Laajennetut Preparata-koodit

Pro gradu -tutkielma

Petri Eklund

1512717

Matemaattisten tieteiden laitos

Oulun yliopisto

Kevät 2016

Sisältö

Johdanto

Tässä Pro gradu tutkielmassa käsitellään laajennettuja Preparata-koodeja. Tutkielman alussa esitetään yleisiä koodausteorian käsitteitä ja perustuloksia sekä äärellisiä kuntia koskevia tuloksia, jotka toimivat esitietoina tutkielman varsinaiselle aiheelle. Lukijan oletetaan tuntevan ryhmiin, renkaisiin ja kuntiin liittyvät määritelmät ja peruskäsitteet sekä äärellisten kuntien perusteet.

Tutkielman ensimmäisessä luvussa kerrotaan, mitä tarkoitetaan koodausteorialla ja minkälaisia sovelluskohteita sillä on. Luvussa esitellään tiedonvälitysjärjestelmän peruskäsitteet sekä äärellisiä kuntia koskevia perustuloksia.

Toisessa luvussa esitetään tutkielman pääaiheen käsittelyssä tarvittavat määritelmät ja tulokset. Näitä ovat lineaarisiin koodeihin liittyvät määritelmät ja perustulokset, syklisten koodien perusteet sekä BCH-koodit.

Kolmannessa luvussa on tutkielman keskeinen teoria. Luvussa esitetään laajennettujen Preparata-koodien määritelmä sekä useita koodeja koskevia tuloksia, joiden avulla voidaan mm. muodostaa uusia koodisanoja tunnettujen koodisanojen avulla. Lisäksi luvussa osoitetaan laajennetut Preparata-koodit etäisyysinvarianteiksi sekä löydetään niiden minimietäisyys, joka on 6. Tästä tuloksesta saadaan selville myös koodin virheenkorjauskyky. Luvun päätuloksena osoitetaan, että laajennetut Preparata-koodit ovat epälineaarisia.

Loppuosa tutkielmasta keskittyy laajennettujen Preparata-koodien koodaukseen ja dekoodaukseen. Neljännessä ja viidennessä luvussa esitetään algoritmit viestisanan koodaamiseksi koodisanaksi sekä vastaanotetun koodisanan dekoodaus takaisin viestisanaksi sekä esimerkit näistä. Koodausalgoritmin yhteydessä saadaan myös selville laajennettujen Preparata-koodien koodisanojen lukumäärä. Dekoodausalgoritmi puolestaan sisältää menetelmän enintään kahden koodisanassa esiintyvän virheen korjaamiseksi.

Luku 1

Esitietoja

1.1 Yleistä

Koodausteorian taustalla voidaan ajatella olevan yksinkertainen tiedonsiirtojärjestelmä, joka koostuu kolmesta osasta: tietolähteestä, tiedonsiirtokanavasta ja tiedon vastaanottajasta. Tietolähde lähettää tiedonsiirtokanavaan viestin. Kanava voi aiheuttaa virheitä lähetettyyn viestiin. Koska vastaanottaja ei voi tietää kanavaan lähetettyä viestiä, on hänen pystyttävä tulkitsemaan viesti kanavasta vastaanotetun viestin perusteella, vaikka siinä olisi virheitä.

Virheenkorjauksen mahdollistamiseksi lisätään tiedonsiirtojärjestelmään kaksi osaa: kooderi ja dekooderi. Kooderi muodostaa lähetetystä viestistä $\mathbf{m}$ koodisanan $\mathbf{c}$, joka lähetetään kanavaan. Vastaanottaja vastaanottaa tiedon $\mathbf{r}$. Jos viestiin on tullut kanavassa virheitä, on $\mathbf{c} \neq \mathbf{r}$. Dekooderi arvaa vastaanotetun tiedon $\mathbf{r}$ perusteella, mikä alkuperäinen viesti on, ts. se muodostaa arvauksen $\mathbf{m}*$. Tiedonsiirtojärjestelmässä käsiteltävä tieto on yleensä jonkin äärellisen kunnan vektori.

Tässä luvussa esitellään yleisiä koodausteoriaan liittyviä tuloksia, joita tarvitaan laajennetuista Preparata-koodeista kertovan pääosion tukena. Suurin osa tuloksista on todistettu Koodausteoria-kurssilla sekä muilla Oulun yliopiston Matemaattisten tieteiden laitoksen algebraan liittyvillä kursseilla.

1.2 Tiedonvälitysjärjestelmä

Määritellään seuraavaksi tiedonvälitysjärjestelmä täsmällisemmin. Olkoot M ja A äärellisiä epätyhjiä joukkoja, $n \in \mathbb{Z}_+$ ja γ injektio $M \to A^n$.

Määritelmä 1.2.1. Järjestettyä nelikköä (M, A, n, γ) sanotaan *koodausjärjestelmäksi*. Joukkoa M sanotaan *viestiaakkostoksi* ja joukkoa A *koodiaakkostoksi*. Joukkoa $C = \gamma(M)$ sanotaan *koodiksi*, lukua n koodin C *pituudeksi* ja kuvausta γ *koodauskuvaukseksi*.

Olkoon ? symboli, joka ei kuulu joukkoon M ja δ kuvaus $A^n \to M \cup \{?\}$, jolle

$$\delta(\gamma(\mathbf{m})) = \mathbf{m} \quad \text{kaikilla } \mathbf{m} \in M.$$

Määritelmä 1.2.2. Järjestettyä kuusikkoa $(M, A, n, \gamma, ?, \delta)$ sanotaan *koodaus-dekoodausjärjestelmäksi*. Kuvausta δ sanotaan *dekoodauskuvaukseksi* ja symbolia ? *virheilmoitussymboliksi*.

Määritelmä 1.2.3. Järjestettyä paria (K, D), missä K on Määritelmän 1.2.2 mukainen koodaus-dekoodausjärjestelmä ja D on diskreetti muistiton kanava, sanotaan *tiedonvälitysjärjestelmäksi*. Kanavan D syöttö- ja tulostusaakkosto on äärellinen epätyhjä joukko A.

Jatkossa merkintä $\mathbb{F}_q$ tarkoittaa kertalukua q olevaa äärellistä kuntaa. Oletetaan, että $A = \mathbb{F}_q$. Mikäli kunnan kertaluvusta ei ole epäselvyyttä, voidaan sitä merkitä lyhyesti $\mathbb{F}$. Joukkoa $\mathbb{F}^n = \{(f_1, f_2, \ldots, f_n) \mid f_i \in \mathbb{F}\}$ tarkastellaan lineaariavaruutena kunnan $\mathbb{F}$ suhteen.

Määritelmä 1.2.4. Avaruuden $\mathbb{F}^n$ alkioiden $\mathbf{a}$ ja $\mathbf{b}$ *Hamming-etäisyydeksi* sanotaan niiden komponenttien lukumäärää, joissa vektorit $\mathbf{a}$ ja $\mathbf{b}$ eroavat toisistaan. Tätä merkitään $\mathrm{d}_H(\mathbf{a}, \mathbf{b}) = \mathrm{d}(\mathbf{a}, \mathbf{b})$.

Määritelmä 1.2.5. Avaruuden $\mathbb{F}^n$ alkion $\mathbf{a}$ *Hamming-painoksi* sanotaan vektorin $\mathbf{a}$ nolla-alkiosta eroavien komponenttien määrää. Tätä merkitään $\mathrm{wt}_H(\mathbf{a}) = \mathrm{wt}(\mathbf{a})$. Vektorin $\mathbf{a}$ paino on siis $\mathrm{wt}(\mathbf{a}) = \mathrm{d}(\mathbf{a}, \mathbf{0})$.

Pari $(\mathbb{F}^n, \mathrm{d}_H)$ muodostaa metrisen avaruuden. Joukkoa

$$B(\mathbf{a}, e) = \{\mathbf{x} \in \mathbb{F}^n \mid \mathrm{d}(\mathbf{x}, \mathbf{a}) \leq e\}$$

sanotaan **a**-*keskiseksi e-säteiseksi palloksi.* Joukkoa

$$S(\mathbf{a}, e) = \{\mathbf{x} \in \mathbb{F}^n \mid \mathrm{d}(\mathbf{x}, \mathbf{a}) = e\}$$

sanotaan **a**-*keskisen e-säteisen pallon pinnaksi.*

Määritelmä 1.2.6. Koodin C *minimietäisyydeksi* sanotaan lukua

$$\mathrm{d}_{\min} C = \min \{\mathrm{d}(\mathbf{a}, \mathbf{b}) \mid \mathbf{a}, \mathbf{b} \in C, \mathbf{a} \neq \mathbf{b}\}.$$

Jos koodin C kaikki koodisanakeskiset e-säteiset pallot ovat erillisiä, sanotaan koodia *e virhettä korjaavaksi koodiksi.* Jos lisäksi nämä pallot yhdessä täyttävät koko avaruuden $\mathbb{F}^n$, sanotaan koodia C *täydelliseksi e* virhettä korjaavaksi koodiksi.

Huomautus 1.2.7. Sen, että koodi C on e virhettä korjaava, voi ilmaista myös muodossa $d_{\min} C \geq 2e + 1$.

Määritelmä 1.2.8. Dekoodausfunktiota δ sanotaan *e virhettä korjaavaksi*, jos $\delta(\mathbf{r}) = \mathbf{m}$ aina, kun $\mathrm{d}(\gamma(\mathbf{m}), \mathbf{r})) \leq e$.

1.3 Äärelliset kunnat

Jos kunnan alkioiden lukumäärä on äärellinen, sanotaan sitä *äärelliseksi kunnaksi.* Äärellisiä kuntia kutsutaan myös *Galois'n kunniksi* ja niitä merkitään $\mathrm{GF}(n)$, missä n on kunnan kertaluku. Tarkastellaan aluksi muutamia äärellisten kuntien perusominaisuuksia.

