matricën H në formën standard, duke i mbledhur rreshtit të parë të dytin:

$$H' = \begin{pmatrix} 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 0 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{pmatrix},$$

duke zëvendësuar në matricën e përftuar çdo element me të kundërtin e tij:

$$H'' = \begin{pmatrix} 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 \\ 10 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix},$$

e së fundi duke i zbritur rreshtit të dytë dyfishin e rreshtit të parë:

$$H''' = \begin{pmatrix} 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 \\ 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 0 & 1 \end{pmatrix}.$$

Matrica përftuese e kodit do të jetë

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 8 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 7 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 4 & 6 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 5 & 5 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 6 & 4 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 7 & 3 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 8 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 9 & 1 \end{pmatrix}.$$

2. Për të koduar fjalën (1 1 0 0 0 0 0 0), shumëzojmë:

$$(1\,1\,0\,0\,0\,0\,0\,0) \cdot G = (1\,1\,0\,0\,0\,0\,0\,0\,5\,4).$$

31 Përgjigje 3.

38 Zgjidhje. Çdo dy shtylla janë linearisht të pavarura, ndërkohë që ekzistojnë tri shtylla (për shembull e para, e dyta dhe e fundit) linearisht të varura. Pra distanca minimale e këtij kodi është 3, dhe ai ndreq 1 e gjen 2 gabime.

39a Zgjidhje. Duket qartë që matrica përftuese e kodit është

$$\widehat{G} = \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{array}\right),$$

që nga dhe $\widehat{G} = \widehat{H}$.

39b Zgjidhje. Matrica përftuese e kodit dual të tij është matrica e kontrollit e $\mathcal{H}_{3,2}$. Meqë G është në trajtë standard, ajo matricë është:

$$\dot{\overline{G}} = {}^{+II}\begin{pmatrix} -1 & -1 & 1 & 0 \\ -1 & 1 & 0 & 1 \end{pmatrix} \sim$$

$$\sim {}_{+I}\begin{pmatrix} 1 & 0 & 1 & 1 \\ -1 & 1 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix} = G.$$

Pra matrica përftuese e kodit dual të $\mathcal{H}_{3,2}$ është matricë përftuese e vetë kodit $\mathcal{H}_{3,2}$. Kjo tregon se ai kod është vetë dual.

40 Zgjidhje. Nuk ekzistojnë kode lineare vetë duale me gjatësi 3, sepse në qoftë se C është kod $[3, k]$ ku $k \in \{1, 2, 3\}$, $C^\perp$, duhet të jetë $[3, 3-k]$ kod. Por nuk ka k të tillë që $k = 3 - k$. Kodi me gjatësi 4

$$C_1 = \{0000, 1010, 0101, 1111\},$$

është vetë dual. Matrica:

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

është matricë përftuese e C_1. Shihet lehtë që $G = H = G^\perp$, pra C_1 është vetë-dual.

41a Zgjidhje. Me qënë se $C \subset C^\perp$, atëherë ka vend vargu i implikimeve:

$$\begin{aligned} a \in C \quad & \Rightarrow a \in C^\perp \Rightarrow (\forall b \in C \quad a \cdot b = 0) \Rightarrow \\ & \Rightarrow a \cdot a = 0 \Rightarrow \omega(a) = 0 \mod 2. \end{aligned}$$

41b Zgjidhje. Për të treguar pjesën e dytë, mjafton të tregojmë se fjala $\mathbf{1} = 11\cdots1$ është ortogonale me çdo fjalë a të kodit C. Kjo do të thotë se

$$\forall a \in C, \quad \mathbf{1} \cdot a = 0,$$

ose, ndryshe,

$$\forall a \in C, \quad \omega(a) = 0 \mod 2.$$

41c Vërtetimi kryhet njësoj si te vërtetimi i pjesës së parë te 41a, por sipas $\mod 3$.

