BCH-koodeista

Juhani Sjöman

Matematiikan pro gradu

Jyväskylän yliopisto
Matematiikan ja tilastotieteen laitos
Kevät 2021

Tiivistelmä: Juhani Sjöman, *BCH-koodeista* (engl. *about BCH codes*), matematiikan pro gradu -tutkielma, 73 s., Jyväskylän yliopisto, Matematiikan ja tilastotieteen laitos, kevät 2021.

Tämän tutkielman tarkoituksena on tutustuttaa lukija BCH-koodeihin. BCH-koodit ovat syklisiä koodeja ja ne pystyvät korjaamaan useita virheitä. Tutkielmassa esitetään erilaisia tapoja korjata koodisanoihin tulleita virheitä käyttäen hyväksi äärellisten kuntien teoriaa ja lineaari- sekä polynomialgebraa.

Yksinkertainen kahden sanan koodi koostuu esimerkiksi koodisanoista 000 ja 111. Koodisanojen etäisyys on niiden positioiden määrä, missä sanat eroavat toisistaan. Sanojen 000 ja 111 etäisyys on siis 3. Koodin virheenkorjauskyky on sidottu koodin minimietäisyyteen $d(C)$, joka on kaikkien koodin koodisanojen välinen minimietäisyys. Koodi korjaa t virhettä, jos $d(C) \geq 2t + 1$. Tämä esimerkkikoodi $\{000, 111\}$ korjaa siis yhden virheen. Virheenkorjaus tapahtuu lähimmän naapurin -periaatteella, missä vastaanotettu sana koodataan siksi koodisanaksi, jota se on lähimpänä eli johon sen etäisyys on lyhin. Ekvivalentti koodi on sellainen koodi, jolla on samat ominaisuudet kuin alkuperäisellä koodilla. Esimerkiksi koodi $\{010, 101\}$ on ekvivalentti koodin $\{000, 111\}$ kanssa.

Edistyneemmissä koodeissa, kuten lineaarisissa koodeissa, koodisanojen määrä on suuri. Kaikkia lineaarisen koodin koodisanoja ei kuitenkaan tarvitse luetella vaan niiden muodostamisessa käytetään apuna virittäjämatriisia. Vastaavasti lineaarinen koodi on helppo dekoodata pariteetintarkistusmatriisin avulla. Virittäjä- ja pariteetintarkistusmatriisi voidaan kumpikin esittää standardimuodossa, joka sisältää yksikkömatriisin. Syndrooma on koodisanavektorin ja pariteetintarkistusmatriisin transpoosin tulo. Se ilmaisee koodisanassa virheen paikan.

Sykliset koodit ovat lineaarisia koodeja, mutta näille esitetään virittäjä ja pariteetintarkistus polynomien avulla. Polynomeille voidaan suorittaa modulolaskentaa samoin kuin kokonaisluvuillekin. Tämä vahvuus tekee syklisistä koodeista haluttuja niiden koodauksen ja dekoodauksen suhteellisen helppouden ja nopeuden ansiosta.

Lineaariset Hammingin koodit korjaavat vain yhden virheen. Sykliset koodit pystyvät polynomiominaisuuksiensa ansiosta korjaamaan niin sanottuja purskevirheitä eli peräkkäin esiintyviä virheitä. Jopa 6-pituinen purskevirhe on mahdollista korjata käyttäen vain 2-pituisen purskeen korjaavaa koodia, kun käytetään lomitustekniikkaa. Siinä koodisanoja ei lähetetäkään peräkkäin, vaan kolmen koodisanan ryppäinä lomitettuna. Jos siis halutaan lähettää 7-pituiset koodisanat $\mathbf{A} = A_0A_1 \cdots A_6$, $\mathbf{B} = B_0B_1 \cdots B_6$ ja $\mathbf{C} = C_0C_1 \cdots C_6$, niin sen sijaan, että lähetetään koodisanat peräkkäin: $A_0A_1 \cdots A_6B_0B_1 \cdots B_6C_0C_1 \cdots C_6$, lähetetäänkin ne lomittain: $A_0B_0C_0A_1B_1C_1 \cdots A_6B_6C_6$. Nyt 6-pituisen purskevirheen sattuessa kukin koodisana $\mathbf{A}, \mathbf{B}$ ja $\mathbf{C}$ kärsii vain kahdesta virheestä, jotka voidaan korjata erikseen kunkin koodisanan kohdalla.

BCH-koodit voidaan esittää syklisinä koodeina ja täten niille pätevät kaikki syklisten koodien algebralliset ominaisuudet. BCH-koodeille esitetään niin sanottu BCH-avainyhtälö, jonka avulla vastaanotetut sanat ovat helposti ja nopeasti dekoodattavissa koodisanoiksi virheistä huolimatta.

Sisällys

Johdanto

Yleensä matematiikkaa tehdään kehittämällä erilaisia teorioita ja vasta vuosien päästä niihin löydetään sopivia käytännön sovelluksia — jos sittenkään. Matematiikka on pohjimmiltaan siis hyvin abstraktia tiedettä. Koodausteoriassa tilanne on ehkä päinvastainen. Viestintälaitteiden kehittyessä on tullut tarve etsiä systeemejä, joiden avulla informaatiota voidaan salata ja sitä voidaan turvallisesti lähettää kohinaisen kanavan läpi. Nämä systeemit ovat nimeltään koodeja. Koodit koostuvat pääasiassa yhtä pitkistä viestisanoista, joihin lisätään tiedon ylimäärää eli redundanssia. Lähetetään siis viestin 0 sijasta viesti 000. Redundanssia tarvitaan, jotta viestiin tuleva mahdollinen virhe voidaan ensinnäkin havaita ja tämän jälkeen korjata. Yhden virheen sattuessa, jos vastaanotetaankin viesti 001, niin redundanssin ansiosta tiedetään heti, että lähetetty viesti on alun perin ollut 000.

Hyvä esimerkki on avaruusluotain, jonka lähettämät kuvat haluttaisiin saada mahdollisimman tarkkoina Maahan. Lähetyksen tulisi olla mahdollisimman lyhytkestoinen, mutta toisaalta taas mahdollisimman paljon informaatiota sisältävä. Lisäksi siihen tulevat mahdolliset virheet täytyisi osata korjata. Tällaisessa lähetyskanavassa virheet esiintyvät useimmiten purskeina. Lähetyksessä on siis pienen hetken ajan kohinaa, vaikka normaalisti viesti olisikin tasalaatuista ja tulkittavissa olevaa. Avuksi tulevat BCH-koodit, sillä ne osaavat korjata kyseisiä purskevirheitä.

Koodien konstruointi ei ole välttämättä mikään yksinkertainen toimenpide. On kuitenkin olemassa koodeja, joihin saadaan ujutettua eräänlaista ”symmetriaa”, joka takaa koodin helpomman konstruoinnin ja dekoodauksen eli vastaanotetun sanan tulkinnan. Näistä koodeista käytetään nimitystä lineaariset koodit. Ne ovat aliavaruuksia, joille on määritelty yhteen- ja kertolasku siten, että kahden koodisanan summa on koodisana ja skalaarilla kerrottu koodisana on myös koodisana. Syklinen koodi on lineaarisuuden lisäksi sellainen, että jos 1100 on koodisana, niin syklisesti myös 0110, 0011 ja 1001 ovat koodisanoja.

BCH-koodit ovat syklisiä ja ne vaativat taakseen vahvaa lineaari- ja polynomialgebraa sekä lukuteoriaa. Niitä voidaan koodata ja dekoodata matriisien ja polynomien avulla. Tästä syystä ne ovat helposti implementoitavissa tietokonejärjestelmien käyttöön.

Tutkielma alkaa kevyesti johdatuksella virheenkorjauskoodeihin ja etenee vähitellen äärellisten kuntien kautta lineaarisiin ja syklisiin koodeihin. Lopuksi tutustutaan BCH-koodeihin. Pääasiallisina lähdeteoksina on käytetty lukujen 1-4 osalta Raymond Hillin kirjaa *A First Course in Coding Theory* ja luvuissa 5-6 Robert J. McEliecen kirjaa *The Theory of Information and Coding*. Suuret kiitokset tutkielman ohjaajalle Ari Lehtoselle kärsivällisestä ja taitavasta ohjauksesta.

LUKU 1

Johdatus virheenkorjauskoodeihin

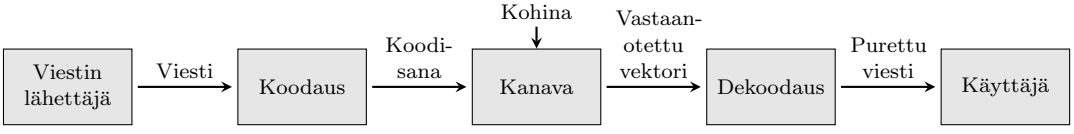
Virheenkorjauskoodien avulla korjataan virheitä, joita ilmenee viesteissä, kun niitä lähetetään kohinaista kanavaa pitkin. Kanavalla tarkoitetaan esimerkiksi puhelinlinjaa, korkeataajuuksisia radioaaltoja tai satelliittiviestintälinkkiä. Kohinalla taas tarkoitetaan esimerkiksi inhimillistä virhettä, salamointia, lämpökohinaa tai vioittuneita laitteita, jotka aiheuttavat virheitä vastaanotettavaan tietoon. Tämän luvun pääasiallisena lähteenä on käytetty kirjaa Raymond Hill: A First Course in Coding Theory (1986) [**2**].

Yleinen digitaalinen viestintäsysteemi on esitetty Kuvassa 1.1. Kuvassa 1.2 on yksinkertainen esimerkki tilanteesta, jossa lähetettävä viesti ”KYLLÄ” = 00000 kulkee kanavan läpi ja viestiin tulee kaksi virhettä ja vastaantotettu vektori on 00110, joka korjataan lähimpään koodisanaan 00000 eli ”KYLLÄ”.

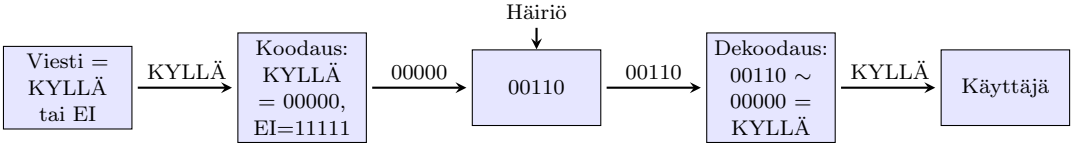
Kanavakoodauksen tavoitteena on rakentaa koodaus ja dekoodaus siten, että seuraavat toteutuisivat: [**4**, s. 3–4]

(1) nopeasti koodattavissa olevat viestit;
(2) koodattujen viestien helppo lähettäminen;
(3) vastaanotettujen viestien nopea dekoodaus;
(4) maksimaalinen informaation lähettäminen aikayksikköä kohden;
(5) maksimaalinen virheen havaitsemis- tai korjauskyky.

Binäärinen koodi Kuvassa 1.2 on $\{00000, 11111\}$ ja se on nimeltään *toistokoodi*, jonka pituus on viisi. Binäärinen koodi koostuu ykkösistä ja nollista ja tätä alkioiden joukkoa $\{0, 1\}$ kutsutaan *koodiaakkostoksi*. Yleisemmin *q-äärinen koodi* on annettu joukko merkkisarjoja, joissa kukin merkki valitaan koodiaakkostosta $F_q = \{\lambda_1, \lambda_2, \ldots, \lambda_q\}$. Useimmiten koodiaakkosto valitaan joukosta $\mathbb{Z}_q = \{0, 1, 2, \ldots, q-1\}$.



KUVA 1.1. Koodatun viestin kulku kanavaa pitkin lähettäjältä käyttäjälle.



KUVA 1.2. Lähetettyyn viestiin tulee kaksi virhettä, jotka korjataan.

Toistokoodi on hyvä esimerkki siitä, miten redundanssia eli tiedon ylimäärää voidaan lisätä koodiin, jotta siitä tulee vähemmän virhealtis.

Esimerkki 1.1 ([**2**, s. 2]). Englannin kielen kaikki sanat on koodi 26-kirjaimisesta aakkostosta {A, B, ..., Z}.

Esimerkki 1.2 ([**2**, s. 3]). Kaikki 10-numeroiset puhelinnumerot on 10-äärinen koodi, jonka pituus on 10. Tästä joukosta voidaan valita yli 82 miljoonaa puhelinnumeroa siten, että yhden virheen sattuessa soitto menee silti oikeaan numeroon.

Esimerkki 1.3 ([**2**, s. 3–4]). Oletetaan, että päämajassa HQ ja paikassa X on identtiset kartat kuten Kuvassa 1.3. Vain HQ tietää reitin, jolla välttää vihollisen alue ja paikasta X voi palata turvallisesti päämajaan HQ. Päämajasta HQ halutaan lähettää binääridatana reitti NNWNNWWSSWWNNNNWWN paikkaan X. Tässä tapauksessa luotettavuus on lähetysnopeutta tärkeämpi asia. Tarkastellaan miten neljä viestiä N, S, E ja W voidaan koodata binäärisiksi koodisanoiksi. Nopein tai lyhin koodi, jota voidaan käyttää on

$$C_1 = \begin{cases} 0 & 0 & = & \mathrm{N} \\ 0 & 1 & = & \mathrm{W} \\ 1 & 0 & = & \mathrm{E} \\ 1 & 1 & = & \mathrm{S} \end{cases}.$$

Näin on identifioitu neljä viestiä N, W, E ja S neljällä vektorilla avaruudesta $(F_2)^2$. Jotta voitaisiin suojella viestiä kohinalta, tulee lisätä redundanssia. Lisätään koodiin siis yksi numeromerkki

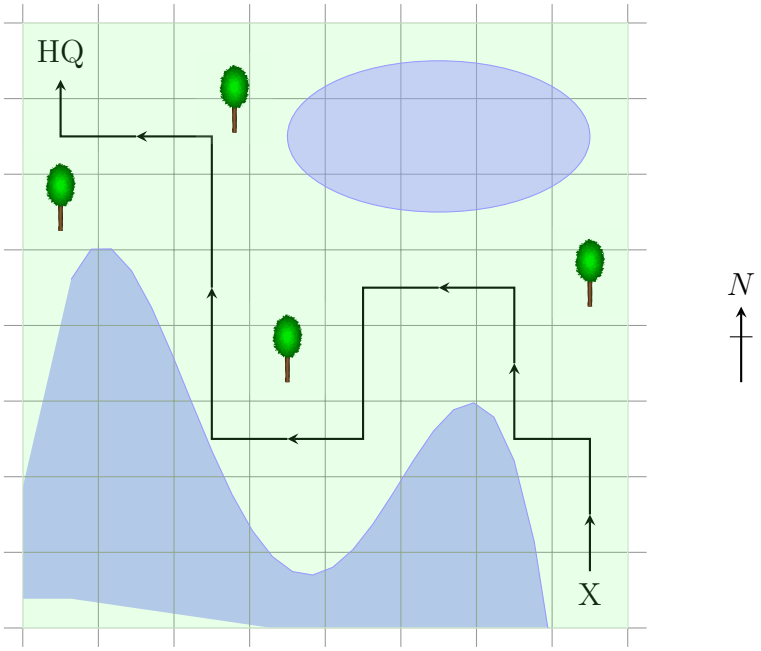
$$C_2 = \begin{cases} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{cases}.$$

Tämä lisää viestin lähetysaikaa, mutta jos viestissä ilmenee yksi virhe, niin vastaanotettu vektori ei voi olla koodisana. Tällöin vastaanottaja voi pyytää, että viesti lähetettäisiin uudelleen. Koodi C_2 pystyy *havaitsemaan* yhden virheen, jolloin sanotaankin, että se on yhden virheen havaitseva koodi.

Oletaan seuraavaksi, että paikka X voi vastaanottaa dataa päämajasta HQ, mutta sieltä ei voida pyytää viestin uudelleenlähetystä, koska kyseessä on esimerkiksi *yksisuuntainen kanava*. Sopivalla kahden numeromerkin lisäyksellä jokaiseen koodisanaan koodista C_2 saadaan 5-pituinen koodi

$$C_3 = \begin{cases} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 \end{cases}.$$

Mikäli yksi virhe ilmaantuu mihin tahansa koodisanaan koodissa C_3, niin nyt ei voida pelkästään havaita, vaan myös *korjata* vastaanotetun vektorin virhe lähimpään koodisanaan.



KUVA 1.3. Reitti paikasta X päämajaan HQ ohi vihollisen alueen.

Tähän asti on käytetty väljästi ilmaisua vektori on ”lähimpänä” jotain koodisanaa kuin toista, joten määritellään tämä käsite tarkemmin ottamalla käyttöön etäisyysfunktio avaruudessa $(F_q)^n$ nimeltä Hammingin etäisyys.

Hammingin etäisyys $d(\mathbf{x}, \mathbf{y})$ kahden n-jonon $\mathbf{x}$ ja $\mathbf{y}$ välillä avaruudessa $(F_q)^n$ on niiden paikkojen lukumäärä, jossa ne eroavat toisistaan. Esimerkiksi avaruudessa $(F_2)^5$ on $d(00111, 11001) = 4$ ja avaruudessa $(F_3)^4$ on $d(0122, 1220) = 3$.

Hammingin etäisyys on aito etäisyysfunktio eli metriikka, sillä se täyttää kolme ehtoa:

(i) $d(\mathbf{x}, \mathbf{y}) = 0$ jos ja vain jos $\mathbf{x} = \mathbf{y}$.
(ii) $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{y}, \mathbf{x})$ kaikilla $\mathbf{x}$ ja $\mathbf{y} \in (F_q)^n$.
(iii) $d(\mathbf{x}, \mathbf{y}) \leq d(\mathbf{x}, \mathbf{z}) + d(\mathbf{z}, \mathbf{y})$ kaikilla $\mathbf{x}, \mathbf{y}$ ja $\mathbf{z} \in (F_q)^n$.

Kaksi ensimmäistä ehtoa ovat helposti tarkistettavia. Kolmas, nimeltään kolmioepäyhtälö todistetaan seuraavasti. Havaitaan, että $d(\mathbf{x}, \mathbf{y})$ on minimimäärä numeromerkkien vaihtoja, mitä tarvitaan muuttamaan vektori $\mathbf{x}$ vektoriksi $\mathbf{y}$. Mutta voidaan myös vaihtaa vektori $\mathbf{x}$ vektoriksi $\mathbf{y}$ tekemällä ensin $d(\mathbf{x}, \mathbf{z})$ vaihdosta (muutetaan vektori $\mathbf{x}$ vektoriksi $\mathbf{z}$) ja sitten $d(\mathbf{z}, \mathbf{y})$ vaihtoa (muutetaan vektori $\mathbf{z}$ vektoriksi $\mathbf{y}$). Täten $d(\mathbf{x}, \mathbf{y}) \leq d(\mathbf{x}, \mathbf{z}) + d(\mathbf{z}, \mathbf{y})$.

Hammingin etäisyys ei ole ainut mahdollinen eikä todellakaan aina sopivin. Esimerkiksi avaruudessa $(F_{10})^3$ on $d(428, 438) = d(428, 468)$, jolloin käytännössä esimerkiksi puhelimella soitettaessa voisi olla järkevämpää käyttää metriikkaa, jossa vektori 428 on lähempänä vektoria 438 kuin mitä se on vektoria 468.

Koodin purkamisen ongelmaa tarkasteltaessa oletetaan, että tuntematon koodisana $\mathbf{x}$ on lähetetty ja vastaanotetaan vektori $\mathbf{y}$, joka on saattanut häiriintyä kohinan seurauksena. Näyttäisi järkevältä purkaa koodi $\mathbf{y}$ koodisanaksi $\mathbf{x}'$ — joka on toivottavasti sama kuin $\mathbf{x}$ — siten, että etäisyys $d(\mathbf{x}', \mathbf{y})$ on mahdollisimman pieni. Tätä

strategiaa kutsutaan nimellä *lähimmän naapurin dekoodaus*. Tämä menetelmä varmasti maksimoi dekoodaajan todennäköisyyden korjata virheet, kun seuraavat lähetyskanavaa koskevat oletukset ovat voimassa:

(i) Jokaisella lähetetyllä symbolilla on vastaanotettaessa sama virhetodennäköisyys p, $p < \frac{1}{2}$.
(ii) Virheen sattuessa kukin $q-1$ symbolista on yhtä todennäköisesti virheellinen.

Koodin minimietäisyys $d(C)$ on tärkeä parametri. Se kertoo kuinka hyvät koodin virheenkorjausominaisuudet ovat. Koodin minimietäisyys määritellään lyhimpänä etäisyytenä kahden eri koodisanan välillä eli

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

Minimietäisyydet Esimerkin 1.3 koodeille ovat $d(C_1) = 1$, $d(C_2) = 2$ ja $d(C_3) = 3$.

LAUSE 1.4. (i) *Koodi C havaitsee enintään s virhettä mistä tahansa koodisanasta, jos $d(C) \geq s + 1$.*

(ii) *Koodi C korjaa enintään t virhettä mistä tahansa koodisanasta, jos $d(C) \geq 2t + 1$.*

TODISTUS ([**2**, s. 7]).

(i) Oletetaan, että $d(C) \geq s+1$. Oletetaan, että lähetetään koodisana $\mathbf{x}$ ja että virheitä ilmenee s kappaletta tai vähemmän. Tällöin vastaanotettu vektori ei voi olla toinen koodisana ja täten virheet voidaan havaita.

(ii) Oletetaan, että $d(C) \geq 2t + 1$. Oletetaan, että lähetetään koodisana $\mathbf{x}$ ja vastaanotetaan vektori $\mathbf{y}$, jossa virheitä ilmenee t kappaletta tai vähemmän, jolloin $d(\mathbf{x}, \mathbf{y}) \leq t$. Jos $\mathbf{x}'$ on mikä tahansa muu koodisana kuin $\mathbf{x}$, tällöin $d(\mathbf{y}, \mathbf{x}') \geq t+1$. Muulloin $d(\mathbf{y}, \mathbf{x}') \leq t$ ja tästä seuraa kolmioepäyhtälön avulla, että

$$d(\mathbf{x}, \mathbf{x}') \leq d(\mathbf{x}, \mathbf{y}) + d(\mathbf{y}, \mathbf{x}') \leq 2t.$$

Tämä on ristiriita sen kanssa, että $d(C) \geq 2t + 1$. Näin ollen $\mathbf{x}$ on lähimpänä koodisanaa $\mathbf{y}$ ja lähimmän naapurin dekoodaus korjaa virheet.

□

SEURAUS 1.5. *Jos koodilla C on minimietäisyys d, niin C pystyy joko* (i) *havaitsemaan enintään $d-1$ virhettä tai* (ii) *korjaamaan enintään $\left\lfloor \frac{d-1}{2} \right\rfloor$ virhettä missä tahansa koodisanassa.*

TODISTUS ([**2**, s. 8]). (i) $d \geq s + 1$ jos ja vain jos $s \leq d - 1$.
(ii) $d \geq 2t + 1$ jos ja vain jos $t \leq \frac{d-1}{2}$.

□

Esimerkiksi, jos $d(C) = 3$, koodia C voidaan käyttää joko korjaamaan yhden virheen tai havaitsemaan kaksi virhettä. Virheiden havaitsemista ja korjaamista on havainnollistettu yleisemmin Taulukossa 1.1. Koodia, jonka pituus on n ja jossa on M koodisanaa sekä jonka minimietäisyys on d, sanotaan (n, M, d)-koodiksi.

ESIMERKKI 1.6 ([**2**, s. 8]). (i) Esimerkin 1.3 koodit nimetään seuraavasti: C_1 on $(2, 4, 1)$-koodi, C_2 on $(3, 4, 2)$-koodi ja C_3 on $(5, 4, 3)$-koodi.

TAULUKKO 1.1. Minimietäisyyden vaikutus koodin C havaitsemien ja korjaamien virheiden lukumääriin.

$d(C)$	Koodin C havaitsemien virheiden lukumäärä	Koodin C korjaamien virheiden lukumäärä
1	0	0
2	1	0
3	2	1
4	3	1
5	4	2
6	5	2
7	6	3
⋮	⋮	⋮

(ii) q-äärinen toistokoodi, jonka pituus on n ja jonka koodisanat ovat

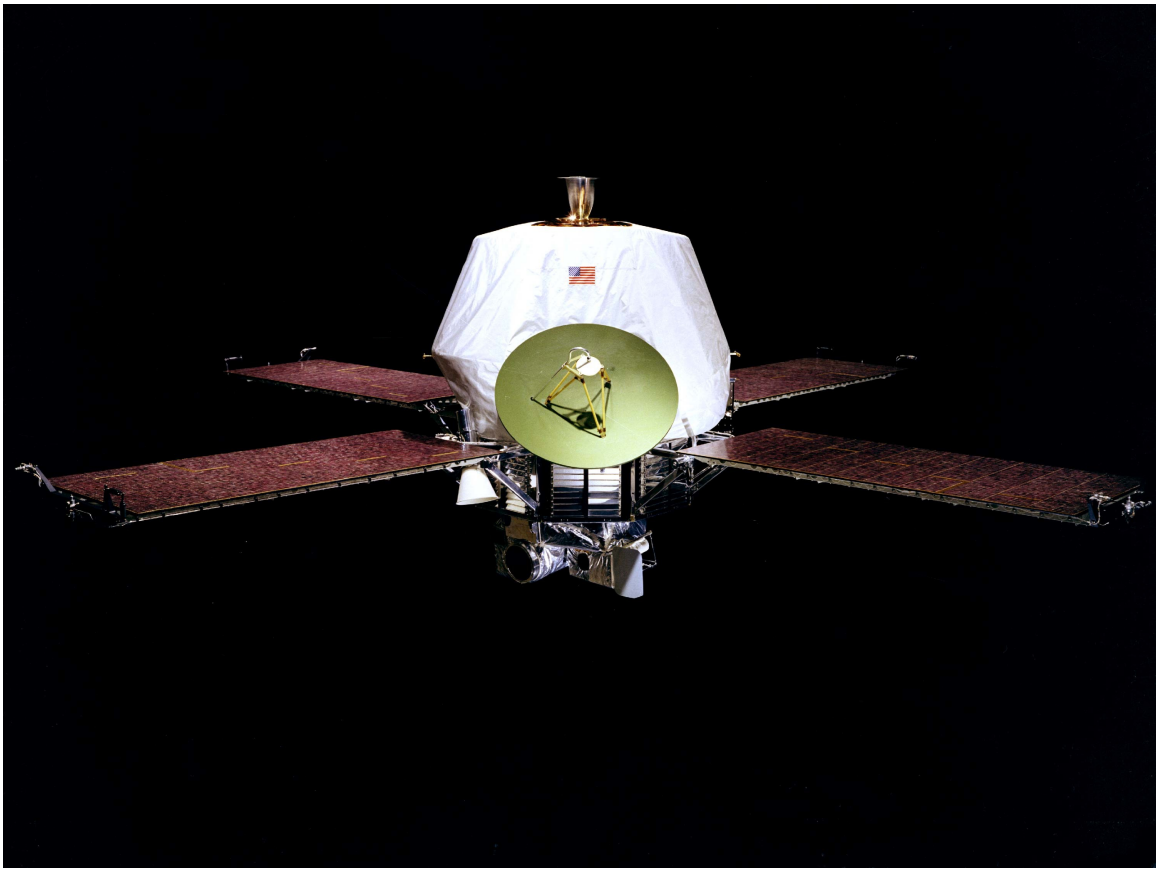
$$\begin{array}{cccc} 0 & 0 & \dots & 0 \\ 1 & 1 & \dots & 1 \\ \vdots & \vdots & & \vdots \\ (q-1) & (q-1) & \dots & (q-1) \end{array}$$

on (n, q, n)-koodi.

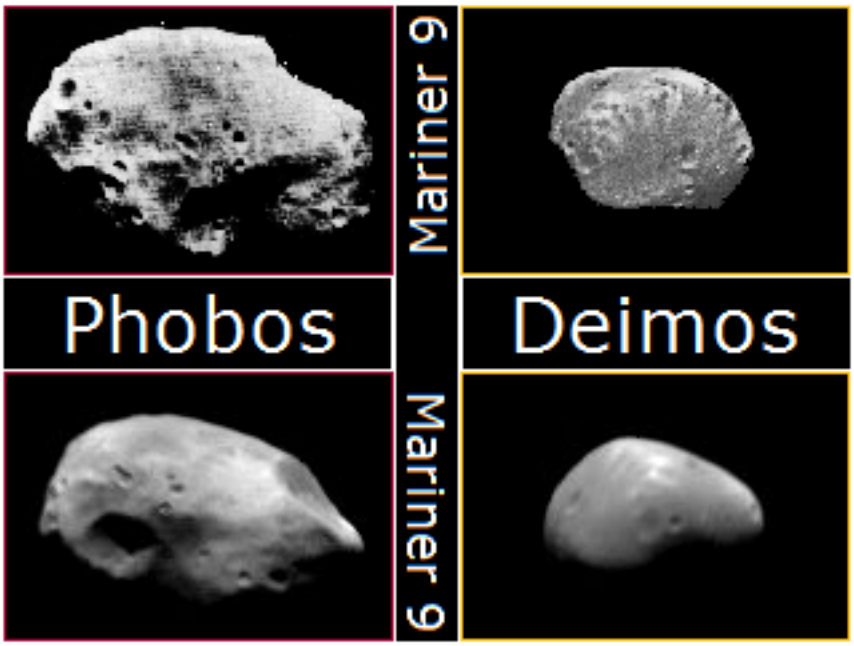
1.1. Valokuvien lähettäminen ulkoavaruudesta

NASA laukaisi toukokuun 30. päivä 1971 Mariner 9 -luotaimen (Kuva 1.4) tarkoituksena asettua Marsin kiertoradalle [**7**]. Luotain lähetti mustavalkokuvia Marsista binäärisen $(32, 64, 16)$-koodin avulla. Tämä Reedin ja Mullerin koodina tunnettu koodi sopii hyvin kohinaiselle kanavalle, sillä se korjaa jopa 7 virhettä ja lisäksi sillä on nopea dekoodausalgoritmi. Koodissa on 6-pituinen viestisana, johon lisätään redundanssina 26 bittiä, jolloin koodisanan pituudeksi tulee 32 bittiä. Tämä 6-pituinen viestisana kuvasi mustavalkoista kirkkaustasoa valkoisesta (= 000000) mustaan (= 111111).

Mariner 9 ehti kartoittaa noin 85 % Marsin pinta-alasta 7329 valokuvalla, jotka sisälsivät vähintään 80 kuvaa Marsin kuista Phoboksesta ja Deimoksesta (Kuva 1.5), kunnes se lakkasi toimimasta ja viimeisin yhteys siihen saatiin 27. lokakuuta 1972 [**7**]. Vuonna 1976 Viking 1 -luotain laskeutui Marsiin ja lähetti korkealaatuisia *värivalokuvia*. Värivalokuvat muodostettiin ottamalla useita mustavalkokuvia erilaisten värisuodattimien läpi, jolloin Maassa voitiin rekonstruoida mustavalkokuvat värikuviksi.



KUVA 1.4. Nasan lähes 7 metriä pitkä Mariner 9 -luotain [**7**].