Olkoot $m \in \mathbb{Z}_+$ ja $a, b \in \mathbb{Z}$. Sanotaan, että luvut a ja b ovat kongruentteja modulo m, jos $m \mid (a - b)$. Kongruenssi modulo m on ekvivalenssirelaatio, joka jakaa joukon $\mathbb{Z}$ alkiot jäännösluokkiin modulo m. Tällöin alkion $a \in \mathbb{Z}$ määräämä jäännösluokka on $\overline{a} = \{a + nm \mid n \in \mathbb{Z}\}$. Näitä jäännösluokkia on m kappaletta ja niiden muodostamalle joukolle käytetään merkintää $\mathbb{Z}_m$.

Määritellään joukon $\mathbb{Z}_m$ alkioiden yhteenlaskuksi $\overline{a}+\overline{b} = \overline{a+b}$ ja kertolaskuksi $\overline{a} \cdot \overline{b} = \overline{ab}$, jolloin joukosta $\mathbb{Z}_m$ saadaan rengas.

Lause 1.3.1. *Jäännösluokkarengas $\mathbb{Z}_m$ on kunta, jos ja vain jos m on alkuluku.*

Määritelmä 1.3.2. Olkoon $\mathbb{F}$ kunta. Jos on olemassa pienin sellainen luku $n \in \mathbb{Z}_+$, jolle

$$na = \underbrace{a + \cdots + a}_{n \text{ kpl}} = 0 \quad \text{kaikilla } a \in \mathbb{F},$$

sanotaan lukua n kunnan $\mathbb{F}$ *karakteristikaksi.* Jos tällaista lukua n ei ole olemassa, kunnan $\mathbb{F}$ karakteristika on 0.

Lause 1.3.3. *Kunnan karakteristika on aina alkuluku tai 0.*

Lause 1.3.4. *Äärellisen kunnan $\mathbb{F}$ alkioiden lukumäärä, eli kertaluku $|\mathbb{F}|$ on p^m, missä p on alkuluku ja $m \in \mathbb{Z}_+$. Tällöin kunnan $\mathbb{F}$ karakteristika on p.*

Lause 1.3.5. *Kaikki samaa kertalukua olevat äärelliset kunnat ovat isomorfisia.*

1.4 Äärellisen kunnan $\mathbb{F}_{p^m}$ konstruointi

Merkitään polynomirengasta kunnan $\mathbb{F}$ suhteen merkinnällä $\mathbb{F}[x]$. Olkoon $g \in \mathbb{F}[x]$ astetta $m \geq 1$ oleva polynomi ja $p, q \in \mathbb{F}[x]$ polynomeja. Polynomit p ja q ovat kongruentteja modulo g jos $g \mid (p-q)$. Tätä merkitään $p \equiv q \pmod{g}$.

Kongruenssi modulo g on ekvivalenssirelaatio, joka jakaa joukon $\mathbb{F}[x]$ alkiot jäännösluokkiin modulo g. Mille tahansa polynomille $f \in \mathbb{F}[x]$ pätee jakoyhtälö

$$f(x) = s(x)g(x) + r(x), \quad \text{missä } \deg r(x) < m.$$

Kun nollapolynomin asteeksi sovitaan $\deg 0 = -\infty$, voi edellä olla $r(x) = 0$. Näin ollen jakoyhtälön perusteella $f \equiv r \pmod{g}$, joten jokaisesta jäännösluokasta löytyy edustaja, jonka aste on pienempi kuin m. Edellä esitetyssä tapauksessa

$$f \in \{r + pg \mid p \in \mathbb{F}[x]\} = \overline{r},$$

joten kyseessä on polynomin r määräämä jäännösluokka.

Toisaalta, jos r_1 ja r_2 ovat kaksi eri polynomia, joille $\deg r_1 < m$ ja $\deg r_2 < m$, niin $\overline{r_1} \neq \overline{r_2}$, koska $g \nmid (r_1 - r_2)$. Jäännösluokkien modulo g joukko on siis

$$\mathbb{F}[x]/\langle g(x)\rangle = \left\{ \overline{r} \;\middle|\; r(x) = \sum_{i=0}^{m-1} a_i x^i,\ a_i \in \mathbb{F} \right\}.$$

Määritellään joukon $\mathbb{F}[x]/\langle g(x)\rangle$ alkioiden yhteenlaskuksi $\overline{r_1} + \overline{r_2} = \overline{r_1 + r_2}$ ja kertolaskuksi $\overline{r_1} \cdot \overline{r_2} = \overline{r_1 r_2}$, jolloin joukosta $\mathbb{F}[x]/\langle g(x)\rangle$ saadaan rengas.

Lause 1.4.1. *Olkoon p alkuluku ja $g \in \mathbb{Z}_p[x]$ astetta $m \geq 1$ oleva polynomi. Tällöin jäännösluokkarengas $\mathbb{Z}_p[x]/\langle g(x)\rangle$ on kunta jos ja vain jos g on jaoton. Kyseisessä kunnassa on p^m alkiota.*

Merkitään $\beta = \overline{x}$ jäännösluokkarenkaassa $\mathbb{Z}_p[x]/\langle g(x)\rangle$. Tällöin yllä olevan mukaan

$$\mathbb{F}_{p^m} = \left\{ \sum_{i=0}^{m-1} a_i \beta^i \;\middle|\; a_i \in \mathbb{Z}_p, g(\beta) = 0 \right\},$$

missä $g \in \mathbb{Z}_p[x]$ on jaoton polynomi ja $\deg g = m \geq 1$. Kunta $\mathbb{F}_{p^m}$ voidaan siis konstruoida, kun löydetään astetta m oleva jaoton polynomi.

Määritelmä 1.4.2. Kunnan $\mathbb{F}$ alkion $a \in \mathbb{F}^*$ *kertaluvuksi* sanotaan pienintä sellaista lukua $k \in \mathbb{Z}_+$, että $a^k = 1$. Tätä merkitään $k = \operatorname{ord} a$ tai $k = |a|$.

Määritelmä 1.4.3. Kunnan $\mathbb{F}_q$ alkiota $\gamma \neq 0$ sanotaan *primitiiviseksi*, eli kunnan $\mathbb{F}_q$ *primitiivialkioksi*, jos $\operatorname{ord} \gamma = q - 1$. Tällöin

$$\mathbb{F}_q^* = \langle \gamma \rangle = \left\{ \gamma^k \mid 0 \leq k < q - 1 \right\}.$$

Astetta m olevaa polynomirenkaan $\mathbb{F}_q[x]$ polynomia sanotaan *primitiiviseksi*, jos sillä on nollakohta, joka on kunnan $\mathbb{F}_{q^m}$ primitiivialkio.

Lause 1.4.4. *Äärellisen kunnan nolla-alkiosta eroavien alkioiden muodostama ryhmä on syklinen, eli jokaisessa äärellisessä kunnassa on primitiivialkio.*

Jos γ on kunnan $\mathbb{F}_q$ yksi primitiivialkio, niin kunnan $\mathbb{F}_q$ primitiivialkiot ovat täsmälleen alkiot γ^j, missä $\operatorname{syt}(j, q-1) = 1$.

Lause 1.4.5. *Jos kunnan $\mathbb{F}$ karakteristika on p, niin kunnassa pätee yhtälö*

$$(x+y)^p = x^p + y^p.$$

Esimerkki 1.4.6. Konstruoidaan kunta $\mathbb{F}_{2^3} = \mathbb{F}_8$ käyttämällä renkaassa $\mathbb{Z}_2[x]$ jaotonta polynomia $g(x) = x^3 + x + 1$. Olkoon β kunnan primitiivialkio, jolle $\beta^3 + \beta + 1 = 0$. Tällöin

$$\mathbb{F}_8 = \left\{ \sum_{i=0}^{2} a_i \beta^i \;\middle|\; a_i \in \mathbb{Z}_2,\ \beta^3 + \beta + 1 = 0,\ \text{ts. } \beta^3 = \beta + 1 \right\}.$$

Kunnan alkiot ovat siis $0, 1, \beta, \beta^2, \beta^3 = \beta + 1, \beta^4 = \beta^2 + \beta, \beta^5 = \beta^2 + \beta + 1, \beta^6 = \beta^2 + 1$. Jos kunnan alkioilla suoritetaan laskutoimituksia, on usein alkio $a_0 + a_1\beta + a_2\beta^2$ käytännöllistä ilmaista jonona $a_0a_1a_2$. Kunnan alkiot tällä tavalla esitettynä ovat

$$\begin{array}{cccc} 0 = 000 & 1 = 100 & \beta = 010 & \beta^2 = 001 \\ \beta^3 = 110 & \beta^4 = 011 & \beta^5 = 111 & \beta^6 = 101 \end{array}$$

Luku 2

Lineaarisista koodeista

2.1 Yleistä

Tässä luvussa esitellään lineaaristen koodien määritelmä sekä niihin liittyviä perustuloksia. Lisäksi luvussa perehdytään muutamiin syklisten koodien tuloksiin ja esitellään BCH-koodi, joka on tietyntyyppisen polynomin generoima syklinen koodi.

Näiden koodien osalta esitellään joitain lähdeteoksien [1] ja [2] tuloksia, jotka koskevat syklisiä koodeja ja BCH-koodeja. Näitä tuloksia ei todisteta tässä yhteydessä.

2.2 Määritelmä ja perusominaisuuksia

Olkoon $\mathbb{F}$ äärellinen kunta. Joukko $\mathbb{F}^n$ on vektoriavaruus kunnan $\mathbb{F}$ suhteen.

Määritelmä 2.2.1. Koodausjärjestelmää $(M, \mathbb{F}, n, \gamma)$ sanotaan *lineaariseksi*, jos M on vektoriavaruus $\mathbb{F}^k$, missä $k \leq n$ ja koodauskuvaus γ on injektiivinen lineaarinen kuvaus $M \to \mathbb{F}^n$.

Tällöin koodi $C = \gamma(M)$ on selvästi avaruuden $\mathbb{F}^n$ k-ulotteinen aliavaruus.