42 Zgjidhje. Shënojmë $\mathbf{c}$ një fjalë të kodit $C^\perp$ që është zero në të gjitha koordinatat e S, ndërsa $\mathbf{c}^*$ fjalën që merret nga $\mathbf{c}$ duke fshirë koordinatat e S. Pra $\mathbf{c}^* \in (\mathcal{C}^\perp)_S$. Për çdo $\mathbf{x} \in \mathcal{C}$, duke shënuar $\mathbf{x}^*$ fjalën $\mathbf{x}$ të shpuar në S, kemi

$$0 = \mathbf{x} \cdot \mathbf{c} = \mathbf{x}^* \cdot \mathbf{c}^*.$$

Pra treguam që

$$(\mathcal{C}^\perp)_S \subset (\mathcal{C}^S)^\perp.$$

Le të jetë $\mathbf{c} \in (\mathcal{C}^S)^\perp$. E shtrijmë atë vektor deri në një vektor $\overline{\mathbf{c}}$ me gjatësi n duke shtuar 0 në koordinatat e S. Në qoftë se $\mathbf{x} \in \mathcal{C}$, e shpojmë $\mathbf{x}$ në S duke marrë $\mathbf{x}^*$, për të cilin kemi

$$0 = \mathbf{x}^* \cdot \mathbf{c} = \mathbf{x} \cdot \overline{\mathbf{c}},$$

që nga $\mathbf{c} \in (\mathcal{C}^\perp)_S$. Treguam kështu që $(\mathcal{C}^\perp)_S = (\mathcal{C}^S)^\perp$.
Duke zëvendësuar $\mathcal{C}$ me $\mathcal{C}^\perp$ përftojmë barazimin tjetër

$$(\mathcal{C}^\perp)^S = (\mathcal{C}_S)^\perp.$$

43 Zgjidhje. Në qoftë se kodi është me gjatësi numrin tek n, atëherë sferat janë me rreze $\frac{n-1}{2}$, prandaj kushti i nevojshëm dhe i mjaftueshëm që ky kod të jetë i përsosur është:

$$2\left[C_n^0 + C_n^1 + \cdots + C_n^{\frac{n-1}{2}}\right] = 2^n.$$

Meqë ky barazim është i vërtetë, atëherë kodi binar me përsëritje me gjatësi tek është i përsosur.

45 Zgjidhje. Supozojmë se ndodhin $e+1$ gabime dhe le të jetë a një fjalë e gabuar në a' me $d(a,a') = e+1$. Atëherë a' do të jetë më afër një fjale kod tjetër (meqë do të jetë në një sferë tjetër), të ndryshme nga a, prandaj do të dekodohet gabimisht si ajo.

46 Përgjigje. $A_0 = A_6 = 1, A_2 = A_4 = 3$

49. Zgjidhje. Duket që $A_C(z) = 1 + 3z^2$. Për të gjetur $C^\perp$ formojmë së pari matricën përftuese të C:

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

Atëhere matrica e kontrollit e tij, që është matricë përftuese për kodin dual $C^\perp$, është $H = (1\,1\,1)$. Që këndej, kodi dual ëshë kodi me përsëritje $C^\perp = \{000, 111\}$, me numërues peshash $A_{C^\perp}(z) = 1 + z^3$.

8.5 Disa kode lineare

2 Zgjidhje. Meqë $2^m - 1 = 3$, atëherë $m = 2$ dhe matrica e kontrollit është:

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

Ndërsa matrica përtuese është $G = (111)$ dhe rrjedhimisht kodi Hamming me gjatësi 3 është kodi me përsëritje.

3 Zgjidhje. Renditim shtyllat e matricës H në rradhën rritëse, atëherë shtyllat e saj janë paraqitjet binare të numrave $1, 2, \ldots, 2^r - 1$. Me këto shënime, vektori $1\,1\,1\,0\,0 \ldots, 0\,0$ është ortogonal me të gjithë rreshtat e matricës H, prandaj dhe është fjalë kod e kodit Hamming.

4 Zgjidhje. Në qoftë se H është matrica e kontrollit e kodit $Ham(m, 2)$, atëherë ky kod është hapësira e zgjidhjeve të sistemit të ekuacioneve lineare homogjene me matricë H, prandaj dimensioni i kësaj hapësire është $n - m = 2^m - 1 - m$.