KUVA 1.5. Mariner 9 -luotaimen ottamia kuvia Marsin kuista [**5**].

LUKU 2

Koodausteorian pääongelma

Hyvä (n, M, d)-koodi on sellainen, jolla on mahdollisimman lyhyt sanapituus n, suuri koodisanajoukko M ja suuri minimietäisyys d. Näillä ominaisuuksilla mahdollistetaan optimaalinen viestien lähettämisnopeus, monenlaisten viestien lähettäminen ja useiden virheiden korjaaminen. Suureksi harmiksi, mutta myös haasteeksi, nämä ominaisuudet ovat konfliktissa keskenään. Koodausteorian pääongelma onkin optimoida jokin parametreistä n, M tai d, kun kaksi näistä parametreistä on kiinnitetty. Yleensä ongelmaa lähestytään siten, että annetaan koodisanan pituus ja minimietäisyys ja yritetään näiden avulla ratkaista mahdollisimman monta koodisanaa. Luvun pohjana toimii Raymond Hillin kirja A First Course in Coding Theory (1986) [**2**].

Merkitään suurinta koodisanojen lukumäärää $M = A_q(n, d)$ sillä oletuksella, että tälläinen q-äärinen (n, M, d)-koodi on olemassa. Ongelma on helposti ratkaistavissa, kun $d = 1$ ja $d = n$, kaikilla q:

LAUSE 2.1. (i) $A_q(n, 1) = q^n$, (ii) $A_q(n, n) = q$.

TODISTUS ([**2**, s. 11]).

(i) Jotta koodin minimietäisyys olisi 1, tulee kaikkien koodisanojen olla erisuuret. Tällöin suurin q-äärinen $(n, M, 1)$-koodi on koko avaruus $(F_q)^n$, jolloin $M = q^n$.

(ii) Oletetaan, että C on q-äärinen (n, M, n)-koodi. Tällöin mitkä tahansa kaksi eri koodisanaa koodista C eroavat kaikissa n positiossa. Täten missä tahansa tarkasteltavassa positiossa oleva symboli M koodisanassa täytyy olla eri, saadaan $M \leq q$. Siispä $A_q(n,\ n) \leq q$. Toisaalta n-pituinen q-äärinen toistokoodi on (n, q, n)-koodi (Esimerkki 1.6), joten $A_q(n, n) = q$.

□

ESIMERKKI 2.2 ([**2**, s. 11]). Määrätään koodisanojen $A_2(5, 3)$ lukumäärä. Esimerkissä 1.3 C_3 on binäärinen $(5, 4, 3)$-koodi, joten $A_2(5, 3) \geq 4$. Voidaanko koodisanoja keksiä enemmän? Raakaa voimaa käytettäessä jouduttaisiin tarkastelemaan kaikkia 5-alkioisia osajoukkoja avaruudesta $(F_2)^5$ ja laskemaan minimietäisyys näille jokaiselle. Tällaisia osajoukkoja olisi yli 200 000. Vaihtoehtojen määrää voidaan kuitenkin vähentää ottamalla käyttöön merkintätapa ekvivalenteille koodeille. Palataan sen jälkeen takaisin tähän esimerkkiin.

2.1. Koodien ekvivalenttius

Joukon $S = \{x_1, x_2, \ldots, x_n\}$ permutaatio on injektio joukosta S itseensä. Merkitään permutaatiota f

$$\begin{pmatrix} x_1 & x_2 & \ldots & x_n \\ \downarrow & \downarrow & & \downarrow \\ f(x_1) & f(x_2) & \ldots & f(x_n) \end{pmatrix}.$$

MÄÄRITELMÄ 2.3. Kahta q-ääristä koodia kutsutaan ekvivalenteiksi, jos toinen voidaan saada toisesta seuraavien tyyppisten toimintojen yhdistelmällä:

(A) koodin positioiden permutaatio;
(B) kiinnitetyssä paikassa olevien symbolien permutaatio.

Jos koodi esitetään matriisimuodossa $M \times n$, jonka rivit ovat koodisanoja, niin toiminto (A) vastaa matriisien sarakkeiden uudelleen järjestämistä. Toiminto (B) taas vastaa symbolien uudelleen nimeämistä annetussa sarakkeessa. Selvästi näiden operaatioiden seurauksena koodisanojen etäisyys ei muutu ja näin ekvivalenteilla koodeilla on samat parametrit (n, M, d) ja samat virheenkorjausominaisuudet.

ESIMERKKI 2.4 ([**2**, s. 12]). Binäärikoodi

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

on ekvivalentti Esimerkin 1.3 koodin C_3 kanssa. Käytetään permutaatiota

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

kolmannessa positiossa oleviin symboleihin koodissa C ja sitten vaihdetaan keskenään positiot 2 ja 4. On hyvä huomata, että koodisanat on listattu eri järjestyksessä kuin Esimerkissä 1.3:

$$C = \begin{pmatrix} 0 & 0 & \overset{01}{\underset{10}{1}} & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 \end{pmatrix} \longrightarrow C = \begin{pmatrix} 0 & \overset{\downarrow}{0} & 0 & \overset{\downarrow}{0} & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 \end{pmatrix} \longrightarrow C = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{pmatrix} \begin{matrix} \leftarrow \\ \leftarrow \end{matrix}$$

Siis

$$C = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 \end{pmatrix} \longleftrightarrow C_3 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 \end{pmatrix}$$

LEMMA 2.5. *Mikä tahansa q-äärinen koodi aakkostolla $\{0, 1, \ldots, q-1\}$ on ekvivalentti (n, M, d)-koodin kanssa, mikä sisältää nollavektorin $\mathbf{0} = 00\cdots0$.*

TODISTUS ([**2**, s. 13]). Valitaan mikä tahansa koodisana $x_1x_2\cdots x_n$ ja jokaiselle $x_i \neq 0$ käytetään positiossa i oleville symboleille permutaatiota

$$\begin{pmatrix} 0 & x_i & j \\ \downarrow & \downarrow & \downarrow \\ x_i & 0 & j \end{pmatrix} \text{ kaikilla } j \neq 0, x_i \Bigg).$$

□

ESIMERKKI 2.2 (JATKOA). ([**2**, s. 13–14]). Osoitetaan nyt, että binäärisessä $(5, M, 3)$-koodissa täytyy olla $M \leq 4$ ja että $(5, 4, 3)$-koodi on yksikäsitteinen ekvivalenssimerkityksessä. Olkoon C $(5, M, 3)$-koodi, jossa $M \geq 4$. Tällöin Lemman 2.5 mukaan voidaan olettaa, että C sisältää nollavektorin $\mathbf{0} = 00000$. Nyt C sisältää enintään yhden koodisanan, jossa on 4 tai 5 ykköstä. Jos koodissa C olisi kaksi tällaista koodisanaa $\mathbf{x}$ ja $\mathbf{y}$, niin $\mathbf{x}$ ja $\mathbf{y}$ sisältäisivät vähintään 3 ykköstä samoissa positioissa, jolloin $d(\mathbf{x}, \mathbf{y}) \leq 2$, mikä olisi ristiriidassa koodin minimietäisyyden $d(C) = 3$ kanssa.

Koska $\mathbf{0} \in C$, ei voi olla koodisanoja, jotka sisältävät yhden tai kaksi ykköstä. Koska $M \geq 4$, niin täytyy olla vähintään kaksi koodisanaa, jotka sisältävät tasan 3 ykköstä. Positioiden uudelleenjärjestelyn jälkeen voidaan olettaa, että C sisältää koodisanat

$$\begin{array}{ccccc} 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0. \\ 0 & 0 & 1 & 1 & 1 \end{array}$$

Nyt voidaan helposti osoittaa yrityksen ja erehdyksen avulla, että ainut mahdollinen uusi koodisana voi olla 11011.

Näin on näytetty, että $A_2(5, 3) = 4$ ja että saatu koodi on yksikäsitteinen ekvivalenssimerkityksessä.

Taulukkoon 2.1 on kerätty viimeksi vuonna 2019 päivitetty lista löydetyistä eitriviaaleista arvoista binäärisille koodisanamäärille $A_2(n, d)$, kun $n \leq 28$ ja $d \leq 12$. Kun tarkkaa lukumäärää $A_2(n, d)$ ei tunneta, niin esimerkiksi merkintä 258–340 tarkoittaa, että $258 \leq A_2(n, d) \leq 340$. Taulukkoon ei tarvitse merkitä kuin parilliset etäisyydet d, sillä jos d on pariton, niin $A_2(n, d) = A_2(n+1, d+1)$ (ks. Lause 2.8). Ei ole suositeltavaa, että lukija käyttäisi liikaa aikaa ratkaisemattomiin tapauksiin Taulukossa 2.1, sillä vaikka monia työtunteja on käytetty, niin tämän hetkisiä parhaita rajoja on silti epäonnistuttu parantamaan.

Asetetaan F_2 joukoksi $\{0, 1\}$ ja määritellään kaksi operaatiota avaruudessa $(F_2)^n$. Olkoot $\mathbf{x} = x_1x_2\ldots x_n$ ja $\mathbf{y} = y_1y_2\ldots y_n$ kaksi vektoria avaruudessa $(F_2)^n$. Tällöin *summa* $\mathbf{x} + \mathbf{y}$ on vektori avaruudessa $(F_2)^n$ ja se määritellään

$$\mathbf{x} + \mathbf{y} = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)$$

ja samoin *tulo* $\mathbf{x} \cdot \mathbf{y} = \mathbf{x}\,\mathbf{y}$ on vektori avaruudessa $(F_2)^n$ ja se määritellään

$$\mathbf{x}\,\mathbf{y} = (x_1y_1, x_2y_2, \ldots, x_ny_n).$$

Termit $x_i + y_i$ ja x_iy_i lasketaan modulo 2 ilman muistinumeroa seuraavasti

$$\begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array} \qquad \begin{array}{c|cc} \cdot & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}.$$

Esimerkiksi $11100 + 00111 = 11011$
ja $11100 \cdot 00111 = 00100$.

Vektorin $\mathbf{x}$ *paino* $w(\mathbf{x})$ avaruudessa $(F_2)^n$ on vektorissa $\mathbf{x}$ olevien ykkösten lukumäärä.

LEMMA 2.6. *Jos* $\mathbf{x}$ *ja* $\mathbf{y} \in (F_2)^n$, *niin* $d(\mathbf{x}, \mathbf{y}) = w(\mathbf{x} + \mathbf{y})$.

TODISTUS. Summassa $\mathbf{x}+\mathbf{y}$ on 1 siinä kohtaa, missä $\mathbf{x}$ ja $\mathbf{y}$ eroavat ja 0 muualla. □

LEMMA 2.7. *Jos* $\mathbf{x}$ *ja* $\mathbf{y} \in (F_2)^n$, *niin*

$$d(\mathbf{x}, \mathbf{y}) = w(\mathbf{x}) + w(\mathbf{y}) - 2w(\mathbf{x}\,\mathbf{y}).$$

TAULUKKO 2.1. Tunnettuja binääristen koodisanojen lukumäärän $A_2(n, d)$ arvoja, kun $6 \leq n \leq 28$ [**1**].

n	$d = 4$	$d = 6$	$d = 8$	$d = 10$	$d = 12$
6	4	2	1	1	1
7	8	2	1	1	1
8	16	2	2	1	1
9	20	4	2	1	1
10	40	6	2	2	1
11	72	12	2	2	1
12	144	24	4	2	2
13	256	32	4	2	2
14	512	64	8	2	2
15	1024	128	16	4	2
16	2048	256	32	4	2
17	2816–3276	258–340	36	6	2
18	5632–6552	512–673	64	10	4
19	10496–13104	1024–1237	128	20	4
20	20480–26168	2048–2279	256	40	6
21	40960–43688	2560–4096	512	42–47	8
22	81920–87333	4096–6941	1024	64–84	12
23	163840–172361	8192–13674	2048	80–150	24
24	327680–344308	16384–24106	4096	136–268	48
25	2^{19}–599184	17920–47538	4096–5421	192–466	52–55
26	2^{20}–1198368	32768–84260	4104–9275	384–836	64–96
27	2^{21}–2396736	65536–157285	8192–17099	512–1585	128–169
28	2^{22}–4792950	131072–291269	16384–32151	1024–2817	178–288

TODISTUS ([**2**, s. 15]). Tehdään suora todistus lähtien väitteen vasemmalta puolelta päätyen oikealle puolelle:

$$\begin{aligned} d(\mathbf{x},\mathbf{y}) &= w(\mathbf{x}+\mathbf{y}) \\ &= \text{ (ykkösten määrä vektorissa } \mathbf{x}) + \text{ (ykkösten määrä vektorissa } \mathbf{y}) \\ &\quad - 2 \text{ (niiden positioiden lukumäärä, missä } \mathbf{x} \text{ ja } \mathbf{y} \text{ ovat molemmat ykkösiä)} \\ &= w(\mathbf{x}) + w(\mathbf{y}) - 2w(\mathbf{x}\,\mathbf{y}). \end{aligned}$$

□

LAUSE 2.8. *Olkoon d pariton. Tällöin binäärinen (n, M, d)-koodi on olemassa jos ja vain jos binäärinen $(n+1, M, d+1)$-koodi on olemassa.*

TODISTUS ([**2**, s. 16]). "vain jos": Olkoon C binäärinen (n, M, d)-koodi, missä d on pariton. Olkoon $\hat{C}$ sellainen koodi, jonka pituus on $n+1$ ja joka on saatu koodista C pidentämällä sen jokaista koodisanaa $\mathbf{x}$ seuraavan säännön mukaisesti

$$\mathbf{x} = x_1x_2\cdots x_n \to \hat{\mathbf{x}} = \begin{cases} x_1x_2\cdots x_n0 & \text{jos } w(\mathbf{x}) \text{ on parillinen} \\ x_1x_2\cdots x_n1 & \text{jos } w(\mathbf{x}) \text{ on pariton.} \end{cases}$$

Ekvivalentisti voidaan määritellä

$$\hat{\mathbf{x}} = x_1x_2\cdots x_nx_{n+1},$$

missä $x_{n+1} = \sum_{i=1}^{n} x_i$ modulo 2.

Tätä konstruktiota $\hat{C}$ kutsutaan nimellä "yleinen pariteettitarkistuksen lisääminen".

Koska paino $w(\mathbf{x})$ on parillinen jokaiselle koodisanalle $\hat{\mathbf{x}}$ koodissa $\hat{C}$, niin Lemman 2.7 mukaan $d(\hat{\mathbf{x}}, \hat{\mathbf{y}})$ on parillinen kaikilla $\hat{\mathbf{x}}, \hat{\mathbf{y}} \in \hat{C}$. Siksi $d(\hat{C})$ on parillinen. Selvästi $d \le d(C) \le d+1$ ja koska d on pariton, niin täytyy olla $d(\hat{C}) = d+1$. Täten $\hat{C}$ on $(n+1, M, d+1)$-koodi.

"jos": Olkoon D $(n+1, M, d+1)$-koodi, missä d on pariton. Valitaan koodisanat $\mathbf{x}$ ja $\mathbf{y}$ koodista D siten, että $d(\mathbf{x}, \mathbf{y}) = d+1$. Valitaan positio, missä $\mathbf{x}$ ja $\mathbf{y}$ eroavat ja poistetaan tämä positio kaikista koodisanoista. Tuloksena on (n, M, d)-koodi. □

SEURAUS 2.9. *Jos d on pariton, niin $A_2(n+1, d+1) = A_2(n, d)$. Ekvivalentisti, jos d on parillinen, niin $A_2(n, d) = A_2(n-1, d-1)$.*

ESIMERKKI 2.10 ([**2**, s. 16]). Esimerkissä 2.2 $A_2(5, 3) = 4$. Siispä Seurauksen 2.9 mukaan $A_2(6, 4) = 4$. Havainnollistetaan Lauseen 2.8 "vain jos"-kohtaa ja konstruoidaan $(6, 4, 4)$-koodi Esimerkin 1.3 $(5, 4, 3)$-koodin avulla.

$(5,4,3)$-koodi							$(6,4,4)$-koodi					
0	0	0	0	0			0	0	0	0	0	0
0	1	1	0	1	$\xrightarrow[\text{pariteettitarkistus}]{\text{lisätään yleinen}}$		0	1	1	0	1	1
1	0	1	1	0			1	0	1	1	0	1
1	1	0	1	1			1	1	0	1	1	0

2.2. Binomikertoimet

Jos n ja m ovat kokonaislukuja ja $0 \leq m \leq n$, niin määritellään binomikerroin

$$\binom{n}{m} = \frac{n!}{m!(n-m)!},$$

missä $m! = m(m-1)\cdots 3 \cdot 2 \cdot 1$, kun $m > 0$ ja $0! = 1$.

LEMMA 2.11. *Binomikerroin $\binom{n}{m}$ kertoo kuinka monella tapaa voidaan valita m alkiota n-alkioisesta joukosta, kun järjestyksellä ei ole väliä.*

TODISTUS ([**2**, s. 17]). Järjestetty valinta erilaisista alkioista m joukosta n voidaan tehdä

$$n(n-1)\cdots(n-m+1) = \frac{n!}{(n-m)!}$$

tavalla, sillä ensimmäinen alkio voidaan valita n tavalla, toinen $n-1$ tavalla jne. Koska m alkiota voidaan järjestää $m(m-1)\cdots 2 \cdot 1$ tavalla, niin valintojen määrä, kun järjestyksellä ei ole väliä, on

$$\frac{n!}{m!(n-m)!}.$$

□

ESIMERKKI 2.12 ([**2**, s. 17–18]). (i) Havainnollistetaan Lemman 2.11 todistusta luettelemalla valinnat kuinka 2 oliota voidaan valita 4:n joukosta. Järjestettyjä pareja on $4 \cdot 3 = \frac{4!}{2!} = 12$ kappaletta:

$$(1,2),(1,3),(1,4),(2,1),(2,3),(2,4),(3,1),(3,2),(3,4),(4,1),(4,2),(4,3).$$

Kun järjestyksellä ei ole väliä, niin pareja on $\frac{4!}{2!2!} = \binom{4}{2} = 6$ kappaletta:

$$\{1,2\},\{1,3\},\{1,4\},\{2,3\},\{2,4\},\{3,4\}.$$

(ii) Pitkävedossa valitaan strategiaksi pelata 10 tasapeliherkästä ottelusta lappuja, joissa on täsmälleen 8 tasapeliä. Tällöin tarvittava määrä erilaisia pitkävetolappuja on $\binom{10}{8} = 45$.

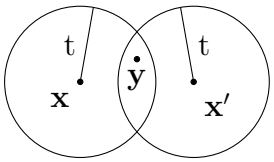
(iii) Erilaisten binäärikoodien lukumäärä parametreillä $M = 5$ ja $n = 5$ on $\binom{2^5}{5} = \binom{32}{5} = 201376$ kappaletta. Tietysti ei-ekvivalentteja koodeja on paljon pienempi määrä kuin tämä.

(iv) Painoa i olevien binääristen vektoreiden lukumäärä avaruudessa $(F_2)^n$ on $\binom{n}{i}$. Tämä vastaa tilannetta, jossa valitaan kuinka monella eri tavalla i ykköstä voidaan valita n positioiden joukosta. Esimerkiksi kahden painoisia vektoreita avaruudessa $(F_2)^4$ on $\binom{4}{2} = 6$ kappaletta: $1100, 1010, 1001, 0110, 0101, 0011$.

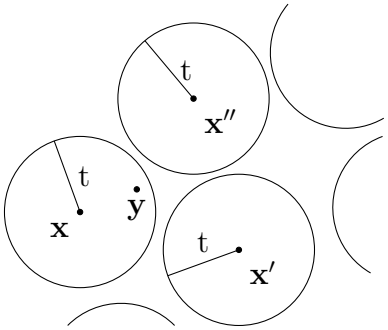
Seuraavaksi esitellään pallon käsite joukossa $(F_q)^n$. Vaikka puhutaankin pallosta, on ehkä hyödyllistä ajatella $(F_q)^n$ avaruutena, joka ei ole kolmiulotteinen. Kahden pisteen välinen etäisyys avaruudessa $(F_q)^n$ on tietysti Hammingin etäisyys, joten seuraava määritelmä on varsin luonnollinen.

MÄÄRITELMÄ 2.13. Jokaiselle vektorille $\mathbf{u}$ avaruudessa $(F_q)^n$ ja mille tahansa kokonaisluvulle $r \geq 0$, r-säteinen ja $\mathbf{u}$-keskinen *pallo* $S(\mathbf{u}, r)$ on joukko

$$S(\mathbf{u}, r) = \{\mathbf{v} \in (F_q)^n \mid d(\mathbf{u}, \mathbf{v}) \leq r\}.$$



KUVA 2.1. Pallot leikkaavat eikä vastaanotettua vektoria $\mathbf{y}$ voida korjata.



KUVA 2.2. Pallot eivät leikkaa ja vastaanotettu vektori $\mathbf{y}$ voidaan korjata.

HUOMAUTUS 2.14 ([**2**, s. 19]). Tulkitaan Lausetta 1.4 (ii) visuaalisesti. Jos $d(C) \geq 2t+1$, niin koodin C koodisanakeskeiset ja t-säteiset pallot ovat pistevieraita eli ne eivät mene päällekäin. Sillä, jos vektori $\mathbf{y}$ olisi sekä pallossa $S(\mathbf{x}, t)$ että pallossa $S(\mathbf{x}', t)$ koodisanoilla $\mathbf{x}$ ja $\mathbf{x}'$ (Kuva 2.1), niin kolmioepäyhtälön nojalla olisi

$$d(\mathbf{x}, \mathbf{x}') \leq d(\mathbf{x}, \mathbf{y}) + d(\mathbf{x}', \mathbf{y}) \leq t + t = 2t,$$

joka on ristiriita oletuksen $d(C) \geq 2t+1$ kanssa.

Jos enintään t virhettä ilmenee koodisanassa $\mathbf{x}$, niin vastaanotettu vektori $\mathbf{y}$ saattaa olla eri kohdassa kuin pallon $S(\mathbf{x}, t)$ keskusta, mutta se ei voi "paeta" pallosta ja siten se "vedetään" koodisanaan $\mathbf{x}$ lähimmän naapurin dekoodauksella (Kuva 2.2).

LEMMA 2.15. *Avaruudessa $(F_q)^n$ oleva r-säteinen pallo sisältää täsmälleen*

$$\binom{n}{0} + \binom{n}{1}(q-1) + \binom{n}{2}(q-1)^2 + \cdots + \binom{n}{r}(q-1)^r$$

vektoria.

TODISTUS ([**2**, s. 20]). Olkoon $\mathbf{u}$ kiinnitetty vektori avaruudessa $(F_q)^n$. Tarkastellaan kuinka monta vektoria $\mathbf{v}$ on täsmälleen etäisyydellä m vektorista $\mathbf{u}$, missä $m \leq n$. Olkoon m niiden positioiden määrä, joissa vektori $\mathbf{v}$ eroaa vektorista $\mathbf{u}$. Kussakin positiossa voidaan valita $q-1$ kappaletta erilaisia alkioita aakkostosta. Täten erilaisten vektoreiden $\mathbf{v}$ määrä, jotka eroavat tasan m kohdassa vektorista $\mathbf{u}$, on $\binom{n}{m}(q-1)^m$. Täten yhteensä vektorien lukumäärä pallossa $S(\mathbf{u}, r)$ on

$$\binom{n}{0} + \binom{n}{1}(q-1) + \binom{n}{2}(q-1)^2 + \cdots + \binom{n}{r}(q-1)^r$$

kappaletta. □

LAUSE 2.16 (Pakkauspalloraja tai Hammingin raja). *q-ääriselle $(n, M, 2t+1)$-koodille on voimassa*

$$M\left\{\binom{n}{0} + \binom{n}{1}(q-1) + \cdots + \binom{n}{t}(q-1)^t\right\} \leq q^n. \tag{2.1}$$

TODISTUS ([**2**, s. 20]). Olkoon C q-äärinen $(n, M, 2t+1)$-koodi. Huomatuksessa 2.14 todettiin, että millään kahdella erillisellä koodisanakeskeisellä t-säteisellä pallolla ei ole yhteisiä vektoreita. Tällöin M kappaletta koodisanakeskisiä t-säteisiä palloja

sisältää yhteensä epäyhtälön (2.1) vasemman puolen määrän vektoreita. Tämän määrän täytyy olla enintään q^n eli kaikkien vektorien määrä avaruudessa $(F_q)^n$. □

Jatkoa ajatellen ilmaistaan epäyhtälö (2.1) erityisesti binäärisille koodeille: jokaiselle binääriselle $(n, M, 2t+1)$-koodille on voimassa

$$M\left\{1+\binom{n}{1}+\binom{n}{2}+\cdots+\binom{n}{t}\right\} \leq 2^n. \tag{2.2}$$

Annetuille arvoille q, n ja d pakkauspalloraja tarjoaa ylärajan koodisanamäärälle $A_q(n,d)$. Esimerkiksi binääriselle $(5, M, 3)$-koodille on voimassa $M\{1+5\} \leq 2^5 = 32$, joten $A_2(5,3) \leq 5$. Tietysti, vaikka joukolle lukuja n, M ja d on voimassa pakkauspalloraja, se ei kuitenkaan tarkoita sitä, että tällainen koodi näillä parametreilla olisi olemassa. Kuten Esimerkistä 2.2 nähtiin, ei ole olemassa binääristä $(5,5,3)$-koodia ja todellinen arvo koodisanamäärälle $A_2(5,3)$ on vain 4.

2.3. Perfektit koodit

Koodia sanotaan *perfektiksi*, jos se saavuttaa pakkauspallorajan eli yhtäsuuruus toteutuu epäyhtälössä (2.1). Perfektillä t virhettä korjaavalla koodilla voidaan ”täyttää” koko avaruus $(F_q)^n$ M kappaleella koodisanakeskisillä t-säteisillä palloilla ilman, että pallot leikkaavat. Tai toisin sanoen, jokainen vektori avaruudessa $(F_n)^q$ on enintään etäisyydellä t täsmälleen yhdestä koodisanasta.

Binäärinen toistokoodi

$$\begin{cases} 0 & 0 & \cdots & 0 \\ 1 & 1 & \cdots & 1 \end{cases}',$$

jonka pituus on n, missä n on pariton, on perfekti $(n, 2, n)$-koodi. Tällaisia koodeja yhdessä yhden koodisanan mittaisten koodien tai koodien, jotka ovat koko avaruus $(F_q)^n$ kanssa, ovat nimeltään *triviaaleja* perfektejä koodeja.

Kaikkien perfektien koodien löytäminen on tarjonnut matemaatikoille yhden suurimmista haasteista koodausteoriassa. Niin sanotut Hammingin koodit ovat täydellisiä ei-triviaaleja perfektejä koodeja, mutta näihin koodeihin ei tutustuta tarkemmin tässä tutkielmassa. Hammingin koodit ovat kuitenkin helppoja konstruoida.

LUKU 3

Johdatus äärellisiin kuntiin

Jotta virheenkorjauskoodit olisivat helpompia käyttää ja analysoida, on tarpeellista asettaa hieman algebrallista rakennetta niihin. On äärimmäisen käytännöllistä, että käytetään aakkostoa, jonka alkioita on mahdollista laskea yhteen, vähentää, kertoa ja jakaa ilman rajoituksia. Toisin sanoen halutaan antaa kunnan rakenne joukolle F_q. Luku pohjautuu pääosin Raymond Hillin kirjaan A First Course in Coding Theory (1986) [**2**].

MÄÄRITELMÄ 3.1. Kunta F on epätyhjä joukko alkioita varustettuna kahdella laskutoimituksella + (yhteenlasku) ja $\cdot$ (kertolasku) seuraavin ominaisuuksin, kaikilla $a, b, c \in F$:

(i) F on suljettu yhteenlaskun ja kertolaskun suhteen eli $a + b \in F$ ja $a \cdot b \in F$.
(ii) Vaihdannaisuus: $a + b = b + a, \quad a \cdot b = b \cdot a$.
(iii) Liitännäisyys: $(a + b) + c = a + (b + c), \quad a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
(iv) Distributiivisyys: $a \cdot (b + c) = a \cdot b + a \cdot c$.
Lisäksi kahden neutraalialkion 0 ja 1 täytyy olla olemassa joukossa F ja niille on voimassa:
(v) $a + 0 = a$, kaikilla $a \in F$.
(vi) $a \cdot 1 = a$, kaikilla $a \in F$.
(vii) Mille tahansa $a \in F$ on olemassa yhteenlaskun vasta-alkio $-a$ joukossa F siten, että $a + (-a) = 0$.
(viii) Mille tahansa $a \neq 0 \in F$ on olemassa kertolaskun käänteisalkio $a^{-1} \in F$ siten, että $a \cdot a^{-1} = 1$.

HUOMAUTUS 3.2. Tästä eteenpäin merkitään yleisesti, että $a \cdot b$ on sama kuin ab.

LEMMA 3.3. *Millä tahansa kunnalla F on seuraavat ominaisuudet:*

(i) $a0 = 0$ *kaikilla* $a \in F$.
(ii) $ab = 0 \Rightarrow a = 0$ *tai* $b = 0$.

TODISTUS ([**2**, s. 32]).

(i) Määritelmän 3.1 (iv ja v) mukaan $a0 = a(0+0) = a0+a0$. Lisätään yhteenlaskun käänteisalkio $-a0$ molemmille puolille, jolloin
$$a0 + (-a0) = a0 + a0 + (-a0) \Leftrightarrow 0 = a0.$$
(ii) Oletetaan $ab = 0$. Jos $a \neq 0$, niin a:lla on käänteisalkio kertolaskun suhteen, jolloin $b = 1 \cdot b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}0 = 0$. Täten $ab = 0 \Rightarrow a = 0$ tai $b = 0$.

□

Joukko F, joka täyttää Määritelmän 3.1 ehdot (i)–(vii) on nimeltään (kommutatiivinen) *rengas*. Kunta, jossa on vain äärellinen määrä alkioita on nimeltään *äärellinen kunta*. Äärellisen kunnan alkioiden määrää kutsutaan nimellä kunnan *kertaluku*.

Pienintä positiivista kokonaislukua n, jolle

$$\overbrace{1 + \cdots + 1}^{n \text{ kappaletta}} = 0,$$

sanotaan kunnan *karakteristikaksi*.

LAUSE 3.4. *Äärellinen kertalukua q oleva kunta on olemassa jos ja vain jos q on alkulukupotenssi ts. $q = p^h$, missä p on alkuluku ja h positiivinen kokonaisluku. Lisäksi, jos q on alkulukupotenssi, niin on olemassa nimeämisen suhteen vain yksi tämän kertaluvun omaava kunta.*

TODISTUS. Todistus sivuutetaan; katso [**3**, s. 49–56] tai [**9**, s. 511–515]. □

Kertalukua q olevia äärellisiä kuntia kutsutaan usein *Galois'n kunniksi* ja niitä merkitään $\mathrm{GF}(q)$ tai $\mathbb{F}_q$.

MÄÄRITELMÄ 3.5. Olkoon m kiinnitetty positiivinen kokonaisluku. Sanotaan, että kaksi kokonaislukua a ja b ovat *kongruentteja* modulo m eli

$$a \equiv b \bmod m,$$

jos $a - b$ on jaollinen kokonaisluvulla m, eli jos $a = km + b$ jollekin kokonaisluvulle k.