Määritelmä 2.2.2. *Lineaariseksi koodiksi* sanotaan lineaarisen koodausjärjestelmän koodia $C = \gamma(M)$, joka on avaruuden $\mathbb{F}^n$ k-ulotteinen aliavaruus. Tämän

perusteella jokainen lineaarisen koodin koodisanoista muodostettu lineaarikombinaatio on myös koodisana. Aliavaruuden ollessa k-ulotteinen ja koodin minimietäisyyden ollessa d, koodia kutsutaan $[n, k, d]$-koodiksi tai lyhyemmin $[n, k]$-koodiksi. Lukua k sanotaan myös lineaarisen koodin dimensioksi.

Jos C on $[n, k]$-koodi ja $\{\mathbf{g}_1, \ldots, \mathbf{g}_k\}$ sen kanta, niin koodin C sanat ovat muotoa

$$a_1\mathbf{g}_1 + a_2\mathbf{g}_2 + \cdots + a_k\mathbf{g}_k = (a_1 \ldots a_k)G,$$

missä kertoimet $a_1, \ldots, a_k \in \mathbb{F}$ ja

$$G = \begin{bmatrix} \mathbf{g}_1 \\ \mathbf{g}_2 \\ \vdots \\ \mathbf{g}_k \end{bmatrix}_{k \times n}.$$

Koodauskuvaus γ voidaan siis valita niin, että viestivektori $\mathbf{m} \in \mathbb{F}^k$ kerrotaan matriisilla G, eli valitaan $\gamma(\mathbf{m}) = \mathbf{m}G$. Tällöin

$$C = \{\mathbf{c} \mid \mathbf{c} = \mathbf{m}G, \mathbf{m} \in \mathbb{F}^k\}.$$

Määritelmä 2.2.3. Edellä mainittua koodin kantavektoreista muodostettua $k \times n$-matriisia G sanotaan $[n, k]$-koodin C *generoijamatriisiksi.*

Esimerkki 2.2.4. Seuraavassa on esimerkkejä lineaarisista koodeista kunnan $\mathbb{F}_2$ suhteen annettuna generoijamatriisin avulla.

$$C_1: \quad G_1 = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} \quad [3, 2]\text{-koodi}$$

$$C_2: \quad G_2 = \begin{bmatrix} 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{bmatrix} \quad [5, 2]\text{-koodi}$$

$$C_3: \quad G_3 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \quad [7, 4]\text{-koodi}$$

Valitsemalla matriisiksi G muotoa $\begin{bmatrix} I_k & P \end{bmatrix}$ oleva matriisi, missä I_k on k-rivinen yksikkömatriisi ja P on $k \times (n-k)$-matriisi, saadaan koodisana $\mathbf{c} = \mathbf{m}G$ muotoon, jossa k ensimmäistä komponenttia muodostavat viestisanan $\mathbf{m}$ ja muut $n-k$ komponenttia ovat tarkistussymboleja:

$$\underbrace{\cdots\cdots\cdots\cdots\cdots\cdots}_{\substack{k \\ \text{informaatio}}}\underbrace{\cdots\cdots\cdots}_{\substack{n-k \\ \text{tarkistus}}}$$

Tätä muotoa olevaa koodausta sanotaan *systemaattiseksi koodaukseksi.*

Määritelmä 2.2.5. Lineaarisen $[n,k]$-koodin C *tarkistusmatriisiksi* kutsutaan sellaista $n \times (n-k)$-matriisia H, jolle

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

Lause 2.2.6. *Olkoon C $[n,k]$-koodi ja olkoon sen generoijamatriisi systemaattisessa muodossa $G = \begin{bmatrix} I_k & P \end{bmatrix}$. Silloin matriisi $H = \begin{bmatrix} -P^{\mathrm{T}} \\ I_{n-k} \end{bmatrix}$ on koodin C tarkistusmatriisi.*

Todistus. Ks. [2], Lause 3.2.3. □

Esimerkki 2.2.7. Olkoon C kunnan $\mathbb{F}_2$ suhteen oleva [6,3]-koodi, jonka generoijamatriisi G on

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

ja tarkistusmatriisi H on

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

Koodin C sanat $\mathbf{c}_i$ ovat kaikki vektoriavaruuden $\mathbb{F}_2^3$ vektorit kerrottuna matriisilla G, eli

$$\mathbf{c}_1 = 000000 \qquad \mathbf{c}_2 = 100011 \qquad \mathbf{c}_3 = 010101 \qquad \mathbf{c}_4 = 001110$$
$$\mathbf{c}_5 = 110110 \qquad \mathbf{c}_6 = 101101 \qquad \mathbf{c}_7 = 011011 \qquad \mathbf{c}_8 = 111000$$

Tarkistusmatriisia hyödynnetään lineaaristen koodien dekoodauksessa. Oletetaan, että lähetettäessä kanavaan sana $\mathbf{c}$ saadaan sana $\mathbf{r} = \mathbf{c} + \mathbf{e}$, missä $\mathbf{e}$ on häiriön aiheuttama virhe. Dekoodaaja ei tunne vektoria $\mathbf{c}$ eikä vektoria $\mathbf{e}$. Näiden löytämiseksi käytetään syndromia.

Määritelmä 2.2.8. Vektorin $\mathbf{x} \in \mathbb{F}^n$ *syndromiksi* sanotaan vektoria $s(\mathbf{x}) = \mathbf{x}H$.

Määritelmästä seuraa, että $s(\mathbf{x}) = \mathbf{0}$ täsmälleen silloin, kun $\mathbf{x} \in C$. Koska C on ryhmä yhteenlaskun suhteen, voidaan muodostaa sivuluokat $\mathbf{x}+C = \{\mathbf{x}+\mathbf{c} \mid \mathbf{c} \in C\}$. Osoitetaan, että syndromin arvo liittyy juuri sivuluokkiin.

Lause 2.2.9. *Vektorit* $\mathbf{x}$ *ja* $\mathbf{y}$ *ovat samassa koodin* C *sivuluokassa täsmälleen silloin, kun niillä on sama syndromi.*

Todistus. Ks. [2], Lause 3.3.2. □

Jos $s(\mathbf{r}) = \mathbf{s}$, niin virhevektori $\mathbf{e}$ voi olla mikä tahansa sana, jonka syndromi on $\mathbf{s}$, ts. mikä tahansa sivuluokan $\mathbf{r} + C$ alkio. Todennäköisimmät ehdokkaat ovat ne, joiden painot ovat pienimmät. Valitaan jokaisesta sivuluokasta tällainen alkio ja sanotaan sitä kyseisen *sivuluokan johtajaksi*. Tarkastellaan seuraavaa *standardikaaviota*, jonka

1. ensimmäiselle riville tulee koodisanat vektorista $\mathbf{0}$, sivuluokan C johtajasta, alkaen: $\mathbf{0}, \mathbf{c}_2, \ldots, \mathbf{c}_{q^k}$;

2. ensimmäiseen sarakkeeseen tulee sivuluokkien johtajat $\mathbf{0}, \mathbf{e}_2, \ldots, \mathbf{e}_{q^{n-k}}$;

3. rivin i ja sarakkeen j risteykseen tulee alkio $\mathbf{e}_i + \mathbf{c}_j$.

Dekoodaaja δ käyttää taulukkoa seuraavasti: saatu sana $\mathbf{r}$ muutetaan sen yläpuolella olevaksi koodisanaksi $\mathbf{c}^*$, jolloin $\mathrm{wt}(\mathbf{r}-\mathbf{c}^*)$ on pienin mahdollinen eli $\mathbf{r}-\mathbf{c}^*$ on todennäköisin virhe.

Esimerkki 2.2.10. Olkoon C $[4, 2]$-koodi kunnan $\mathbb{F}_3 = \{0, 1, 2\}$ suhteen ja olkoon sen generoijamatriisi

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

Tarkistusmatriisiksi tulee

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

Koodille C saadaan seuraava standardikaavio:

r	$\mathbf{c}_1$	$\mathbf{c}_2$	$\mathbf{c}_3$	$\mathbf{c}_4$	$\mathbf{c}_5$	$\mathbf{c}_6$	$\mathbf{c}_7$	$\mathbf{c}_8$	$\mathbf{e}_9$
$\mathbf{e}_1$	0000	1011	2022	0112	0221	1120	2210	1202	2101
$\mathbf{e}_2$	1000	2011	0022	1112	1221	2120	0210	2202	0101
$\mathbf{e}_3$	2000	0011	1022	2112	2221	0120	1210	0202	1101
$\mathbf{e}_4$	0100	1111	2122	0212	0021	1220	2010	1002	2201
$\mathbf{e}_5$	0200	1211	2222	0012	0121	1020	2110	1102	2001
$\mathbf{e}_6$	0010	1021	2002	0122	0201	1100	2220	1212	2111
$\mathbf{e}_7$	0020	1001	2012	0102	0211	1110	2200	1222	2121
$\mathbf{e}_8$	0001	1012	2020	0110	0222	1121	2211	1200	2102
$\mathbf{e}_9$	0002	1010	2021	0111	0220	1122	2212	1201	2100

Edellä esitetty täydellinen kaavio vaatii yleensä liikaa tilaa. Koska jokaisella rivillä on sama syndromi, riittää tallentaa sivuluokkien johtajat ja niiden syndromit.

Näin saadun *syndromiluettelon* avulla voidaan toimia seuraavasti: Jos saadaan sana $\mathbf{r}$, niin

1. lasketaan syndromi $\mathbf{r}H$;
2. etsitään syndromiluettelon avulla vastaava sivuluokan johtaja $\mathbf{e}_i$;
3. lasketaan $\mathbf{r} - \mathbf{e}_i = \mathbf{c}^*$.