5 Zgjidhje. Në qoftë se matrica e kontrollit e kodit $Ham(m, 2)$ ka m rreshta dhe $n = 2^m - 1$ shtylla, atëherë $\dim(Ham(m, 2)) = n - m = 2^m - 1 - m$. Kjo do të thotë se në këtë hapësirë ka $n - m = 2^m - 1 - m$ vektorë linearisht të pavavur, që e përftojnë atë. Atëherë numri i vektorëve të $Ham(m, 2)$ do të jetë sa numri i kombinimeve lineare të këtyre vektorëve, me koeficientë në $GF(2)$: $2^{n-m} = 2^{2^m - 1 - m}$.

6 Zgjidhje. Kthejmë matricën e kontrollit të kodit të Hamming-ut në formë standard:

$$\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \sim$$

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Në transformimin e parë i është mbledhur rreshtit të parë rreshti i dytë, tek i dyti i kemi mbledhur rreshtit të tretë rreshtin e parë, ndërsa tek i treti i është mbledhur rreshtit të dytë rreshti i tretë i përftuar.
Matrica e fundit, e konsideruar në trajtën $(A_{3\times 4}|I_3)$, ka matricë ortogonale matricën $(I_4|A^\top)$:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

7 Zgjidhje. Matrica e kontrollit e kodit binar Hamming me gjatësi 15 është:

$$H = \begin{pmatrix} 0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1\,1 \\ 0\,0\,0\,1\,1\,1\,1\,0\,0\,0\,0\,1\,1\,1\,1 \\ 0\,1\,1\,0\,0\,1\,1\,0\,0\,1\,1\,0\,0\,1\,1 \\ 1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1 \end{pmatrix}.$$

Njehsojmë sindromat $s = H \cdot x^T$ në secilin rast:

1. $s_a = \begin{pmatrix} 0 & 0 & 1 & 0 \end{pmatrix}^T = 13$. Dekodojmë duke ndryshuar bitin e trembedhjetë në fjalën e marrë x: $y = 001000001100000$.

2. $s_b = \begin{pmatrix} 0 & 0 & 0 & 0 \end{pmatrix}^T = 0$, pra fjala e marë është fjalë kod. Dekodojmë duke mos ndryshuar gjë në fjalën e marrë x: $y = 101001110101100$.

3. $s_c = \begin{pmatrix} 0 & 1 & 0 & 0 \end{pmatrix}^T = 4$. Dekodojmë duke ndryshuar bitin e katërt në fjalën e marrë x: $y = 000000100011000$.

4. $s_d = \begin{pmatrix} 0 & 1 & 0 & 1 \end{pmatrix}^T = 5$. Dekodojmë duke ndryshuar bitin e pestë në fjalën e marrë x: $y = 000000100011000$.

5. $s_e = \begin{pmatrix} 1 & 1 & 0 & 1 \end{pmatrix}^T = 13$. Dekodojmë duke ndryshuar bitin e trembëdhjetë në fjalën e marrë x: $y = 110011100011000$.

6. $s_f = \begin{pmatrix} 0 & 0 & 1 & 0 \end{pmatrix}^T = 2$. Dekodojmë duke ndryshuar bitin e dytë në fjalën e marrë x: $y = 110001000011101$.

8 Zgjidhje. Renditim shtyllat e matricës H në rradhën rritëse, atëherë shtyllat e saj janë paraqitjet binare të numrave $1, 2, \ldots, 2^r - 1$. Me këto shënime, duket që çdo dy shtylla janë linearisht të pavarura, ndërsa tri shtyllat e para

$$\begin{pmatrix} \vdots \\ 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} \vdots \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} \vdots \\ 0 \\ 1 \\ 1 \end{pmatrix},$$

(për shembull) janë linerisht të varura.