Jos a ja b eivät ole kongruentteja modulo m, niin kirjoitetaan $a \not\equiv b \bmod m$.

Jokainen kokonaisluku, joka jaetaan luvulla m saa yksikäsitteisen jakojäännöksen, joka löytyy joukosta $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$. On helppo osoittaa, että kaksi kokonaislukua ovat kongruentteja modulo m jos ja vain jos niillä on sama jakojäännös jaettaessa luvulla m.

ESIMERKKI 3.6 ([**2**, s. 33]).

$$\begin{array}{lll} 3 \equiv 24 \bmod 7, & 13 \equiv -2 \bmod 5, & 25 \not\equiv 12 \bmod 7, \\ 15 \equiv 0 \bmod 3, & 15 \equiv 0 \bmod 5, & 15 \not\equiv 0 \bmod 2. \end{array}$$

LAUSE 3.7. *Olkoon $a \equiv a' \bmod m$ ja $b \equiv b' \bmod m$. Tällöin*

(i) $a + b \equiv a' + b' \bmod m$

(ii) $ab \equiv a'b' \bmod m$.

TODISTUS ([**2**, s. 34]). Joillekin kokonaisluvuille k ja l pätee $a \equiv a' + km$ ja $b \equiv b' + lm$. Tällöin (i) $a + b = a' + b' + (k + l)m$ ja siis $a + b \equiv a' + b' \bmod m$ ja (ii) $ab = a'b' + (kb' + a'l + klm)m$ ja siis $ab \equiv a'b' \bmod m$. □

Lause 3.7 mahdollistaa kongruenssien laskemisen työskentelemättä suurempien lukujen kanssa. Huomataan, että jos $a \equiv a'$, niin (ii):n toistuva käyttö osoittaa, että kaikilla positiivisilla kokonaisluvuilla n, $a^n \equiv (a')^n \bmod m$.

ESIMERKKI 3.8 ([**2**, s. 34]). (i) Mikä on jakojäännös kun $73 \cdot 52$ jaetaan luvulla 7? Lasketaan ensin $73 \equiv 3 \bmod 7$ ja $52 \equiv 3 \bmod 7$. Täten Lauseen 3.7 (ii) nojalla $73 \cdot 52 \equiv 3 \cdot 3 \equiv 9 \equiv 2 \bmod 7$. Jakojäännös on siis 2. (Ei siis tarvitse kertoa $73 \cdot 52$ ja jakaa vastausta luvulla 7.)

(ii) Tutkitaan, onko $(2^{15})(14^{40})+1$ jaollinen luvulla 11. Huomataan, että $2^5 \equiv 32 \equiv -1 \bmod 11$. Samoin $14^2 \equiv 3^2 \equiv -2 \bmod 11$. Täten

$$\begin{aligned}(2^{15})(14^{40}) &\equiv (2^5)^3(3^2)^{20} \equiv (-1)^3(-2)^{20} \\ &\equiv (-1)(2^{20}) \equiv (-1)(2^5)^4 \equiv (-1)(-1)^4 \equiv -1 \bmod 11.\end{aligned}$$

Siispä $(2^{15})(14^{40})+1 \equiv 0 \bmod 11$ eli luku on jaollinen luvulla 11.

Luvun $k \in \mathbb{Z}$ *jäännösluokka* $[k]_m$ modulo m on luvun k kanssa kongruenttien lukujen joukko eli

$$[k]_m = \{a \in \mathbb{Z} \mid a \equiv k \bmod m\} = \{k + lm \mid l \in \mathbb{Z}\}.$$

Kokonaislukujen jakoyhtälön nojalla on olemassa yksikäsitteiset kokonaisluvut q ja r siten, että

$$k = qm + r \text{ ja } 0 \leq r < m.$$

(Määritellään jakojäännökselle $r := q \operatorname{rem} m$). Näin ollen luvun k jäännösluokalle on

$$[k]_m = [r]_m,\ r \in \{0, \ldots, m-1\},$$

missä lukua r kutsutaan jäännösluokan $[k]_m$ *edustajaksi*.

Kokonaislukujen jäännösluokkien yhteen- ja kertolasku määritellään kaavoilla

$$\begin{aligned}[a]_m + [b]_m &:= [a+b]_m \text{ ja} \\ [a]_m \cdot [b]_m &:= [a \cdot b]_m.\end{aligned}$$

Lisäksi on voimassa, että $[a]_m = [a']_m$ jos ja vain jos $a \equiv a' \bmod m$. Tällöin Lauseesta 3.7 seuraa, että

$$\begin{aligned}[a+b]_m &= [a'+b']_m \\ [ab]_m &= [a'b']_m.\end{aligned}$$

Lause 3.7 osoittaa, että yhteen- ja kertolasku on hyvin määriteltyjä joukossa $\mathbb{Z}_m = \{[k]_m \mid k \in \mathbb{Z}\}$ ja on helposti tarkistettavissa, että kunnan ominaisuudet (i)–(vii) ovat voimassa mille tahansa m (vasta-alkio yhteenlaskun suhteen on $m-a$). Täten, $\mathbb{Z}_m$ on rengas mille tahansa kokonaisluvulle $m \geq 2$. Mutta mille luvun m arvoille kunnan ehto (viii) pätee? Seuraava lause vastaa tähän kysymykseen.

LAUSE 3.9. *Joukko $\mathbb{Z}_m$ on kunta jos ja vain jos m on alkuluku.*

TODISTUS ([**2**, s. 35]). Aluksi oletetaan, että m ei ole alkuluku. Tällöin $m = ab$ joillekin kokonaisluvuille a ja b, jotka molemmat ovat pienempiä kuin m. Täten

$$ab \equiv 0 \bmod m, \quad a \not\equiv 0 \bmod m \quad \text{ja} \quad b \not\equiv 0 \bmod m.$$

Eli joukossa $\mathbb{Z}_m$ nollasta eroavien alkioiden a ja b tulo on nolla ja täten Lemman 3.3 (ii) nojalla $\mathbb{Z}_m$ ei ole kunta.

Oletetaan nyt, että m on alkuluku. Tähän lauseeseen johtaneiden huomioiden avulla joukon $\mathbb{Z}_m$ kunnaksi osoittamiseksi riittää osoittaa, että jokaisella nollasta eroavalla alkiolla joukosta $\mathbb{Z}_m$ on käänteisalkio kertolaskun suhteen. Olkoon a nollasta eroava alkio joukosta $\mathbb{Z}_m$ ja tarkastellaan $m-1$ alkiota $1a, 2a, \ldots, (m-1)a$.

Nämä alkiot ovat nollasta eroavia, sillä alkioilla ia ei voi olla alkulukua m jakajana, jos i ja a eivät ole jaollisia luvulla m. Myöskin, alkiot ovat keskenään erisuuret, sillä

$$\begin{aligned} ia = ja &\Rightarrow (i-j)a \equiv 0 \bmod m \\ &\Rightarrow m \text{ jakaa } (i-j)a \\ &\Rightarrow m \text{ jakaa } i-j, \text{ sillä } m \text{ on alkuluku ja ei jaa lukua } a. \\ &\Rightarrow i = j, \text{ sillä molemmat } i \text{ ja } j \in \{1, 2, \ldots, m-1\}. \end{aligned}$$

Joukossa $\mathbb{Z}_m$ olevien alkioiden $1a, 2a, \ldots, (m-1)a$ on siis oltava yhtä suuria kuin alkiot $1, 2, \ldots, m-1$ jossain järjestyksessä ja yhden niistä, sanotaan ja, tulee olla yhtä suuri kuin 1. Tämä j on haluttu luvun a käänteisalkio. □

ESIMERKKI 3.10 ([**2**, s. 35–36]). (1) Yhteen- ja kertolaskutaulut joukolle $\mathbb{F}_2 = \mathbb{Z}_2 = \{0, 1\}$ ovat

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

.

(2) Yhteen- ja kertolaskutaulut joukolle $\mathbb{F}_3 = \mathbb{Z}_3 = \{0, 1, 2\}$ ovat

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

.

(3) Lauseen 3.9 mukaan joukko $\mathbb{Z}_4$ ei ole kunta. Tätä voidaan tarkastella tutkimalla joukon $\mathbb{Z}_4$ kertolaskutaulua, josta huomataan, ettei luvulla 2 ole käänteisalkiota:

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

.

Kuitenkin, vaikka $4 = 2^2$ ei ole alkuluku, se on alkulukupotenssi, jolloin Lauseen 3.4 mukaan kunta $\mathbb{F}_4$ on olemassa. Voidaankin määritellä, että $\mathbb{F}_4 = \{0, 1, a, b\}$ tauluilla:

+	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

·	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

.

(4) Joukot $\mathbb{Z}_6$ ja $\mathbb{Z}_{10}$ eivät ole kuntia, eikä ole olemassa yhtään kuntaa (Lause 3.9), jonka kertaluku on 6 tai 10.

3.1. Polynomialgebraa

Olkoon $F[x]$ F-kertoimisten polynomien joukko kunnan F suhteen. Jos $f(x) = f_0 + f_1 x + \cdots + f_m x^m$ on polynomi ja $f_m \neq 0$, niin m on polynomin $f(x)$ *aste* eli $\deg f(x)$. Nollapolynomin aste $\deg 0 := -\infty$. Kerroin f_m on nimeltään *johtava kerroin*. Jos $f_m = 1$, niin polynomi on nimeltään *pääpolynomi*.

Joukon $F[x]$ polynomeja voidaan laskea yhteen, vähentää ja kertoa normaaliin tapaan. Joukko $F[x]$ toteuttaa aksioomat (i)–(vii) ja on siis *rengas*.

3.1.1. Polynomien jakoalgoritmi. Jakoalgoritmi sanoo, että jokaista polynomiparia $a(x)$ ja $b(x) \neq 0 \in F[x]$ kohti on olemassa yksikäsitteinen polynomipari $q(x)$ (*osamäärä*) ja $r(x)$ (*jakojäännös*) siten, että

$$a(x) = q(x)b(x) + r(x), \text{ missä } \deg r(x) < \deg b(x).$$

Tämä on vastaava tutulle kokonaislukurenkaiden jakoalgoritmille. Polynomit $q(x)$ ja $r(x)$ löydetään jakokulman avulla. Esimerkiksi joukossa $\mathbb{F}_2[x]$ voidaan jakaa polynomi $x^3 + x + 1$ polynomilla $x^2 + x + 1$ seuraavasti:

$$\begin{array}{rl} & \quad\;\; x - 1 \\ \cline{2-2} x^2 + x + 1 \big) & \; x^3 \quad\;\; + x + 1 \\ & -x^3 - x^2 - x \\ \cline{2-2} & \quad\;\; -x^2 \quad\;\; + 1 \\ & \quad\;\; x^2 + x + 1 \\ \cline{2-2} & \quad\;\; x + 2 \end{array}$$

Näin ollen $x^3 + x + 1 = (x - 1)(x^2 + x + 1) + (x + 2)$, jota muokataan kunnan $\mathbb{F}_2$ kertoimien ($-1 \equiv 1$, ja $2 \equiv 0$) mukaisesti $x^3 + x + 1 = (x + 1)(x^2 + x + 1) + x$, jolloin haluttu muoto polynomille $x^3 + x + 1$ on $q(x)(x^2 + x + 1) + r(x)$.

3.1.2. Polynomirengas modulo $f(x)$. Olkoon $f(x)$ kiinnitetty polynomi joukossa $F[x]$. Kaksi polynomia $g(x)$ ja $h(x)$ joukossa $F[x]$ ovat *kongruentteja modulo* $f(x)$ eli

$$g(x) \equiv h(x) \bmod f(x),$$

jos $g(x) - h(x)$ on jaollinen polynomilla $f(x)$.

Jakoalgoritmin mukaan mikä tahansa polynomi $a(x) \in F[x]$ on kongruentti modulo $f(x)$ yksikäsitteiselle polynomille $r(x)$, jonka aste $\deg r(x) < \deg f(x)$; $r(x)$ on siis jakojäännös, kun $a(x)$ jaetaan polynomilla $f(x)$.

Polynomin $a(x) \in F[x]$ ekvivalenssiluokkaa merkitään $[a(x)]_{f(x)}$. Kongruenssiluokkien joukkoa merkitään $F[x]/\langle f(x)\rangle$. Voidaan helposti todeta, että joukko $F[x]/\langle f(x)\rangle$ on rengas, kun laskutoimitukset on määritelty seuraavasti:

$$[a(x)]_{f(x)} + [b(x)]_{f(x)} \coloneqq [a(x) + b(x)]_{f(x)} \quad \text{ja} \quad [a(x)]_{f(x)}[b(x)]_{f(x)} \coloneqq [a(x)b(x)]_{f(x)}.$$

Nämä laskutoimitukset on hyvin määritelty, sillä jos $a(x) \equiv \tilde{a}(x)$ ja $b(x) \equiv \tilde{b}(x)$, niin

$$a(x) + b(x) \equiv \tilde{a}(x) + \tilde{b}(x) \bmod f(x) \quad \text{ja} \quad a(x)b(x) \equiv \tilde{a}(x)\tilde{b}(x) \bmod f(x).$$

Polynomin $a(x)$ jakojäännös $r(x)$, kun $a(x)$ jaetaan polynomilla $f(x)$ on yksikäsitteinen polynomi, jolle $[r(x)]_{f(x)} = [a(x)]_{f(x)}$ ja $\deg r(x) < \deg f(x)$. Tätä polynomia $r(x)$ kutsutaan jäännösluokan $[a(x)]_{f(x)}$ *edustajaksi*.

Joukon $F[x]$ polynomijoukkoa, jonka aste on pienempi kuin $\deg f(x)$ merkitään $F[x]/f(x)$. Yhteen- ja vähennyslasku modulo $f(x)$ suoritetaan seuraavasti. Olkoon $a(x)$ ja $b(x)$ polynomeja joukossa $F[x]/f(x)$. Tällöin summa $a(x) + b(x) \in F[x]/f(x)$ on sama kuin joukossa $F[x]$, koska $\deg(a(x) + b(x)) < \deg f(x)$. Tulo $a(x)b(x) \in F[x]/f(x)$ on yksikäsitteinen polynomi, jolle $a(x)b(x)$ on kongruentti modulo $f(x)$ ja jonka aste on pienempi kuin $\deg f(x)$.

Lasketaan esimerkiksi $(x+1)^2 \in \mathbb{F}_2[x]/(x^2+x+1)$:

$$(x+1)^2 = x^2+2x+1 \equiv x^2+1 \equiv x \bmod (x^2+x+1).$$

Siis $[(x+1)^2] = [x]$ joukossa $\mathbb{F}_2[x]/(x^2+x+1)$.

Samoin kuin $\mathbb{Z}_m$ on rengas, niin vastaavasti myös $F[x]/\langle f(x)\rangle$ on *polynomirengas (kunnan F suhteen) modulo $f(x)$*.

MÄÄRITELMÄ 3.11. Polynomi $f(x) \in F[x]$ on *jaollinen*, jos $f(x) = a(x)b(x)$, missä $a(x), b(x) \in F[x]$ ja $\deg a(x)$ ja $\deg b(x)$ ovat molemmat pienempiä kuin $\deg f(x)$. Jos $f(x)$ ei ole jaollinen, se on *jaoton*.

LEMMA 3.12. (i) *Polynomilla $f(x)$ on lineaarinen tekijä $x-a$ jos ja vain jos $f(a)=0$.*

(ii) *Polynomi $f(x) \in F[x]$, jonka aste on 2 tai 3 on jaoton jos ja vain jos $f(a) \neq 0$ kaikilla $a \in F$.*

(iii) *Jokaisessa kunnassa $x^n - 1 = (x-1)(x^{n-1}+x^{n-2}+\cdots+x+1)$* (jälkimmäinen tekijä voi hyvinkin olla jaollinen).

TODISTUS ([**2**, s. 144–145]).

(i) Jos $f(x) = (x-a)g(x)$, niin varmasti $f(a)=0$. Toisaalta oletetaan, että $f(x) = 0$. Jakoalgoritmin mukaan $f(x) = q(x)(x-a)+r(x)$, missä $\deg r(x) < 1$. Täten $r(x)$ on vakio, jonka täytyy olla nolla, sillä $0 = f(a) = r(a)$.

(ii) Polynomi, jonka aste on 2 tai 3 on jaollinen jos ja vain jos sillä on vähintään yksi lineaarinen kerroin. Tulos seuraa välittömästi kohdasta (i).

(iii) Kohdan (i) mukaan $x-1$ on polynomin x^n-1 tekijä ja jakokulman avulla löydetään toinen tekijä.

□

ESIMERKKI 3.13 ([**2**, s. 145]). Lemman 3.12 (iii) mukaan polynomi $x^3-1 \in \mathbb{F}_2[x]$ on $x^3-1 = (x-1)(x^2+x+1)$ kaikissa kunnissa. Lemman 3.12 (ii) mukaan x^2+x+1 on jaoton kunnassa $\mathbb{F}_2[x]$. Mutta kunnassa $\mathbb{F}_3[x]$ polynomi $x-1$ on Lemman 3.12 (i) mukaan polynomin x^2+x+1 tekijä ja tekijöihin jako antaa $x^3-1 = (x-1)^3$.

3.1.3. Äärelliset kunnat $\mathbb{F}_{p^h}, h > 1$. Renkaan $F[x]$ jaottomuus vastaa täysin kokonaisluvuissa alkulukuja. Lauseessa 3.9 osoitettiin, että rengas $\mathbb{Z}_m$ on kunta jos ja vain jos m on alkuluku ja seuraava lause todistetaan vastaavalla tavalla.

LAUSE 3.14. *Rengas $F[x]/\langle f(x)\rangle$ on kunta jos ja vain jos $f(x)$ on jaoton renkaassa $F[x]$.*

TODISTUS. Todistus samoin kuin Lauseen 3.9 todistus. □

Voidaan osoittaa (Lause 3.4), että mille tahansa alkuluvulle p ja mille tahansa positiiviselle kokonaisluvulle h *on olemassa* jaoton astetta h oleva polynomi kunnassa $\mathbb{F}_p$. Tämä tulos yhdessä lauseen 3.14 kanssa antaa olemassaolon kunnille $\mathbb{F}_{p^h}$ kaikille kokonaisluvuille $h \geq 1$. Nämä ovat pääasiallisesti ainoat äärelliset kunnat.

MÄÄRITELMÄ 3.15. Äärellisen kunnan $\mathbb{F}_q$ alkio α on nimeltään kunnan $\mathbb{F}_q$ *primitiivinen juuri*, jos $\mathbb{F}_q = \{0, \alpha, \alpha^2, \ldots, \alpha^{q-1}\}$.

Polynomi $f(x)$ on nimeltään *minimipolynomi*, jos se on pääpolynomi ja se on pienintä astetta oleva ehdon $f(\alpha) = 0$ täyttävä polynomi.

ESIMERKKI 3.16 ([**4**, s. 27]). Tarkastellaan kuntaa $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$, missä α on jaottoman polynomin $x^2 + x + 1 \in \mathbb{F}_2[x]$ juuri. Tällöin

$$\alpha^2 = -(1+\alpha) = 1 + \alpha, \quad \alpha^3 = \alpha(\alpha^2) = \alpha(1+\alpha) = \alpha + \alpha^2 = \alpha + 1 + \alpha = 1.$$

Täten $\mathbb{F}_4 = \{0, \alpha, 1+\alpha, 1\} = \{0, \alpha, \alpha^2, \alpha^3\}$ eli α on primitiivinen juuri.

3.2. Vektoriavaruus äärellisen kunnan suhteen

Tässä kappaleessa oletetaan, että q on alkulukupotenssi ja merkintä $\mathbb{F}_q$ tarkoittaa äärellistä kuntaa, jossa on q alkiota. Nämä alkiot ovat nimeltään *skalaareja*. Kaikkia järjestettyjä n-jonoja joukosta $\mathbb{F}_q$ merkitään $\mathbb{F}_q^n$.

Määritellään kaksi laskutoimitusta joukossa $\mathbb{F}_q^n$:

(i) vektorien *yhteenlasku*: jos $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ ja $\mathbf{y} = (y_1, y_2, \ldots, y_n) \in \mathbb{F}_q^n$, niin

$$\mathbf{x} + \mathbf{y} = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)$$

(ii) skalaarilla *kertominen*: jos

$$\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n \quad \text{ja} \quad a \in \mathbb{F}_q,$$

niin $a\mathbf{x} = (ax_1, ax_2, \ldots, ax_n)$.

Ei ole vaikeaa tarkistaa, että joukolle $\mathbb{F}_q^n$ on voimassa *vektoriavaruuden* aksioomat eli, että kaikille $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathbb{F}_q^n$ ja kaikille $a, b \in \mathbb{F}_q$,

(i) $\mathbf{u} + \mathbf{v} \in \mathbb{F}_q^n$
(ii) $(\mathbf{u} + \mathbf{v}) + \mathbf{w} = \mathbf{u} + (\mathbf{v} + \mathbf{w})$
(iii) nollavektori $\mathbf{0} = (0, 0, \ldots, 0) \in \mathbb{F}_q^n$ ja sille on voimassa $\mathbf{u} + \mathbf{0} = \mathbf{0} + \mathbf{u} = \mathbf{u}$.
(iv) Annetulle $\mathbf{u} = (u_1, u_2, \ldots, u_n) \in \mathbb{F}_q^n$, alkio $-\mathbf{u} = (-u_1, -u_2, \ldots, -u_n) \in \mathbb{F}_q^n$ ja sille on voimassa $\mathbf{u} + (-\mathbf{u}) = \mathbf{0}$.
(v) $\mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u}$.
(Ominaisuudet (i)–(v) tarkoittavat, että $\mathbb{F}_q^n$ on Abelin ryhmä yhteenlaskun suhteen).
(vi) (Suljettu skalaarilla kertomisen suhteen) $a\mathbf{v} \in \mathbb{F}_q^n$.
(vii) (Distributiivisuus) $a(\mathbf{u} + \mathbf{v}) = a\mathbf{u} + a\mathbf{v}$, $(a + b)\mathbf{u} = a\mathbf{u} + b\mathbf{u}$.
(viii) $(ab)\mathbf{u} = a(b\mathbf{u})$.
(ix) $1\mathbf{u} = \mathbf{u}$, missä 1 on joukon $\mathbb{F}_q$ kertolaskun neutraalialkio.

Joukon $\mathbb{F}_q^n$ osajoukko on nimeltään *aliavaruus*, jos se itse on vektoriavaruus yhteenlaskun ja skalaarilla kertomisen suhteen, kuten joukolle $\mathbb{F}_q^n$ on määritelty.

Triviaalisti joukko $\{\mathbf{0}\}$ ja koko avaruus $\mathbb{F}_q^n$ ovat joukon $\mathbb{F}_q^n$ aliavaruuksia. Aliavaruus on *ei-triviaali*, jos se sisältää vähintään yhden nollavektorista eroavan vektorin ja ei ole koko avaruus $\mathbb{F}_q^n$.

LAUSE 3.17. *Joukon $\mathbb{F}_q^n$ epätyhjä osajoukko C on aliavaruus jos ja vain jos C on suljettu yhteenlaskun ja skalaarilla kertomisen suhteen eli joukolle C on voimassa seuraavat kaksi ehtoa:*

(1) *Jos $\mathbf{x}, \mathbf{y} \in C$, niin $\mathbf{x} + \mathbf{y} \in C$.*
(2) *Jos $a \in \mathbb{F}_q$ ja $\mathbf{x} \in C$, niin $a\mathbf{x} \in C$.*

TODISTUS ([**2**, s. 42]). On helposti todennettavissa, että jos C toteuttaa ehdot (1) ja (2), niin C toteuttaa kaikki vektoriavaruuden aksiomat (i)–(ix) (kun $\mathbb{F}_q^n$ korvataan joukolla C). (Osoitettaessa, että $\mathbf{0} \in C$ valitaan mikä tahansa $\mathbf{x} \in C$; jolloin (2):

$\mathbf{0} = 0\mathbf{x} \in C$. Ominaisuuden (2) mukaan myös, jos $\mathbf{v} \in C$, niin $-\mathbf{v} \in C$, sillä $-\mathbf{v} = (-1)\mathbf{v}$.) □

Äärettömien kuntien vektoriavaruuksien määritelmät ja tulokset siirtyvät yleensä myös äärellisille kunnille. Kuten esimerkiksi seuraavat tulokset.

Vektoreiden $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_r$ *lineaarikombinaatio* joukossa $\mathbb{F}_q^n$ on muodoltaan $a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_r\mathbf{v}_r$, missä a_i:t ovat skalaareja.

Voidaan helposti tarkistaa, että kaikkien lineaarikombinaatioiden joukko annetusta vektorijoukosta $\mathbb{F}_q^n$ on joukon $\mathbb{F}_q^n$ aliavaruus.

Vektorijoukko $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_r\}$ on *lineaarisesti riippuva* jos löytyy jokin nollasta eroava skalaari $a_1, a_2, \ldots, a_r$ siten, että

$$a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_r\mathbf{v}_r = \mathbf{0}.$$

Vektorijoukko on *lineaarisesti riippumaton* jos se ei ole lineaarisesti riippuva eli

$$a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_r\mathbf{v}_r = \mathbf{0} \Rightarrow a_1 = a_2 = \cdots = a_r = 0.$$

Olkoon C joukon $\mathbb{F}_q^n$ aliavaruus. Tällöin joukon C osajoukko $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_r\}$ on nimeltään joukon C *virittävä joukko*, jos jokainen joukon C vektori voidaan ilmaista vektoreiden $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_r$ lineaarikombinaatiolla.

Joukon C virittävä joukko, joka on myös lineaarisesti riippumaton on nimeltään joukon C *kanta*. Esimerkiksi joukko

$$\{(1, 0, 0, \ldots, 0), (0, 1, 0, \ldots, 0), \ldots, (0, 0, 0, \ldots, 1)\}$$

on koko avaruuden $\mathbb{F}_q^n$ kanta.

LAUSE 3.18. *Olkoon C ei-triviaali joukon $\mathbb{F}_q^n$ aliavaruus. Tällöin mikä tahansa joukon C virittävä joukko sisältää joukon C kannan.*

TODISTUS ([**2**, s. 42]). Olkoon $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_r\}$ joukon C virittävä joukko. Jos se on lineaarisesti riippuva, niin tällöin löytyy jokin nollasta eroava skalaari $a_1, a_2, \ldots, a_r$ siten, että

$$a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_r\mathbf{v}_r = \mathbf{0}.$$

Jos a_j on nollasta eroava, niin

$$\mathbf{v}_j = -a_j^{-1} \sum_{i=1,\, i\neq j}^{r} a_i\mathbf{v}_i,$$

jolloin $\mathbf{v}_j$ on toisen vektorin $\mathbf{v}_i$ lineaarikombinaatio. Tosin $\mathbf{v}_j$ on virittäjänä tarpeeton ja se voidaan poistaa joukosta $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_r\}$, jolloin joukolle C saadaan pienempi virittävä joukko. Tällä tavoin voidaan yksi kerrallaan poistaa ylimääräiset virittäjät, kunnes saavutetaan lineaarisesti riippumaton virittävä joukko. Tämän prosessin täytyy loppua, sillä aloitettaessa joukko oli äärellinen. □

Koska mikä tahansa joukon $\mathbb{F}_q^n$ aliavaruus C sisältää äärellisen virittävän joukon (esimerkiksi C itse), Lauseesta 3.18 seuraa, että jokaisella ei-triviaalilla aliavaruudella on kanta. Kannan voidaan ajatella olevan minimaalinen virittävä joukko, joka ei sisällä ylimääräisiä virittäjiä.

LAUSE 3.19. *Olkoon* $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$ *joukon* $\mathbb{F}_q^n$ *aliavaruuden* C *kanta. Tällöin*

(i) *jokainen joukon* C *vektori voidaan ilmaista yksikäsitteisesti kantavektoreiden lineaarikombinaationa;*

(ii) *joukko* C *sisältää täsmälleen* q^k *vektoria jollekin* k*.*

TODISTUS ([**2**, s. 44]).

(i) Olkoon joukon C vektori $\mathbf{x}$ esitettynä kahdella tapaa vektoreiden $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$ lineaarikombinaationa:

$$\mathbf{x} = a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_k\mathbf{v}_k$$
$$\text{ja } \mathbf{x} = b_1\mathbf{v}_1 + b_2\mathbf{v}_2 + \cdots + b_k\mathbf{v}_k.$$

Tällöin $(a_1 - b_1)\mathbf{v}_1 + (a_2 - b_2)\mathbf{v}_2 + \cdots + (a_k - b_k)\mathbf{v}_k = \mathbf{0}$. Joukko $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$ on kuitenkin lineaarisesti riippumaton ja täten $a_i - b_i = 0$, kun $i = 1, 2, \ldots, k$, toisin sanoen $a_i = b_i$, kun $i = 1, 2, \ldots, k$.

(ii) Kohdan (i) mukaan q^k vektoria $\sum_{i=1}^{k} a_i\mathbf{v}_i (a_i \in \mathbb{F}_q)$ ovat täsmälleen joukon C eri vektorit.

□

Lauseesta 3.19 seuraa, että mitkä tahansa kaksi aliavaruuden C kantaa sisältää saman määrän k vektoreita, missä $|C| = q^k$ ja tätä lukua k kutsutaan aliavaruuden C *dimensioksi*. Merkitään tätä $\dim(C)$. Aikaisemmin on osoitettu, että joukon $\mathbb{F}_q^n$ kannalla on n vektoria, joten $\dim(\mathbb{F}_q^n) = n$.

LUKU 4

Lineaariset koodit

Tässä luvussa oletetaan, että aakkosto $\mathbb{F}_q$ on Galois'n kunta GF(q), missä q on alkulukupotenssi ja $\mathbb{F}_q^n$ on vektoriavaruus. Vektori $(x_1, x_2, \ldots, x_n)$ kirjoitetaan yleensä pelkistetysti $x_1x_2\cdots x_n$. Luvun pääasiallisena pohjana on käytetty Raymond Hillin kirjaa A First Course in Coding Theory (1986) [**2**].

Lineaarinen koodi kunnan $\mathbb{F}_q$ suhteen on joukon $\mathbb{F}_q^n$ aliavaruus jollain positiivisella kokonaisluvulla n.

Osajoukko $C \subset \mathbb{F}_q^n$ on lineaarinen koodi jos ja vain jos
(1) $\mathbf{u} + \mathbf{v} \in C$ kaikilla $\mathbf{u}$ ja $\mathbf{v} \in C$ ja
(2) $a\mathbf{u} \in C$ kaikilla $\mathbf{u} \in C$, $a \in \mathbb{F}_q$.

Erityisesti binäärinen koodi on lineaarinen jos ja vain jos kahden koodisanan summa on koodisana. Voidaan helposti tarkistaa, että Esimerkin 1.3 koodit C_1, C_2 ja C_3 ovat kaikki lineaarisia.

Jos C on joukon $\mathbb{F}_q^n$ k-dimensioinen aliavaruus, niin lineaarinen koodi C on nimeltään $[n, k]$-koodi tai $[n, k, d]$-koodi, kun koodin C minimietäisyys on d.

