



Konv.koodit

Konv.koodit

Esimerkki 4A.1

Esimerkki 4A.2

Esimerkki 4B.1

Esimerkki 4B.2

Esimerkki 4B.3

Esimerkki 4B.4

Esimerkki 4B.5

Esimerkki 4B.6

Demotehtäviä

Esimerkkejä luvusta 4, 10.02.-20.02.2020



Esimerkki 4A.1

Konv.koodit

Esimerkki 4A.1

Esimerkki 4A.2

Esimerkki 4B.1

Esimerkki 4B.2

Esimerkki 4B.3

Esimerkki 4B.4

Esimerkki 4B.5

Esimerkki 4B.6

Demotehtäviä

Osoitetaan, että $(2, 1, 5, d)$ -konvoluutiokoodille pätee raja $d \leq 8$ Table 4.1:n mukaisesti.

Ratkaisu:

Tehdään vastaoletus, että olisi olemassa $(2, 1, 5, d)$ koodi $\mathcal{C}$, jonka vapaa etäisyys $d \geq 9$. Olkoon $G(D)$ koodin $\mathcal{C}$ kanoninen generaattorimatriisi. Tutkitaan 3-ulotteista avaruutta

$$V = \{u(D)G(D) \mid u(D) \in \mathbb{F}[D], \deg u(D) \leq 2\}.$$

Koska $G(D)$:n komponentit ovat astetta enintään 5, niin avaruuden V koodisanojen komponentit ovat astetta ≤ 7 . Näin ollen V on $\mathbb{F}$ -avaruuden

$$K = \{(f_1(D), f_2(D)) \mid f_i(D) = \sum_{j=0}^7 f_{ij}D^j, i = 1, 2\}$$

aliavaruus.



Esimerkki 4A.2

Konv.koodit

Esimerkki 4A.1

Esimerkki 4A.2

Esimerkki 4B.1

Esimerkki 4B.2

Esimerkki 4B.3

Esimerkki 4B.4

Esimerkki 4B.5

Esimerkki 4B.6

Demotehtäviä

Koska kertoimia f_{ij} on 16 kappaletta, voimme pitää avaruutta V binäärisenä lineaarisena koodina, jonka pituus $n = 16$. Kerroinpolynomit $u(D) = u_0 + u_1D + u_2D^2$ muodostavat 3-ulotteisen $\mathbb{F}$ -avaruuden, joten $\dim V = k = 3$. Griesmerin raja antaa meille näin epäyhtälön

$$n = 16 \geq \sum_{i=0}^{3-1} \left\lceil \frac{d}{2^i} \right\rceil = d + \left\lceil \frac{d}{2} \right\rceil + \left\lceil \frac{d}{4} \right\rceil.$$

Jos tässä $d \geq 9$, niin $\lceil d/2 \rceil \geq 5$ ja $\lceil d/4 \rceil \geq 3$. Näin ollen oikean puolen summa on $\geq 9 + 5 + 3 = 17$. Tämä on ristiriita.



Esimerkki 4B.1

Konv.koodit

Esimerkki 4A.1

Esimerkki 4A.2

Esimerkki 4B.1

Esimerkki 4B.2

Esimerkki 4B.3

Esimerkki 4B.4

Esimerkki 4B.5

Esimerkki 4B.6

Demotehtäviä

Tehtävä: Etsi jokin kanoninen generaattori matriisi Table 4.2:n $(3, 1, 3, 10)$ -koodin $\mathcal{C}$ duaalikoodille $\mathcal{C}^\perp$.

Ratkaisu: Käytetään monisteen Theorem 4.2:n yläpuolella olevan kappaleen ideaa. Täydennämme siis ensiksi generaattorimatriisin

$$G(D) = (1 + D + D^3, 1 + D^2 + D^3, 1 + D + D^2 + D^3)$$

unimodulaariseksi 3×3 matriisiksi. Eräs tapa selvittää tehtävästä on hyödyntää sitä, että

$$\text{syt}(1 + D + D^3, 1 + D^2 + D^3) = 1.$$

Yleistetyllä Eukleideen algoritmilla löydämme Bezout'n identiteetin lupaamat kertoimet:



Esimerkki 4B.2

Konv.koodit

Esimerkki 4A.1

Esimerkki 4A.2

Esimerkki 4B.1

Esimerkki 4B.2

Esimerkki 4B.3

Esimerkki 4B.4

Esimerkki 4B.5

Esimerkki 4B.6

Demotehtäviä

$$D(1 + D + D^3) + (1 + D)(1 + D^2 + D^3) = 1.$$

Näin ollen oheisen matriisin

$$U = \begin{pmatrix} 1 + D + D^3 & 1 + D^2 + D^3 & 1 + D + D^2 + D^3 \\ 1 + D & D & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

determinantti on $\det U = 1$ (kehitä determinantti alimman vaakarivin suhteen). U kelpaa siis etsityksi unimodulaarimatriisiksi.