9 Zgjidhje. Matrica e kontrollit e kodit Hamming me shtylla të renditura drejt është:

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

rrjedhimisht sindroma e fjalës së marrë x është:

$$H \cdot x^T = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}.$$

Në sistemin dhjetor ky numër është 6, prandaj ndreqet biti i gjashtë në fjalën x e merret

$$y = x + (0,0,0,0,0,1,0) = (1,1,0,1,0,0,1)$$

12 Zgjidhje. Kodi $Ham(3,3)$ ka parametra të formës:

$$\left(\frac{3^3-1}{3-1}, \frac{3^3-1}{3-1} - 3, 3 \right) = (13, 10, 3).$$

Për të ndërtuar matricën e kontrollit shkruhen kollonat e saj në rendin rritës si numra ternarë, por për të cilët simboli i parë jozero në çdo kollonë duhet të jetë 1. Matrica e kontrollit $H(3,3)$ do të jepej si më poshtë:

$$H(3,3) = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 1 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \end{pmatrix}.$$

Për të dekoduar ω, fillimisht gjejmë sindromën e saj:

$$s = H(3,3) \cdot \omega^T = 200.$$

$s = 2 \cdot (100)$ dhe sindroma është e formës $\alpha \cdot e_i \cdot H^T$, ku e_i është gabimi që ka ndodhur në bitin e i-të. Meqë $100_2 = 5_{10}$, gabimi ka ndodhur në bitin e 5-të.
Vektori i gabimit është:

$$(0000200000000).$$

Fjala kod e dërguar është:

$$c = \omega - e = (2222021111111).$$

Në të njëjtën mënyrë dekodohet edhe γ si (1101110211201).

13 Zgjidhje. Duhet të tregojmë që për parametrat e $Ham(m, 2)$ plotësohet kondita e nevojshme dhe e mjaftueshme që një kod të jetë i

përsosur.
Vërtet, për parametrat $n = 2^m - 1, M = 2^{n-m}, t = 1$ kemi:

$$2^{n-m}\left(1 + C_n^1\right) = 2^{n-m}(1 + 2^m - 1) = 2^{n-m} \cdot 2^m = 2^n.$$

15 Zgjidhje.

1. $q = 2, n = 7, d = 3 \Longrightarrow r = \left[\frac{d-1}{2}\right] = \left[\frac{3-1}{2}\right] = 1 \Longrightarrow A_2(7,3) \leq \frac{2^7}{C_7^0 + C_7^1} = \frac{2^7}{1+7} = 16.$

2. $q = 2, n = 7, d = 4 \Longrightarrow r = \left[\frac{d-1}{2}\right] = \left[\frac{4-1}{2}\right] = 1 \Longrightarrow A_2(7,4) \leq \frac{2^7}{C_7^0 + C_7^1} = \frac{2^7}{1+7} = 16.$

3. $q = 2, n = 8, d = 3 \Longrightarrow r = \left[\frac{d-1}{2}\right] = \left[\frac{3-1}{2}\right] = 1 \Longrightarrow A_2(8,3) \leq \frac{2^8}{C_8^0 + C_8^1} = \frac{2^8}{1+8} = 28.4$

4. $q = 2, n = 15, d = 3 \Longrightarrow r = \left[\frac{d-1}{2}\right] = \left[\frac{3-1}{2}\right] = 1 \Longrightarrow A_2(15,3) \leq \frac{2^{15}}{C_{15}^0 + C_{15}^1} = \frac{2^{15}}{1+15} = 2048.$

5. $q = 2, n = 23, d = 7 \Longrightarrow r = \left[\frac{d-1}{2}\right] = \left[\frac{7-1}{2}\right] = 3 \Longrightarrow A_2(23,7) \leq \frac{2^{23}}{C_{23}^0 + C_{23}^1 + C_{23}^2 + C_{23}^3} = 4096.$

6. $q = 3, n = 12, d = 5 \Longrightarrow r = \left[\frac{d-1}{2}\right] = \left[\frac{5-1}{2}\right] = 2 \Longrightarrow A_3(12,5) \leq \frac{3^{12}}{C_{12}^0 + C_{12}^1 \cdot 2 + C_{12}^2 \cdot 2^2} = 183.89...$

16 Zgjidhje. Kodi Hamming është i përsosur për ndreqjen e një gabimi, pra kur ndodhin 2 gabime ai ndreq gabim (se i ndreq patjetër).
Po ashtu, ai ndreq gabim kur ndodhin 3, 4, 5, 6 e 7 gabime. Me një fjalë ai ndreq mirë vetëm kur ndodh 1 gabim, çka ndodh me probabilitet $C_7^1 p(1-p)^6$, dhe kur nuk ndodh asnjë gabim, me probabilitet $(1-p)^7$. Rrjedhimisht, probabiliteti i gabimit është

$$1 - (1-p)^7 - C_7^1 p(1-p)^6 = 1 - 0,99^7 - 7 \cdot 0,99^6 \cdot 0,01 \approx 0.002.$$