HUOMAUTUS 4.1 ([**2**, s. 47]). (i) Lauseen 3.19 mukaan q-äärinen $[n, k, d]$-koodi on myös q-äärinen (n, q^k, d)-koodi, mutta ei tietenkään jokainen (n, q^k, d)-koodi ole $[n, k, d]$-koodi.
(ii) Nollavektori $\mathbf{0}$ sisältyy automaattisesti lineaariseen koodiin.
(iii) Jotkut kirjoittajat viittaavat lineaarisiin koodeihin nimellä "ryhmäkoodit".

Määritellään, että vektorin $\mathbf{x} \in \mathbb{F}_q^n$ *paino* $w(\mathbf{x})$ on vektorin $\mathbf{x}$ nollasta eroavien alkioiden lukumäärä. Yksi lineaaristen koodien hyödyllisimmistä ominaisuuksista on se, että koodin minimietäisyys on yhtä suuri kuin nollasta eroavien koodisanojen pienin paino. Tämän todistamiseksi tarvitaan yksinkertainen lemma:

LEMMA 4.2. *Jos* $\mathbf{x}$ *ja* $\mathbf{y} \in \mathbb{F}_q^n$, *niin*

$$d(\mathbf{x}, \mathbf{y}) = w(\mathbf{x} - \mathbf{y}).$$

TODISTUS ([**2**, s. 47]). Vektorilla $\mathbf{x} - \mathbf{y}$ on nollasta eroavia alkioita täsmälleen niissä paikoissa, missä $\mathbf{x}$ ja $\mathbf{y}$ eroavat. □

HUOMAUTUS 4.3 ([**2**, s. 48]). Kun $q = 2$, Lemma 2.7 on sama kuin Lemma 4.2, sillä "plus" on sama kuin "miinus", kun toimitaan modulo 2.

LAUSE 4.4. *Olkoon* C *lineaarinen koodi ja* $w(C)$ *koodin* C *nollasta eroavien koodisanojen pienin paino. Tällöin* $d(C) = w(C)$.

TODISTUS ([**2**, s. 48]). On olemassa koodisanat $\mathbf{x}$ ja $\mathbf{y} \in C$ siten, että $d(C) = d(\mathbf{x}, \mathbf{y})$. Tällöin Lemman 4.2 mukaan

$$d(C) = w(\mathbf{x} - \mathbf{y}) \geq w(C),$$

koska $\mathbf{x} - \mathbf{y}$ on lineaarisen koodin C koodisana.

Toisaalta, jollekin koodisanalle $\mathbf{x} \in C$

$$w(C) = w(\mathbf{x}) = d(\mathbf{x}, \mathbf{0}) \geq d(C),$$

koska $\mathbf{0}$ sisältyy lineaariseen koodiin C. Täten $d(C) \geq w(C)$ ja $w(C) \geq d(C)$, jolloin $d(C) = w(C)$. □

Lineaaristen koodien hyötynä on koodin minimietäisyyden helppo määrittäminen. Tavalliselle koodille, jossa on M koodisanaa, täytyisi minimietäisyyden selvittämiseksi tehdä $\binom{M}{2} = \frac{1}{2}M(M-1)$ vertailua. Lauseen 4.4 ansiosta *lineaarisen* koodin minimietäisyys löytyy kuitenkin vain $M - 1$ nollasta eroavien koodisanojen pienimmän painon tutkimisella.

Toinen merkittävä hyöty lineaarisille $[n, k]$-koodeille on koodisanojen ilmoittaminen yksinkertaisesti kannan k koodisanan avulla. Ei-lineaaristen koodien kaikki koodisanat tulee listata yksitellen.

MÄÄRITELMÄ 4.5. Sellainen $k \times n$ -matriisi, jonka rivit muodostavat lineaarisen $[n, k]$-koodin kannan, on nimeltään koodin *virittäjämatriisi*.

ESIMERKKI 4.6 ([**2**, s. 49]). (i) Esimerkin 1.3 koodi C_2 on $[3, 2, 2]$-koodi, jonka virittäjämatriisi on

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

(ii) Kunnan $\mathbb{F}_q$ q-äärinen ja n-pituinen toistokoodi on $[n, 1, n]$-koodi, jonka virittäjämatriisi on

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \end{bmatrix}.$$

Lineaaristen koodien etuna on myös koodisanojen muodostamisen ja purkamisen helppous. Tätä asiaa käsitellään tarkemmin Kappaleessa 4.2.

Lineaaristen q-ääristen koodien haittapuolena on se, että ne eivät ole määriteltyjä ellei q ole alkulukupotenssi. Kuitenkin järkevät q-ääriset koodit, missä q ei ole alkulukupotenssi, voidaan usein muodostaa lineaarisista koodeista suuremmalla aakkostolla. Lineaarisiin koodeihin rajoittuminen saattaa merkitä myös rajoittumista heikompiin koodeihin kuin on toivottu. Osoittautuu kuitenkin, että joillain kriteerein opimaaliset koodit ovat hyvin usein lineaarisia. Esimerkiksi jokaiselle parametrijoukolle, jolle tiedetään olevan olemassa ei-triviaali perfekti koodi, löytyy *lineaarinen* perfekti koodi ko. parametreillä. On huomioitavaa myös kuinka usein $A_2(n, d)$ arvo Taulukossa 2.1 on luvun 2 potenssi. Tavallisesti, mutta ei aina, $A_2(n, d)$ arvo saavutetaan lineaarisella koodilla.

4.1. Lineaaristen koodien ekvivalenttius

Koodien ekvivalenttiuden määritelmä Kappaleessa 2.1 muokkaantuu koskemaan lineaarisia koodeja, kun sallitaan vain sellaiset symbolien permutaatiot, mitkä saadaan kertomalla nollasta eroavalla skalaarilla. Täten kaksi lineaarista koodia kunnassa $\mathbb{F}_q$ ovat *ekvivalentit*, jos ensimmäinen voidaan saada toisesta seuraavan tyyppisten toimintojen yhdistelmällä:

(A) koodin positioiden permutaatio;
(B) kiinnitetyssä positiossa olevien alkioiden kertominen nollasta eroavalla skalaarilla.

LAUSE 4.7. *Kaksi $k \times n$ -matriisia virittää ekvivalentit lineaariset $[n, k]$-koodit kunnassa $\mathbb{F}_q$, jos toinen matriisi voidaan muodostaa toisesta sarjana seuraavan tyyppisiä toimintoja:*
(R1) *Rivien permutaatio.*
(R2) *Rivin kertominen nollasta eroavalla skalaarilla.*
(R3) *Skalaarilla kerrotun rivin lisääminen toiseen riviin.*
(C1) *Sarakkeiden permutaatio.*
(C2) *Sarakkeen kertominen nollasta eroavalla skalaarilla.*

TODISTUS ([**2**, s. 50]). Rivioperaatiot (R1), (R2) ja (R3) säilyttävät virittäjämatriisin rivien lineaarisen riippumattomuuden ja yksinkertaisesti korvaavat saman koodin yhden kannan toisella. Sarakeoperaatiot (C1) ja (C2) muuntavat virittäjämatriisin ekvivalentin koodin virittäjämatriisiksi. □

LAUSE 4.8. *Olkoon G $[n, k]$-koodin virittäjämatriisi. Tällöin suorittamalla toiminnot* (R1), (R2), (R3), (C1) *ja* (C2) *voidaan G muuntaa* standardimuotoon

$$\left[I_k \mid A \right],$$

missä I_k on $k \times k$ -yksikkömatriisi ja A on $k \times (n-k)$ -matriisi.

TODISTUS ([**2**, s. 51]). Matriisin G muunnosoperaatioiden sarjan aikana merkintä g_{ij} tarkoittaa *kulloinkin* käsiteltävän matriisin (i, j). alkiota ja merkintä $\mathbf{r}_1, \mathbf{r}_2, \ldots, \mathbf{r}_k$ matriisin rivejä ja $\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_k$ matriisin sarakkeita.

Kullekin $j = 1, 2, \ldots, k$ suoritetaan vuorollaan seuraava kolmen askeleen menetelmä. Kukin j muuttaa sarakkeen $\mathbf{c}_j$ haluttuun muotoon, missä positiossa j on alkio 1 ja 0 muualla. Näin ensimmäiset $j-1$ saraketta, jotka on jo transformoitu sopivasti, jäävät ennalleen. Oletetaan, että G on transformoitu muotoon

$$\begin{bmatrix} 1 & 0 & \cdots & 0 & g_{1j} & \cdots & g_{1n} \\ 0 & 1 & \cdots & 0 & g_{2j} & \cdots & g_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 & g_{j-1,j} & \cdots & g_{j-1,n} \\ 0 & 0 & \cdots & 0 & g_{jj} & \cdots & g_{jn} \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 & g_{kj} & \cdots & g_{kn} \end{bmatrix}.$$

Askel 1 Jos $g_{jj} \neq 0$, siirrytään kohtaan Askel 2. Jos $g_{jj} = 0$ ja jos jollekin $i > j$, $g_{ij} \neq 0$, niin vaihdetaan rivit $\mathbf{r}_j$ ja $\mathbf{r}_i$ keskenään. Jos $g_{jj} = 0$ ja $g_{ij} = 0$ kaikilla $i > j$, niin valitaan h siten, että $g_{jh} \neq 0$ ja vaihdetaan sarakkeet $\mathbf{c}_j$ ja $\mathbf{c}_h$ keskenään.
Askel 2 Nyt $g_{jj} \neq 0$. Kerrotaan riviä $\mathbf{r}_j$ käänteisalkiolla g_{jj}^{-1}.
Askel 3 Nyt $g_{jj} = 1$. Kun $i \neq j$, kullekin $i = 1, 2, \ldots, k$: vaihdetaan $\mathbf{r}_i$ paikalle $\mathbf{r}_i - g_{ij}\mathbf{r}_j$.

Sarake $\mathbf{c}_j$ on nyt halutussa muodossa.

Virittäjämatriisi on standardimuodossa, kun tämä toimenpide on tehty kaikille $j = 1, 2, \ldots, k$. □

HUOMAUTUS 4.9 ([**2**, s. 51–52]). (1) Jos G voidaan transformoida pelkästään rivioperaatioilla (tämä on mahdollista jos ja vain jos G:n ensimmäiset k saraketta ovat lineaarisesti riippumattomat) matriisin standardimuotoon G', niin G' virittää *saman* koodin, jonka G virittää. Mutta, jos käytetään myös operaatioita (C1) ja (C2), niin G' virittää ekvivalentin koodin, mutta se ei välttämättä ole sama kuin virittäjämatriisin G virittämä. Edellisessä todistuksessa kuvailtu menetelmä on suunniteltu antamaan standardimuotoisen virittäjämatriisin samalle koodille aina kun se on mahdollista.
(2) Esimerkistä 4.12 tullaan huomaamaan, että käytännössä virittäjämatriisin G tutkiminen paljastaa nopeamman tavan transformoida se standardimuotoon.
(3) Virittäjämatriisin standardimuoto $\left[I_k \mid A\right]$ ei ole yksikäsitteinen. Esimerkiksi matriisin A rivien permutointi antaa virittäjämatriisin ekvivalentille koodille.

ESIMERKKI 4.10 ([**2**, s. 52]). Esimerkin 4.6 (i)-kohdan virittäjämatriisille saadaan standardimuoto vaihtamalla rivit keskenään:

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

ESIMERKKI 4.11 ([**2**, s. 49, 52]). Käytetään Lauseen 4.8 menetelmää ja transformoidaan $[7, 4, 3]$-koodin virittäjämatriisi standardimuotoon.

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \xrightarrow[\substack{\mathbf{r}_2 \to \mathbf{r}_2 - \mathbf{r}_1 \\ \mathbf{r}_3 \to \mathbf{r}_3 - \mathbf{r}_1}]{} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$\xrightarrow[\substack{\mathbf{r}_1 \to \mathbf{r}_1 - \mathbf{r}_2 \\ \mathbf{r}_4 \to \mathbf{r}_4 - \mathbf{r}_2}]{} \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

$$\xrightarrow[\mathbf{r}_2 \to \mathbf{r}_2 - \mathbf{r}_3]{} \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

$$\xrightarrow[\mathbf{r}_3 \to \mathbf{r}_3 - \mathbf{r}_4]{} \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

ESIMERKKI 4.12 ([**2**, s. 52–53]). Tarkastellaan $[6, 3]$-koodin virittäjämatriisia kunnassa $\mathbb{F}_3$:

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

Selvästi sarakkeiden permutaatio $\mathbf{c}_1 \leftrightarrow \mathbf{c}_4$, $\mathbf{c}_4 \leftrightarrow \mathbf{c}_3$ antaa ekvivalentille koodille virittäjämatriisin standardimuodon

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

4.2. Lineaarisen koodin konstruointi

Olkoon C $[n,k]$-koodi kunnassa $\mathbb{F}_q$ ja jonka virittäjämatriisi on G. Koodi C sisältää q^k koodisanaa, joten sitä voidaan käyttää kommunikointiin millä tahansa q^k eri viestillä. Identifioidaan nämä viestit q^k k-jonolla joukosta $\mathbb{F}_q^k$ ja *koodataan* viestivektori $\mathbf{u} = u_1u_2\cdots u_k$ kertomalla sitä matriisilla G oikealta. Jos matriisin G rivit ovat $\mathbf{r}_1, \mathbf{r}_2, \cdots, \mathbf{r}_k$, niin

$$\mathbf{u}G = \sum_{i=1}^{k} u_i\mathbf{r}_i$$

ja näin $\mathbf{u}G$ todella on koodin C koodisana, sillä se on virittäjämatriisin rivien lineaarikombinaatio. On hyvä huomata, että koodaava funktio $\mathbf{u} \mapsto \mathbf{u}G$ kuvaa vektoriavaruuden $\mathbb{F}_q^k$ k-dimensioiseksi aliavaruudeksi (koodiksi C) joukossa $\mathbb{F}_q^n$.

Tämä koodaussääntö on yksinkertaisempi, jos G on standardimuodossa. Oletetaan $G = [I_k \mid A]$, missä $A = [a_{ij}]$ on $k \times (n-k)$ -matriisi. Tällöin viestivektori $\mathbf{u}$ koodaantuu

$$\mathbf{x} = \mathbf{u}G = x_1x_2\cdots x_kx_{k+1}\cdots x_n,$$

missä $x_i = u_i$, $1 \le i \le k$, ovat *viestimerkkejä* ja

$$x_{k+i} = \sum_{j=1}^{k} a_{ji}u_j, \qquad 1 \le i \le n-k$$

ovat *tarkistusmerkkejä*. Tarkistusmerkit edustavat redundanssia, joka on lisätty suojelemaan viestiä kohinalta.

Esimerkki 4.13 ([**2**, s. 55–56]). Olkoon C binäärinen $[7,4]$-koodi, jonka standardimuotoinen virittäjämatriisi on

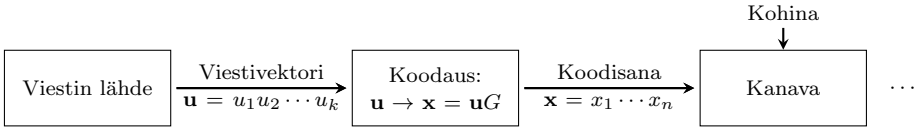
$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

Viestivektori (u_1, u_2, u_3, u_4) koodataan seuraavasti

$$(u_1, u_2, u_3, u_4, u_1+u_2+u_3, u_2+u_3+u_4, u_1+u_2+u_4).$$

Esimerkiksi,

$$\begin{array}{lll} 0\,0\,0\,0 & \text{koodataan} & 0\,0\,0\,0\,0\,0\,0, \\ 1\,0\,0\,0 & \text{koodataan} & 1\,0\,0\,0\,1\,0\,1, \\ 1\,1\,1\,0 & \text{koodataan} & 1\,1\,1\,0\,1\,0\,0. \end{array}$$



KUVA 4.1. Lineaarisen koodin viestisanan koodauksen vaiheet.

Yleisen lineaarisen koodin osalta tiivistetään viestintäjärjestelmän koodaava osa Kuvalla 4.1.

4.3. Lineaarisen koodin dekoodaus

Olkoon koodisana $\mathbf{x} = x_1x_2\cdots x_n$ lähetetty kanavan läpi ja vastaanotettu vektori on $\mathbf{y} = y_1y_2\cdots y_n$. Määritellään *virhevektori* $\mathbf{e}$,

$$\mathbf{e} = \mathbf{y} - \mathbf{x} = e_1e_2\cdots e_n.$$

Dekoodaajan tulee ratkaista vastaanotetusta vektorista $\mathbf{y}$, mikä koodisana $\mathbf{x}$ lähetettiin tai yhtäpitävästi mikä virhevektori $\mathbf{e}$ ilmaantui.

MÄÄRITELMÄ 4.14. Olkoon C $[n,k]$-koodi kunnassa $\mathbb{F}_q$ ja $\mathbf{a}$ mikä tahansa vektori joukosta $\mathbb{F}_q^n$. Määritellään joukko $\mathbf{a}+C$,

$$\mathbf{a}+C = \{\mathbf{a}+\mathbf{x} \mid \mathbf{x} \in C\}$$

on nimeltään koodin C *sivuluokka*.

LEMMA 4.15. *Olkoon $\mathbf{a}+C$ koodin C sivuluokka ja $\mathbf{b} \in \mathbf{a}+C$. Tällöin*

$$\mathbf{b}+C = \mathbf{a}+C.$$

TODISTUS ([**2**, s. 57]). Koska $\mathbf{b} \in \mathbf{a}+C$ niin $\mathbf{b} = \mathbf{a}+\mathbf{x}$ jollain $\mathbf{x} \in C$. Nyt, jos $\mathbf{b}+\mathbf{y} \in \mathbf{b}+C$ niin

$$\mathbf{b}+\mathbf{y} = (\mathbf{a}+\mathbf{x})+\mathbf{y} = \mathbf{a}+(\mathbf{x}+\mathbf{y}) \in \mathbf{a}+C.$$

Näin ollen $\mathbf{b}+C \subseteq \mathbf{a}+C$. Toisaalta, jos $\mathbf{a}+\mathbf{z} \in \mathbf{a}+C$, niin

$$\mathbf{a}+\mathbf{z} = (\mathbf{b}-\mathbf{x})+\mathbf{z} = \mathbf{b}+(\mathbf{z}-\mathbf{x}) \in \mathbf{b}+C.$$

Näin ollen $\mathbf{a}+C \subseteq \mathbf{b}+C$ ja tällöin $\mathbf{b}+C = \mathbf{a}+C$. □

LAUSE 4.16 (Lagrange). *Olkoon C $[n,k]$-koodi kunnassa $\mathbb{F}_q$. Tällöin*

(i) *jokainen joukon $\mathbb{F}_q^n$ vektori on jossain koodin C sivuluokassa,*
(ii) *jokainen sivuluokka sisältää täsmälleen q^k vektoria,*
(iii) *kaksi sivuluokkaa ovat joko erilliset tai samat.*

TODISTUS ([**2**, s. 57]).

(i) Jos $\mathbf{a} \in \mathbb{F}_q^n$, niin $\mathbf{a} = \mathbf{a}+\mathbf{0} \in \mathbf{a}+C$.
(ii) Kuvaus $C \mapsto \mathbf{a}+C$,

$$\mathbf{x} \mapsto \mathbf{a}+\mathbf{x}$$

on helppo osoittaa bijektioksi. Näin ollen $|\mathbf{a}+C| = |C| = q^k$.

(iii) Oletetaan, että sivuluokat $\mathbf{a}+C$ ja $\mathbf{b}+C$ leikkaavat. Tällöin jollekin vektorille $\mathbf{v}$ pätee $\mathbf{v} \in (\mathbf{a}+C) \cap (\mathbf{b}+C)$. Siispä jollekin $\mathbf{x}$, $\mathbf{y} \in C$,

$$\mathbf{v} = \mathbf{a}+\mathbf{x} = \mathbf{b}+\mathbf{y}.$$

Näin ollen $\mathbf{b} = \mathbf{a}+(\mathbf{x}-\mathbf{y}) \in \mathbf{a}+C$, jolloin Lemman 4.15 mukaan $\mathbf{b}+C = \mathbf{a}+C$. □

ESIMERKKI 4.17 ([**2**, s. 57–58]). Olkoon C binäärinen $[4,2]$-koodi ja jonka virittäjämatriisi on

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

Toisin sanoen $C = \{0000, 1011, 0101, 1110\}$.

Tällöin koodin C sivuluokat ovat

$$\begin{aligned} 0000 + C &= C \text{ itse}, \\ 1000 + C &= \{1000, 0011, 1101, 0110\}, \\ 0100 + C &= \{0100, 1111, 0001, 1010\}, \\ 0010 + C &= \{0010, 1001, 0111, 1100\}. \end{aligned}$$

Huomataan, että sivuluokka $0001+C$ on $\{0001, 1010, 0100, 1111\}$, joka on sama kuin sivuluokka $0100+C$. Tämän olisi voinut ennustaa Lemmasta 4.15, sillä $0001 \in 0100+C$. Vastaavasti täytyy olla esimerkiksi $0111 + C = 0010 + C$.

MÄÄRITELMÄ 4.18. Sivuluokan minimipainoisin vektori on nimeltään *sivuluokan johtaja*.

Jos minimipainoisia vektoreita on useita, niin valitaan näistä yksi satunnaisesti sivuluokan johtajaksi. Esimerkissä 4.17 on 0001 vaihtoehtoinen sivuluokan johtaja sivuluokalle $0100 + C$.

Lauseen 4.16 mukaan joukko $\mathbb{F}_q^n$ on jaettu koodin C erillisiin sivuluokkiin:

$$\mathbb{F}_q^n = (\mathbf{0}+C) \cup (\mathbf{a}_1+C) \cup \cdots \cup (\mathbf{a}_s+C),$$

missä $s = q^{n-k}-1$ ja Lemman 4.15 mukaan voidaan valita $\mathbf{0}, \mathbf{a}_1, \ldots, \mathbf{a}_s$ sivuluokan johtajiksi.

Standarditaulukko [**2**, s. 58] (tai Slepianin taulukko) $[n,k]$-koodille C on $q^{n-k} \times q^k$ taulukko kaikista joukon $\mathbb{F}_q^n$ vektoreista. Taulukossa ensimmäinen rivi on koodi C itse, koodisanan $\mathbf{0}$ ollessa vasemmalla ja muut rivit ovat sivuluokkia $\mathbf{a}_i+C$, sivuluokan johtajan ollessa vasemmaisin. Standarditaulukko rakennetaan seuraavasti:

Askel 1 Listataan koodi C ensimmäiselle riville aloittaen koodisanasta $\mathbf{0}$.

Askel 2 Valitaan mikä tahansa minimipainoinen vektori $\mathbf{a}_1$, joka ei ole ensimmäisellä rivillä. Listataan sivuluokka $\mathbf{a}_1+C$ toiselle riville ja asetetaan $\mathbf{a}_1$ koodisanan $\mathbf{0}$ alle ja $\mathbf{a}_1+\mathbf{x}$ jokaisen $\mathbf{x} \in C$ alle.

Askel 3 Niistä vektoreista, jotka eivät ole kahdella ensimmäisellä rivillä valitaan minimipainoisin $\mathbf{a}_2$ ja listataan sivuluokka $\mathbf{a}_2+C$ kuten Askeleessa 2 ja saadaan kolmas rivi.

Askel 4 Näin jatketaan kunnes kaikki sivuluokat on listattu ja jokainen joukon $\mathbb{F}_q^n$ vektori esiintyy täsmälleen kerran.

Esimerkki 4.19 ([**2**, s. 59]). Standarditaulukko Esimerkin 4.17 koodille on

$$\begin{array}{lcccc} \text{Koodisanat} & \to & 0000 & 1011 & 0101 & 1110 \\ & & 1000 & 0011 & 1101 & 0110 \\ & & 0100 & 1111 & 0001 & 1010 \\ & & 0010 & 1001 & 0111 & 1100 \\ & & \uparrow & & & \\ & & \text{Sivuluokan johtajat} & & & \end{array}$$

Kun vastaanotetaan vektori $\mathbf{y}$ (vaikka 1111 Esimerkissä 4.19), sen paikka löydetään taulukosta. Tämän jälkeen dekoodaaja päättää, että virhevektori $\mathbf{e}$ on sivuluokan johtaja (0100), jolloin $\mathbf{y}$ dekoodataan koodisanaksi $\mathbf{x} = \mathbf{y} - \mathbf{e} = 1011$, joka on ylimmäinen siinä sarakkeessa, joka sisältää vektorin $\mathbf{y}$.

Lyhesti sanottuna, standarditaulukossa oleva vastaanotettu vektori dekoodataan saman sarakkeen ylimmäiseksi koodisanaksi.

Virhevektorit, jotka korjataan ovat täsmälleen sivuluokan johtajia riippumatta siitä mikä koodisana on lähetetty. Valitsemalla minimipainoisen vektorin jokaisesta sivuluokasta sivuluokan johtajaksi takaa sen, että standarditaulukon avulla dekoodattu sana on tapahtunut lähimmän naapurin -periaatteella.

Esimerkin 4.19 taulukossa yksi virhe korjaantuu, jos se esiintyy missä tahansa ensimmäisessä kolmessa positiossa. Esimerkiksi tapauksessa (a) alla virhe korjaantuu. Mutta jos virhe esiintyy neljännessä positiossa, niin se ei korjaannu eli tapaus (b) alla.

	Viesti		Koodi-sana		Kanava + kohina		Vastaan-otettu vektori		Dekoodattu sana		Vastaan-otettu viesti
(a)	01	$\to$	0101	$\to$	0101	$\to$	0001	$\to$	0101	$\to$	01
(b)	01	$\to$	0101	$\to$	0101	$\to$	0100	$\to$	0000	$\to$	00

On hyvä huomata, että käytännössä edellä esitetty dekoodausjärjestelmä on liian hidas suurille koodeille ja myös liian kallis tilavaatimusten kannalta. Kehittyneempi tapa suorittaa standarditaulukon mukainen dekoodaus tunnetaan nimellä ”syndroomadekoodaus”, johon tutustutaan Kappaleessa 4.6.

4.4. Koodin duaali

Kahden vektorin $\mathbf{u} = u_1u_2\cdots u_n$ ja $\mathbf{v} = v_1v_2\cdots v_n$ *pistetulo* $\mathbf{u}\cdot\mathbf{v}$ joukossa $\mathbb{F}_q^n$ on skalaari

$$\mathbf{u}\cdot\mathbf{v} = u_1v_1 + u_2v_2 + \cdots + u_nv_n.$$

Esimerkiksi joukossa $\mathbb{F}_2^4$, $(1001)\cdot(1101) = 0$,
$(1111)\cdot(1110) = 1$
ja joukossa $\mathbb{F}_3^4$, $(2011)\cdot(1210) = 0$,
$(1212)\cdot(2121) = 2$.

Jos $\mathbf{u}\cdot\mathbf{v} = 0$, niin vektorit $\mathbf{u}$ ja $\mathbf{v}$ ovat *ortogonaaliset*.

LEMMA 4.20. *Jokaiselle* $\mathbf{u}$, $\mathbf{v}$ *ja* $\mathbf{w} \in \mathbb{F}_q^n$ *ja* $\lambda, \mu \in \mathbb{F}_q$ *on voimassa*
(i) $\mathbf{u} \cdot \mathbf{v} = \mathbf{v} \cdot \mathbf{u}$
(ii) $(\lambda\mathbf{u} + \mu\mathbf{v}) \cdot \mathbf{w} = \lambda(\mathbf{u} \cdot \mathbf{w}) + \mu(\mathbf{v} \cdot \mathbf{w})$.

TODISTUS. Todistus on suoraviivainen. Käytetään vaihdannaisuutta, liitännäisyyttä ja osittelulakia. □

Lineaarisen $[n, k]$-koodin C *duaali* $C^\perp$ on joukon $\mathbb{F}_q^n$ niiden vektorien joukko, jotka ovat ortogonaalisia jokaiselle koodin C koodisanalle eli

$$C^\perp = \{\mathbf{v} \in \mathbb{F}_q^n \mid \mathbf{v} \cdot \mathbf{u} = 0 \quad \text{kaikilla } \mathbf{u} \in C\}.$$

LEMMA 4.21. *Olkoon* C $[n, k]$*-koodi ja sen virittäjämatriisi* G*. Tällöin vektori* $\mathbf{v}$ *joukosta* $\mathbb{F}_q^n$ *kuuluu duaaliin* $C^\perp$ *jos ja vain jos* $\mathbf{v}$ *on ortogonaalinen jokaisen matriisin* G *rivin kanssa. Toisin sanoen* $\mathbf{v} \in C^\perp \Leftrightarrow \mathbf{v}G^T = 0$*, missä* G^T *on matriisin* G *transpoosi.*

TODISTUS ([**2**, s. 68]). "Vain jos" on selvä, sillä matriisin G rivit ovat koodisanoja. "Jos": Oletetaan, että matriisin G rivit ovat $\mathbf{r}_1, \mathbf{r}_2, \ldots, \mathbf{r}_k$ ja että $\mathbf{v} \cdot \mathbf{r}_i = 0$ jokaisella i. Jos $\mathbf{u}$ on mikä tahansa koodin C koodisana, niin tällöin $\mathbf{u} = \sum_{i=1}^k \lambda_i \mathbf{r}_i$ jollain skalaarilla λ_i ja siten

$$\begin{aligned}\mathbf{v} \cdot \mathbf{u} &= \sum_{i=1}^k \lambda_i(\mathbf{v} \cdot \mathbf{r}_i) \quad \text{(Lemman 4.20 (ii) mukaan.)} \\ &= \sum_{i=1}^k \lambda_i 0 = 0.\end{aligned}$$

Täten $\mathbf{v}$ on ortogonaalinen jokaisen koodin C koodisanan kanssa, jolloin se kuuluu joukkoon $C^\perp$. □

LAUSE 4.22. *Olkoon* C $[n, k]$*-koodi kunnassa* $\mathbb{F}_q$*. Tällöin duaalikoodi* $C^\perp$ *on lineaarinen* $[n, n-k]$*-koodi.*

TODISTUS. Todistus sivuutetaan; katso [**2**, s. 68]. □

ESIMERKKI 4.23 ([**2**, s. 69]). Voidaan helposti tarkistaa, että
(i) jos

$$C = \begin{cases} 0000 \\ 1100 \\ 0011 \\ 1111 \end{cases}, \text{niin } C^\perp = C.$$

(ii) jos

$$C = \begin{cases} 000 \\ 110 \\ 011 \\ 101 \end{cases}, \text{niin } C^\perp = \begin{cases} 000 \\ 111 \end{cases}.$$

LAUSE 4.24. *Mille tahansa* $[n, k]$*-koodille* C *pätee* $(C^\perp)^\perp = C$.