Esimerkki 2.2.11. Esimerkin 2.2.10 koodille saadaan seuraava syndromiluettelo:

$$\begin{array}{lll} \mathbf{e}_1: \ s(0000) = 00 & \mathbf{e}_4: \ s(0100) = 21 & \mathbf{e}_7: \ s(0020) = 20 \\ \mathbf{e}_2: \ s(1000) = 22 & \mathbf{e}_5: \ s(0200) = 12 & \mathbf{e}_8: \ s(0001) = 01 \\ \mathbf{e}_3: \ s(2000) = 11 & \mathbf{e}_6: \ s(0010) = 10 & \mathbf{e}_9: \ s(0002) = 02 \end{array}$$

Esimerkiksi sanan $\mathbf{r} = 1221$ syndromi on

$$s(\mathbf{r}) = \mathbf{r}H = (1221)\begin{bmatrix} 2 & 2 \\ 2 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} = 22,$$

joten todennäköisin virhe on $\mathbf{e}_2$ ja $\mathbf{r}$ tulee dekoodattua sanaksi $\mathbf{c} = \mathbf{r} - \mathbf{e}_2 = 0221$. Vastaavasti

$$s(1110) = (1110)H = 20 = s(\mathbf{e}_7),$$

ja

$$\mathbf{c} = 1110 - 0020 = 1120.$$

2.3 Sykliset koodit ja BCH-koodit

Laajennettujen Preparata-koodien koodauksessa hyödynnetään erään BCH-koodin tarkistusmatriisia. BCH-koodit ovat lineaaristen ja syklisten koodien alalaji, joiden hyöty perustuu suhteellisen helppoon dekoodausalgoritmiin. Ennen BCH-koodin määrittelyä esitetään muutamia syklisten koodien tuloksia.

Olkoon $\mathbb{F} = \mathbb{F}_{p^m}$, missä p on alkuluku. Syklisten koodien yhteydessä käytetään jäännösluokkarengasta

$$R_n = \mathbb{F}[x]/\langle x^n - 1\rangle,$$

jonka alkiot ovat jäännösluokkia

$$\bar{f} = \{f(x) + h(x)(x^n - 1) \mid h(x) \in \mathbb{F}[x]\}.$$

Koska $\deg(x^n - 1) = n$, kappaleen 1.4 tarkastelujen mukaan jäännösluokkien edustajistoksi voidaan valita joukko

$$\{a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \mid a_i \in \mathbb{F}\}.$$

Käytetään seuraavassa polynomia $a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$ tarkoittamaan myös sen määräämää jäännösluokkaa. Asiayhteydestä käy ilmi, onko kyseessä polynomi vai jäännösluokka.

Summa ja tulo määritellään renkaassa R_n tuttuun tapaan edustajien avulla: Jos

$$f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \in R_n$$

ja

$$g(x) = b_0 + b_1 x + \cdots + b_{n-1}x^{n-1} \in R_n,$$

niin

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_{n-1} + b_{n-1})x^{n-1} \in R_n$$

ja

$$f(x)g(x) = r(x) \in R_n,$$

missä

$$f(x)g(x) = h(x)(x^n - 1) + r(x)$$

ja

$$\deg r \leq n - 1.$$

Jakojäännös $r(x)$ saadaan tulosta $f(x)g(x)$ nopeasti huomaamalla, että renkaassa

R_n pätee $x^n = 1$, $x^{n+1} = x$, jne.

Jäännösluokkarengas R_n varustettuna yhteenlaskulla ja skalaarilla, eli kunnan $\mathbb{F}$ alkiolla, kertomisella on vektoriavaruus kunnan $\mathbb{F}$ suhteen. Tämä vektoriavaruus on isomorfinen vektoriavaruuden $\mathbb{F}^n$ kanssa ja isomorfismin välittää kuvaus

$$a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \mapsto (a_0, a_1, \ldots, a_{n-1}) = a_0 a_1 \ldots a_{n-1}.$$

Seuraavassa samaistetaan nämä kolme merkintää ja puhutaan samaa tarkoittaen polynomeista, vektoreista ja sanoista.

Jäännösluokkarenkaan R_n rengasrakennetta ja edellä mainittua isomorfiaa käyttäen saadaan määriteltyä vektoriavaruudessa $\mathbb{F}^n$ kertolasku asettamalla $\mathbf{ab} = \mathbf{c}$, kun

$$\begin{aligned} a(x) \in R_n &\Rightarrow \mathbf{a} \in \mathbb{F}^n, \\ b(x) \in R_n &\Rightarrow \mathbf{b} \in \mathbb{F}^n, \\ a(x)b(x) \in R_n &\Rightarrow \mathbf{c} \in \mathbb{F}^n. \end{aligned}$$

Syklisten koodien kannalta renkaan R_n keskeinen ominaisuus on se, että alkiolla x kertominen merkitsee yhden askelen syklistä siirtoa:

$$\begin{aligned} x(a_0, a_1, \ldots, a_{n-1}) &= x(a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}) \\ &= a_0 x + a_1 x^2 + \cdots + a_{n-2}x^{n-1} + a_{n-1} \\ &= (a_{n-1}, a_0, a_1, \ldots, a_{n-2}). \end{aligned}$$

Määritelmä 2.3.1. Polynomia, jonka korkeimman potenssin kerroin on 1, sanotaan *pääpolynomiksi*.

Tarkastellaan kunnan $\mathbb{F}_q$ äärellistä laajennuskuntaa $\mathbb{F}_{q^r}$. Jokainen $\alpha \in \mathbb{F}_{q^r}$ toteuttaa yhtälön

$$x^{q^r} - x = 0,$$

joten jokainen $\alpha \in \mathbb{F}_{q^r}$ on renkaan $\mathbb{F}_q[x]$ jonkin pääpolynomin nollakohta.

Määritelmä 2.3.2. Alkion $\alpha \in \mathbb{F}_{q^r}$ *minimipolynomiksi* kunnan $\mathbb{F}_q$ suhteen, merkitään $m_\alpha(x)$, sanotaan sitä mahdollisimman alhaista astetta olevaa renkaan $\mathbb{F}_q[x]$ pääpolynomia, jonka nollakohtana α on, ts. $m_\alpha(\alpha) = 0$.

Minimipolynomi m_α on yksikäsitteinen. Jos $\alpha \in \mathbb{F}_q$, niin $m_\alpha(x) = x - \alpha$.

Määritelmä 2.3.3. Lineaarista koodia $C \subseteq \mathbb{F}^n$ sanotaan *sykliseksi koodiksi*, jos $(c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C$ aina, kun $(c_0, c_1, \ldots, c_{n-1}) \in C$.

Lause 2.3.4. *Olkoon jäännösluokkarengas $R_n = \mathbb{F}[x]/\langle x^n - 1\rangle$. Jos $g(x) \mid (x^n - 1)$ renkaassa $\mathbb{F}[x]$ ja $\deg g(x) = n - k$, niin polynomin $g(x)$ generoima jäännösluokkarenkaan R_n ideaali $\langle g(x)\rangle$ on syklinen $[n, k]$-koodi. Jos C on syklinen $[n, k]$-koodi, niin on olemassa sellainen astetta $n - k$ oleva pääpolynomi $g(x)$, että $g(x) \mid (x^n - 1)$ renkaassa $\mathbb{F}[x]$ ja C on polynomin $g(x)$ generoima renkaan R_n ideaali.*

Todistus. Ks. [2], Lause 4.2.3. □

Määritelmä 2.3.5. Lauseessa 2.3.4 esiintyvää $[n, k]$-koodin C mahdollisimman alhaista astetta olevaa pääpolynomia $g(x)$ sanotaan syklisen koodin C *generoijapolynomiksi.*

Olkoon $g(x) = g_0 + g_1x + \cdots + g_{n-k}x^{n-k}$ koodin C generoijapolynomi, eli koodi C on $[n, k]$-koodi. Tällöin joukko $\{g(x), xg(x), \ldots, x^{k-1}g(x)\}$ on koodin C kanta, ja generoijamatriisiksi voidaan ottaa matriisi

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

Olkoon $m(x)$ viestisana $\mathbf{m}$ esitettynä polynomimuodossa. Koodauskuvaukseksi voidaan valita generoijapolynomilla $g(x)$ kertominen:

$$\begin{aligned} m(x)g(x) &= (m_0g_0,\ m_0g_1 + m_1g_0,\ m_0g_2 + m_1g_1 + m_2g_0, \ldots,\ m_{k-1}g_{n-k}) \\ &= \mathbf{m}G. \end{aligned}$$

Koska $\deg(m(x)) = k - 1$, voidaan polynomi $m(x)$ muodostaa $|\mathbb{F}|^k$ eri tavalla. Tulo $m(x)g(x)$ muodostaa siis $|\mathbb{F}|^k$ kappaletta keskenään erilaisia koodin C koodisanoja. Lisäksi $\deg(m(x)g(x)) < n$, koska $\deg(g(x)) = n - k$. Koodin C koodisanojen lukumäärä on $|\mathbb{F}|^k$, joten tuloa $m(x)g(x)$ ei tarvitse laskea jäännösluokkarenkaassa $\mathbb{F}[x]/\langle x^n - 1\rangle$, vaan se voidaan laskea polynomirenkaassa $\mathbb{F}[x]$.

Syklisen koodin kaikki koodisanat saadaan siis kertomalla kaikki polynomirenkaan $\mathbb{F}[x]$ polynomit $m(x)$, joille $\deg(m(x)) < k$ generoijapolynomilla $g(x)$.

Lemma 2.3.6. *Tarkastellaan kuntaa $\mathbb{F}_q$. Olkoon luku $n \in \mathbb{Z}_+$ sellainen, joka toteuttaa ehdon* $\text{syt}(n, q) = 1$. *Tällöin on olemassa sellainen luku $m \in \mathbb{Z}_+$, että $n \mid (q^m - 1)$. Tästä johtuen jossakin kunnan $\mathbb{F}_q$ laajennuksessa $\mathbb{F}_{q^m}$ on olemassa primitiivinen n:s ykkösen juuri α, jolle*

$$\alpha^n = 1, \alpha^i \neq \alpha^j \quad \textit{kaikilla } 0 \leq i < j \leq n-1.$$

Todistus. Ks. [2], kappale 4.1.3. □

Olkoon $\mathbb{F} = \mathbb{F}_q$, $\text{syt}(n, q) = 1$ ja m luvun q multiplikatiivinen kertaluku modulo n, jolloin $n \mid (q^m - 1)$. Olkoon α kunnan $\mathbb{F}_{q^m}$ primitiivinen n:s ykkösen juuri. Kuten aiemmin, käytetään alkion α^i minimipolynomille merkintää $m_{\alpha^i}(x)$.