Monisteen päättely edellyttää, että etsimme U :n käänteismatriisin. Lineaarialgebran menetelmin (vaakarivimuunnoksilla tai Cramerin säännöllä) löydämme



Esimerkki 4B.3

Konv.koodit

Esimerkki 4A.1

Esimerkki 4A.2

Esimerkki 4B.1

Esimerkki 4B.2

Esimerkki 4B.3

Esimerkki 4B.4

Esimerkki 4B.5

Esimerkki 4B.6

Demotehtäviä

$$U^{-1} = \begin{pmatrix} D & 1 + D^2 + D^3 & D + D^2 + D^3 + D^4 \\ 1 + D & 1 + D + D^3 & 1 + D^4 \\ 0 & 0 & 1 \end{pmatrix}.$$

Tämän matriisin 2 viimeistä saraketta muodostavat monisteen argumentin perusteella duaalikoodin $\mathcal{C}^\perp$ basic generaattorimatriisin.

$$G_1(D) = \begin{pmatrix} D + D^2 + D^3 + D^4 & 1 + D^4 & 1 \\ 1 + D^2 + D^3 & 1 + D + D^3 & 0 \end{pmatrix}.$$



Esimerkki 4B.4

Konv.koodit

Esimerkki 4A.1

Esimerkki 4A.2

Esimerkki 4B.1

Esimerkki 4B.2

Esimerkki 4B.3

Esimerkki 4B.4

Esimerkki 4B.5

Esimerkki 4B.6

Demotehtäviä

Nimittäin selvästi $G_1(D)$ voidaan täydentää unimodulaariseksi (lisäämällä U^{-1} :n 1. sarake viimeiseksi riviksi), joten se on basic. Matriisitulon $UU^{-1} = I_3$ ensimmäisen rivin 2 viimeistä alkia puolestaan kertovat, että $G_1(D)$ vaakarivit ovat kohtisuorassa $G(D)$:tä vastaan.

Yleisen teorian mukaan $G_1(D)$ voidaan muuntaa kanoniseksi generaattorimatriisiksi tekemällä siihen ulkoista astetta vähentäviä vaakarivioperaatioita kunnes saadaan reduced matriisi. Lisäämällä alempi ylempään D :llä kerrottuna saadaan

$$G_1(D) \rightarrow \begin{pmatrix} D^2 & 1 + D + D^2 & 1 \\ 1 + D^2 + D^3 & 1 + D + D^3 & 0 \end{pmatrix}.$$



Esimerkki 4B.5

Konv.koodit

Esimerkki 4A.1

Esimerkki 4A.2

Esimerkki 4B.1

Esimerkki 4B.2

Esimerkki 4B.3

Esimerkki 4B.4

Esimerkki 4B.5

Esimerkki 4B.6

Demotehtäviä

Lisäämällä lopuksi ylempi rivi alempaan kerrottuna $(1 + D)$:llä saadaan

$$\rightarrow \begin{pmatrix} D^2 & 1 + D + D^2 & 1 \\ 1 & D & 1 + D \end{pmatrix},$$

mikä nähdään helposti kanoniseksi. Alarivistä näemme, että duaalikoodin vapaa etäisyys on enintään 4. Se on itse asiassa tarkalleen 4 (harjoitustehtävä).



Esimerkki 4B.6

Konv.koodit

Esimerkki 4A.1

Esimerkki 4A.2

Esimerkki 4B.1

Esimerkki 4B.2

Esimerkki 4B.3

Esimerkki 4B.4

Esimerkki 4B.5

Esimerkki 4B.6

Demotehtäviä

Aina ei unimodulaariseksi täydentäminen suju yhtä helposti. Vaihtoehtoinen tapa olisi ollut huomata, että vektorit $(1 + D^2 + D^3, 1 + D + D^3, 0)$ ja $(1 + D + D^2 + D^3, 0, 1 + D + D^3)$ selvästi ovat lineaarisesti riippumattomia yli $\mathbb{F}(D)$:n ja kohtisuorassa $G(D)$:tä vastaan. Matriisi, jonka riveinä nämä ovat, on siis eräs duaalikoodin generaattorimatriisi. Se ei kuitenkaan ole basic (selvästi $1 + D + D^3$ jakaa kaikki 2×2 alideterminantit). Näin ollen tässä joudutaan tekemään enemmän laskuja (esimerkiksi Theorem 1.2:n todistuksen idean mukaisesti etsimällä sen Smithin normaalimuotoon liittyvät matriisit P ja Q).