TODISTUS ([**2**, s. 69]). Selvästi $C \subseteq (C^\perp)^\perp$, sillä jokainen koodin C vektori on ortogonaalinen jokaisen joukon $C^\perp$ vektorin kanssa. Mutta $\dim((C^\perp)^\perp) = n-(n-k) = k = \dim C$, joten $C = (C^\perp)^\perp$. □

4.5. Pariteetintarkistusmatriisi

MÄÄRITELMÄ 4.25. Olkoon C $[n,k]$-koodi. Koodin C *pariteetintarkistusmatriisi* H on duaalin $C^\perp$ virittäjämatriisi.

Matriisi H on siis $(n-k)\times n$ -matriisi, jolle pätee $GH^T = \mathbf{0}$, missä H^T on matriisin H transpoosi ja $\mathbf{0}$ on kaikkialla nollaa oleva matriisi. Lemman 4.21 ja Lauseen 4.24 perusteella, jos H on koodin C pariteetintarkistusmatriisi, tällöin

$$C = \{\mathbf{x} \in \mathbb{F}_q^n \mid \mathbf{x}H^T = \mathbf{0}\}.$$

Pariteetintarkistusmatriisin rivit ovat koodisanojen *pariteettitarkistuksia*. Niiden mukaan jokaisen koodisanan koordinaattien tietyt lineaariset yhdistelmät ovat nollia. Pariteetintarkistusmatriisi määrää koodin täysin. Esimerkiksi, jos

$$H = \begin{bmatrix} 1100 \\ 0011 \end{bmatrix},$$

niin koodi C on

$$\{(x_1, x_2, x_3, x_4) \in \mathbb{F}_2^4 \mid x_1 + x_2 = 0,\ x_3 + x_4 = 0\}.$$

Yhtälöt $x_1 + x_2 = 0$, ja $x_3 + x_4 = 0$ ovat nimeltään *pariteetintarkistusyhtälöitä*.

Jos $H = \begin{bmatrix} 111 \end{bmatrix}$, niin koodi C koostuu joukon $\mathbb{F}_2^3$ niistä vektoreista, joiden koordinaattien summa on nolla (modulo 2). Yleisemmin, parillisen painon omaava koodi E_n voidaan määritellä olevan kaikki joukon $\mathbb{F}_2^n$ ne vektorit $x_1x_2\cdots x_n$, joille pätee yksi ainoa pariteetintarkistusyhtälö

$$x_1 + x_2 + \cdots + x_n = 0.$$

LAUSE 4.26. *Jos $G = \begin{bmatrix} I_k \mid A \end{bmatrix}$ on $[n,k]$-koodin C standardimuotoinen virittäjämatriisi, niin tällöin koodin C pariteetintarkistusmatriisi on $H = \begin{bmatrix} -A^T \mid I_{n-k} \end{bmatrix}$.*

TODISTUS ([**2**, s. 70–71]). Olkoon

$$G = \left[\begin{array}{ccc|ccc} 1 & & 0 & a_{11} & \cdots & a_{1,n-k} \\ & \ddots & & \vdots & & \vdots \\ 0 & & 1 & a_{k1} & \cdots & a_{k,n-k} \end{array}\right].$$

Olkoon

$$H = \left[\begin{array}{ccc|ccc} -a_{11} & \cdots & -a_{k1} & 1 & & 0 \\ \vdots & & \vdots & & \ddots & \\ -a_{1,n-k} & \cdots & -a_{k,n-k} & 0 & & 1 \end{array}\right].$$

Nyt matriisilla H on pariteetintarkistusmatriisilta vaadittava koko ja sen rivit ovat lineaarisesti riippumattomat. Täten riittää osoittaa, että jokainen matriisin H rivi on ortogonaalinen matriisin G jokaisen rivin kanssa. Sisätulo matriisin G rivin i ja matriisin H sarakkeen j suhteen on

$$0 + \cdots + 0 + (-a_{ij}) + 0 + \cdots + 0 + a_{ij} + 0 + \cdots + 0 = 0.$$

□

Lause 4.26 antaa helpon tavan konstruoida lineaarisen koodin pariteetintarkistusmatriisin annetusta virittäjämatriisista ja päinvastoin.

ESIMERKKI 4.27 ([**2**, s. 71]). Esimerkin 4.11 koodilla on standardimuotoinen virittäjämatriisi

$$G = \left[\begin{array}{c|c} & 101 \\ I_4 & 111 \\ & 110 \\ & 011 \end{array}\right].$$

Tällöin sen pariteetintarkistusmatriisi on

$$H = \left[\begin{array}{c|c} 1110 & \\ 0111 & I_3 \\ 1101 & \end{array}\right].$$

On hyvä muistaa, että miinusmerkit ovat turhia binäärikoodin tapauksessa!

MÄÄRITELMÄ 4.28. Pariteetintarkistusmatriisi H on *standardimuodossa*, jos $H = \left[B \mid I_{I_n-k}\right]$.

Lauseen 4.26 todistus osoittaa, että jos koodi määritellään pariteetintarkistusmatriisin standardimuodossa $H = \left[B \mid I_{n-k}\right]$, niin koodin virittäjämatriisi on $G = \left[I_k \mid -B^T\right]$. Mikäli koodin pariteetintarkistusmatriisi H ei ole annettu standardimuodossa, tällöin H voidaan pelkistää standardimuotoon samalla tapaa kuin virittäjämatriisikin.

4.6. Syndroomadekoodaus

Olkoon $[n, k]$-koodin C pariteetintarkistusmariisi H. Tällöin vektorin $\mathbf{y} \in \mathbb{F}_q^n$ *syndrooma* $S(\mathbf{y})$ on $1 \times (n-k)$ -rivivektori

$$S(\mathbf{y}) = \mathbf{y}H^T.$$

HUOMAUTUS 4.29 ([**2**, s. 72]). (i) Jos matriisin H rivit ovat $\mathbf{h}_1, \mathbf{h}_2, \ldots, \mathbf{h}_{n-k}$, niin $S(\mathbf{y}) = (\mathbf{y} \cdot \mathbf{h}_1, \mathbf{y} \cdot \mathbf{h}_2, \ldots, \mathbf{y} \cdot \mathbf{h}_{n-k})$.
(ii) $S(\mathbf{y}) = 0 \Leftrightarrow \mathbf{y} \in C$.

LEMMA 4.30. *Kaksi vektoria* $\mathbf{u}$ *ja* $\mathbf{v}$ *ovat koodin* C *samassa sivuluokassa jos ja vain jos niillä on sama syndrooma.*

TODISTUS ([**2**, s. 72]). Vektorit $\mathbf{u}$ ja $\mathbf{v}$ ovat samassa sivuluokassa

$$\begin{aligned} &\Leftrightarrow \mathbf{u} + C = \mathbf{v} + C \\ &\Leftrightarrow \mathbf{u} - \mathbf{v} \in C \\ &\Leftrightarrow (\mathbf{u} - \mathbf{v})H^T = \mathbf{0} \\ &\Leftrightarrow \mathbf{u}H^T = \mathbf{v}H^T \\ &\Leftrightarrow S(\mathbf{u}) = S(\mathbf{v}). \end{aligned}$$

□

SEURAUS 4.31. *Sivuluokkien ja syndroomien välinen kuvaus on injektiivinen.*

ESIMERKKI 4.32 ([**2**, s. 72–74]). Esimerkissä 4.17,

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

jolloin Lauseen 4.26 mukaan pariteetintarkistusmatriisi on

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

Näin ollen sivuluokkien johtajien syndroomat ovat (katso Esimerkki 4.19):

$$S(0000) = 00$$
$$S(1000) = 11$$
$$S(0100) = 01$$
$$S(0010) = 10.$$

Standarditaulukoksi saadaan:

Sivuluokan johtajat				Syndroomat
0 0 0 0	1 0 1 1	0 1 0 1	1 1 1 0	0 0
1 0 0 0	0 0 1 1	1 1 0 1	0 1 1 0	1 1
0 1 0 0	1 1 1 1	0 0 0 1	1 0 1 0	0 1
0 0 1 0	1 0 0 1	0 1 1 1	1 1 0 0	1 0

Dekoodausalgoritmi menee seuraavalla tavalla: kun vektori $\mathbf{y}$ on vastaanotettu, lasketaan $S(\mathbf{y}) = \mathbf{y}H^T$ ja paikannetaan $S(\mathbf{y})$ taulukosta "Syndroomat"-sarakkeesta. Paikannetaan $\mathbf{y}$ vastaavalla rivillä ja dekoodataan siksi koodisanaksi, joka on vektorin $\mathbf{y}$ sisältämän sarakkeen ylimmäisin sana.

Tietokoneohjelmoinnissa, jossa dekoodauksen apuna käytetään standarditaulukkoa, tarvitsee varata muistia ainoastaan kahdelle sarakkeelle. Tällaista taulukkoa kutsutaan nimellä *syndroomahakutaulukko*. Tämän esimerkin syndroomahakutaulukko on seuraavanlainen:

Syndrooma $\mathbf{z}$	Sivuluokan johtaja $f(\mathbf{z})$
0 0	0 0 0 0
1 1	1 0 0 0
0 1	0 1 0 0
1 0	0 0 1 0

Dekoodaus suoritetaan noudattamalla seuraavia askeleita:

Askel 1 Lasketaan syndrooma $S(\mathbf{y}) = \mathbf{y}H^T$ vastaanotetulle vektorille $\mathbf{y}$.

Askel 2 Olkoon $\mathbf{z} = S(\mathbf{y})$ ja paikannetaan $\mathbf{z}$ ensimmäisestä sarakkeesta syndroomahakutaulukosta.

Askel 3 Dekoodataan $\mathbf{y}$ olemaan $\mathbf{y} - f(\mathbf{y})$.

Esimerkiksi, jos vastaanotetaan vektori $\mathbf{y} = 1111$, niin $S(\mathbf{y}) = 01$ ja dekoodataan $1111 - 0100 = 1011$.

LUKU 5

Sykliset koodit

Sykliset koodit ovat tärkeä osa koodausteoriaa monesta syystä. Teoreettisesti ne edustavat rikasta algebrallista struktuuria, joten ne ovat tehokkaasti implementoitavissa olemassa oleviin systeemeihin. Monet tärkeät koodit, kuten binääriset Hammingin koodit tai BCH-koodit voidaan muodostaa niin, että ne ovat ekvivalentteja syklisille koodeille. Tämän luvun pohjana on käytetty kirjaa Robert McEliece: The Theory of Information and Coding (2002) [**6**].

MÄÄRITELMÄ 5.1. Lineaarinen $[n, k]$-koodi kunnan F suhteen on syklinen, jos jokaisen koodisanan $\mathbf{C} = (C_0, C_1, \ldots, C_{n-1})$ syklinen siirto oikealle eli $\mathbf{C}^R = (C_{n-1}, C_0, \ldots, C_{n-2})$ on myös koodisana.

ESIMERKKI 5.2 ([**2**, s. 141]). (i) Binäärinen koodi $\{000, 101, 011, 110\}$ on syklinen.

(ii) Binäärinen lineaarinen koodi $\{0000, 1001, 0110, 1111\}$ ei ole syklinen, mutta se on ekvivalentti syklisen koodin $\{0000, 1010, 0101, 1111\}$ kanssa.

ESIMERKKI 5.3 ([**6**, s. 168]). Olkoon F on mikä tahansa kunta ja $n \geq 3$ kokonaisluku. Tällöin kunnassa F on olemassa vähintään neljä n-pituista syklistä koodia, niin sanotut triviaaliset sykliset koodit:

- Nollakoodi $[n, 0]$.
- Toistokoodi $[n, 1]$, sisältäen kaikki koodisanat, jotka ovat muotoa $(a, a, \ldots, a)$, missä $a \in F$.
- Yhden pariteetin tarkistuskoodi $[n, n-1]$, joka sisältää kaikki vektorit $(C_0, C_1, \ldots, C_{n-1})$ siten, että $\sum_i C_i = 0$.
- Ei-pariteetti-koodi $[n, n]$, joka sisältää kaikki n-pituiset vektorit.

ESIMERKKI 5.4 ([**6**, s. 168–169]). Tarkastellaan kunnan $\mathbb{F}_2$ lineaarista $[7, 3]$-koodia, joka määritellään virittäjämatriisin G avulla

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

Tässä koodissa on kahdeksan koodisanaa. Merkitään $\mathbf{C}_0 = 0000000$ ja matriisin G rivejä $\mathbf{C}_1, \mathbf{C}_2$ ja $\mathbf{C}_3$, jolloin koodisanat ovat:

$$\begin{aligned} \mathbf{C}_0 &= 0000000, & \mathbf{C}_4 &= \mathbf{C}_1 + \mathbf{C}_2 = 1110010, \\ \mathbf{C}_1 &= 1011100, & \mathbf{C}_5 &= \mathbf{C}_1 + \mathbf{C}_3 = 1001011, \\ \mathbf{C}_2 &= 0101110, & \mathbf{C}_6 &= \mathbf{C}_2 + \mathbf{C}_3 = 0111001, \\ \mathbf{C}_3 &= 0010111, & \mathbf{C}_7 &= \mathbf{C}_1 + \mathbf{C}_2 + \mathbf{C}_3 = 1100101. \end{aligned}$$

Tämä koodi on syklinen. Tarkistetaan se käymällä läpi jokaisen koodisanan syklinen siirto oikealle. Esimerkiksi koodisanan $\mathbf{C}_1$ syklinen siirto oikealle on koodisana $\mathbf{C}_2$, merkitään tätä $\mathbf{C}_1 \to \mathbf{C}_2$. Kaikkien koodisanojen siirrot:

$$\begin{aligned} &\mathbf{C}_0 \to \mathbf{C}_0, && \mathbf{C}_4 \to \mathbf{C}_6,\\ &\mathbf{C}_1 \to \mathbf{C}_2, && \mathbf{C}_5 \to \mathbf{C}_7,\\ &\mathbf{C}_2 \to \mathbf{C}_3, && \mathbf{C}_6 \to \mathbf{C}_1,\\ &\mathbf{C}_3 \to \mathbf{C}_5, && \mathbf{C}_7 \to \mathbf{C}_4. \end{aligned}$$

Jos $\mathbf{C} = (C_0, C_1, \ldots, C_{n-1})$ on koodisana, niin sitä vastaava polynomi on

$$C(x) = C_0 + C_1 x + \cdots + C_{n-1}x^{n-1}.$$

Polynomien avulla saadaan yksinkertainen algebrallinen karakterisointi koodisanan syklisestä siirrosta oikealle. Tätä karakterisointia varten tarvitsee määritellä tärkeät "mod"- ja "rem"-operaattorit kokonaisluvuille ja polynomeille, mikä on tehty yksityiskohtaisemmin Luvussa 3.

Jos p ja m ovat kokonaislukuja ja $m > 0$, niin merkintä "$p \operatorname{rem} m$" on jakojäännös, joka saadaan kun p jaetaan luvulla m. Täten $p \operatorname{rem} m$ on kokonaisluku r siten, että m jakaa luvun $p - r$ ja $0 \le r \le m - 1$. Vastaavasti, jos $P(x)$ ja $Q(x)$ ovat polynomeja, niin merkintä "$P(x) \operatorname{rem} M(x)$" on jakojäännös, kun $M(x)$ jakaa $P(x)$. Tällöin $P(x) \operatorname{rem} M(x)$ on yksikäsitteinen polynomi $R(x)$ siten, että $M(x)$ jakaa polynomin $P(x) - R(x)$ ja $\deg R(x) < \deg M(x)$.

LEMMA 5.5. *(a) Jos* $\deg P(x) < \deg M(x)$*, niin* $P(x) \operatorname{rem} M(x) = P(x)$.
(b) Jos $M(x) | P(x)$*, niin* $P(x) \operatorname{rem} M(x) = 0$.
(c) $(P(x) + Q(x)) \operatorname{rem} M(x) = P(x) \operatorname{rem} M(x) + Q(x) \operatorname{rem} M(x)$.
(d) $(P(x)Q(x) \operatorname{rem} M(x) = (P(x)(Q(x) \operatorname{rem} M(x))) \operatorname{rem} M(x)$.
(e) Jos $M(x) | N(x)$*, niin* $(P(x) \operatorname{rem} N(x)) \operatorname{rem} M(x) = P(x) \operatorname{rem} M(x)$.

TODISTUS. Jokaisen kohdan todistus on suoraan määritelmän avulla selvähkö ja sivuutetaan. □

LAUSE 5.6. *Koodisanaa* $\mathbf{C} = (C_0, C_1, \ldots, C_{n-1})$ *vastaava polynomi olkoon* $C(x) = C_0 + C_1 x + \cdots + C_{n-1}x^{n-1}$. *Tällöin syklistä siirtoa oikealle* $\mathbf{C}^R$ *vastaava polynomi* $C^R(x)$ *saadaan kaavasta*

$$C^R(x) \equiv xC(x) \bmod (x^n - 1).$$

TODISTUS ([**6**, s. 172]). Nyt

$$\begin{aligned} C(x) &= C_0 + C_1 x + \cdots + C_{n-1}x^{n-1} \quad \big| \cdot x\\ xC(x) &= C_0 x + \cdots + C_{n-2}x^{n-1} + C_{n-1}x^n,\\ C^R(x) &= C_{n-1} + C_0 x + \cdots + C_{n-2}x^{n-1}. \end{aligned}$$

Näin ollen $xC(x) - C^R(x) = C_{n-1}(x^n - 1)$. Koska $\deg C^R(x) < \deg(x^n - 1)$ ja $x^n - 1$ jakaa $xC(x) - C^R(x)$, niin tulos seuraa jakoyhtälöstä. □

Lauseen 5.6 mukaan, jos $C(x)$ on syklisen koodin koodisana, niin myös

$$xC(x) \operatorname{rem}(x^n - 1)$$

on koodisana. Toistamalla syklinen siirto oikealle huomataan, että

$$x^i C(x) \operatorname{rem}(x^n - 1)$$

on koodisana kaikilla $i \geq 0$.

Seuraava lause on yleistys tällä huomiolle. Otetaan käyttöön merkintä

$$[P(x)]_n \coloneqq P(x) \operatorname{rem}(x^n - 1).$$

On syytä pitää mielessä, että $x^n \equiv 1 \bmod (x^n - 1)$. Nyt voidaan supistaa mikä tahansa polynomi modulo $(x^n - 1)$ korvaamalla $x^n = 1$, $x^{n+1} = x$, $x^{n+2} = x^2$ ja niin edelleen. [**2**, s. 146]

LAUSE 5.7. *Jos C on syklinen $[n, k]$-koodi ja jos $C(x)$ on koodin C koodisana, niin jokaiselle polynomille $P(x)$ pätee, että $[P(x)C(x)]_n$ on myös koodin C koodisana.*

TODISTUS ([**6**, s. 172]). Olkoon $P(x) = \sum_{i=0}^{m} P_i x^i$. Tällöin Lemman 5.5 (c) nojalla

$$\begin{aligned}[P(x)C(x)]_n &= \left[\left(\sum_{i=0}^{m} P_i x^i\right) C(x)\right]_n \\ &= \sum_{i=0}^{m} P_i [x^i C(x)]_n.\end{aligned}$$

Mutta tätä lausetta edeltävän huomion mukaan $[x^i C(x)]_n$ on koodisana kaikilla i, jolloin lineaarisen koodin lineaarikombinaatio $\sum P_i [x^i C(x)]_n$ on myös koodisana. □

ESIMERKKI 5.8 ([**6**, s. 173]). Tarkastellaan Esimerkin 5.4 syklistä $[7, 3]$-koodia. Koodisana $\mathbf{C}_5 = 1001011$ on polynomina $1 + x^3 + x^5 + x^6$. Lauseen 5.7 mukaan tätä polynomia voidaan kertoa toisella polynomilla ja supistaa tulos modulo $x^7 - 1$, jolloin saatu polynomi on koodisana. Esimerkiksi:

$$\begin{aligned}[(1 + x)(1 + x^3 + x^5 + x^6)]_7 &= 1 + x^3 + x^5 + x^6 + x + x^4 + x^6 + \underset{=1}{x^7} \\ &= 2 + x + x^3 + x^4 + x^5 + 2x^6 \\ &= x + x^3 + x^4 + x^5 = \mathbf{C}_2, \\ [(1 + \underset{=x^{49+4}}{x^{53}} + \underset{=x^{98+2}}{x^{100}})(1 + x^3 + x^5 + x^6)]_7 &= [(1 + x^4 + x^2)(1 + x^3 + x^5 + x^6)]_7 \\ &= \cdots = 1 + x + x^4 + x^6 = \mathbf{C}_7, \\ [(1 + x^2 + x^3)(1 + x^3 + x^5 + x^6)]_7 &= \cdots = \mathbf{0} = \mathbf{C}_0.\end{aligned}$$

MÄÄRITELMÄ 5.9. Olkoon C syklinen koodi. Alinta astetta oleva koodin C nollasta eroava polynomi on nimeltään koodin C *virittäjäpolynomi* $g(x)$.

ESIMERKKI 5.10 ([**6**, s. 173]). Esimerkin 5.4 koodisana $\mathbf{C}_1 = 1011100$ polynomina on alinta astetta oleva nollasta eroava koodisana, jolloin tämän koodin virittäjäpolynomi on $g(x) = 1 + x^2 + x^3 + x^4$.

Seuraavan lemman ensimmäinen osa osoittaa, että syklisen koodin virittäjäpolynomi on aina yksikäsitteinen nollasta eroavaa vakiotekijää lukuunottamatta. Siksi onkin perusteltua viitata syklisen koodin virittäjäpolynomiin ja olettaa, että se on pääpolynomi.

LEMMA 5.11. *Olkoon C syklinen koodi, jonka virittäjäpolynomi on $g(x)$.*

(a) Jos $g'(x)$ on toinen virittäjäpolynomi, niin $g'(x) = \lambda g(x)$, jollain nollasta eroavalla alkiolla $\lambda \in F$.

(b) Jos $P(x)$ on polynomi siten, että $[P(x)]_n$ on koodisana, niin $g(x)$ jakaa polynomin $P(x)$.

TODISTUS ([**6**, s. 173–174]).

(a) Olkoot $g(x) = g_r x^r + \cdots + g_0$ ja $g'(x) = g'_r x^r + \cdots + g'_0$, missä $g_r \neq 0$ ja $g'_r \neq 0$. Tällöin, jos $\lambda = g'_r/g_r$, niin polynomin $g''(x) = g'(x) - \lambda g(x)$ aste on pienempi kuin r ja $g''(x)$ kuuluu koodiin C. Mutta r on alin mahdollinen aste nollasta eroavista koodisanoista koodissa C. Siispä $g''(x) = 0$ eli $g'(x) = \lambda g(x)$.

(b) Olkoon $Q(x)$ osamäärä ja $R(x)$ jakojäännös, kun $P(x)$ jaetaan polynomilla $g(x)$ eli

$$P(x) = Q(x)g(x) + R(x), \quad \text{missä } \deg R(x) < \deg g(x). \tag{5.1}$$

Kun supistetaan jokainen näistä polynomeista modulo $(x^n - 1)$ ja kun tiedetään, että $\deg R(x) < \deg g(x) \leq n - 1$ (jälkimmäinen on epäyhtälö, sillä $g(x)$ on koodisana), saadaan

$$R(x) = [P(x)]_n - [Q(x)g(x)]_n.$$

Mutta $[P(x)]_n$ on koodisana oletuksen nojalla ja Lauseen 5.7 mukaan $[Q(x)g(x)]_n$ on koodisana. Täten, koska C on lineaarinen, niin $R(x)$ on myös koodisana. Mutta $\deg R(x) < \deg g(x)$ ja $g(x)$ on alinta astetta oleva nollasta eroava koodisana, joten $R(x) = 0$ ja yhtälö (5.1) supistuu muotoon

$$P(x) = Q(x)g(x),$$

mikä osoittaa, että $g(x)$ jakaa polynomin $P(x)$.

□

Nyt voidaan todistaa syklisten koodien päälause. Polynomi $x^n - 1$ voidaan jakaa tekijöihin siten, että kukin tekijöistä on pääpolynomi. Tällöin saadaan injektio n-pituisten syklisten koodien joukolta polynomin $x^n - 1$ tekijöiden joukolle.

LAUSE 5.12. *(a) Olkoon C syklinen $[n, k]$-koodi kunnan F suhteen. Tällöin virittäjäpolynomi on polynomin $x^n - 1$ tekijä. Lisäksi vektori $\mathbf{C} = (C_0, C_1, \ldots, C_{n-1})$ on koodisana jos ja vain jos sitä vastaava polynomi $C(x) = C_0 + C_1 x + \cdots + C_{n-1}x^{n-1}$ on jaollinen polynomilla $g(x)$. Olkoon k koodin C dimensio. Tällöin $k = n - \deg g(x)$.*

(b) Kääntäen, jos $g(x)$ on polynomin $x^n - 1$ tekijä, niin tällöin on olemassa syklinen $[n, k]$-koodi, jonka virittäjäpolynomi on $g(x)$ ja $k = n - \deg g(x)$. Tämä koodi koostuu kaikista niistä vektoreista $(C_0, C_1, \ldots, C_{n-1})$, joita vastaavat polynomit ovat jaollisia polynomilla $g(x)$.

TODISTUS ([**6**, s. 174–175]).

(a) Olkoon $P(x) = x^n - 1$. Nyt $[P(x)]_n = 0$, joka on koodisana. Lemman 5.11 (b) mukaan polynomi $g(x)$ jakaa polynomin $x^n - 1$. Lauseen 5.7 mukaan mikä tahansa n-pituinen vektori, jota vastaava polynomi on polynomin $g(x)$ monikerta, on koodisana. Kääntäen, jos $C(x) = C_0 + C_1x + \cdots + C_nx^{n-1}$ on koodisana, niin Lemman 5.5 (a) mukaan $[C(x)]_n = C(x)$ ja tällöin Lemmasta 5.11 seuraa, että $g(x)$ jakaa polynomin $C(x)$. Lopuksi $C(x) = C_0 + C_1x + \cdots + C_{n-1}x^{n-1}$ on polynomin $g(x)$ monikerta jos ja vain jos $C(x) = g(x)I(x)$, missä $\deg I(x) \leq n - 1 - \deg g(x)$.

(b) Olkoon $g(x)$ polynomin $x^n - 1$ tekijä. Tällöin $C(x) = (C_0, C_1, \ldots, C_{n-1})$ on polynomin $g(x)$ monikerta jos ja vain jos $C(x) = g(x)I(x)$, missä $\deg g(x) + \deg I(x) \leq n - 1$. Täten kaikkien tälläisten sanojen joukko on $[n, k]$-koodi, missä $k = n - \deg g(x)$. Jotta tämä olisi syklinen koodi, tulee jokaisen koodisanan syklinen siirto oikealle olla koodisana. Siis olkoon $I(x)g(x)$ mikä tahansa koodisana. Lauseen 5.7 mukaan sen syklinen siirto oikealle on $[xI(x)g(x)]_n$. Mutta koska $g(x)$ jakaa polynomin $x^n - 1$, niin

$$\begin{aligned} [xI(x)g(x)]_n \operatorname{rem} g(x) &= [xI(x)g(x)] \operatorname{rem} g(x) && \text{(Lemman 5.5 (e) mukaan)} \\ &= 0 && \text{(Lemman 5.5 (b) mukaan),} \end{aligned}$$

mikä todistaa, että $[xI(x)g(x)]_n$ on polynomin $g(x)$ monikerta. Koodi on siis syklinen.

□

Lause 5.12 osoittaa syklisen koodin virittäjäpolynomin tärkeyden. Tämän läheistä sukulaista *pariteetintarkistuspolynomia* merkitään symbolilla $h(x)$ ja sen määritelmä on

$$h(x) = \frac{x^n - 1}{g(x)}.$$

Seuraavat Lauseen 5.12 seuraukset antavat eksplisiittisen kuvauksen syklisen koodin virittäjä- ja pariteetintarkistusmatriisille polynomien $g(x)$ ja $h(x)$ avulla.