Määritelmä 2.3.7. Polynomin

$$\text{pyj}(m_\alpha(x), m_{\alpha^2}(x), \ldots, m_{\alpha^{d-1}}(x))$$

generoimaa n-pituista syklistä koodia sanotaan *(kapea-alaiseksi) BCH-koodiksi*, jonka *suunniteltu etäisyys* on d.

BCH-koodi voidaan siis konstruoida usealla eri polynomilla riippuen siitä, mikä virheenkorjauskyky koodille halutaan. Jos BCH-koodin suunniteltu etäisyys on $2t + 1$, sanotaan sitä tavallisesti t virhettä korjaavaksi BCH-koodiksi.

Esimerkki 2.3.8. Olkoon kunta $\mathbb{F}_{2^4}$ konstruoitu polynomin $p(x) = x^4 + x + 1$ avulla ja β kunnan primitiivialkio, eli primitiivinen 15. ykkösen juuri. Tällöin $m_\beta(x) = m_{\beta^2}(x) = m_{\beta^4}(x) = x^4 + x + 1$ ja $m_{\beta^3}(x) = x^4 + x^3 + x^2 + x + 1$ ovat alkioiden β, β^2, β^3 ja β^4 minimipolynomit. (Ks. [1], Esim. 5.2.5)

Nyt polynomi

$$\begin{aligned} g(x) &= \text{pyj}\left(m_\beta(x), m_{\beta^2}(x), m_{\beta^3}(x), m_{\beta^4}(x)\right) \\ &= m_\beta(x) m_{\beta^3}(x) = x^8 + x^7 + x^6 + x^4 + 1 \end{aligned}$$

generoi kaksi virhettä korjaavan BCH-koodin, jonka pituus on 15.

Lemma 2.3.9. *Olkoon β kunnan $\mathbb{F}_{2^r}$ primitiivialkio. Matriisi*

$$H = \begin{bmatrix} \beta^0 & \beta^0 \\ \beta^1 & \beta^3 \\ \beta^2 & \beta^6 \\ \vdots & \vdots \\ \beta^i & \beta^{3i} \\ \vdots & \vdots \\ \beta^{2^r-2} & \beta^{3(2^r-2)} \end{bmatrix}$$

on tarkistusmatriisi kaksi virhettä korjaavalle BCH-koodille. Tämän koodin pituus on $2^r - 1$ ja sen generoi polynomi $g(x) = m_{\beta^1}(x)m_{\beta^3}(x)$. Tarkistusmatriisin H koko on tällöin $(2^r - 1) \times (2r)$, kun alkiot β^i käsitellään r-pituisina vaakavektoreina. Lisäksi $\deg(m_\beta(x)) = \deg(m_{\beta^3}(x)) = r$, joten $\deg(g(x)) = 2r$. Näin ollen koodin dimensio on $k = 2^r - 2r - 1$.

Todistus. Ks. [1], Lemma 5.4.5. □

Lause 2.3.10. *Olkoon β kunnan $\mathbb{F}_{2^r}$ primitiivialkio ja olkoon $r \geq 4$ kokonaisluku. Tällöin on olemassa polynomin $g(x) = m_{\beta^1}(x)m_{\beta^3}(x)$ generoima kaksi virhettä korjaava BCH-koodi. Tämän koodin pituus on $n = 2^r - 1$, dimensio on $k = 2^r - 2r - 1$ ja minimietäisyys on $d = 5$.*

Todistus. Ks. [1], Lause 5.4.6. □

Lemma 2.3.11. *Olkoon β kunnan $\mathbb{F}_{2^r}$ primitiivialkio. Tarkastellaan kaksi virhettä korjaavaa BCH-koodia, jonka generoi polynomi $g(x) = m_{\beta^1}(x)m_{\beta^3}(x)$. Olkoon matriisi H lemman 2.3.9 mukainen tarkistusmatriisi kyseiselle koodille. Tällöin matriisin H mitkä tahansa $2r$ perättäistä riviä ovat lineaarisesti riippumattomia.*

Todistus. Koska BCH-koodi on syklinen, niin sen kaikki koodisanat saadaan kertomalla kaikki polynomirenkaan $\mathbb{F}[x]$ polynomit $m(x)$, joille $\deg(m(x)) < k$, koodin generoijapolynomilla $g(x)$. Näin ollen minkään polynomimuodossa esitetyn koodisanan aste ei voi olla pienempi kuin generoijapolynomin aste $\deg(g(x)) = 2r$.

Oletetaan nyt, että mielivaltaisesti valitut $2r$ peräkkäistä matriisin H riviä ovat lineaarisesti riippuvaisia. Tällöin on olemassa nollavektorista poikkeava vektori

$\mathbf{c} \in \mathbb{F}_2^n$ muotoa

$$\mathbf{c} = [0, \ldots, 0, c_i, \ldots, c_{i+2r-1}, 0, \ldots, 0], \ 1 \leq i \leq n - 2r,$$

jolle $\mathbf{c}H = \mathbf{0}$. Koska H on tarkistusmatriisi, niin määritelmän 2.2.5 perusteella $\mathbf{c}$ on koodisana.

Edelleen, koska BCH-koodi on syklinen koodi, ovat kaikki koodisanasta $\mathbf{c}$ määritelmän 2.3.3 mukaisesti syklisillä siirroilla saadut sanat koodisanoja. Näin ollen myös sana $\mathbf{c}' = [c_i, \ldots, c_{i+2r-1}, 0, \ldots, 0]$ on koodisana. Polynomimuodossa tämä tarkoittaa polynomia

$$c'(x) = c_i + c_{i+1}x + c_{i+2}x^2 + \cdots + c_{i+2r-1}x^{2r-1}.$$

Näin ollen on olemassa koodisana $c'(x)$, jolle $\deg(c'(x)) < 2r$. Tämä on ristiriita, joten minkä tahansa matriisista H valittujen $2r$ perättäisen rivin on oltava lineaarisesti riippumattomia. □

Nyt lemman 2.3.11 perusteella minkä tahansa matriisin H alimatriisin, joka on muodostettu $2r$ peräkkäisestä rivistä, aste on $2r$ ja sillä on olemassa käänteismatriisi.

Olkoon A matriisin H alimatriisi, joka muodostuu matriisin H viimeisistä $2r$ rivistä. Tällä matriisilla on olemassa käänteismatriisi A^{-1}. Olkoon H' matriisin H alimatriisi, joka muodostuu poistamalla matriisista H sen $2r$ alinta riviä. Näitä matriiseja tarvitaan kappaleessa 4.2 olevien tulosten osoittamiseen.

Esimerkki 2.3.12. Olkoon kunta $\mathbb{F}_8$ konstruoitu polynomin x^3+x+1 avulla, kuten esimerkissä 1.4.6. Tällöin

$$H = \begin{bmatrix} \beta^0 & \beta^0 \\ \beta^1 & \beta^3 \\ \beta^2 & \beta^6 \\ \beta^3 & \beta^9 \\ \beta^4 & \beta^{12} \\ \beta^5 & \beta^{15} \\ \beta^6 & \beta^{18} \end{bmatrix} = \begin{bmatrix} \beta^0 & \beta^0 \\ \beta^1 & \beta^3 \\ \beta^2 & \beta^6 \\ \beta^3 & \beta^2 \\ \beta^4 & \beta^5 \\ \beta^5 & \beta^1 \\ \beta^6 & \beta^4 \end{bmatrix} = \begin{bmatrix} 100 & 100 \\ 010 & 110 \\ 001 & 101 \\ 110 & 001 \\ 011 & 111 \\ 111 & 010 \\ 101 & 011 \end{bmatrix}$$

ja

$$A = \begin{bmatrix} \beta^1 & \beta^3 \\ \beta^2 & \beta^6 \\ \beta^3 & \beta^2 \\ \beta^4 & \beta^5 \\ \beta^5 & \beta^1 \\ \beta^6 & \beta^4 \end{bmatrix} = \begin{bmatrix} 010 & 110 \\ 001 & 101 \\ 110 & 001 \\ 011 & 111 \\ 111 & 010 \\ 101 & 011 \end{bmatrix},$$

jolloin

$$A^{-1} = \begin{bmatrix} 001 & 011 \\ 111 & 010 \\ 011 & 101 \\ 110 & 100 \\ 101 & 110 \\ 111 & 001 \end{bmatrix}.$$

Luku 3

Laajennetut Preparata-koodit

3.1 Yleistä

Laajennetut Preparata-koodit määritellään kunnan $\mathbb{F}_{2^r}$ osajoukkojen avulla. Osajoukot kuvataan kunnan $\mathbb{F}_2$ vektoreiksi, joiden on täytettävä tietyt ehdot ollakseen koodisanoja.

Laajennetuilla Preparata-koodeilla on useita samankaltaisia ominaisuuksia kuin lineaarisilla koodeilla. Esimerkkinä voidaan mainita, että laajennetut Preparata-koodit ovat etäisyysinvariantteja, kuten lineaariset kooditkin. Kuitenkin tässä luvussa tullaan osoittamaan, että laajennetut Preparata-koodit ovat epälineaarisia. Näin ollen lineaaristen koodien koodaus- ja dekoodausmenetelmiä ei voida soveltaa niihin. Mielenkiintoinen laajennettujen Preparata-koodien ominaisuus on myös se, että niiden minimietäisyys on aina sama riippumatta luvun r arvosta.