Konv.koodit

Esimerkki 4A.1

Esimerkki 4A.2

Esimerkki 4B.1

Esimerkki 4B.2

Esimerkki 4B.3

Esimerkki 4B.4

Esimerkki 4B.5

Esimerkki 4B.6

Demotehtäviä

Exercise 4.1/1

Exercise 4.1/2

Exercise 4.1/3

Exercise 4.5/1

Exercise 4.5/2

Radiokuuntelija/1

Radiokuuntelija/2

Radiokuuntelija/3

Radiokuuntelija/4

Demotehtäviä



Exercise 4.1/1

Konv.koodit

Esimerkki 4A.1

Esimerkki 4A.2

Esimerkki 4B.1

Esimerkki 4B.2

Esimerkki 4B.3

Esimerkki 4B.4

Esimerkki 4B.5

Esimerkki 4B.6

Demotehtäviä

Exercise 4.1/1

Exercise 4.1/2

Exercise 4.1/3

Exercise 4.5/1

Exercise 4.5/2

Radiokuuntelija/1

Radiokuuntelija/2

Radiokuuntelija/3

Radiokuuntelija/4

Tehtävässä haetaan optimaalisia $(2, 1, 4)$ -koodeja. Olkoon $G(D) = (p_1(D), p_2(D))$ sellaisen koodin kanoninen generaattorimatriisi. Jos rajataan syöte $u(D)$ astetta ≤ 1 oleviin polynomeihin, koodisanat $u(D)G(D)$ ovat astetta ≤ 5 . Normaalilla menettelyllä 2-ulotteinen binäärinen lineaarinen koodi, jonka pituus on $n = 2(5 + 1) = 12$. Griesemerin rajan nojalla minimietäisyys d toteuttaa epäyhtälön $d + (d/2) \leq 12$, mistä $d \leq 8$.

Tehdään vastaoletus, että $d_{free} \geq 8$ olisi mahdollinen. Olkoot w_i polynomien $p_i(D)$, $i = 1, 2$, Hamming-painot. Rajoituksetta voidaan olettaa, että $w_1 \geq w_2$. Koska polynomit ovat astetta ≤ 4 , niin lisäksi $5 \geq w_1$.

Koska $G(D)$ on koodisana, niin $w_1 + w_2 \geq 8$.



Exercise 4.1/2

Konv.koodit

Esimerkki 4A.1

Esimerkki 4A.2

Esimerkki 4B.1

Esimerkki 4B.2

Esimerkki 4B.3

Esimerkki 4B.4

Esimerkki 4B.5

Esimerkki 4B.6

Demotehtäviä

Exercise 4.1/1

Exercise 4.1/2

Exercise 4.1/3

Exercise 4.5/1

Exercise 4.5/2

Radiokuuntelija/1

Radiokuuntelija/2

Radiokuuntelija/3

Radiokuuntelija/4

Vaihtoehtoja on

- $w_1 = w_2 = 5$,
- $w_1 = 5, w_2 = 4$,
- $w_1 = 5, w_2 = 3$,
- $w_1 = w_2 = 4$.

Ensimmäisessä tapauksessa väistämättä

$p_1(D) = p_2(D) = 1 + D + D^2 + D^3 + D^4$. Näillä on ei-triviaali yhteinen tekijä, joten tämä $G(D)$ ei ole kanoninen.

Viimeisessä tapauksessa kumpikin polynomi on parillista painoa, ja näin ollen jaollinen polynomilla $1 + D$ (niillä $D = 1$ on nollakohtana). Näin ollen sekään $G(D)$ ei ole kanoninen.