SEURAUS 5.13. *Jos C on syklinen $[n, k]$-koodi, jonka virittäjäpolynomi on $g(x) = g_0 + g_1x + \cdots + g_rx^r$ (missä $r = n - k$) ja pariteetintarkistuspolynomi $h(x) = h_0 + h_1x + \cdots + h_kx^k$, niin koodin C virittäjä- G_1 ja pariteetintarkistusmatriisi H_1 ovat*

$$G_1 = \begin{bmatrix} g_0 & g_1 & \ldots & \ldots & g_r & 0 & \ldots & \ldots & 0 \\ 0 & g_0 & g_1 & \ldots & \ldots & g_r & 0 & \ldots & 0 \\ \vdots & & & & & & & & \vdots \\ 0 & \ldots & \ldots & 0 & g_0 & g_1 & \ldots & \ldots & g_r \end{bmatrix} = \begin{bmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{k-1}g(x) \end{bmatrix},$$

$$H_1 = \begin{bmatrix} h_k & h_{k-1} & \ldots & \ldots & h_0 & 0 & \ldots & \ldots & 0 \\ 0 & h_k & h_{k-1} & \ldots & \ldots & h_0 & 0 & \ldots & 0 \\ \vdots & & & & & & & & \vdots \\ 0 & \ldots & \ldots & 0 & h_k & h_{k-1} & \ldots & \ldots & h_0 \end{bmatrix} = \begin{bmatrix} \tilde{h}(x) \\ x\tilde{h}(x) \\ \vdots \\ x^{r-1}\tilde{h}(x) \end{bmatrix},$$

missä $\tilde{h}(x) = h_k + h_{k-1} + \cdots + h_0x^k$. Lisäksi, jos vektori $\mathbf{I} = (I_0, I_1, \ldots, I_{k-1})$ on koodattu muodossa $\mathbf{C} = \mathbf{I}G_1$, niin polynomien $I(x) = I_0 + I_1x + \cdots + I_{k-1}x^{k-1}$ ja $C(x) = C_0 + C_1x + \cdots + C_{n-1}x^{n-1}$ välillä on yhteys

$$C(x) = I(x)g(x).$$

TODISTUS. Todistus sivuutetaan; katso [**6**, s. 176]. □

SEURAUS 5.14. *Olkoon C syklinen $[n,k]$-koodi, jonka virittäjäpolynomi on $g(x)$. Olkoon $G_{2,i}$ kaikilla $i = 0,1,\ldots,k-1$ n-pituinen vektori, jota vastaava polynomi on $G_{2,i}(x) = x^{r+i} - x^{r+i} \operatorname{rem} g(x)$. Tällöin koodin C virittäjämatriisi G_2 on $k \times n$ -matriisi*

$$G_2 = \begin{bmatrix} G_{2,0} \\ G_{2,1} \\ \vdots \\ G_{2,k-1} \end{bmatrix}.$$

Vastaavasti, jos $H_{2,i}$ on r-pituinen vektori, jota vastaava polynomi on $H_{2,j}(x) = x^j \operatorname{rem} g(x)$, niin koodin C pariteetintarkistusmatriisi H_2 on $r \times n$ -matriisi

$$H_2 = [H_{2,0}^T, H_{2,1}^T, \ldots, H_{2,n-1}^T].$$

Lisäksi, jos vektori $\mathbf{I} = (I_0, I_1, \ldots, I_{k-1})$ on koodattu muodossa $\mathbf{C} = \mathbf{I}G_2$, niin polynomien $I(x)$ ja $C(x)$ välillä on yhteys

$$C(x) = x^r I(x) - [x^r I(x)] \operatorname{rem} g(x).$$

Jos vektorin $\mathbf{R} = (R_0, R_1, \ldots, R_{n-1})$ syndrooma on laskettu $\mathbf{S}^T = H_2\mathbf{R}^T$, niin polynomien $R(x)$ ja $S(x)$ välillä on yhteys

$$S(x) = R(x) \operatorname{rem} g(x).$$

TODISTUS. Todistus sivuutetaan; katso [**6**, s. 177]. □

ESIMERKKI 5.15 ([**6**, s. 177–179]). Esimerkissä 5.10 näytettiin, että Esimerkin 5.4 syklisen $[7,3]$-koodin virittäjäpolynomi on $g(x) = x^4 + x^3 + x^2 + 1$. Tällöin tätä vastaava pariteetintarkistuspolynomi on $h(x) = (x^7+1)/(x^4+x^3+x^2+1) = x^3+x^2+1$. Polynomin $g(x)$ monikerroista saadaan kahdeksan koodisanaa:

$$\begin{aligned}
\mathbf{C}_0 &= 0 \cdot g(x), \\
\mathbf{C}_1 &= 1 \cdot g(x), \\
\mathbf{C}_2 &= x \cdot g(x), \\
\mathbf{C}_3 &= x^2 \cdot g(x), \\
\mathbf{C}_4 &= (1+x) \cdot g(x), \\
\mathbf{C}_5 &= (1+x^2) \cdot g(x), \\
\mathbf{C}_6 &= (x+x^2) \cdot g(x), \\
\mathbf{C}_7 &= (1+x+x^2) \cdot g(x).
\end{aligned}$$

Seurauksen 5.13 mukaiset virittäjä- G_1 ja pariteetintarkistusmatriisi H_1 ovat

$$G_1 = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} g(x) \\ xg(x) \\ x^2 g(x) \end{bmatrix},$$

$$H_1 = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} \tilde{h}(x) \\ x\tilde{h}(x) \\ x^2\tilde{h}(x) \\ x^3\tilde{h}(x) \end{bmatrix}.$$

Seurauksen 5.14 mukaiset virittäjä- G_2 ja pariteetintarkistusmatriisi H_2 ovat

$$G_2 = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} x^4 - x^4 \operatorname{rem} g(x) \\ x^5 - x^5 \operatorname{rem} g(x) \\ x^6 - x^6 \operatorname{rem} g(x) \end{bmatrix},$$

$$H_2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} = [1, x, x^2, x^3, x^4 \operatorname{rem} g(x), x^5 \operatorname{rem} g(x), x^6 \operatorname{rem} g(x)].$$

On hyvä huomata, että matriisin G_2 oikealle puolelle muodostuu 3×3 -yksikkömatriisi ja matriisin H_2 vasemmalle puolelle 4×4 -yksikkömatriisi. Tämä tekee näistä matriiseista ”systemaattisia”. Rakennetaan virittäjä- ja pariteetintarkistusmatriisi muodossa $G = [I_k \ A]$ ja $H = [-A^T \ I_{n-k}]$ kuten Lauseessa 4.26. Syklisen koodin ominaisuuksia hyödyntäen tehdään matriisien G_2 ja H_2 riveille syklinen siirto oikealle kolme kertaa, jolloin saadaan

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

$$H_3 = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Jos koodataan vektori $\mathbf{I} = [101]$ käyttäen matriisia G_1, niin saadaan koodisana $(1 + x^2)(1 + x^2 + x^3 + x^4) = 1 + x^3 + x^5 + x^6 = [1001011]$. Sen sijaan, jos käytetään matriisia G_2, saadaan koodisanaksi $x^4(1 + x^2) - [x^4(1 + x^2)] \operatorname{rem}(x^4 + x^3 + x^2 + 1) = x^6 + x^4 + x + 1 = [11001010]$. Vektorin $\mathbf{R} = [1010011]$ syndrooma H_1 suhteen on $[1101]$. Toisaalta, jos käytetään matriisia H_2 saadaan syndrooma ”jakojäännöksenä” eli $R(x) \operatorname{rem} g(x) = (1+x^2+x^5+x^6) \operatorname{rem}(1+x^2+x^3+x^4) = x^3+x^2$, siis $\mathbf{S} = [0011]$. Jakolaskut on esitetty tarkemmin Liitteessä B.

5.1. Purskevirheen korjaaminen

Monilla käytännön tärkeillä kanavilla virheet esiintyvät *purskeina*. Fyysisesti tämä aiheutuu siitä, kun kanavan kohina lisääntyy hetkellisesti ja sitten palautuu normaaliksi. Syklisiä koodeja käytetään havaitsemaan ja korjaamaan tällaisia tilanteita.

Määritellään purskevirhe matemaattisesti. Lähetetään koodisana $\mathbf{C}$ ja vastaanotetaan viesti $\mathbf{R} = \mathbf{C} + \mathbf{E}$. Virhevektoria $\mathbf{E}$ kutsutaan *b-pituiseksi purskeeksi*, jos virhevektorin $\mathbf{E}$ nollasta eroavat komponentit rajoittuvat b-pituisiksi peräkkäisiksi komponenteiksi. Esimerkiksi $\mathbf{E} = (010000110)$ on 7-pituinen purske:

$$\begin{array}{ccccccccc} & * & * & * & * & * & * & * & \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \end{array}$$

Kuviossa $*$ merkitsee purskevirheen paikkaa. Koska korjataan syklisen koodin purskevirheitä, on syytä määritellä myös *syklinen purske*. Virhevektoria $\mathbf{E}$ kutsutaan *b-pituiseksi sykliseksi purskeeksi*, jos virhevektorin $\mathbf{E}$ nollasta eroavat komponentit rajoittuvat b-pituisiksi syklisesti peräkkäisiksi komponenteiksi. Edellä kuvatussa virhevektorissa $\mathbf{E} = (010000110)$ on 7-pituinen purske, mutta sen syklinen purske on 5-pituinen:

$$\begin{array}{cccccccccc} * & * & & & & & * & * & * \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \end{array}$$

Tästä eteenpäin ”purskeella” tarkoitetaan ”syklistä pursketta”. Otetaan käyttöön myös kaksi muuta termiä: purskeen *kuvio* ja *paikka*. Nollasta eroavan purskevirhevektorin $\mathbf{E}$ *purskekuvio* on symbolijono, joka alkaa ensimmäisestä nollasta eroavasta symbolista vektorissa $\mathbf{E}$ ja päättyy viimeiseen nollasta eroavaan symboliin. *Purskeen paikka* on purskeen ensimmäisen nollasta eroavan symbolin indeksoitu paikka. Esimerkiksi vektorin $\mathbf{E} = (010000110)$ 7-pituinen purskekuvio on 1000011 ja purskeen paikka on 1, jos oletetaan komponenttien indeksoidun järjestyksen olevan $0, 1, \ldots, 8$. Valitettavasti ”purskeen kuvio – purskeen paikka” -kuvaus ei ole yksikäsitteinen useimmille vektoreille $\mathbf{E}$, sillä mikä tahansa vektorin $\mathbf{E}$ nollasta eroava symboli voidaan valita syklisen purskeen ensimmäiseksi symboliksi. Täten virhevektorilla, jonka paino on w, on w kappaletta purskekuvauksia. Esimerkiksi vektorilla $\mathbf{E} = (010000110)$ on kolme purskekuvausta:

Kuvio	Paikka
1000011	1
11001	6
100100001	7

Tämä monitulkintaisuus on harmillinen, mutta se ei tavallisesti ole vakavaa, sillä käytännössä korjattavat virhepurskeet ovat melko lyhyitä.

LAUSE 5.16. *Olkoon* $\mathbf{E}$ *n-pituinen virhevektori, jolla on kaksi purskekuvausta* $(kuvio_1, paikka_1)$ *ja* $(kuvio_2, paikka_2)$. *Jos* $pituus(kuvio_1) + pituus(kuvio_2) \leq n+1$, *niin kaksi kuvausta ovat identtiset, toisin sanoen* $kuvio_1 = kuvio_2$ *ja* $paikka_1 = paikka_2$.

TODISTUS ([**6**, s. 200–201]). Kuten aikaisemmin huomattiin, jos vektorilla $\mathbf{E}$ on paino w, niin vektorilla $\mathbf{E}$ on täsmälleen w eri purskekuvausta. Jos $w = 0$ tai $w = 1$, niin ei ole mitään todistettavaa, joten oletetaan, että $w \geq 2$.

Vektorin $\mathbf{E}$ purske sisältää siis kaikki vektorin $\mathbf{E}$ nollasta eroavat komponentit, jolloin tämän purskekuvion ulkopuolelle jäävät nollat muodostavat syklisen *nollajonon*. Esimerkiksi vektorilla $\mathbf{E} = (010000110)$ on kolme purskekuvausta. Ensimmäinen purskekuvio näistä on 1000011, jonka paikka alkaa positiosta 1 ja päättyy positioon 7. Näin ollen tähän liittyvä nollajono on $(8, 0)$. Yhteensä on kolme nollajonoa, yksi jokaista vektorin $\mathbf{E}$ purskekuvausta kohden:

Kuvio	Paikka	Nollajono
1000011	1	$(8, 0)$
11001	6	$(2, 3, 4, 5)$
100100001	7	tyhjä

Viimeisessä purskekuvauksessa nollajonoa ei ole, jolloin merkitään sitä sanalla ”tyhjä”. Selvästi eri nollajonot ovat eri kohdissa ja sisältävät eri nollat. Nollajonojen kokonaispituus on $n - w$, missä w on vektorin $\mathbf{E}$ paino. Jos vektorilla $\mathbf{E}$ on kaksi eri purskekuvausta

$$(\text{kuvio}_1, \text{paikka}_1) \text{ ja } (\text{kuvio}_2, \text{paikka}_2),$$

niin tällöin vektorissa $\mathbf{E}$ olevien nollien määräksi saadaan

$$(n - \text{pituus}(\text{kuvio}_1)) + (n - \text{pituus}(\text{kuvio}_2)),$$

sillä eri purskeiden nollajonot koostuvat eri nollista. Nyt

$$\begin{aligned}(n - \text{pituus}(\text{kuvio}_1)) + (n - \text{pituus}(\text{kuvio}_2)) &= n - w \\ \Leftrightarrow 2n - (\text{pituus}(\text{kuvio}_1) + \text{pituus}(\text{kuvio}_2)) &= n - w.\end{aligned}$$

Mutta koska oletuksen mukaan $\text{pituus}(\text{kuvio}_1) + \text{pituus}(\text{kuvio}_2) \leq n + 1$, niin

$$\begin{aligned}2n - (n + 1) &\leq n - w \\ \Leftrightarrow n - 1 &\leq n - w \\ \Leftrightarrow w &\leq 1.\end{aligned}$$

Tämä on ristiriita sen kanssa, että vektorilla $\mathbf{E}$ on paino $w \geq 2$. Täten purskekuvaukset ovat identtiset. □

Seuraus 5.17. *Virhevektorilla* $\mathbf{E}$ *voi olla enintään yksi purskekuvaus, jonka purskeen pituus on enintään* $(n + 1)/2$.

Todistus ([**6**, s. 201]). Kaksi eri kuvausta, joiden purskeen pituus olisi enintään $(n + 1)/2$ olisi ristiriidassa Lauseen 5.16 kanssa. □

Lause 5.18. *Kaksikirjaimisessa aakkostossa on täsmälleen* $n2^{b-1} + 1$ n*-pituista vektoria, joiden purskeen pituus on enintään* b*, kun* $1 \leq b \leq (n + 1)/2$.

Todistus ([**6**, s. 202]). Jos $0 < b \leq (n + 1)/2$, niin Seurauksen 5.17 mukaan b-pituinen purskekuvaus on yksikäsitteinen. Kuvauksen paikalle on n eri mahdollisuutta. Kuvio alkaa symbolilla 1 ja sen pituus on korkeintaan b. Näin ollen mahdolliset kuviot ovat bijektiivinen kuvaus ykkösellä alkaville b-pituisille 2^{b-1} binäärijonoille. Täten mahdollisten kuvioiden lukumäärä on 2^{b-1} ja nollasta eroavia enintään b-pituisia purskeita on yhteensä $n \cdot 2^{b-1}$ kappaletta. Lisätään tähän nollavektori, jolloin saadaan $n2^{b-1} + 1$ kuten pitikin.

□

Kaksi seuraavaa lausetta antavat käytännölliset rajat koodeille, jotka korjaavat purskevirheitä. Tällainen koodi, joka kykenee korjaamaan kaikki enintään b-pituiset purskekuviot on nimeltään *b-pituisen purskevirheen korjauskoodi.*

Lause 5.19 (Hammingin raja purskevirheen korjaamiseen). *Jos* $1 \leq b \leq (n+1)/2$, *niin binäärisessä b-pituisen purskevirheen korjauskoodissa on enintään* $2^n/(n2^{b-1}+1)$ *koodisanaa.*

Todistus ([**6**, s. 202]). Lauseen 5.18 mukaan on olemassa $n2^{b-1} + 1$ enintään b-pituista purskevirhekuviota. Jos on olemassa M koodisanaa, niin tällöin on olemassa $M(n2^{b-1} + 1)$ sanaa, jotka eroavat koodisanasta enintään b-pituisen purskeen verran. Nämä sanat ovat keskenään erisuuret, joten $M(n2^{b-1} + 1) \leq 2^n$. □

SEURAUS 5.20 (Abramsonin rajat). *Jos* $1 \leq b \leq (n+1)/2$, *niin binääriselle lineaariselle b-pituisen purskevirheen korjaavalle* $[n,k]$*-koodille pätee*

$$n \leq 2^{r-b+1} - 1 \qquad \textit{(vahva Abramsonin raja)},$$

missä $r = n - k$ *on koodin redundanssi. Vaihtoehtoinen muotoilu on*

$$r \geq \lceil \log_2(n+1) \rceil + (b-1) \qquad \textit{(heikko Abramsonin raja)}.$$

TODISTUS ([**6**, s. 202]). Lineaarisessa $[n,k]$-koodissa on $M = 2^k$ koodisanaa. Tällöin Lauseen 5.19 mukaan $2^k \leq 2^n/(n2^{b-1}+1)$. Uudelleen järjestämällä saadaan $n \leq 2^{r-b+1} - 2^{-b+1}$. Koska n täytyy olla kokonaisluku, rajaa voidaan parantaa vahvaksi Abramsonin rajaksi $n \leq 2^{r-b+1} - 1$. Ratkaisemalla tämä redundanssin r suhteen, saadaan heikko Abramsonin raja. □

LAUSE 5.21. *Jos* $b \leq n/2$, *niin binäärisessä b-pituisen purskevirheen korjauskoodissa on enintään* 2^{n-2b} *koodisanaa.*

TODISTUS ([**6**, s. 203]). Jos $M > 2^{n-2b}$, niin kyyhkyslakkaperiaatteen[1] mukaan täytyy olla kaksi eri koodisanaa, joilla on samat ensimmäiset $n-2b$ koordinaattia. Nämä kaksi koodisanaa voidaan esittää seuraavasti:

$$\begin{aligned} X = \overbrace{* \;\; * \;\; * \;\; * \;\; * \;\; * \;\; * \;\; *}^{n-2b} \; \overbrace{A \;\; A \;\; A \;\; A \;\; A \;\; A}^{2b} \\ Y = * \;\; * \;\; * \;\; * \;\; * \;\; * \;\; * \;\; * \; B \;\; B \;\; B \;\; B \;\; B \;\; B, \end{aligned}$$

missä "*" ovat samoja, mutta A ja B mielivaltaisia. Nyt sana

$$Z = * \;\; * \;\; * \;\; * \;\; * \;\; * \;\; * \;\; * \; A \;\; A \;\; A \;\; B \;\; B \;\; B$$

eroaa kummastakin sanasta X ja Y enintään b-pituisen purskeen verran, mikä on ristiriita. □

SEURAUS 5.22 (Reigerin raja). *Jos* $0 \leq b \leq n/2$, *niin binääriselle lineaariselle b-pituisen purskevirheen korjaavalle* $[n,k]$*-koodille pätee*

$$r \geq 2b,$$

missä $r = n - k$ *on koodin redundanssi.*

TODISTUS ([**6**, s. 203]). Koodisanojen lukumäärä binäärisessä $[n,k]$-koodissa on 2^k, joka Lauseen 5.21 mukaan täytyy olla $\leq 2^{n-2b}$. Tämä vastaa seurauksen väittämää. □

Tarkastellaan seuraavaksi muutamia esimerkkejä. Näissä esimerkeissä syklinen koodi saavuttaa joko vahvan Abramsonin rajan tai Reigerin rajan. Jos on olemassa koodi, jonka redundanssi on täsmälleen rajan arvo sanotaan, että kyseinen raja on *tiukka*. Jos tällaista koodia ei löydy, niin raja on *väljä*.

[1]Jos parvessa on enemmän kyyhkysiä kuin kyyhkyslakassa pesiä, lentää johonkin pesäkoloon vähintään kaksi kyyhkystä.

Esimerkki 5.23 ([**6**, s. 203]). Binäärinen $[n, 1]$-toistokoodi, jonka virittäjäpolynomi $g(x) = x^{n-1} + x^{n-2} + \cdots + x + 1$, missä n on pariton pystyy korjaamaan painoltaan $\leq (n-1)/2$ olevat kaikki virhekuviot. Se on siis $((n-1)/2)$-pituisen purskevirheen korjauskoodi. Reigerin raja on tiukka, sillä $r = n - 1$.

Esimerkki 5.24 ([**6**, s. 204]). Kaikki mahdolliset n-pituiset koodisanat sisältävä $[n, n]$-koodi on syklinen ja sen $g(x) = 1$. Se on 0-pituisen ($b = 0$) purskevirheen korjauskoodi ja koska myös $r = 0$, niin Reigerin raja on tiukka.

Esimerkki 5.25 ([**6**, s. 204]). Jokainen syklinen Hammingin koodi, josta on poistettu kaikki parittoman painoiset koodisanat on 2-pituisen ($b = 2$) purskevirheen korjauskoodi nimeltään *Abramsonin koodi*. Nämä koodit ovat syklisiä ja niiden virittäjäpolynomi on muotoa $g(x) = (x+1)p(x)$, missä $p(x)$ on primitiivipolynomi eli primitiivisen juuren minimipolynomi. Pienin Abramsonin koodi on syklinen $[7, 3]$-koodi, jonka virittäjäpolynomi on $g(x) = (x + 1)(x^3 + x + 1)$ ja pariteetintarkistusmatriisi

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix},$$

missä α on yhtälön $\alpha^3 + \alpha + 1 = 0$ primitiivinen juuri kunnassa $\mathbb{F}_8$. Tarkistetaan vielä, että koodi on varmasti 2-pituisen purskeen korjaava koodi. Tähän riittää osoittaa, että kaikki enintään 2-pituiset purskeet ovat erisuuria. Nollakuviolle $b = 0$ syndrooma on $\binom{0}{0}$. Kun $b = 1$, niin purskekuvauksen $(1, i)$ syndrooma on $\binom{\alpha^i}{1}$. Kun $b = 2$, niin purskekuvauksen $(11, i)$ syndrooma on $\binom{\alpha^i(\alpha+1)}{0}$. Nämä $1 + 2n$ ovat kaikki eri syndroomia, joten koodi on todella 2-pituisen purskevirheen korjaava. Lopuksi on hyvä huomata, että jos $g(x) = (x + 1)p(x)$, missä $p(x)$ on astetta m oleva primitiivipolynomi, niin $n = 2^m - 1$, $r = m + 1$ ja $b = 2$ tarkoittaen, että vahva Abramsonin raja on tiukka. (Kun $m = 3$, kuten esimerkiksi $b = 2$ $[7, 3]$-koodi, niin Reigerin raja on tiukka, mutta kaikille suuremmille arvoille m raja on väljä.)

Seuraava esimerkki havainnollistaa tärkeän *lomitustekniikan*, joka on yksinkertainen tapa parantaa koodin purskevirheiden korjaamismahdollisuuksia.

Esimerkki 5.26 ([**6**, s. 207]). Tarkastellaan edelleen Abramsonin $b = 2$ $[7, 3]$-koodia, jonka $g(x) = x^4 + x^3 + x^2 + 1$. Olkoon $\mathbf{A}, \mathbf{B}$ ja $\mathbf{C}$ mitkä tahansa kolme sanaa tästä koodista. Ilmaistaan tämä 3×7 taulukkona:

$$\begin{matrix} A_0 & A_1 & A_2 & A_3 & A_4 & A_5 & A_6 \\ B_0 & B_1 & B_2 & B_3 & B_4 & B_5 & B_6 \\ C_0 & C_1 & C_2 & C_3 & C_4 & C_5 & C_6 \end{matrix}.$$

Seuraavaa 21-pituista vektoria, joka on muodostettu taulukon sarakkeista kutsutaan sanojen $\mathbf{A}, \mathbf{B}$ ja $\mathbf{C}$ *lomitukseksi*:

$$A_0\ B_0\ C_0\ A_1\ B_1\ C_1\ A_2\ B_2\ C_2\ A_3\ B_3\ C_3\ A_4\ B_4\ C_4\ A_5\ B_5\ C_5\ A_6\ B_6\ C_6.$$

Oletetaan, että tämä pitkä koodisana lähetetään purskekohinaisen kanavan läpi ja tapahtuu 6-pituinen purskevirhe, jota merkitään symbolilla $*$:

$$A_0\ B_0\ C_0\ A_1\ B_1\ C_1\ A_2\ B_2\ C_2\ A_3\ *\ *\ *\ *\ *\ *\ B_5\ C_5\ A_6\ B_6\ C_6.$$

Nyt on mahdollista korjata näin suuri purskevirhe yksinkertaisesti palauttamalla tämän pitkän koodisanan lomitus takaisin kolmeen koodisanaan, joista kukin on kärsinyt vain 2-pituisen purskevirheen:

$$\begin{array}{ccccccc} A_0 & A_1 & A_2 & A_3 & * & * & A_6 \\ B_0 & B_1 & B_2 & * & * & B_5 & B_6 \\ C_0 & C_1 & C_2 & * & * & C_5 & C_6 \end{array}.$$

Koodi, joka koostuu kaikista mahdollisista Abramsonin $[7, 3]$-koodin kolmen koodisanan lomituksista, on nimeltään syvyyden 3 lomitus. Se on lineaarinen $[21, 9]$-koodi. Aiempi perustelu osoittaa, että se on todella 6-pituisen purskeen korjaava koodi. Yleisemmin kaikille positiivisille kokonaisluvuille j, syvyydellä j oleva Abramsonin $[7, 3]$-koodi on $2j$-pituisen purskeen korjaava $[7j, 3j]$-koodi. On hyvä huomata, että jokainen näistä koodeista saavuttaa Reigerin rajan yhtäsuuruuden (koska $r = 4j$ ja $b = 2j$), joten tässä mielessä koodi ei menetä tehokkuuttaan, kun se lomitetaan.

LAUSE 5.27. *Jos C on lineaarinen b-pituisen purskevirheen korjaava $[n, k]$-koodi, niin syvyydellä j lomitettu koodin C koodi on bj-pituisen purskevirheen korjaava $[nj, kj]$-koodi.*

TODISTUS. Esimerkissä 5.26 tehty yleistys. □

Ei ole itsestään selvää, mutta joka tapauksessa totta, että jos syklinen koodi lomitetaan syvyydellä j, niin saatu koodi on myös syklinen. Tämän todistamiseksi tarvitaan seuraava aputulos. Merkitään lomitusoperaattoria symbolilla "≀". Siispä vektoria, joka on saatu lomittamalla j koodisanaa $\mathbf{C}_0, \mathbf{C}_1, \ldots, \mathbf{C}_{j-1}$ merkitään $\mathbf{C}_0 \wr \mathbf{C}_1 \wr \cdots \wr \mathbf{C}_{j-1}$.

LEMMA 5.28. *Syvyydellä j lomitetun syklisen koodin C koodisanan sykliselle siirrolle oikealle pätee*

$$[\mathbf{C}_0 \wr \mathbf{C}_1 \wr \cdots \wr \mathbf{C}_{j-1}]^R = [\mathbf{C}_{j-1}^R \wr \mathbf{C}_0 \wr \cdots \wr \mathbf{C}_{j-2}].$$

TODISTUS. (Kirjoittajan oma todistus). Ilmaistaan koodi $\mathbf{C}$ taulukkona:

$$\begin{array}{cccccc} C_{0,0} & C_{0,1} & \cdots & \cdots & C_{0,n-2} & C_{0,n-1} \\ C_{1,0} & C_{1,1} & \cdots & \cdots & C_{1,n-2} & C_{1,n-1} \\ \vdots & \vdots & & & \vdots & \vdots \\ C_{j-1,0} & C_{j-1,1} & \cdots & \cdots & C_{j-1,n-2} & C_{j-1,n-1} \end{array}.$$

Tehdään tälle lomitus $[\mathbf{C}_0 \wr \mathbf{C}_1 \wr \cdots \wr \mathbf{C}_{j-1}]$, jolloin saadaan vektori

$$C_{0,0}\ C_{1,0}\ \cdots\ C_{j-1,0}\ C_{0,1}\ C_{1,1}\ \cdots\ C_{j-1,n-2}\ C_{0,n-1}\ C_{1,n-1}\ \cdots\ C_{j-2,n-1}\ C_{j-1,n-1}\ .$$

Tehdään vektorille syklinen siirto oikealle eli $[\mathbf{C}_0 \wr \mathbf{C}_1 \wr \cdots \wr \mathbf{C}_{j-1}]^R$:

$$C_{j-1,n-1}\ C_{0,0}\ C_{1,0}\ \cdots\ C_{j-1,0}\ C_{0,1}\ C_{1,1}\ \cdots\ C_{j-1,n-2}\ C_{0,j-1}\ C_{1,n-1}\ \cdots\ C_{j-2,n-1}\ .$$

Palautetaan tämä lomitus takaisin koodiksi taulukkomuotoon:

$$\begin{array}{cccccc} C_{j-1,n-1} & C_{j-1,0} & \cdots & \cdots & C_{j-1,n-3} & C_{j-1,n-2} \\ C_{0,0} & C_{0,1} & \cdots & \cdots & C_{0,n-2} & C_{0,n-1} \\ C_{1,0} & C_{1,1} & \cdots & \cdots & C_{1,n-2} & C_{1,n-1} \\ \vdots & \vdots & & & \vdots & \vdots \\ C_{j-2,0} & C_{j-2,1} & \cdots & \cdots & C_{j-2,n-2} & C_{j-2,n-1} \end{array},$$

josta huomataan, että kyseessä on lomitus $[\mathbf{C}_{j-1}^R \wr \mathbf{C}_0 \wr \cdots \wr \mathbf{C}_{j-2}]$. □

LAUSE 5.29. *Jos C on syklinen $[n,k]$-koodi ja sen virittäjäpolynomi on $g(x)$, niin syvyydellä j oleva lomitus koodista C on syklinen $[nj,kj]$-koodi ja sen virittäjäpolynomi on $g(x^j)$.*

TODISTUS ([**6**, s. 208]). Lemman 5.28 mukaan syvyydellä j lomitettu syklinen koodi on syklinen, koska jos $\mathbf{C}_0, \mathbf{C}_1, \ldots, \mathbf{C}_{j-1}$ ovat jonkun tietyn syklisen koodin sanoja, niin tällöin $\mathbf{C}_{j-1}^R, \mathbf{C}_0, \ldots, \mathbf{C}_{j-2}$ ovat myös koodisanoja. Koska lomitetun koodin redundanssi on rj, sen virittäjäpolynomi on sen yksikäsitteinen rj-asteinen pääpolynomi. Mutta jos $g(x)$ on virittäjäpolynomi alkuperäiselle koodille, niin lomitettu koodisana $[g(x) \wr 0 \wr \cdots \wr 0]$, joka on polynomi $g(x^j)$, on astetta rj. Täten polynomin $g(x^j)$ täytyy olla lomitetun koodin virittäjäpolynomi. □

ESIMERKKI 5.30 ([**6**, s. 208]). Lähdetään liikkeelle Abramsonin $b = 2$ $[7,3]$-koodista, jonka virittäjäpolynomi on $g(x) = x^4+x^3+x^2+1$. Käytettäessä lomitustekniikkaa, saadaan tuotettua ääretön määrä syklisiä $2j$-pituisen purskevirheen korjauskoodeja eli $[7j,3j]$-koodeja, joiden virittäjäpolynomit ovat $g_j(x) = x^{4j} + x^{3j} + x^{2j} + 1$.

5.2. Syklisen purskevirheen korjauskoodin dekoodaus

Oletetaan, että $g(x)$ virittää syklisen $[n,k]$-koodin C. Lähetetään koodisana $C(x)$ ja vastaanotetaan sana

$$R(x) = C(x) + E(x),$$

missä $E(x)$ on virhekuvio. Mikäli dekoodaaja laskee jakojäännössyndrooman

$$S(x) = R(x) \operatorname{rem} g(x),$$

niin vektori $\hat{C}$, joka saadaan polynomien $R(x)$ ja $S(x)$ erotuksena

$$\hat{C}(x) = R(x) - S(x) \tag{5.2}$$

on takuuvarmasti koodisana, sillä $\hat{C}(x) \operatorname{rem} g(x) = R(x) \operatorname{rem} g(x) - S(x) \operatorname{rem} g(x) = 0$.

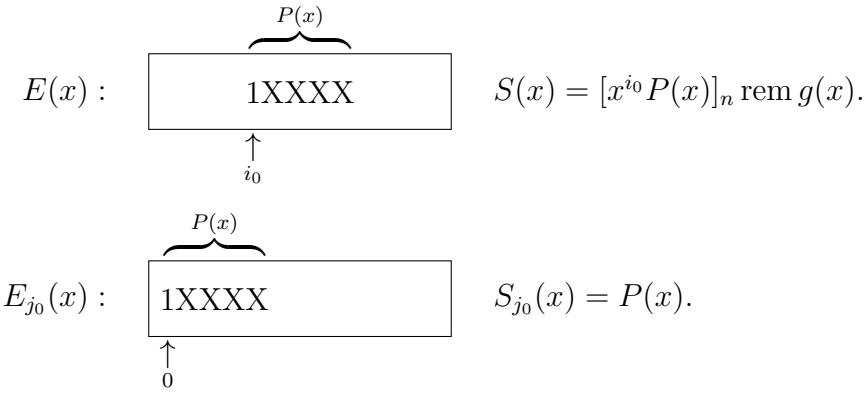
Olkoon C b-pituisen purskevirheen korjauskoodi ja syndroomalle $S(x)$ on voimassa seuraavat kaksi ehtoa

$$\begin{aligned} S(0) &\neq 0, \\ \deg S(x) &\leq b-1. \end{aligned} \tag{5.3}$$

Tämä tarkoittaa sitä, että *syndrooma itse* on enintään b-pituinen purske ja näin ollen dekoodaaja voi olla varma, että yhtälön (5.2) polynomi $\hat{C}(x)$ on lähetetty koodisana. Dekoodaus on siis helppoa, jos epäyhtälö (5.3) toteutuu. Harmittavasti, tämä toteutuu vain kun virhevektorin purske alkaa positiosta 0.