19 Përgjigje.

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

20 Përgjigje. a)

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{pmatrix},$$

b)

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 1 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \end{pmatrix}.$$

21 Zgjidhje. Meqë $Ham(r,q)$ është i përsosur, ai ka numrin maksimal të fjalëve me distancë 3, prandaj $A_q(n,3) = |Ham(r,q)| = q^{n-r}$.

22 Zgjidhje. $S(x) = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}$, që është shtylla e parë e matricës $\overline{H}$ dhe prandaj ndreqet biti i parë.

23 Zgjidhje. $S(x) = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix}$, prandaj kanë ndodhur një numër çift gabimesh, dhe kërkohet ritransmetim.

24 Zgjidhje. Matrica përftuese e kodit $R(1,2)$ është

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

Atëhere një matricë kontrolli e tij është $(1\,1\,1\,1)$, pra $R(1,2)$ është kodi i kontrollit të çiftësisë.

26 Zgjidhje. Vërejmë që matrica e kontrollit e $R(1,3)$ është

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

Po kjo është dhe matrica e kontrollit e $(8,4)$ kodit të shtrirë Hamming, prandaj ka vend pohimi.

27 Zgjidhje.

$$\begin{array}{rcllllllllllllllll}
\mathbf{v}_0 & = & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\mathbf{v}_1 & = & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
\mathbf{v}_2 & = & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
\mathbf{v}_3 & = & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
\mathbf{v}_4 & = & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\mathbf{v}_1 * \mathbf{v}_2 & = & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1. \\
\mathbf{v}_1 * \mathbf{v}_3 & = & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
\mathbf{v}_1 * \mathbf{v}_4 & = & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
\mathbf{v}_2 * \mathbf{v}_3 & = & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
\mathbf{v}_2 * \mathbf{v}_4 & = & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
\mathbf{v}_3 * \mathbf{v}_4 & = & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1
\end{array}$$

28 Zgjidhje.

$$\begin{aligned}
\delta &= 2^{23} - 2^{12}(1 + 23 + C_{23}^2 + C_{23}^3) = 2^{23} - 2^{12}(1 + 23 + 253 + 1771) \\
&= 2^{23} - 2^{12}2048 = 2^{23} - 2^{12}2^{11} = 0.
\end{aligned}$$

29 Vërtetim.

$$\begin{aligned}
\delta &= 3^{11} - 3^6(C_{11}^0 + C_{11}^1 \cdot 2 + C_{11}^2 \cdot 2^2) \\
&= 3^{11} - 3^6(1 + 22 + 220) = 3^{11} - 3^6 \cdot 3^5 = 0.
\end{aligned}$$

8.6 Tabelat standarde

5 Zgjidhje. K_5 jepet nga barazimet e mëposhtme:

$$\begin{aligned} x_4 &= x_1 + x_2 \\ x_5 &= x_1 + x_2 + x_3 + x_4 \end{aligned}$$

Në tabelën drejtkëndëshe fillojmë me kodin K_5. Meqë K_5 ka 3 bite informacioni, ai ka $2^3 = 8$ fjalë kod. Rrjedhimisht kemi $2^{5-3} = 4$ klasa fqinje.

Më tej, zgjedhim si drejtues ndonjë fjalë me peshë 1, për shembull 10000. Kjo nuk është fjalë kod, prandaj mund ta zgjedhim atë si drejtues të klasës fqinje $10000 + K_5$:

Drejtuesi i klasës fqinje							
00000	10010	01010	00101	11000	10111	01111	11101
10000	00010	11010	10101	01000	00111	11111	01101

Zgjedhim tani një drejtues tjetër me peshë Hamming 1 e që nuk ndodhet në dy rreshtat e parë (të tillë ka), për shembull 00001. E zgjedhim atë si drejtues.