3.2 Laajennetun Preparata-koodin $P(r)$ määritelmä

Laajennettujen Preparata-koodien määrittelyssä käytetään kunnan $\mathrm{GF}(2^r) = \mathbb{F}_{2^r}$ alkioita, missä $r \in \mathbb{Z}_+$. Olkoon β kunnan $\mathbb{F}_{2^r}$ primitiivialkio ja $U \subseteq \mathbb{F}_{2^r}$. Olkoon χ kuvaus, joka kuvaa osajoukon U kunnan $\mathbb{F}_2$ vektoriksi (sanaksi), jonka pituus on 2^r. Määritellään $\chi(U)$ olemaan sana, jossa on

$$
\begin{array}{llll}
1 & \text{kohdassa} \quad i & \text{jos} & \beta^i \in U \quad (0 \leq i \leq 2^r - 2), \\
1 & \text{kohdassa} \quad 2^r - 1 & \text{jos} & 0 \in U, \\
0 & \text{muulloin.} & &
\end{array}
$$

Esimerkki 3.2.1. Olkoon β kunnan $\mathbb{F}_8$ primitiivialkio. Tällöin

$$
\begin{aligned}
\chi(\{0\}) &= 00000001, \\
\chi\left(\left\{\beta, \beta^3, \beta^5\right\}\right) &= 01010100, \\
\chi\left(\left\{1, \beta^2, \beta^5, \beta^6\right\}\right) &= 10100110, \text{ ja} \\
\chi(\{\emptyset\}) &= 00000000.
\end{aligned}
$$

Jos α on kunnan $\mathbb{F}_{2^r}$ alkio ja $U \subseteq \mathbb{F}_{2^r}$, niin olkoon joukko $U+\alpha = \{u + \alpha \mid u \in U\}$ ja joukko $\alpha U = \{\alpha u \mid u \in U\}$. Määritellään lisäksi joukkojen $U \subseteq \mathbb{F}_{2^r}$ ja $V \subseteq \mathbb{F}_{2^r}$ *symmetrinen erotus* $U \Delta V$ olemaan joukko $\{x \mid x \in U \text{ tai } x \in V \text{ mutta } x \notin U \cap V\}$.

Olkoon β edelleen kunnan $\mathbb{F}_{2^r}$ primitiivialkio ja $i \in \mathbb{Z}$, $0 \leq i \leq 2^r - 2$. Jos $\beta^i \in U$ tai $\beta^i \in V$, mutta $\beta^i \notin U \cap V$, on tällöin sanan $\chi(U \Delta V)$ kohdassa i arvo 1, muutoin arvo 0. Samoin jos $0 \in U$ tai $0 \in V$, mutta $0 \notin U \cap V$, on tällöin sanan $\chi(U \Delta V)$ kohdassa $2^r - 1$ arvo 1, muutoin arvo 0. Näin ollen $\chi(U) + \chi(V) = \chi(U \Delta V)$.

Määritelmä 3.2.2. *Laajennettu Preparata-koodi* $P(r)$ on niiden koodisanojen joukko, jonka alkuosa koostuu sanasta $\chi(U)$ ja loppuosa sanasta $\chi(V)$, missä U ja V ovat kunnan $\mathbb{F}_{2^r}$ osajoukkoja ja täyttävät seuraavat ehdot:

(i) $|U|$ ja $|V|$ ovat parillisia,

(ii)
$$\sum_{u \in U} u = \sum_{v \in V} v,$$

(iii)
$$\sum_{u \in U} u^3 + \left(\sum_{u \in U} u\right)^3 = \sum_{v \in V} v^3,$$

(iv) luku r on pariton.

Merkitään laajennetun Preparata-koodin koodisanoja merkinnällä $[\chi(U), \chi(V)]$. Koska molempien osien pituus on 2^r, on koodin $P(r)$ pituus 2^{r+1}.

Mikäli $U = \emptyset$, niin määritellään $\sum_{u \in U} u = 0$ ja jos $V = \emptyset$, niin määritellään $\sum_{v \in V} v = 0$.

Esimerkki 3.2.3. Olkoon $\mathbb{F}_8$ konstruoitu samalla tavalla kuin esimerkissä 1.4.6. Olkoon $U = \left\{\beta, \beta^2, \beta^5, 0\right\}$ ja $V = \left\{1, \beta, \beta^2, \beta^3, \beta^6, 0\right\}$. Tutkitaan, onko $[\chi(U), \chi(V)]$ koodin $P(3)$ koodisana. Merkitään laskuissa kunnan $\mathbb{F}_8$ alkiota $a_0 + a_1\beta + a_2\beta^2$ jonona $a_0a_1a_2$, jolloin laskut ovat helpommin seurattavissa. Huomioidaan myös, että $\beta^7 = 1 = \beta^0$.

(i) $|U| = 4$ ja $|V| = 6$, joten ehto (i) toteutuu.

(ii)

$$\sum_{u \in U} u = \beta + \beta^2 + \beta^5 + 0 = 010 + 001 + 111 + 000 = 100 = \beta^0 = 1$$

ja

$$\begin{aligned}\sum_{v \in V} v &= 1 + \beta + \beta^2 + \beta^3 + \beta^6 + 0 \\ &= 100 + 010 + 001 + 110 + 101 + 000 = 100 = \beta^0 = 1,\end{aligned}$$

joten ehto (ii) toteutuu.

(iii)

$$\begin{aligned}\sum_{u \in U} u^3 &= \beta^3 + \beta^6 + \beta^{15} + 0 = \beta^3 + \beta^6 + \beta \\ &= 110 + 101 + 010 = 001 = \beta^2\end{aligned}$$

ja

$$\sum_{u \in U} u^3 + \left(\sum_{u \in U} u\right)^3 = \beta^2 + 1 = 001 + 100 = 101 = \beta^6$$

sekä

$$\sum_{v \in V} v^3 = 1 + \beta^3 + \beta^6 + \beta^9 + \beta^{18} + 0 = 1 + \beta^3 + \beta^6 + \beta^2 + \beta^4$$
$$= 100 + 110 + 101 + 001 + 011 + 000 = 101 = \beta^6,$$

joten ehto (iii) toteutuu.

(iv) Luku $r = 3$ on pariton, joten ehto (iv) toteutuu.

Näin ollen $[\chi(U), \chi(V)] = 01100101\ 11110011$ on koodin $P(3)$ koodisana.

Huomataan, että alkion 0 kuuluminen joukkoihin U ja V ei vaikuta määritelmän 3.2.2 ehtojen (ii) ja (iii) laskuihin, eikä ehdon (iv) toteutumiseen. Laajennettujen Preparata-koodien koodisanojen osat $\chi(U)$ ja $\chi(V)$ ovat molemmat pariteetiltaan parillisia, eli niiden nollasta eroavien alkioiden määrä on aina parillinen. Käytännössä alkiolla 0 siis vaikutetaan vain siihen, toteutuuko ehto (i), eli ovatko $|U|$ ja $|V|$ parillisia. Näin ollen sanojen $\chi(U)$ ja $\chi(V)$ kohdassa $2^r - 1$ oleva arvo toimii pariteetintarkistusbittinä kyseisille sanoille.

3.3 Koodin sanojen etäisyydestä

Lemma 3.3.1. *Olkoot $[\chi(U), \chi(V)]$ ja $[\chi(A), \chi(B)]$ koodin $P(r)$ koodisanoja. Olkoon $\alpha = \sum_{u \in U} u$. Tällöin $[\chi(U \Delta A + \alpha), \chi(V \Delta B)]$ on myös koodin $P(r)$ koodisana.*

Todistus. Osoitetaan, että sana $[\chi(U \Delta A + \alpha), \chi(V \Delta B)]$ toteuttaa Määritelmän 3.2.2 ehdot (i)-(iii). Ehto (iv) on selvästi voimassa, koska luvun r arvo ei muutu.

(i) Koska $|U|$, $|V|$, $|A|$ ja $|B|$ ovat parillisia sekä $|U \Delta A + \alpha| = |U \Delta A|$, niin

$$|U \Delta A + \alpha| = |U \Delta A| = |U| + |A| - 2|U \cap A| \text{ on parillinen, ja}$$
$$|V \Delta B| = |V| + |B| - 2|V \cap B| \text{ on parillinen.}$$

(ii) Olkoot I ja J kunnan $\mathbb{F}_{2^r}$ osajoukkoja ja β kunnan primitiivialkio. Tällöin on voimassa yhtälö

$$\sum_{x \in I \Delta J} x = \sum_{x \in I} x + \sum_{x \in J} x.$$

Yhtäsuuruus on selvä sellaisten alkioiden osalta, jotka sisältyvät vain joukkoon I tai vain joukkoon J. Tarkastellaan vielä mitä tahansa alkiota β^i, joka sisältyy molempiin joukkoihin I ja J. Tällöin β^i ei esiinny ollenkaan yhtälön vasemman puolen summalausekkeessa, mutta β^i esiintyy yhteensä kaksi kertaa yhtälön oikean puolen summalausekkeissa. Huomioidaan, että $2\beta^i = 0$, koska kunnan $\mathbb{F}_{2^r}$ karakteristika on 2. Näin ollen alkio, joka sisältyy molempiin joukkoihin I ja J, ei vaikuta yhtälön yhtäsuuruuteen. Tästä saadaan

$$\sum_{x \in U \Delta A + \alpha} x = \sum_{y \in U \Delta A} (y + \alpha) = \sum_{y \in U \Delta A} y + \alpha |U \Delta A|.$$

Koska $|U \Delta A|$ on parillinen, on $\alpha |U \Delta A| = 0$. Tämän perusteella lauseke saadaan muotoon

$$\sum_{y \in U} y + \sum_{y \in A} y + 0 = \sum_{y \in V} y + \sum_{y \in B} y = \sum_{y \in V \Delta B} y.$$

Näin ollen

$$\sum_{x \in U \Delta A + \alpha} x = \sum_{y \in V \Delta B} y$$

ja ehto (ii) on voimassa.