Exercise 4.1/3

Konv.koodit

Esimerkki 4A.1

Esimerkki 4A.2

Esimerkki 4B.1

Esimerkki 4B.2

Esimerkki 4B.3

Esimerkki 4B.4

Esimerkki 4B.5

Esimerkki 4B.6

Demotehtäviä

Exercise 4.1/1

Exercise 4.1/2

Exercise 4.1/3

Exercise 4.5/1

Exercise 4.5/2

Radiokuuntelija/1

Radiokuuntelija/2

Radiokuuntelija/3

Radiokuuntelija/4

Muissa tapauksissa $w_1 = 5$, joten tiedämme, että $p_1(D) = 1 + D + D^2 + D^3 + D^4$. Näin ollen syöte $u(D) = 1 + D$ johtaa sangen matala-painoiseen tuloon $(1 + D)p_1(D) = 1 + D^5$. Tällöin on toisen koordinaatin $(1 + D)p_2(D)$ oltava painoa ≥ 6 . Koska kyseinen polynomi on astetta ≤ 5 , voimme päätellä, että on oltava

$$(1 + D)p_2(D) = 1 + D + D^2 + D^3 + D^4 + D^5 = (1 + D)(1 + D^2 + D^4).$$

Erityisesti siis on oltava $p_2(D) = 1 + D^2 + D^4$.

Mutta tällöin syöte $u(D) = 1 + D^2$ johtaa painoa 6 olevaan koodisanaan

$$(1 + D^2)G(D) = (1 + D + D^5 + D^6, 1 + D^6).$$

Väite seuraa.



Exercise 4.5/1

Konv.koodit

Esimerkki 4A.1

Esimerkki 4A.2

Esimerkki 4B.1

Esimerkki 4B.2

Esimerkki 4B.3

Esimerkki 4B.4

Esimerkki 4B.5

Esimerkki 4B.6

Demotehtäviä

Exercise 4.1/1

Exercise 4.1/2

Exercise 4.1/3

Exercise 4.5/1

Exercise 4.5/2

Radiokuuntelija/1

Radiokuuntelija/2

Radiokuuntelija/3

Radiokuuntelija/4

Tutkittavan koodin tarkistusmatriisi on

$$H(D) = (13 \ 15 \ 17) = (1 + D + D^3, 1 + D^2 + D^3, 1 + D + D^2 + D^3).$$

Kalvolla Esimerkki 4B.5 näimme, että sana $(1, D, 1 + D)$ kuuluu koodiin, joten vapaa etäisyys ei voi olla ≥ 4 .

Tehdään vastaoletus, että olisi olemassa painoa kolme oleva sana (painoja 1 olevia sanoja ei selvästikään ole, ja painoa 2 oleva sana edellyttäisi, että tarkistusmatriisin jotkin kaksi komponenttia eroaisivat vain tekijällä, joka on D :n potenssi, ja näin ei ole). Oletetaan, että 3-painoisen sanan termit ovat D^r, D^s, D^t . Rajoituksetta $r \leq s \leq t$. Tarkistusyhtälö saa tällöin muodon

$$D^r h_i(D) + D^s h_j(D) + D^t h_k(D) = 0, \quad (*)$$

missä i, j, k ovat indeksejä $\in \{1, 2, 3\}$, ei välttämättä eri suuria.



Exercise 4.5/2

Konv.koodit

Esimerkki 4A.1

Esimerkki 4A.2

Esimerkki 4B.1

Esimerkki 4B.2

Esimerkki 4B.3

Esimerkki 4B.4

Esimerkki 4B.5

Esimerkki 4B.6

Demotehtäviä

Exercise 4.1/1

Exercise 4.1/2

Exercise 4.1/3

Exercise 4.5/1

Exercise 4.5/2

Radiokuuntelija/1

Radiokuuntelija/2

Radiokuuntelija/3

Radiokuuntelija/4

Huomaamme, että tarkistumatriisin kaikissa polynomeissa esiintyvät 0-asteinen termi 1 ja 3-asteinen termi D^3 . Näin ollen yhtälön $(*)$ vasemman puolen tulojen matala-asteisimmat termit ovat D^r , D^s ja D^t riippumatta indeksien i, j, k arvoista. Koska kumoutuminen on täydellistä, seuraa, että on oltava $r = s < t$.

Toisaalta yhtälön $(*)$ vasemman puolen tulojen korkea-asteisimmat termit ovat D^{r+3} , D^{s+3} ja D^{t+3} .

Näidenkin on kumottava toisensa, joten voimme päätellä, että $r < s = t$. Saadut epäyhtälöt eivät voi kaikki olla samanaikaisesti voimassa, joten vastaoletus on kumottu.



Radiokuuntelija/1

Konv.koodit

Esimerkki 4A.1

Esimerkki 4A.2

Esimerkki 4B.1

Esimerkki 4B.2

Esimerkki 4B.3

Esimerkki 4B.4

Esimerkki 4B.5

Esimerkki 4B.6

Demotehtäviä

Exercise 4.1/1

Exercise 4.1/2

Exercise 4.1/3

Exercise 4.5/1

Exercise 4.5/2

Radiokuuntelija/1

Radiokuuntelija/2

Radiokuuntelija/3

Radiokuuntelija/4

Demotehtävä V/6.