Voisiko purskeen siirtää aina positioon 0? Koska koodi on syklinen, niin tämän pitäisi onnistua! Jos virhevektori $E(x)$ on nollasta eroava ja siinä on korkeintaan b-pituinen purske, niin polynomilla $E(x)$ on yksikäsitteinen purskekuvaus, joka on muotoa $(P(x), i_0)$, missä $P(0) \neq 0$ ja $\deg P(x) \leq b-1$. Tällöin $E(x) = [x^{i_0} P(x)]_n$ ja jakojäännössyndrooma on

$$S(x) = [x^{i_0} P(x)]_n \operatorname{rem} g(x),$$



KUVA 5.1. Purskekuvion pakotettu siirto positioon 0.

missä $g(x)$ on koodin generoijapolynomi. Tämä tilanne on piirretty Kuvan 5.1 yläosaan. Kuten aiemmin todettiin, jos purske sijaitsee positiossa 0 eli $i_0 = 0$, niin $S(x) = P(x)$ ja purskevirhe voidaan korjata heti. Jos kuitenkin $i_0 \neq 0$, niin tehdään syklinen siirto oikealle, kunnes purskekuvio $P(x)$ alkaa positiosta 0, kuten Kuvan 5.1 alaosa. Syklisten siirtojen määrä on kokonaisluku j_0 välillä $0 \leq j_0 \leq n-1$ siten, että $i_0 + j_0 \equiv 0 \bmod n$ eli

$$j_0 \equiv (-i_0) \bmod n.$$

Tarkoittakoon nyt merkintä $R_{j_0}(x)$ sitä, että polynomia $R(x)$ on siirretty j_0 kertaa syklisesti oikealle. Tällöin

$$R_{j_0}(x) = C_{j_0}(x) + E_{j_0}(x),$$

missä $C_{j_0}(x)$ ja $E_{j_0}(x)$ ovat vastaavasti syklisiä siirtoja j_0 verran oikealle. Koska koodi on syklinen, niin $C_{j_0}(x)$ on koodisana ja j_0:n määritelmästä johtuen $E_{j_0}(x) = P(x)$. Tällöin merkintä $S_{j_0}(x)$ on polynomin $R_{j_0}(x)$ jakojäännössyndrooma. Siis

$$\begin{aligned} S_{j_0}(x) &= R_{j_0}(x) \operatorname{rem} g(x) \\ &= (C_{j_0}(x) + E_{j_0}(x)) \operatorname{rem} g(x) \\ &= P(x). \end{aligned}$$

Nyt S_{j_0} toteuttaa ehdot (5.3) ja dekoodaaja voi varmistua siitä, että

$$\hat{C}_{j_0}(x) = R_{j_0}(x) - S_{j_0}(x)$$

on lähetetyn koodisanan j_0:s syklinen siirto oikealle.

Tästä seuraa että, jos dekoodaaja onnistuneesti laskee $S_0(x), S_1(x), \ldots$ ja testaa jokaisen polynomin ehdoilla (5.3), niin lopulta purske löytyy ja sana voidaan korjata. Purskevirhekuvio saadaan polynomista S_{j_0} ja purskevirheen paikka saadaan yhtälöstä $i_0 \equiv (-j_0) \bmod n$, missä j_0 on tarvittavien siirtojen määrä. Vaikka tällainen ajatus on jo hyvä, niin sitä voidaan vielä yksinkertaistaa, sillä purskevirheen paikka $S_j(x)$ voidaan laskea nopeammin seuraavan tuloksen avulla.

LAUSE 5.31 (Meggitt'n lemma). *Määritellään polynomin $R(x)$ j:nnen syklisen siirron jakojäännössyndrooma*

$$S_j(x) = [x^j R(x)]_n \operatorname{rem} g(x), \quad j \geq 0.$$

Tällöin

$$S_{j+1}(x) = [xS_j(x)] \operatorname{rem} g(x), \quad j \geq 0.$$

TODISTUS ([**6**, s. 217]). Ensiksi huomataan Lemmasta 5.5(e), että

$$S_j(x) = [x^j R(x)] \operatorname{rem} g(x),$$

sillä $g(x)$ jakaa polynomin $x^n - 1$. Seuraavaksi

$$\begin{aligned}[xS_j(x)] \operatorname{rem} g(x) &= [x([x^j R(x)] \operatorname{rem} g(x))] \operatorname{rem} g(x) \\ &= [x^{j+1} R(x)] \operatorname{rem} g(x) \quad \text{Lemma 5.5(d)} \\ &= S_{j+1}(x).\end{aligned}$$

□

ESIMERKKI 5.32 ([**6**, s. 217–218]). Havainnollistetaan näitä ajatuksia käyttäen Abramsonin $b = 2$ $[7, 3]$-koodia generoijapolynomilla $g(x) = x^4 + x^3 + x^2 + 1$. Olkoon vastaanotettu vektori $\mathbf{R} = [1010011]$ eli $R(x) = x^6 + x^5 + x^2 + 1$. Tällöin (Liite B)

$$\begin{aligned}S_0(x) &= R(x) \operatorname{rem} g(x) \\ &= (x^6 + x^5 + x^2 + 1) \operatorname{rem}(x^4 + x^3 + x^2 + 1) \\ &= x^3 + x^2.\end{aligned}$$

Meggitt'n lemman avulla saadaan onnistuneesti laskettua $S_1(x), S_2(x), \ldots$:

$$\begin{aligned}S_1(x) &= [xS_0(x)] \operatorname{rem} g(x) \\ &= (x^4 + x^3) \operatorname{rem}(x^4 + x^3 + x^2 + 1) \\ &= x^2 + 1.\end{aligned}$$

Vastaavasti, (katso Liite B)

$$\begin{aligned}S_2(x) &= x^3 + x \\ S_3(x) &= (x^4 + x^2) \operatorname{rem}(x^4 + x^3 + x^2 + 1) = x^3 + 1 \\ S_4(x) &= (x^4 + x) \operatorname{rem}(x^4 + x^3 + x^2 + 1) = x^3 + x^2 + x + 1 \\ S_5(x) &= (x^4 + x^3 + x^2 + x) \operatorname{rem}(x^4 + x^3 + x^2 + 1) = x + 1.\end{aligned}$$

Nyt voidaan pysähtyä, sillä $S_5(x)$ toteuttaa ehdot (5.3) ja purskevirhekuvio "11" on löydetty. Purskevirheen paikka on $(-5) \operatorname{rem} 7 = 2$. Täten virhevektori on $E = [0011000]$ ja korjattu koodisana on $\mathbf{R} + \mathbf{E} = [1001011]$.

LUKU 6

BCH-koodit

Johdantona BCH-koodeihin tehdään pikakatsaus Hammingin koodeihin. Koska tässä tutkielmassa on tarkempi Hammingin koodien tutkiminen jätetty vähemmälle huomiolle, niin niitä koskevat lauseiden todistukset ja asioiden perustelut saatetaan sivuuttaa, sillä ne löytyvät kyllä helposti alan kirjallisuudesta. Luvun pohjana on käytetty kirjaa Robert McEliece: The Theory of Information and Coding (2002) [**6**].

MÄÄRITELMÄ 6.1 (binäärinen Hammingin koodi). Merkitään $n = 2^m - 1$ ja $k = n - m$. Olkoon H sellainen binäärinen $m \times n$ -matriisi, jonka sarakkeet ovat vektoriavaruuden $\mathbb{F}_2^m$ nollasta eroavat vektorit (jossain järjestyksessä). Tällöin sellaista lineaarista $[n, k]$-koodia kunnan $\mathbb{F}_2$ suhteen, jonka pariteetintarkistusmatriisi H on, sanotaan *n-pituiseksi binääriseksi Hammingin koodiksi*.

ESIMERKKI 6.2 ([**10**, s. 34]). Binäärisen Hammingin $[7, 3]$-koodin pariteetintarkistusmatriisi on

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

missä sarakkeet ilmaisevat binäärilukuna kokonaisluvut $1, 2, \ldots, 7$. Ternäärisen Hammingin $[13, 10]$-koodin pariteetintarkistusmatriisi on

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

Näissä esimerkeissä on havainnollistettu tapaa, kuinka Hammingin koodien pariteetintarkistusmatriisit muodostetaan: luetaan ylhäältä alas ja valitaan ne sarakkeet, joiden ensimmäinen nollasta eroava alkio on 1.

Pariteetintarkistusmatriisi binääriselle Hammingin koodille on siis

$$H = \begin{bmatrix} \mathbf{v}_0 & \mathbf{v}_1 & \cdots & \mathbf{v}_{n-1} \end{bmatrix}, \tag{6.1}$$

missä $(\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_{n-1})$ ovat vektoriavaruuden $\mathbb{F}_2^m$ nollasta eroavat vektorit (jossain järjestyksessä). Matriisin dimensio on $m \times n$, mikä tarkoittaa sitä, että tarvitaan m pariteetintarkistusbittiä yhden virheen korjaamiseen. Jos halutaan korjata *kaksi* virhettä, niin on perusteltua olettaa, että pariteetintarkistusbittejä tarvitaan lisää m kappaletta. Tehdään siis arvaus, että yleistä muotoa oleva matriisi

$$H_2 = \begin{bmatrix} \mathbf{v}_0 & \mathbf{v}_1 & \cdots & \mathbf{v}_{n-1} \\ \mathbf{w}_0 & \mathbf{w}_1 & \cdots & \mathbf{w}_{n-1} \end{bmatrix},$$

missä $\mathbf{w}_0, \mathbf{w}_1, \ldots, \mathbf{w}_{n-1} \in \mathbb{F}_2^m$, on pariteetintarkistusmatriisi kahden virheen korjaavalle n-pituiselle koodille. Koska kuitenkin vektorit $\mathbf{v}_i$ ovat keskenään erisuuret, saadaan vastaavuus $\mathbf{v}_i \to \mathbf{w}_i$ funktiona avaruudesta $\mathbb{F}_2^m$ itselleen ja kirjoitetaan matriisi H_2 muodossa

$$H_2 = \begin{bmatrix} \mathbf{v}_0 & \mathbf{v}_1 & \cdots & \mathbf{v}_{n-1} \\ \mathbf{f}(\mathbf{v}_0) & \mathbf{f}(\mathbf{v}_1) & \cdots & \mathbf{f}(\mathbf{v}_{n-1}) \end{bmatrix}. \tag{6.2}$$

Kuinka funktio $\mathbf{f}$ sitten valitaan? Tämän selvittämiseksi tarvitaan yksi lause ja sen seuraus avuksi.

LAUSE 6.3. *Jos C on lineaarinen $[n,k]$-koodi kunnan F_q suhteen ja sen pariteetintarkistusmatriisi on H, niin koodin C minimietäisyys $d(C)$ on pienin matriisin H lineaarisesti riippuvien sarakkeiden lukumäärä. Siksi, jos jokainen matriisin H osajoukko korkeintaan $2t$ sarakkeesta on lineaarisesti riippumaton, niin koodi korjaa kaikki virhekuviot, joiden paino on enintään t. (Jos $q = 2$, niin sanonta "lineaarisesti riippuvien" voidaan korvata sannonnalla "nollaksi summautuvien").*

TODISTUS. Todistus sivuutetaan; katso [**6**, s. 148]. □

SEURAUS 6.4. *Jos $q = 2$ ja kaikki mahdolliset lineaarikombinaatiot matriisin H korkeintaan mistä tahansa e sarakkeesta ovat keskenään erisuuria, niin $d(C) \geq 2e+1$ ja tällöin koodi C korjaa kaikki virhekuviot, joiden paino on enintään e.*

TODISTUS. Todistus sivuutetaan; katso [**4**, s. 54] ja [**6**, s. 148]. □

Näiden tulosten valossa H_2 määrittelee kahden virheen korjaavan koodin jos ja vain jos painoltaan 0, 1 ja 2 olevat syndroomat $1+n+\binom{n}{2}$ virhekuviosta ovat keskenään erisuuret. Nyt mikä tahansa syndrooma on matriisin H_2 joidenkin sarakkeiden summa ja täten se on joukon $\mathbb{F}_2^{2m}$ vektori. Jaetaan syndrooma $\mathbf{s} = (s_1, \ldots, s_{2m})$ kahteen osaan: $\mathbf{s} = (\mathbf{s}_1, \mathbf{s}_2)$, missä $\mathbf{s}_1 = (s_1, \ldots, s_m)$ ja $\mathbf{s}_2 = (s_{m+1}, \ldots, s_{2m})$. Nämä kumpikin ovat joukossa $\mathbb{F}_2^m$. Tämän avulla nollasyndroomaa voidaan merkitä $(\mathbf{0}, \mathbf{0})$. Positiossa i olevan yhden virheen syndrooma $\mathbf{s} = (\mathbf{v}_i, \mathbf{f}(\mathbf{v}_i))$ ja kahdelle posititoissa i ja j olevalle virheelle saadaan syndrooma $\mathbf{s} = (\mathbf{v}_i+\mathbf{v}_j, \mathbf{f}(\mathbf{v}_i)+\mathbf{f}(\mathbf{v}_j))$. Nämä kolme tapausta voidaan yhdistää määrittämällä $\mathbf{f}(\mathbf{0}) = \mathbf{0}$. Tällöin keskenään erisuurien syndroomien ehdosta johtuen yhtälöillä

$$\begin{aligned} \mathbf{u} + \mathbf{v} &= \mathbf{s}_1, \\ \mathbf{f}(\mathbf{u}) + \mathbf{f}(\mathbf{v}) &= \mathbf{s}_2 \end{aligned} \tag{6.3}$$

on korkeintaan yksi ratkaisu $(\mathbf{u}, \mathbf{v})$ jokaiselle vektoriparille joukosta $\mathbb{F}_2^m$. (Luonnollisesti ratkaisut $(\mathbf{u}, \mathbf{v})$ ja $(\mathbf{v}, \mathbf{u})$ ovat samoja.)

Yritetään seuraavaksi löytää edellä olevien ominaisuuksien täyttävä funktio $\mathbf{f} : \mathbb{F}_2^m \to \mathbb{F}_2^m$, $\mathbf{f}(\mathbf{0}) = \mathbf{0}$. Lineaarikuvaus $\mathbf{f}(\mathbf{v}) = T\mathbf{v}$ ei toimi, joten $\mathbf{f}$ täytyy olla epälineaarinen. On mahdollista määritellä joukon $\mathbb{F}_2^m$ vektoreiden yhteen- ja kertolasku siten, että saadaan kunnan rakenne epälineaariselle funktiolle. Helpohkosti nähdään, että jokainen funktio $\mathbf{f} : \mathbb{F}_2^m \to \mathbb{F}_2^m$ voidaan esittää polynomina. Korkeintaan astetta kaksi olevat polynomit eivät kuitenkaan toimi, mutta $\mathbf{f}(\mathbf{v}) = \mathbf{v}^3$ toimii. Sen vuoksi, jos $(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ on mielivaltainen järjestys nollasta eroavista kunnan $\mathbb{F}_{2^m}$ alkioista, tällöin matriisi

$$H_2 = \begin{bmatrix} \alpha_0 & \alpha_1 & \ldots & \alpha_{n-1} \\ \alpha_0^3 & \alpha_1^3 & \ldots & \alpha_{n-1}^3 \end{bmatrix} \tag{6.4}$$

on pituudeltaan $n = 2^m - 1$ olevan binäärisen kahden virheen korjaavan koodin pariteetintarkistusmatriisi. Ekvivalentisti $\mathbf{C} = (C_0, C_1, \ldots, C_{n-1}) \in V_n$ on koodisana koodissa, jonka pariteetintarkistusmatriisi on H_2 jos ja vain jos $\sum_{i=0}^{n} C_i\alpha_i = \sum_{i=0}^{n} C_i\alpha_i^3 = 0$. Koska kunnan $\mathbb{F}_2$ suhteen olevassa matriisissa H_2 on $2m$ lineaarisesti riippumatonta riviä (kun $m \geq 3$), niin koodin dimensio on vähintään $n - 2m = 2^m - 1 - 2m$.

Seuraava maineikas lause todistaa, että yhtälön (6.4) matriisi H_2 todellakin määrittelee kahden virheen korjaavan koodin. Lisäksi se antaa yleistyksen t virheen korjaaville koodeille.

LAUSE 6.5. *Olkoot $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ n keskenään erisuurta kunnan $\mathbb{F}_{2^m}$ alkiota. Lisäksi olkoon $t \leq (n-1)/2$ positiivinen kokonaisluku. Tällöin $t \times n$ -matriisi*

$$H = \begin{bmatrix} \alpha_0 & \alpha_1 & \ldots & \alpha_{n-1} \\ \alpha_0^3 & \alpha_1^3 & \ldots & \alpha_{n-1}^3 \\ \alpha_0^5 & \alpha_1^5 & \ldots & \alpha_{n-1}^5 \\ \vdots & & & \\ \alpha_0^{2t-1} & \alpha_1^{2t-1} & \ldots & \alpha_{n-1}^{2t-1} \end{bmatrix}$$

on binäärisen $[n, k]$-koodin pariteetintarkistusmatriisi. Lisäksi koodi korjaa kaikki korkeintaan painoltaan t olevat virhekuviot ja koodin dimensio on $k \geq n - mt$.

TODISTUS ([**6**, s. 232–233]). Vektori $\mathbf{C} = (C_0, \ldots, C_{n-1}) \in V_n$ on koodisana jos ja vain jos $H\mathbf{C}^T = 0$. Tämä vastaa seuraavaa t lineaarisen yhtälön systeemiä C_i:ssä:

$$\sum_{i=0}^{n-1} C_i\alpha_i^j = 0, \quad j = 1, 3, \ldots, 2t-1. \tag{6.5}$$

Neliöimällä j:s yhtälö saadaan $0 = \left(\sum C_i\alpha_i^j\right)^2 = \sum C_i^2\alpha_i^{2j} = \sum C_i\alpha_i^{2j}$ (koska $(x+y)^2 = x^2 + 2xy + y^2 = x^2 + y^2$ kunnan $\mathbb{F}_2$ suhteen ja $x^2 = x$ kunnassa $\mathbb{F}_2$). Siksi koodisanan ekvivalentti määritelmä on seuraava $2t$ yhtälön systeemi:

$$\sum_{i=0}^{n-1} C_i\alpha_i^j = 0, \quad j = 1, 2, \ldots, 2t. \tag{6.6}$$

Tästä seuraa, että voidaan yhtä hyvin käyttää koodin kuvaamisen $2t \times n$ -pariteetintarkistusmatriisia

$$H' = \begin{bmatrix} \alpha_0 & \alpha_1 & \ldots & \alpha_{n-1} \\ \alpha_0^2 & \alpha_1^2 & \ldots & \alpha_{n-1}^2 \\ \vdots & & & \\ \alpha_0^{2t} & \alpha_1^{2t} & \ldots & \alpha_{n-1}^{2t} \end{bmatrix}.$$

Lauseen 6.3 mukaan H on t virheen korjaavan koodin pariteetintarkistusmatriisi jos ja vain jos jokainen matriisin H' korkeintaan $2t$ sarakkeen osajoukko on lineaarisesti riippumaton. Nyt matriisin H' $r \leq 2t$ sarakkeen osajoukko on muodoltaan

$$B = \begin{bmatrix} \beta_1 & \ldots & \beta_r \\ \beta_1^2 & \ldots & \beta_r^2 \\ \vdots & & \\ \beta_1^{2t} & \ldots & \beta_r^{2t} \end{bmatrix},$$

missä $\beta_1, \beta_2, \ldots, \beta_r$ ovat nollasta eroavia keskenään erisuuria kunnan $\mathbb{F}_2$ alkioita. Tarkastellaan nyt matriisia B', joka on muodostettu β:n ensimmäisestä r rivistä:

$$B' = \begin{bmatrix} \beta_1 & \ldots & \beta_r \\ \vdots & & \\ \beta_1^r & \ldots & \beta_r^r \end{bmatrix},$$

Matriisi B' on kääntyvä, koska sen determinantti on vakiotekijää vaille Vandermonden determinantti

$$\begin{aligned} \det(B') &= \beta_1 \ldots \beta_r \det \begin{bmatrix} 1 & \ldots & 1 \\ \beta_1 & \ldots & \beta_r \\ \vdots & & \\ \beta_1^{r-1} & \ldots & \beta_r^{r-1} \end{bmatrix} \\ &= \beta_1 \ldots \beta_r \prod_{i<j} (\beta_j - \beta_i) \neq 0. \end{aligned}$$

Siksi matriisin B' sarakkeet, saati matriisin B, eivät voi olla lineaarisesti riippuvia, joten koodi korjaa kaikki enintään painon t virhekuviot. Rajan $k \geq n - mt$ varmistamiseksi dimension suhteen tulee huomioida, että alkuperäinen pariteetintarkistusmatriisi H, jonka alkiot ovat kunnasta $\mathbb{F}_2$ eikä kunnasta $\mathbb{F}_{2^m}$, on $mt \times n$ -matriisi. Tämä tarkoittaa sitä, että koodin duaalilla on korkeintaan dimensio mt. Tällöin koodin itsensä dimensio on vähintään $n - mt$. □

Lauseessa 6.5 kuvatut koodit ovat nimeltään *BCH-koodeja* keksijöidensä Bose, Ray-Chaudhuri ja Hocquenghem mukaan. Nämä koodit ovat tärkeitä, sillä niille löytyy tehokkaita koodaus- ja dekoodausalgoritmeja. Seuraavaksi huomataan, että jos alkiot $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ valitaan sopivassa järjestyksessä, niin BCH-koodeista tulee maagisesti syklisiä koodeja.

6.1. Sykliset BCH-koodit

Palautetaan mieliin n-pituisen ($n = 2^m - 1$) t-virheen korjaavan BCH-koodin määritelmä: $\mathbf{C} = (C_0, \ldots, C_{n-1})$ on koodisana jos ja vain jos $\sum_{i=0}^{n-1} C_i \alpha_i^j = 0$, kun $j = 1, 3, \ldots, 2t-1$ (ekvivalentisti, kun $j = 1, 2, 3, \ldots, 2t$) ja missä $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ ovat nollasta eroavia keskenään erisuuria kunnan $\mathbb{F}_{2^m}$ alkioita. Jos alkiot valitaan sopivasti, koodista tulee syklinen ja sille on voimassa kaikki syklisille koodeille sovellettavat koneistot. Nämä "sykliset" luettelot ovat muotoa

$$1, \alpha, \ldots, \alpha^{n-1},$$

missä n on luvun $2^m - 1$ tekijä ja α on kertalukua n oleva kunnan $\mathbb{F}_{2^m}$ alkio. Luettelon osalta määritelmäksi saadaan: $\mathbf{C} = (C_0, C_1, \ldots, C_{n-1})$ on koodisana jos ja vain jos

$$\sum_{i=0}^{n-1} C_i \alpha^{ij} = 0, \qquad \text{kun } j = 1, 3, \ldots, 2t-1 \quad (\text{tai } j = 1, 2, 3, \ldots, 2t). \tag{6.7}$$

Näin BCH-koodista on saatu syklinen. Tarkistetaan vielä tämä, joten olkoon koodisanaa $\mathbf{C}$ vastaava polynomi $C(x) = C_0 + C_1 x + \cdots + C_{n-1} x^{n-1}$. Tällöin yhtälö (6.7) saadaan muotoon

$$C(\alpha^j) = 0, \quad j = 1, 2, \ldots, 2t. \tag{6.8}$$

Olkoon sitten $\mathbf{C}^R$ koodisanan $\mathbf{C}$ syklinen siirto oikealle. Lauseen 5.6 mukaan sitä vastaava polynomi on $C^R(x) \equiv xC(x) \bmod (x^n - 1)$ eli $C^R(x) = xC(x)M(x)(x^n - 1)$, jollekin polynomille $M(x)$. Täten, kun $j = 1, 2, \ldots, 2t$, niin

$$C^R(\alpha^j) = \alpha^j C(\alpha^j) + M(\alpha^j)(a^{jn} - 1).$$

Mutta yhtälön (6.8) mukaan $C(\alpha^j) = 0$ ja $\alpha^{jn} - 1 = 0$ sillä $\alpha^n = 1$. Tästä seuraa, että $C^R(\alpha^j) = 0$, kun $j = 1, 2, \ldots, 2t$. Siis $\mathbf{C}^R$ on myös yhtälön (6.7) mukaisessa BCH-koodissa, mikä tarkoittaa sitä, että koodi on syklinen.

Nyt lauseesta 5.12 seuraa, että jokainen BCH-koodi voidaan karakterisoida sen virittäjäpolynomin $g(x)$ avulla. Miten sitten $g(x)$ lasketaan? Määritelmän mukaan $g(x)$ on koodin alinta astetta oleva polynomi, joka toteuttaa yhtälöt $g(\alpha) = g(\alpha^3) = \cdots = g(\alpha^{2t-1}) = 0$. Nyt polynomin $g(x)$ kertoimet ovat kunnassa $\mathbb{F}_2$, mutta eri α:n potenssit ovat suuremmassa kunnassa $\mathbb{F}_{2^m}$. Täten se on alkion α minimipolynomi kunnan $\mathbb{F}_2$ suhteen osajoukosta $A = \{\alpha, \alpha^3, \ldots, \alpha^{2t-1}\}$ kunnassa $\mathbb{F}_{2^m}$ (katso [**6**, Appendix C s. 375–379]). Täten, jos määritellään, että A^* on kaikki kunnan $\mathbb{F}_2$ konjugaatit joukon A alkioista eli $A^* = \{\beta^{2^i} : \beta \in A, i \geq 0\}$, tällöin

$$g(x) = \prod_{\beta \in A^*} (x - \beta). \tag{6.9}$$

Tiivistetään nämä tulokset lauseeksi.

Lause 6.6. *Olkoon n-pituinen t-virheen korjaava BCH-koodi määritelty kuten yhtälössä* (6.7) *tai* (6.8)*. Tällöin koodi on syklinen ja sen virittäjäpolynomi $g(x)$ muodostuu kaavan* (6.9) *mukaisesti. Täten koodin dimensio on $n - \deg g(x)$ eli $k = n - |A^*|$, missä A^* on joukon $A = \{\alpha, \alpha^3, \ldots, \alpha^{2t-1}\}$ konjugaattijoukko kunnan $\mathbb{F}_2$ suhteen kunnassa $\mathbb{F}_{2^m}$.* □

Esimerkki 6.7 ([**6**, s. 235]). Tarkastellaan 15-pituista kolmen virheen korjaavaa BHC-koodia. Olkoon α primitiivinen juuri kunnassa $\mathbb{F}_{16}$. Lauseen 6.6 mukaan virittäjäpolynomi on joukon $A = \{\alpha, \alpha^3, \alpha^5\}$ minimipolynomi. Konjugaatit ovat

$$\begin{aligned} \alpha &: (\alpha, \alpha^2, \alpha^4, \alpha^8), \\ \alpha^3 &: (\alpha^3, \alpha^6, \alpha^{12}, \alpha^9), \\ \alpha^5 &: (\alpha^5, \alpha^{10}). \end{aligned}$$

Siksi

$$A^* = \{\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^8, \alpha^9, \alpha^{10}, \alpha^{12}\},$$

jolloin Lauseen 6.6 mukaan koodin dimensio on $15 - 10 = 5$.

Virittäjäpolynomin laskemiseksi tälle esimerkille tarvitaan konkreettisempi toteutus kunnalle $\mathbb{F}_{16}$. Taulukossa 6.1 on esitetty kunta $\mathbb{F}_{16}$ primitiivisen juuren potenssien mukaan, mikä toteuttaa yhtälön $\alpha^4 = \alpha + 1$. Alkio α^j on esitetty polynomina, jonka aste on korkeintaan 3. Esimerkiksi $\alpha^{11} = \alpha^3 + \alpha^2 + \alpha$. Virittäjäpolynomi $g(x)$ on alkioiden α, α^3 ja α^5 minimipolynomien tulo. Määritelmän mukaan alkion α minimipolynomi on $x^4 + x + 1$. Alkion α^3 minimipolynomin $g_3(x) = g_{30} + g_{31}x + g_{32}x^2 + g_{33}x^3 + g_{34}x^4$ täytyy toteuttaa $g_3(\alpha^3) = 0$. Taulukosta 6.1 katsottuna tämä on ekvalenttia yhtälölle $g_{30}[0001] + g_{31}[1000] + g_{32}[1100] + g_{33}[1010] + g_{34}[1111] = [0000]$. Ainut epätriviaali ratkaisu tälle 4 joukon homogeenisille yhtälöille 5 tuntemattoman joukosta on $[g_{30}, g_{31}, g_{32}, g_{33}, g_{34}] = [11111]$. Siis $g_3 = x^4 + x^3 + x^2 + x + 1$. Vastaavasti

TAULUKKO 6.1. Kunta $\mathbb{F}_{16}$ esitettynä α:n potensseina, missä $\alpha^4 = \alpha + 1$.

i									α^i
0								1	0001
1					α				0010
2			α^2						0100
3	α^3								1000
4					α	$+$	1		0011
5			α^2	$+$	α				0110
6	α^3	$+$	α^2						1100
7	α^3			$+$	α	$+$	1		1011
8			α^2			$+$	1		0101
9	α^3			$+$	α				1010
10			α^2	$+$	α	$+$	1		0111
11	α^3	$+$	α^2	$+$	α				1110
12	α^3	$+$	α^2	$+$	α	$+$	1		1111
13	α^3	$+$	α^2			$+$	1		1101
14	α^3					$+$	1		1001

$g_5(x) = g_{50} + g_{51}x + g_{52}x^2 = \cdots = x^2 + x + 1$. Täten 15-pituisen kolmen virheen korjaavan BCH-koodin virittäjäpolynomi on $g(x) = (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1) = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1$. Vastaavasti pariteetintarkistuspolynomi on $h(x) = (x^{15} + 1)/g(x) = x^5 + x^3 + x + 1$ (Katso Liite (B)). Korostettakoon vielä, että $g(x)$ riippuu Taulukon 6.1 kunnan $\mathbb{F}_{16}$ esityksestä $\alpha^4 = \alpha + 1$.