(iii) Tarkastellaan ehdon (iii) mukaista summaa

$$\sum_{x \in U \Delta A + \alpha} x^3 + \left(\sum_{x \in U \Delta A + \alpha} x \right)^3.$$

Ehdon (ii) perusteella

$$\sum_{x \in U \Delta A + \alpha} x = \sum_{y \in V \Delta B} y,$$

joten

$$\sum_{x\in U\Delta A+\alpha} x^3 + \left(\sum_{x\in U\Delta A+\alpha} x\right)^3 = \sum_{y\in U\Delta A} (y+\alpha)^3 + \left(\sum_{y\in V\Delta B} y\right)^3$$
$$= \sum_{y\in U}(y+\alpha)^3 + \sum_{y\in A}(y+\alpha)^3 + \left(\sum_{y\in V} y + \sum_{y\in B} y\right)^3$$
$$= \sum_{y\in U} y^3 + \alpha\sum_{y\in U} y^2 + \alpha^2\sum_{y\in U} y + \alpha^3|U| + \sum_{y\in A} y^3 + \alpha\sum_{y\in A} y^2 + \alpha^2\sum_{y\in A} y + \alpha^3|A|$$
$$+\left(\sum_{y\in V} y\right)^3 + \left(\sum_{y\in V} y\right)^2\sum_{y\in B} y + \sum_{y\in V} y\left(\sum_{y\in B} y\right)^2 + \left(\sum_{y\in B} y\right)^3.$$

Huomioidaan nyt, että $\sum_{y\in U} y = \sum_{y\in V} y$ ja $\sum_{y\in A} y = \sum_{y\in B} y$ sekä lauseen 1.4.5 mukaan $\left(\sum_{y\in V} y\right)^2 = \sum_{y\in V} y^2$, jolloin lauseke saadaan muotoon

$$\sum_{y\in U} y^3 + \alpha\left(\sum_{y\in U} y\right)^2 + \alpha^2\sum_{y\in U} y + \alpha^3|U| + \sum_{y\in A} y^3 + \alpha\left(\sum_{y\in A} y\right)^2 + \alpha^2\sum_{y\in A} y + \alpha^3|A|$$
$$+\left(\sum_{y\in U} y\right)^3 + \left(\sum_{y\in U} y\right)^2\sum_{y\in A} y + \sum_{y\in U} y\left(\sum_{y\in A} y\right)^2 + \left(\sum_{y\in A} y\right)^3.$$

Seuraavaksi hyödynnetään tulosta $\alpha = \sum_{y\in U} y = \sum_{y\in V} y$, jonka jälkeen lauseke saadaan muotoon

$$\sum_{y\in U} y^3 + \alpha\alpha^2 + \alpha^2\alpha + \alpha^3|U| + \sum_{y\in A} y^3 + \alpha\left(\sum_{y\in A} y\right)^2 + \alpha^2\sum_{y\in A} y + \alpha^3|A|$$
$$+\left(\sum_{y\in U} y\right)^3 + \alpha^2\sum_{y\in A} y + \alpha\left(\sum_{y\in A} y\right)^2 + \left(\sum_{y\in A} y\right)^3$$

Kaikki lausekkeessa esiintyvät summan termit ovat kunnan $\mathbb{F}_{2^r}$ alkioita ja lisäksi kunnan $\mathbb{F}_{2^r}$ karakteristika on 2. Tämän perusteella kaikki lausekkeessa parillisen määrän kertoja esiintyvät summan termit eivät vaikuta summan suuruuteen, ts. $2a = 0$ kaikille $a \in \mathbb{F}_{2^r}$. Hyödyntämällä tätä tietoa sekä huo-

maamalla, että $|U|$ ja $|A|$ ovat parillisia, lauseke saadaan muotoon

$$\sum_{y\in U} y^3 + \left(\sum_{y\in U} y\right)^3 + \sum_{y\in A} y^3 + \left(\sum_{y\in A} y\right)^3.$$

Hyödynnetään vielä määritelmää 3.2.2, jolloin saadaan

$$\underbrace{\sum_{y\in U} y^3 + \left(\sum_{y\in U} y\right)^3}_{=\sum_{y\in V} y^3} + \underbrace{\sum_{y\in A} y^3 + \left(\sum_{y\in A} y\right)^3}_{=\sum_{y\in B} y^3} = \sum_{y\in V} y^3 + \sum_{y\in B} y^3 = \sum_{y\in V\Delta B} y^3.$$

Näin ollen

$$\sum_{x\in U\Delta A+\alpha} x^3 + \left(\sum_{x\in U\Delta A+\alpha} x\right)^3 = \sum_{y\in V\Delta B} y^3$$

ja ehto (iii) on voimassa.

□

Määritelmä 3.3.2. Koodia sanotaan *etäisyysinvariantiksi*, jos mille tahansa koodisanaparille c_1 ja c_2 pätee se, että koodisanasta c_1 etäisyydellä i sijaitsevien koodisanojen lukumäärä on sama kuin koodisanasta c_2 etäisyydellä i sijaitsevien koodisanojen lukumäärä, missä $1 \leq i \leq n$ ja n on koodin pituus.

Huomautus 3.3.3. Määritelmästä 3.3.2 seuraa suoraan se, että etäisyysinvariantille koodille C pätee

$$d_{\min}C = \min\{\mathrm{wt}(\mathbf{x}) \mid \mathbf{x} \in C, \mathbf{x} \neq \mathbf{0}\}.$$

Lemma 3.3.4. *Olkoot $A, B, C \subseteq \mathbb{F}_{2^r}$ ja $\alpha \in \mathbb{F}_{2^r}$. Tällöin*

(a) $\mathrm{d}(\chi(A), \chi(B)) = \mathrm{d}(\chi(A+\alpha), \chi(B+\alpha))$,

(b) $\mathrm{d}(\chi(A), \chi(B)) = \mathrm{d}(\chi(A\Delta C), \chi(B\Delta C))$.

Todistus. (a) Nyt

$$\mathrm{d}(\chi(A), \chi(B)) = |(A\cup B)\setminus(A\cap B)| = |\{x \mid x \in A \text{ tai } x \in B \text{ mutta } x \notin A\cap U\}|.$$

Koska

$$A + \alpha = \{a + \alpha \mid a \in A\} \text{ ja } B + \alpha = \{b + \alpha \mid b \in B\},$$

on myös

$$|(A + \alpha \cup B + \alpha) \setminus (A + \alpha \cap B + \alpha)| = |(A \cup B) \setminus (A \cap B)|,$$

joten

$$\mathrm{d}(\chi(A), \chi(B)) = \mathrm{d}(\chi(A + \alpha), \chi(B + \alpha)).$$

(b) Olkoon

$$\chi(A) = a_1 a_2 \dots a_n, \chi(B) = b_1 b_2 \dots b_n \text{ ja } \chi(C) = c_1 c_2 \dots c_n.$$

Jos sanojen $\chi(A)$ ja $\chi(B)$ mielivaltaisessa kohdassa k olevat komponentit a_k ja b_k ovat samat, ovat sanojen $\chi(A\Delta C)$ ja $\chi(B\Delta C)$ vastaavassa kohdassa olevat komponentit molemmat joko 0 tai 1 riippuen c_k:n arvosta. Jos taas sanojen $\chi(A)$ ja $\chi(B)$ mielivaltaisessa kohdassa olevat komponentit a_k ja b_k ovat erisuuret, ovat sanojen $\chi(A\Delta C)$ ja $\chi(B\Delta C)$ vastaavassa kohdassa olevat komponentit erisuuria. Näin ollen $\mathrm{d}(\chi(A), \chi(B)) = \mathrm{d}(\chi(A\Delta C), \chi(B\Delta C))$.

□

Seuraus 3.3.5. *Olkoot* $[\chi(U), \chi(V)]$ *ja* $[\chi(A), \chi(B)]$ *laajennetun Preparata-koodin koodisanoja sekä* $\alpha \in \mathbb{F}_{2^r}$ *ja* $C \subset \mathbb{F}_{2^r}$*. Tällöin pätee*

(a) $\mathrm{d}([\chi(U), \chi(V)], [\chi(A), \chi(B)]) = \mathrm{d}([\chi(U + \alpha), \chi(V)], [\chi(A + \alpha), \chi(B)])$,

(b) $\mathrm{d}([\chi(U), \chi(V)], [\chi(A), \chi(B)]) = \mathrm{d}([\chi(U\Delta C), \chi(V)], [\chi(A\Delta C), \chi(B)])$.

Lause 3.3.6. *Koodi* $P(r)$ *on etäisyysinvariantti.*

Todistus. Olkoot $[\chi(U), \chi(V)]$ ja $[\chi(A), \chi(B)]$ mielivaltaisia koodin $P(r)$ koodisanoja, joiden välinen etäisyys on $i \geq 1$. Olkoon $\alpha = \sum_{u \in U} u$.

Lemman 3.3.1 perusteella myös sanat

$$[\chi(U\Delta U + \alpha), \chi(V\Delta V)] \text{ ja } [\chi(U\Delta A + \alpha), \chi(V\Delta B)]$$

ovat koodisanoja. Seurauksen 3.3.5 mukaan

$$\mathrm{d}([\chi(U\Delta U+\alpha),\chi(V\Delta V)],[\chi(U\Delta A+\alpha),\chi(V\Delta B)])=i.$$

Koska joukko $U\Delta U = V\Delta V = \emptyset$, niin $[\chi(U\Delta U+\alpha),\chi(V\Delta V)] = [\chi(\emptyset),\chi(\emptyset)]$ on nollasana. Näin ollen sanan $[\chi(U\Delta A+\alpha),\chi(V\Delta B)]$ paino on i. Siis jokaista mielivaltaisesti valittua koodisanaparia, joiden etäisyys toisistaan on $i \geq 1$, kohden löytyy yksi koodisana, jonka paino on i.

Olkoon nyt koodisanan $[\chi(C),\chi(D)]$ paino i ja olkoon koodisana $[\chi(S),\chi(T)]$ mielivaltainen. Olkoon lisäksi $\beta = \sum_{s\in S}$. Lemman 3.3.1 perusteella myös sanat

$$[\chi(S\Delta\emptyset+\beta),\chi(T\Delta\emptyset)] = [\chi(S+\beta),\chi(T)]$$

ja

$$[\chi(C\Delta S+\beta),\chi(D\Delta T)]$$

ovat koodisanoja. Edelleen seurauksen 3.3.5 perusteella

$$\begin{aligned}\mathrm{wt}([\chi(C),\chi(D)]) &= \mathrm{d}\left([\chi(\emptyset),\chi(\emptyset)],[\chi(C),\chi(D)]\right)\\ &= \mathrm{d}\left([\chi(\emptyset\Delta S+\beta),\chi(\emptyset\Delta T)],[\chi(C\Delta S+\beta),\chi(D\Delta T)]\right)\\ &= \mathrm{d}\left([\chi(S+\beta),\chi(T)],[\chi(C\Delta S+\beta),\chi(D\Delta T)]\right)\\ &= i.\end{aligned}$$

Näin ollen jokaista koodisanaa $[\chi(C),\chi(D)]$, jonka paino on i, vastaa koodisanapari $[\chi(S+\beta),\chi(T)],[\chi(C\Delta S+\beta),\chi(D\Delta T)]$, joiden välinen etäisyys on i.