Arvellaan, että siepattu viesti olisi katkelma koodisanaa

$$(x_1(D), x_2(D)) = u(D)(g_1(D), g_2(D)),$$

missä $g_1(D)$ ja $g_2(D)$ olisivat astetta ≤ 2 olevia polynomeja.

Tällöin koodisanan sisätulo tarkistusvektorin

$H(D) = (g_2(D), g_1(D))$ kanssa olisi nolla. Yhtälö

$$g_2(D)x_1(D) + g_1(D)x_2(D) = 0$$

puolestaan voidaan löytää potenssisarjojen $D^j x_i(D)$, $i = 1, 2$, $j = 0, 1, 2$ lineaarisena riippuvuutena yli kunnan $\mathbb{F}$.



Radiokuuntelija/2

Konv.koodit

Esimerkki 4A.1

Esimerkki 4A.2

Esimerkki 4B.1

Esimerkki 4B.2

Esimerkki 4B.3

Esimerkki 4B.4

Esimerkki 4B.5

Esimerkki 4B.6

Demotehtäviä

Exercise 4.1/1

Exercise 4.1/2

Exercise 4.1/3

Exercise 4.5/1

Exercise 4.5/2

Radiokuuntelija/1

Radiokuuntelija/2

Radiokuuntelija/3

Radiokuuntelija/4

Siepatussa viestissä

$$x_1(D) = \dots 0001100010 \dots$$

ja

$$x_2(D) = \dots 1100011001 \dots$$

Näin ollen potenssisarjat $D^j x_i(D)$ ovat ao. matriisin vaakarivit

$$A = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & ? & ? \\ ? & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & ? \\ ? & ? & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & ? & ? \\ ? & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & ? \\ ? & ? & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Matriisista A tunnetaan siis täysin keskellä olevat 8 saraketta.



Radiokuuntelija/3

Konv.koodit

Esimerkki 4A.1

Esimerkki 4A.2

Esimerkki 4B.1

Esimerkki 4B.2

Esimerkki 4B.3

Esimerkki 4B.4

Esimerkki 4B.5

Esimerkki 4B.6

Demotehtäviä

Exercise 4.1/1

Exercise 4.1/2

Exercise 4.1/3

Exercise 4.5/1

Exercise 4.5/2

Radiokuuntelija/1

Radiokuuntelija/2

Radiokuuntelija/3

Radiokuuntelija/4

Lineaarialgebran menetelmin (eli muuntamalla ko. matriisi vaakarivioperaatioilla redusoituun porrasmuotoon) nähdään, että niiden sarakkeiden muodostaman 6×8 -matriisin aste on viisi. Tarkemmin sanottuna rivien 1,2,4,5 ja 6 summana saadaan nollavektori varmasti tunnetun 8 sarakkeen osalta. Koska matriisi oli astetta $5 = 6 - 1$, ei muita lineaarisen riippuvuuden relaatioita ole. Palauttamalla mieleen rivien merkitykset, tämä tarkoittaa, että mahdollinen relaatio on

$$(1 + D)x_1(D) + (1 + D + D^2)x_2(D) = 0.$$

Mahdollinen generaattorimatriisi olisi siis $G(D) = (1 + D + D^2, 1 + D)$.



Radiokuuntelija/4

Konv.koodit

Esimerkki 4A.1

Esimerkki 4A.2

Esimerkki 4B.1

Esimerkki 4B.2

Esimerkki 4B.3

Esimerkki 4B.4

Esimerkki 4B.5

Esimerkki 4B.6

Demotehtäviä

Exercise 4.1/1

Exercise 4.1/2

Exercise 4.1/3

Exercise 4.5/1

Exercise 4.5/2

Radiokuuntelija/1

Radiokuuntelija/2

Radiokuuntelija/3

Radiokuuntelija/4

Tämä on tietenkin vain indisio ja voi olla myös sattuma. Helposti nähdään, että kuusi satunnaisesti valittua 8-bittistä vektoria ovat lineaarisesti riippumattomia todennäköisyydellä, joka on noin 77%. On hankalampaa selvittää, miten tämä luku muuttuu, kun otetaan huomioon, että nämä kuusi vektoria eivät olleet toisistaan riippumattomia, vaan saatiin kertomalla D :n potensseilla kahta tunnettua jonoa.