Për të vazhduar më tej vërejmë se fjalët me peshë Hamming 1 kanë mbaruar, prandaj zgjedhim si drejtues një me peshë Hamming 2, e pikërisht 10001. Përftohet tabela e mëposhtme:

Drejtuesi i klasës fqinje							
00000	10010	01010	00101	11000	10111	01111	11101
10000	00010	11010	10101	01000	00111	11111	01101
00001	10011.	01011	00100	11001	10110	01110	11100
10001	00011	11011	10100	01001	00110	11110	01100

9 Zgjidhje. Së pari gjejmë një bazë për kodin C, pra 3 vektorë linearisht të pavarur. P.sh matrica përftuese G mund të jetë si më poshtë:

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

Matrica G është matricë përftuese sepse

$$\begin{vmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{vmatrix} = 1 \neq 0.$$

Duke ndërruar rreshtat matrica bëhet në formë standard si më poshtë:

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

Shkruajmë një matricë kontrolli H si më poshtë:

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

Gjejmë sindromat e fjalëve v dhe ω:

$$\begin{aligned} \omega \cdot H^\top &= (1\,1\,0). \\ v \cdot H^\top &= (1\,1\,1). \end{aligned}$$

Ushtrimi mund të zgjidhet dhe pa ndërtuar të gjithë tabelën standard të kodit. Gjejmë përfaqësuesit e klasave fqinje si në tabelën më poshtë:

Gabimi	Sindroma
000000	000
000001	001
000010	010
000100	100
001000	110
010000	101
100000	011
010010	111

Sindroma e ω është 110, atëhere gabimi korrespondues në tabelën e mësipërme është 001000. Gjatë transmetimit të fjalë kodit c ka ndodhur gabimi e, duke u transformuar sipas $c+e$ në ω. Dekodojmë ω sipas:

$$c = \omega - e = 001000 - 101011 = 100011.$$

Përsa i përket v, dekodimi nuk kryhet drejt, pasi pesha e gabimit për sindromën 111 është 2. Në fakt po të gjendet distanca e kodit, rezulton e barabartë me 3, pra kodi ndreq vetëm një gabim.

10b Udhëzim. Të zgjidhet pa ndërtuar të gjithë tabelën standard të kodit. Të ndiqet rruga e zgjidhjes së ushtrimit **9**.

11c Udhëzim. Të zgjidhet pa ndërtuar të gjithë tabelën standard të kodit. Të ndiqet rruga e zgjidhjes së ushtrimit **9**.

8.7 Kodet Ciklike

3 Përgjigje Kodi binar ciklik me polinom përftues $1 + x + x^3$.

8 Përgjigje $g(C_1 \cap C_2) = sh.v.p(g_1(x), g_2(x))$.

9 Zgjidhje. Duke u nisur nga matrica përftuese e kodit ciklik C, i shkruajmë në të kundërt të gjitha rreshtat e saj. Më pas rreshtin e fundit e shkruajmë në fillim, të parafundit të dytin e kështu me rradhë, derisa rreshti i parë të shkruhet në fund. Rezultati është matrica G si më poshtë:

$$G = \begin{pmatrix} g_r & g_{r-1} & \cdots & \cdots & \cdots & \cdots & g_1 & g_0 & 0 & 0 & \cdots & 0 \\ 0 & g_r & g_{r-1} & \cdots & \cdots & \cdots & \cdots & g_1 & g_0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots \\ 0 & 0 & \cdots & 0 & g_r & g_{r-1} & \cdots & \cdots & \cdots & \cdots & g_1 & g_0 \end{pmatrix}.$$

Rreshtat e kësaj matrice duken qartë që i përkasin kodit $C^{[-1]}$. Meqë $g_0 \neq 0$, rreshtat e G, janë linearisht të pavarura. Kjo është një matricë që përfton $C^{[-1]}$.

Dimensioni i $C^{[-1]}$ është i njëjtë me dimensionin e C. Për më tepër rreshti i parë përmban koeficientët e $g^{[-1]}(x)$.

Kodi $C^{[-1]}$ përftohet edhe nga matrica $g_0^{-1} \cdot G$. Në këtë rast, polinomi $g_0^{-1} \cdot g^{[-1]}(x)$ është polinomi monik me shkallë më të vogël (r) dhe përfton $C^{[-1]}$, prandaj ai është polinomi përftues.