6.2. BCH-koodin dekoodaus: avainyhtälö

Tässä luvussa käsitellään niin sanottua *avainyhtälöä*, joka on perusta BCH-koodien dekoodaamisen algoritmille. Olkoon siis F kunta, jolla on primitiivinen n:s yksikköjuuri α. Todetaan ensin, että

$$1 - x^n = \prod_{i=0}^{n-1} (1 - \alpha^i x). \tag{6.10}$$

Yhtälön (6.10) molemmin puolin polynomeilla on aste n, vakiotermi 1 ja juuret α^{-i}, kun $i = 0, 1, \ldots, n-1$. Olkoon

$$\mathbf{V} = (V_0, V_1, \ldots, V_{n-1})$$

n-dimensioinen vektori kunnan F suhteen ja olkoon

$$\hat{\mathbf{V}} = (\hat{V}_0, \hat{V}_1, \ldots, \hat{V}_{n-1})$$

sen *diskreetti Fourier'n muunnos* (discrete Fourier transform, DFT), jonka komponentit määritellään seuraavasti:

$$\hat{V}_j = \sum_{i=0}^{n-1} V_i \alpha^{ij}, \quad \text{kun } j = 0, 1, \ldots, n-1. \tag{6.11}$$

Toisinaan vektorin $\mathbf{V}$ vektoreita V_i kutsutaan ”aika-akselin” ja vektoreita $\hat{V}_j$ ”taajuusakselin” koordinaateiksi. Aika-akselin komponentit saadaan taajuusakselin komponenteista niin kutsutun *Fourier'n käänteismuunnoksen* (inverse DFT, IDFT) avulla:

$$V_i = \frac{1}{n}\sum_{j=0}^{n-1} \hat{V}_j \alpha^{-ij}, \quad \text{kun } i = 0, 1, \ldots, n-1. \tag{6.12}$$

Yhtälössä (6.12) summan edessä oleva tekijä $\frac{1}{n}$ täytyy tulkita huolellisesti kunnan F mahdollisen äärellisen karakteristikan näkökulmasta. Numero ”n” on summa $1 + 1 + \cdots + 1$ (n termiä) ja ”$1/n$” on tämän luvun käänteisluku. Esimerkiksi, jos kunnan F karakteristika on 2 ja n on pariton, tällöin $1/n = 1$. Jos vektoreiden $\mathbf{V}$ ja $\hat{\mathbf{V}}$ komponentit tulkitaan polynomien kertoimina eli jos määritellään polynomit $V(x)$ ja $\hat{V}(x)$

$$V(x) = V_0 + V_1 x + \cdots + V_{n-1}x^{n-1} \tag{6.13}$$

ja

$$\hat{V}(x) = \hat{V}_0 + \hat{V}_1 x + \cdots + \hat{V}_{n-1}x^{n-1}, \tag{6.14}$$

niin tällöin Fourier'n muunnoksen ja käänteismuunnoksen yhtälöt (6.11) ja (6.12) saavat muodon

$$\hat{V}_j = V(\alpha^j) \tag{6.15}$$

ja

$$V_i = \frac{1}{n}\hat{V}(\alpha^{-i}). \tag{6.16}$$

Annetulle vektorille on monia mielenkiintoisia ja käytännöllisiä yhteyksiä aika-akselin ja taajuusakselin koordinaattien välillä. Eräs niistä on se, että ”vaihesiirto” aika-akselissa vastaa ”aikasiirtoa” taajuusakselissa seuraavalla tavalla. Jos kerrotaan $\alpha^{\mu i}$:lla vektorin $\mathbf{V}$ i:nnettä komponenttia eli, jos määritellään uusi vektori

$$\mathbf{V}_\mu = (V_0, V_1\alpha^\mu, \ldots, V_{n-1}\alpha^{\mu(n-1)}), \tag{6.17}$$

niin sen Fourier'n muunnos on

$$\hat{\mathbf{V}}_\mu = (\hat{V}_\mu, \hat{V}_{\mu+1}, \ldots, \hat{V}_{\mu+n-1}), \tag{6.18}$$

missä yhtälön (6.18) alaindeksit ovat modulo n.

Koodausteoriassa ollaan aina kiinnostuneita vektorin *painosta*. Seuraava klassinen lause kertoo kuinka arvioida aika-akselin painoa, jos tiedetään jotakin taajuusakselin vektorista.

Lause 6.8 (BCH-väite). *Olkoon* $\mathbf{V}$ *nollasta eroava vektori, jonka Fourier'n muunnoksen* $\hat{\mathbf{V}}$ *m peräkkäistä komponenttia häviävät eli* $\hat{V}_{j+1} = \hat{V}_{j+2} = \cdots = \hat{V}_{j+m} = 0$. *Tällöin vektorin* $\mathbf{V}$ *paino on vähintään* $m + 1$.

Todistus ([**6**, s. 238–239]). Tehdään vektorille $\hat{\mathbf{V}}$ syklinen kierto, kunnes sen m kappaletta peräkkäin olevat nollat ovat positioissa $n-m, n-m+1, \ldots, n-1$. Merkitään tätä vektoria

$$\hat{\mathbf{W}} = \Big[*\ \ *\ \ \ldots\ \ * \ \overbrace{0\ 0\ \ldots\ 0}^{m} \Big].$$

Yhtälöiden (6.17) ja (6.18) mukaan $\hat{\mathbf{W}}$ on vektorin $\mathbf{W}$ Fourier'n muunnos. Lisäksi vektorin $\mathbf{W}$ paino on yhtä suuri kuin vektorin $\mathbf{V}$ paino. Toisaalta yhtälön (6.12) mukaan $W_i = \frac{1}{n}\hat{W}(\alpha^{-i})$, missä $\hat{W}(x) = \hat{W}_0 + \hat{W}_1 x + \cdots + \hat{W}_{n-m-1}x^{n-m-1}$. Koska $\hat{W}(x)$ on nollasta eroava polynomi ja sen aste on korkeintaan $n-m-1$, niin tästä seuraa, että $W_i = 0$ korkeintaan $n-m-1$ i:n arvolla. Täten $W_i \neq 0$ vähintään $m+1$ i:n arvolla. Täten $w(\mathbf{V}) = w(\mathbf{W}) \geq m+1$. □

Tarvitaan vielä muutama määritelmä, jotta voidaan ottaa käyttöön avainyhtälö. Vektorin $\mathbf{V}$ ollessa kiinnitetty, määritellään sen *kantaja* I seuraavasti:

$$I = \{i : 0 \leq i \leq n-1 \text{ ja } V_i \neq 0\}. \tag{6.19}$$

Määritellään seuraavaksi vektoriin $\mathbf{V}$ liittyviä useita polynomeja. Vektorin $\mathbf{V}$ *virheen-paikannuspolynomi* on

$$\sigma_{\mathbf{V}}(x) = \prod_{i \in I}(1 - \alpha^i x). \tag{6.20}$$

Jokaiselle $i \in I$ arvolle määritellään

$$\begin{aligned} \sigma_{\mathbf{V}}^{(i)}(x) &= \sigma_{\mathbf{V}}(x)/(1-\alpha^i x) \\ &= \prod_{\substack{j \in I \\ j \neq i}}(1-\alpha^j x). \end{aligned} \tag{6.21}$$

Lopuksi määritellään vektorin $\mathbf{V}$ *virhearvopolynomi*

$$\omega_{\mathbf{V}}(x) = \sum_{i \in I} V_i \sigma_{\mathbf{V}}^{(i)}(x). \tag{6.22}$$

Nyt esitellään "avainyhtälö".

Lause 6.9 (Avainyhtälö). *Kiinnitetylle vektorille* $\mathbf{V}$*, polynomeille* $\hat{V}(x)$*,* $\sigma_{\mathbf{V}}(x)$ *ja* $\omega_{\mathbf{V}}(x)$ *on voimassa*

$$\sigma_{\mathbf{V}}(x)\hat{V}(x) = \omega_{\mathbf{V}}(x)(1-x^n). \tag{6.23}$$

Todistus ([**6**, s. 240]). Käytetään määritelmiä (6.11) ja (6.14) jolloin saadaan

$$\begin{aligned} \hat{V}(x) &\overset{(6.14)}{=} \hat{V}_0 + \hat{V}_1 x + \cdots + \hat{V}_{n-1}x^{n-1} \\ &= \sum_{j=0}^{n-1} \hat{V}_j x^j \overset{(6.11)}{=} \sum_{j=0}^{n-1} x^j \sum_{i=0}^{n-1} V_i \alpha^{ij} \\ &= \sum_{i \in I} V_i \sum_{j=0}^{n-1} x^j \alpha^{ij}. \end{aligned} \tag{6.24}$$

Yhtälön (6.21) mukaan $\sigma_{\mathbf{V}}(x) = \sigma_{\mathbf{V}}^{(i)}(x)(1-\alpha^i x)$ kaikilla $i \in I$ ja näin yhtälöstä (6.24) saadaan

$$\begin{aligned}\sigma_{\mathbf{V}}(x)\hat{V}(x) &\overset{(6.21)}{=} \sum_{i\in I} V_i \sigma_{\mathbf{V}}^{(i)}(x)(1-\alpha^i x)\sum_{j=0}^{n-1} x^j \alpha^{ij} \\ &= \sum_{i\in I} V_i \sigma_{\mathbf{V}}^{(i)}(x)(1-\alpha^i x)(1+\alpha^i x+\alpha^{2i}x^2+\cdots+\alpha^{(n-1)i}x^{n-1}).\end{aligned}$$

Tarkastellaan nyt pelkästään lopun kertolaskua ja miten se supistuu. Muistetaan, että yksikköjuurelle pätee $\alpha^n = 1$:

$$\begin{aligned}&(1-\alpha^i x)(1+\alpha^i x+\alpha^{2i}x^2+\cdots+\alpha^{(n-1)i}x^{n-1}) \\ \Leftrightarrow &(1-\cancel{\alpha^i x}+\cancel{\alpha^i x}-\cancel{\alpha^{2i}x^2}+\cancel{\alpha^{2i}x^2}-\cdots-\cancel{\alpha^{(n-1)i}x^{n-1}}+\cancel{\alpha^{(n-1)i}x^{n-1}}-\underbrace{\overbrace{\alpha^{(n-1)i+i}}^{=ni}}_{=(\alpha^n)^i=1^i=1}x^n) \\ \Leftrightarrow &(1-x^n).\end{aligned}$$

Näin ollen määritelmän (6.22) avulla saadaan

$$\begin{aligned}\sigma_{\mathbf{V}}(x)\hat{V}(x) &= \sum_{i\in I} V_i \sigma_{\mathbf{V}}^{(i)}(x)(1-x^n) \\ &\overset{(6.22)}{=} \omega_{\mathbf{V}}(x)(1-x^n).\end{aligned}$$

□

Seuraava Lauseen 6.8 seuraus kertoo kuinka muodostaa vektorin $\mathbf{V}$ nollasta eroavat komponentit polynomien $\sigma_{\mathbf{V}}(x)$ ja $\omega_{\mathbf{V}}(x)$ avulla. Se sisältää polynomin $\sigma_{\mathbf{V}}(x)$ formaalin derivaatan $\sigma'_{\mathbf{V}}(x)$.

Seuraus 6.10. *Kaikilla $i \in I$ pätee*

$$V_i = -\alpha^i \frac{\omega_{\mathbf{V}}(\alpha^{-i})}{\sigma'_{\mathbf{V}}(\alpha^{-i})}. \tag{6.25}$$

Todistus ([**6**, s. 240]). Derivoidaan avainyhtälö (6.23) ja saadaan

$$\sigma_{\mathbf{V}}(x)\hat{V}'(x) + \sigma'_{\mathbf{V}}(x)\hat{V}(x) = \omega_{\mathbf{V}}(x)(-nx^{n-1}) + \omega'_{\mathbf{V}}(x)(1-x^n). \tag{6.26}$$

Jos $x = \alpha^{-i}$ ja $i \in I$, niin yhtälöistä (6.20) ja (6.10) havaitaan, että molemmat polynomit $\sigma_{\mathbf{V}}$ ja $1-x^n$ häviävät. Täten, jos $x = \alpha^{-i}$, niin yhtälö (6.26) saa muodon

$$\sigma'_{\mathbf{V}}(\alpha^{-i})\hat{V}(\alpha^{-i}) = -n\alpha^i \omega_{\mathbf{V}}(\alpha^{-i}). \tag{6.27}$$

Mutta yhtälön (6.16) mukaan $\hat{V}(\alpha^{-i}) = nV_i$. Tämä yhdistettynä yhtälöön (6.27) täydentää todistuksen. □

Seurauksen 6.10 mukaan vektorin $\mathbf{V}$ aika-akselin koordinaatit voidaan palauttaa polynomien $\sigma_{\mathbf{V}}(x)$ ja $\omega_{\mathbf{V}}(x)$ avulla. Seuraavan seurauksen mukaan, jos vektorin $\mathbf{V}$ muutamat ensimmäiset taajuusakselin koordinaatit tunnetaan, niin yksinkertaisen

rekursion avulla saadaan palautettua loput koordinaatit polynomista $\sigma_{\mathbf{V}}(x)$. Seurauksen väitteessä oletetaan, että polynomin $\sigma_{\mathbf{V}}(x)$ kertoimet ovat

$$\sigma_{\mathbf{V}}(x) = 1 + \sigma_1 x + \cdots + \sigma_d x^d.$$

SEURAUS 6.11. *Kaikille indekseille j pätee*

$$\hat{V}_j = -\sum_{i=1}^{d} \sigma_i \hat{V}_{j-i}, \tag{6.28}$$

missä kaikki alaindeksit tulkitaan modulo n.

TODISTUS ([**6**, s. 241]). Avainyhtälöstä seuraa, että

$$\sigma_{\mathbf{V}}(x)\hat{V}(x) \equiv 0 \bmod (1 - x^n). \tag{6.29}$$

Muuttujan x^j kerroin polynomissa $\sigma_{\mathbf{V}}(x)\hat{V}(x) \operatorname{rem} (1 - x^n)$ on nolla, kun j on välillä $0 \leq j \leq n-1$. Mutta tämä kerroin on $\sum_{i=0}^{d} \sigma_i \hat{V}_{(j-i) \operatorname{rem} n}$, jolloin kaikille j välillä $0 \leq j \leq n-1$ pätee

$$\sum_{i=0}^{d} \sigma_i \hat{V}_{j-i} = 0, \tag{6.30}$$

missä alaindeksit tulkitaan modulo n ja $\sigma_0 = 1$. Mutta nyt yhtälö (6.30) on ekvivalentti yhtälön (6.28) kanssa. □

ESIMERKKI 6.12 ([**6**, s. 241–242]). Havainnollistetaan aiempaa teoriaa kunnan $\mathbb{F}_{16}$ avulla. Siinä nollasta eroavat alkiot ovat primitiivisen juuren α potensseja, joille valitaan esitys $\alpha^4 = \alpha + 1$. Tarkastellaan vektoria

$$\mathbf{V} = (0, 0, \alpha^2, 0, 0, 0, 0, \alpha^7, 0, 0, 0, 0, 0, 0, 0).$$

Tällöin yhtälön (6.13) mukainen polynomi $V(x)$ on

$$V(x) = \alpha^2 x^2 + \alpha^7 x^7.$$

Lasketaan vektorin $\mathbf{V}$ Fourier'n muunnos käyttäen yhtälöä (6.11) tai (6.15):

$$\hat{\mathbf{V}} = (\alpha^{12}, \alpha^9, 0, \alpha^3, 1, 0, \alpha^9, \alpha^6, 0, 1, \alpha^{12}, 0, \alpha^6, \alpha^3, 0).$$

Polynomi $\hat{V}(x)$ saadaan yhtälön (6.14) mukaisesti

$$\begin{aligned}
\hat{V}(x) &= \alpha^{12} + \alpha^9 x + \alpha^3 x^3 + x^4 + \alpha^9 x^6 + \alpha^6 x^7 + x^9 + \alpha^{12} x^{10} + \alpha^6 x^{12} + \alpha^3 x^{13} \\
&= (\alpha^{12} + \alpha^9 x)(1 + \alpha^6 x^3 + \alpha^{12} x^6 + \alpha^3 x^9 + \alpha^9 x^{12}) \\
&= (\alpha^{12} + \alpha^9 x)\frac{1 + x^{15}}{1 + \alpha^6 x^3} \\
&= \alpha^{12}\frac{1 + x^{15}}{1 + \alpha^{12} x + \alpha^9 x^2}. \qquad (6.31)
\end{aligned}$$

Vektorin $\mathbf{V}$ kantaja on $I = \{2, 7\}$ ja tällöin vektorin $\mathbf{V}$ virheenpaikannuspolynomi on

$$\sigma_{\mathbf{V}}(x) = (1 + \alpha^2 x)(1 + \alpha^7 x) = 1 + \alpha^{12} x + \alpha^9 x^2. \tag{6.32}$$

Yhtälön (6.21) mukaiset polynomit $\sigma_{\mathbf{V}}^{(i)}(x)$ ovat tässä tapauksessa

$$\sigma_{\mathbf{V}}^{(2)}(x) = 1 + \alpha^7 x, \quad \sigma_{\mathbf{V}}^{(7)}(x) = 1 + \alpha^2 x.$$

Yhtälön (6.22) virhearvopolynomi $\omega_{\mathbf{V}}(x)$ on

$$\omega_{\mathbf{V}}(x) = \alpha^2(1+\alpha^7 x) + \alpha^7(1+\alpha^2 x) = \alpha^{12}. \tag{6.33}$$

Yhdistämällä tulokset (6.31), (6.32) ja (6.33) huomataan, että avainyhtälö on todella voimassa tässä tapauksessa. Seurauksen 6.10 tarkistamiseksi on huomattava, että yhtälöstä (6.32) saadaan $\sigma'_{\mathbf{V}}(x) = \alpha^{12} = \omega_{\mathbf{V}}(x)$. Näin Seuraus 6.10 yksinkertaistuu muotoon $V_i = \alpha^i$ kaikilla $i \in I$, mikä on totta ($V_2 = \alpha^2$ ja $V_7 = \alpha^7$). Lopuksi on hyvä huomata, että Seurauksen 6.11 mukaan

$$\hat{V}_j = \alpha^{12}\hat{V}_{j-1} + \alpha^9\hat{V}_{j-2}, \quad j = 2, 3, \ldots, 14,$$

jolloin (alkuehdoilla $\hat{V}_0 = \alpha^{12}$ ja $\hat{V}_1 = \alpha^9$)

$$\begin{aligned}
\hat{V}_2 &= \alpha^{12}\cdot\alpha^9 + \alpha^9\cdot\alpha^{12} = 0,\\
\hat{V}_3 &= \alpha^{12}\cdot 0 + \alpha^9\cdot\alpha^9 = \alpha^3,\\
\hat{V}_4 &= \alpha^{12}\cdot\alpha^3 + \alpha^9\cdot 0 = 1,\\
&\vdots\\
\hat{V}_{14} &= \alpha^{12}\cdot\alpha^3 + \alpha^9\cdot\alpha^6 = 0,
\end{aligned}$$

mikä on sama tulos kuin aiemmin suoritettu suora lasku vektorille $\hat{\mathbf{V}}$.

6.2.1. BCH-avainyhtälö. Olkoon $\mathbf{C} = (C_0, C_1, \ldots, C_{n-1})$ n-pituisen t-virheen korjaavan BCH-koodin koodisana, kuten yhtälössä (6.6). Lähetetään tämä kohinaista kanavaa pitkin ja vastaanotetaan sana $\mathbf{R} = (R_0, R_1, \ldots, R_{n-1})$. Oletetaan jälleen, että kyseessä on binäärinen koodi eli se koostuu kunnan $\mathbb{F}_2$ alkioista 0 ja 1. Vektori $\mathbf{E} = (E_0, E_1, \ldots, E_n) = \mathbf{R} - \mathbf{C}$ on nimeltään *virhekuvio*. Dekoodaaja laskee *syndroomat* $S_1, S_2, \ldots, S_{2t}$ määritelmän mukaisesti:

$$S_j = \sum_{i=0}^{n-1} R_i\alpha^{ij}, \quad j = 1, 2, \ldots, 2t. \tag{6.34}$$

Koska $\mathbf{R} = \mathbf{C} + \mathbf{E}$ ja $\mathbf{C}$ on koodisana, niin

$$S_j = \sum_{i=0}^{n-1} E_i\alpha^{ij}, \quad j = 1, 2, \ldots, 2t. \tag{6.35}$$

Kuten odotettua, syndrooma riippuu ainoastaan virhekuviosta eikä lähetetystä koodisanasta. Jos verrataan yhtälöä (6.35) yhtälöön (6.11) huomataan, että S_j on Fourier'n muunnoksen virhekuvion j:s komponentti. Toisin sanoen syndrooman avulla nähdään vektorin $\hat{\mathbf{E}}$ peräkkäiset $2t$ komponenttia (ensimmäinen, toinen, …, $2t$:s). Jos määritellään *vääristynyt virhekuvio*

$$\mathbf{V} = (E_0, E_1\alpha, E_2\alpha^2, \ldots, E_{n-1}\alpha^{n-1}), \tag{6.36}$$

niin yhtälöistä (6.17) ja (6.18) seuraa, että $(S_1, S_2, \ldots, S_{2t}) = (\hat{V}_0, \hat{V}_1, \ldots, \hat{V}_{2t-1})$.

Avainyhtälö koskee yhtälössä (6.36) määriteltyä vektoria $\mathbf{V}$. Kuitenkin, koska tiedetään vain ensimmäiset $2t$ polynomin $\hat{V}(x)$ kerrointa eli $\hat{V}_0, \hat{V}_1, \ldots, \hat{V}_{2t-1}$, voidaan keskittyä modulo x^{2t} supistettuun avainyhtälöön eli *BCH-avainyhtälöön*:

$$\sigma_{\mathbf{V}}(x)\hat{V}(x) \equiv \omega_{\mathbf{V}}(x) \bmod x^{2t}. \tag{6.37}$$

Yhtälöistä (6.19) ja (6.36) havaitaan, että vektorin $\mathbf{V}$ kantaja I on indeksijoukko $E_i \neq 0$, toisin sanoen *virhepaikkojen* joukko. Tästä syystä yhtälön (6.37) polynomia $\sigma_{\mathbf{V}}(x)$ kutsutaan nimellä *virheenpaikannuspolynomi*. Vastaavasti polynomi $\omega_{\mathbf{V}}(x)$ on nimeltään *virhearvopolynomi*.

On hyvä huomata, että jos vastaanotetun sanan $\mathbf{R}$ syndrooman tai ekvivalentisti $\hat{V}(x)$ modulo x^{2t} avulla voitaisiin jotenkin "ratkaista" BCH-avainyhtälö (6.37) polynomien $\sigma_{\mathbf{V}}(x)$ ja $\omega_{\mathbf{V}}(x)$ suhteen, niin tällöin voitaisiin helposti palauttaa virhekuvio $\mathbf{E}$ ja lähetetty koodisana $\mathbf{C} = \mathbf{R} - \mathbf{E}$. Laskettaisiin vain ensin n kappaletta arvoja $\sigma_{\mathbf{V}}(\alpha^{-i})$ jokaisella $i = 0, 1, \ldots, n-1$, josta saataisiin yhtälön (6.19) vektorin $\mathbf{V}$ kantaja I. Tämän jälkeen vektorin $\mathbf{V}$ nollasta eroavat komponentit voitaisiin laskea yhtälöstä (6.25), jolloin saataisiin koko vektori $\mathbf{V}$ tai ekvivalentisti $\mathbf{E}$ (6.36). Vaihtoehtoisesti, jos tiedettäisiin mitä on $(\hat{V}_0, \hat{V}_1, \ldots, \hat{V}_{2t-1})$, voitaisiin laskea vektori $\hat{\mathbf{V}}$ yhtälöstä (6.28) ja palauttaa Fourier'n käänteismuunnoksen avulla vektori $\mathbf{V}$.

LIITE A

Merkintöjä

Merkintä	*Selitys*
$\mathbb{Z}_q$	Lukujoukko $\{0, 1, 2, 3, \ldots, q-1\}$
F_q	q-äärinen avaruus
$(F_q)^n$	q-äärinen avaruus, joka koostuu n-pituisista alkioista
$d(\mathbf{x}, \mathbf{y})$	Kahden koodisanan $\mathbf{x}$ ja $\mathbf{y}$ välinen (Hammingin) etäisyys
$d(C)$	Koodin minimietäisyys
$\lfloor x \rfloor$	Lattiafunktio, missä x pyöristyy alaspäin lähimpään kokonaislukuun
(n, M, d)-koodi	Yleinen merkintä (n, M, d)-koodille, missä n on sanan pituus, M sanamäärä ja d sanojen välinen minimietäisyys
$A_q(n, d)$	q-äärisen koodin koodisanojen suurin lukumäärä etäisyydellä d ja pituudella n
$[k]_m$	Luvun $k \in \mathbb{Z}$ jäännösluokka modulo m
$F[x]$	F-kertoimisten polynomien joukko kunnan F suhteen
$\deg f(x)$	Polynomin $f(x)$ aste
$\mathbb{F}_q$	q-alkioinen äärellinen kunta
$\mathrm{GF}(q)$	Galois'n kunta, sama kuin $\mathbb{F}_q$
$\mathbb{F}_q^n$	Kaikki järjestetyt n-jonot joukosta $\mathbb{F}_q$
$[n, k]$-koodi	n-pituinen lineaarinen koodi, jonka dimensio on k
$w(\mathbf{x})$	Vektorin $\mathbf{x} \in F_q^n$ paino
$w(C)$	Koodin C nollasta eroavien koodisanojen pienin paino
$C^\perp$	Koodin C duaali
$\mathbf{C}^R$	Koodisanan $\mathbf{C}$ syklinen siirto oikealle
$C^R(x)$	Koodisanaa $\mathbf{C}^R$ vastaava polynomi
$\sum_{i=0}^{n-1} a_i$	Summa: $a_0 + a_1 + \cdots + a_{n-1}$
$\prod_{i=0}^{n-1} a_i$	Tulo: $a_0 \cdot a_1 \cdots a_{n-1}$

LIITE B

Polynomien jakolaskuja

Sivu 45:

$$
\begin{array}{r|l}
 & x^2 - x + 1 \\
\hline
x^4 + x^3 + x^2 + 1 & x^6 + x^4 \\
 & -x^6 - x^5 - x^4 - x^2 \\
\hline
 & -x^5 - x^2 \\
 & x^5 + x^4 + x^3 + x \\
\hline
 & x^4 + x^3 - x^2 + x \\
 & -x^4 - x^3 - x^2 - 1 \\
\hline
 & -2x^2 + x - 1
\end{array}
$$

Jakojäännös on siis $-2x^2 + x - 1 = x + 1$ kunnan $\mathbb{F}_2$ suhteen.

Sivut 45 ja 53:

$$
\begin{array}{r|l}
 & x^2 - 1 \\
\hline
x^4 + x^3 + x^2 + 1 & x^6 + x^5 + x^2 + 1 \\
 & -x^6 - x^5 - x^4 - x^2 \\
\hline
 & -x^4 + 1 \\
 & x^4 + x^3 + x^2 + 1 \\
\hline
 & x^3 + x^2 + 2
\end{array}
$$

Jakojäännös on siis $x^3 + x^2 + 2 = x^3 + x^2$ kunnan $\mathbb{F}_2$ suhteen.

Sivu 53:

$$
\begin{array}{r|l}
 & 1 \\
\hline
x^4 + x^3 + x^2 + 1 & x^4 + x^3 \\
 & -x^4 - x^3 - x^2 - 1 \\
\hline
 & -x^2 - 1
\end{array}
$$

Jakojäännös on siis $-x^2 - 1 = x^2 + 1$ kunnan $\mathbb{F}_2$ suhteen.

$$
\begin{array}{r|l}
 & 1 \\
\hline
x^4 + x^3 + x^2 + 1 & x^4 + x^2 \\
 & -x^4 - x^3 - x^2 - 1 \\
\hline
 & -x^3 - 1
\end{array}
$$

Jakojäännös on siis $-x^3 - 1 = x^3 + 1$ kunnan $\mathbb{F}_2$ suhteen.

$$
\begin{array}{r|l}
 & 1 \\
\hline
x^4+x^3+x^2+1 & x^4 \qquad\quad +x \\
 & -x^4-x^3-x^2 \quad -1 \\
\hline
 & -x^3-x^2+x-1
\end{array}
$$

Jakojäännös on siis $-x^3-x^2+x-1 = x^3+x^2+x+1$ kunnan $\mathbb{F}_2$ suhteen.

$$
\begin{array}{r|l}
 & 1 \\
\hline
x^4+x^3+x^2+1 & x^4+x^3+x^2+x \\
 & -x^4-x^3-x^2 \quad -1 \\
\hline
 & x-1
\end{array}
$$

Jakojäännös on siis $x-1 = x+1$ kunnan $\mathbb{F}_2$ suhteen.

Sivu 60: Lasku löytyy seuraavalta sivulta. Pariteetintarkistuspolynomi $h(x) = (x^{15}+1)/(x^{10}+x^8+x^5+x^4+x^2+x+1) = x^5-x^3+x-1 = x^5+x^3+x+1$. Jakojäännös on siis $-2x^9+2x^8-2x^6+2x^4+2 = 0$ kunnan $\mathbb{F}_2$ suhteen.

$$
\begin{array}{r|l}
 & x^5 \quad - x^3 \quad + x - 1 \\
\hline
x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1 & \\
\cline{1-1}
- x^{15} & + x^5 \quad + 1 \\
- x^{15} - x^{13} \quad - x^{10} \quad - x^9 \quad - x^7 \quad - x^6 - x^5 & \\
\cline{1-1}
- x^{13} \quad - x^{10} \quad - x^9 \quad - x^7 \quad - x^6 - x^5 & \\
x^{13} + x^{11} \quad + x^8 + x^7 \quad + x^5 \quad + x^4 + x^3 & \\
\cline{1-1}
x^{11} - x^{10} \quad - x^9 \quad + x^8 \quad - x^6 \quad + x^4 + x^3 & \\
- x^{11} \quad - x^9 \quad - x^6 - x^5 \quad - x^3 - x^2 - x & \\
\cline{1-1}
- x^{10} - 2x^9 \quad + x^8 \quad - 2x^6 - x^5 \quad + x^4 \quad - x^2 - x + 1 & \\
x^{10} \quad + x^8 \quad + x^5 \quad + x^4 \quad + x^2 + x + 1 & \\
\cline{1-1}
- 2x^9 + 2x^8 \quad - 2x^6 \quad + 2x^4 \quad + 2 &
\end{array}
$$

Kirjallisuutta

[1] Andries Brouwer. Eindhoven, 2019. *Table of general binary codes.* Elektroninen dokumentti osoitteessa https://www.win.tue.nl/∼aeb/codes/binary-1.html (luettu 7.7.2020).

[2] Raymond Hill: *A First Course in Coding Theory.* Oxford: Clarendon, 1986.

[3] Ari Lehtonen: *Äärelliset kunnat.* Jyväskylä, 2013. Kurssin MATS241 luentomonisteen luku *Olemassaolo ja yksikäsitteisyys* osoitteessa http://users.jyu.fi/∼lehtonen/opetus/sl2013/ (luettu 10.2.2021).

[4] San Ling ja Chaoping Xing: *Coding Theory: A First Course.* Cambridge, UK. New York: Cambridge University Press, 2004.

[5] Mars Moons. 2011. Kuvagalleria Marsin kuista osoitteessa http://marsmoons.blogspot.com/2011/04/mars-moons-gallery.html (luettu 4.7.2020).

[6] Robert J. McEliece: *The Theory of Information and Coding.* Toinen laitos. Cambridge: Cambridge University Press, 2002.

[7] NASA Science. Solar System Exploration. *Mariner 9.* 2019. Nettiartikkeli osoitteessa https://solarsystem.nasa.gov/missions/mariner-09/in-depth/ (luettu 4.7.2020).

[8] Steven Roman: *Introduction to Coding and information Theory.* New York: Springer, 1997.

[9] Victor Shoup: *A Computational introduction to number theory and algebra*, toinen laitos, Cambridge University Press, 2008. http://www.shoup.net/ntb (luettu 12.2.2021).

[10] Henk C.A. van Tilborg: *Coding Theory - A First Course.* Eindhoven University of Technology, 1993.