10 Zgjidhje. Jo çdo kod ekuivalent me një kod ciklik është ciklik. Përshembull, kodi Hamming $[7,4]$ ka matricë kontrolli H si më poshtë:

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

Kodi i mësipërm nuk është ciklik. Fjala 1000011, kontrollohet lehtë që është fjalë kod, kurse zhvendosja ciklike e kësaj fjale, 1100001 nuk është fjalë kod ($H\cdot(1100001)^T \neq 0$). Kodi i mësipërm është ekuivalent me kodin ciklik me matricë kontrolli:

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

Në fakt ka 70 kode binare Hamming $[7,4]$ ekuivalente, por vetëm dy prej tyre janë ciklike.

16 Përgjigje.

1. x^2+1.
2. x^2+x+2.
3. $x^2+2\cdot x+2$.

17 Përgjigje.

1. $(x+1)\cdot(x^2+x+1)\cdot(x^6+x^3+1)$.
2. $(x+1)^2\cdot(x^2+x+1)^2$.
3. $(x-1)^8$.

19 Zgjidhje. Me shënimin $a\cap b = a_1b_1, a_2b_2, \dots, a_nb_n$ për fjalët $a = a_1a_2\cdots a_n$, $b = b_1b_2\cdots b_n$, pra $a\cap b$ ka 1 në vendin e i-të vetëm kur a e b kanë njëkohësisht 1 në atë vend, kemi

$$\omega(a+b) = \omega(a)+\omega(b)-2\omega(a\cap b).$$

Shënojmë

$$K = \{a\in\langle g(x)\rangle \mid \omega(a)\in 2N\},$$

atëherë $\forall a,b\in K \;\; a+b\in K$, meqë

1. $\omega(a+b)$ është çift si shumë 3 numrash çift;
2. zhvendosjet ciklike nuk ndryshojnë peshën e fjalës.

Për të gjetur polinomin përftues të K, vërejmë se vetë $g(x)$ duhet të ketë peshë tek, meqë në rast të kundërt fjalët kod të K, si shuma të zhvendosjeve ciklike të saj, do kishin pesha çift.

Duke qenë $K\subset\langle g(x)\rangle$, polinomi përftues i K do të jetë i trajtës $g(x)q(x)$ për ndonjë $q(x)$ në shkallë minimale. Vërejmë që $q(x) = x+1$ e bën këtë; meqë $(x+1)g(x) = xg(x)+g(x)$ ka peshë çift.

Vërtet, nga

$$\omega(xg(x))+\omega(g(x))-2\omega(xg(x)\cap g(x))$$

duket që në këtë rast pesha e $(x+1)g(x)$ do të ishte çift si shumë e dy numrave tek me një numur çift.

25 Udhëzim. Të shfrytëzohet fakti që $C^\perp$ është kod linear dhe, zhvendosjes ciklike të një fjale nga $C^\perp$, i përgjigjet e njëjta zhvendosje ciklike e të gjitha fjalëve të C.

26 Përgjigje. Jo. Jo.

28 Udhëzim. Të shfrytëzohet ushtrimi 27.

29 Udhëzim. Të shfrytëzohen ushtrimet 27 dhe 28.

30 Udhëzim. Të shfrytëzohen ushtrimet 27 dhe 28.

32 Udhëzim dhe përgjigje. Të ndërtohet matrica përftuese e kodit $C^\perp$ duke e parë atë si dualin e një kodi linear.
Më pas të bëhen transformimet e nevojshme për ta kthyer matricën e mësipërme në matricë përftuese të një kodi ciklik. Polinomi përftues i $C^\perp$ është:

$$g^\perp(x) = x^4+x^3+x^2+1.$$

33 Udhëzim. Të ndiqet rruga e zgjidhjes së ushtrimit **32**.

34 Udhëzim. $x^8 - 1 = (x-1)^8$ e që këtej i vetmi kod me dimension 4 është $< x^4 + 1 >$. Të provohet më pas se $< x^4 + 1 >$ nuk mund të jetë kod Hamming.