Nyt siis jokaista mielivaltaisesti valittua koodisanaparia, joiden välinen etäisyys in i, kohti löydetään sellainen koodisana, jonka paino on i ja samaan aikaan jokaista mielivaltaisesti valittua koodisanaa, jonka paino on i, kohti löydetään nollasanasta eroavat kaksi koodisanaa, joiden välinen etäisyys on i. Näin ollen koodi $P(r)$ on etäisyysinvariantti.

□

3.4 Koodin $P(r)$ minimietäisyys ja epälineaarisuus

Lemma 3.4.1. *Oletetaan, että* $[\chi(U), \chi(V)]$ *on koodin* $P(r)$ *koodisana ja* $\alpha \in \mathbb{F}_{2^r}$ *on mielivaltainen. Tällöin koodi* $P(r)$ *sisältää myös seuraavat koodisanat:*

(a) $[\chi(V), \chi(U)]$,

(b) $[\chi(U + \alpha), \chi(V + \alpha)]$ *mille tahansa* $\alpha \in \mathbb{F}_{2^r}$,

(c) $[\chi(\alpha U), \chi(\alpha V)]$ *mille tahansa* $\alpha \in \mathbb{F}_{2^r}, \alpha \neq 0$.

Todistus. Todistetaan, että väitetyt koodisanat toteuttavat määritelmän 3.2.2 mukaiset ehdot (i)-(iv). Huomioidaan laskuissa erityisesti se, että $\text{char}\, \mathbb{F}_{2^r} = 2$, joten $2a = 0$ kaikille $a \in \mathbb{F}_{2^r}$.

(a) Määritelmän 3.2.2 ehdot (i), (ii) ja (iv) ovat selvästi voimassa.

Tarkastellaan ehdon (iii) mukaista summaa

$$\sum_{v \in V} v^3 + \left(\sum_{v \in V} v \right)^3 .$$

Huomioidaan, että $[\chi(U), \chi(V)]$ on koodisana, jolloin voidaan hyödyntää määritelmän 3.2.2 ehtoja (ii) ja (iii) ja saadaan

$$\begin{aligned} &\sum_{v \in V} v^3 + \left(\sum_{v \in V} v \right)^3 = \sum_{u \in U} u^3 + \left(\sum_{u \in U} u \right)^3 + \left(\sum_{v \in V} v \right)^3 \\ &= \sum_{u \in U} u^3 + \left(\sum_{v \in v} v \right)^3 + \left(\sum_{v \in V} v \right)^3 = \sum_{u \in U} u^3 . \end{aligned}$$

Näin ollen ehto (iii) on voimassa ja $[\chi(V), \chi(U)]$ on koodin $P(r)$ koodisana.

(b) Määritelmän 3.2.2 ehto (iv) on selvästi voimassa. Osoitetaan muiden ehtojen voimassaolo

(i) Koska $|U + \alpha| = |U|$ on parillinen ja $|V + \alpha| = |V|$ on parillinen, ehto on voimassa.

(ii) Tarkastellaan ehdon (ii) mukaista summaa $\sum_{u\in U+\alpha} u$. Huomioidaan jälleen, että $[\chi(U), \chi(V)]$ on koodisana, jolloin saadaan

$$\sum_{u\in U+\alpha} u = \sum_{x\in U}(x+\alpha)\sum_{x\in U} x + \alpha|U| = \sum_{x\in U} x = \sum_{y\in V} y$$
$$= \sum_{y\in V} y + \alpha|V| = \sum_{y\in V}(y+\alpha) = \sum_{v\in V+\alpha} v.$$

Näin ollen

$$\sum_{u\in U+\alpha} u = \sum_{v\in V+\alpha} v$$

ja ehto on voimassa.

(iii) Tarkastellaan ehdon (iii) mukaista summaa

$$\sum_{u\in U+\alpha} u^3 + \left(\sum_{u\in U+\alpha} u\right)^3 = \sum_{y\in U}(y+\alpha)^3 + \left(\sum_{y\in U}(y+\alpha)\right)^3$$
$$= \sum_{y\in U} y^3 + \alpha\sum_{y\in U} y^2 + \alpha^2\sum_{y\in U} y + \alpha^3|U| + \left(\sum_{y\in U} y + \alpha|U|\right)^3.$$

Tämän jälkeen huomioidaan, että $\sum_{y\in U} y^2 = \left(\sum_{y\in U} y\right)^2$ ja $|U|$ on parillinen, jolloin lauseke saadaan muotoon

$$\sum_{y\in U} y^3 + \alpha\left(\sum_{y\in U} y\right)^2 + \alpha^2\sum_{y\in U} y + \alpha^3|U| + \left(\sum_{y\in U} y\right)^3$$
$$= \sum_{y\in U} y^3 + \left(\sum_{y\in U} y\right)^3 + \alpha\left(\sum_{y\in U} y\right)^2 + \alpha^2\sum_{y\in U} y + \alpha^3|U|.$$

Koska $[\chi(U), \chi(V)]$ on koodisana, niin $\sum_{y\in U} y = \sum_{y\in V} y$ ja $\sum_{y\in U} y^3 + \left(\sum_{y\in U} y\right)^3 = \sum_{y\in V} y^3$. Lisäksi $\alpha^3|U| = 0 = \alpha^3|V|$, koska $|U|$ ja $|V|$ ovat parillisia. Myös $\sum_{y\in U} y^2 = \left(\sum_{y\in U} y\right)^2$. Huomioidaan vielä ehdon (ii) voi-

massaolo, jolloin lauseke saadaan muotoon

$$\begin{aligned}
&\sum_{y\in V} y^3 + \alpha\left(\sum_{y\in V} y\right)^2 + \alpha^2 \sum_{y\in V} y + \alpha^3|U| \\
&= \sum_{y\in V} y^3 + \alpha \sum_{y\in V} y^2 + \alpha^2 \sum_{y\in V} y + \alpha^3|V| \\
&= \sum_{y\in V} (y+\alpha)^3 = \sum_{v\in V+\alpha} v^3.
\end{aligned}$$

Näin ollen

$$\sum_{u\in U+\alpha} u^3 + \left(\sum_{u\in U+\alpha} u\right)^3 = \sum_{v\in V+\alpha} v^3,$$

joten ehto on voimassa ja $[\chi(U+\alpha), \chi(V+\alpha)]$ on koodin $P(r)$ koodisana.

(c) Määritelmän 3.2.2 ehto (iv) on selvästi voimassa. Osoitetaan muiden ehtojen voimassaolo:

(i) Koska $|\alpha U| = |U|$ on parillinen ja $|\alpha V| = |V|$ on parillinen, ehto on voimassa.

(ii) Tarkastellaan ehdon (ii) mukaista summaa $\sum_{u\in\alpha U} u$. Huomioidaan jälleen, että $[\chi(U), \chi(V)]$ on koodisana, jolloin saadaan

$$\sum_{u\in\alpha U} u = \sum_{x\in U} (\alpha x) = \alpha \sum_{x\in U} x = \alpha \sum_{y\in V} y = \sum_{y\in V} (\alpha y) = \sum_{v\in\alpha V} v.$$

Näin ollen

$$\sum_{u\in\alpha U} u = \sum_{v\in\alpha V} v$$

ja ehto on voimassa.

(iii) Tarkastellaan ehdon (iii) mukaista summaa

$$\sum_{u\in\alpha U} u^3 + \left(\sum_{u\in\alpha U} u\right)^3 = \sum_{y\in U}(\alpha y)^3 + \left(\sum_{y\in U}\alpha y\right)^3$$
$$=\alpha^3\sum_{y\in U} y^3 + \alpha^3\left(\sum_{y\in U} y\right)^3 = \alpha^3\left(\sum_{y\in U} y^3 + \left(\sum_{y\in U} y\right)^3\right).$$

Koska $[\chi(U), \chi(V)]$ on koodisana, niin $\sum_{y\in U} y^3 + \left(\sum_{y\in U} y\right)^3 = \sum_{y\in V} y^3$, jolloin lauseke saadaan muotoon

$$\alpha^3\sum_{y\in V} y^3 = \sum_{y\in V}(\alpha y)^3 = \sum_{v\in\alpha V} v^3.$$

Näin ollen

$$\sum_{u\in\alpha U} u^3 + \left(\sum_{u\in\alpha U} u\right)^3 = \sum_{v\in\alpha V} v^3,$$

joten ehto on voimassa ja $[\chi(\alpha U), \chi(\alpha V)]$ on koodin $P(r)$ koodisana.

□

Esimerkki 3.4.2. Tarkastellaan koodia $P(3)$. Olkoon $U = \left\{\beta, \beta^2, \beta^5, 0\right\}$ ja $V = \left\{1, \beta, \beta^2, \beta^3, \beta^6, 0\right\}$. Esimerkin 3.2.3 perusteella näistä joukoista muodostettu sana $[\chi(U), \chi(V)] = 01100101\ 11110011$ on koodisana koodissa $P(3)$. Soveltamalla lemmaa 3.4.1 tähän koodisanaan käyttämällä arvoa $\alpha = \beta^3$ saadaan kolme uutta koodisanaa:

(a)

$$[\chi(V), \chi(U)] = 11110011\ 01100101.$$

(b)

$$[\chi(U+\alpha), \chi(V+\alpha)] = \left[\chi\left(\left\{\beta^0, \beta^5, \beta^2, \beta^3\right\}\right), \chi\left(\left\{\beta, \beta^0, \beta^5, 0, \beta^4, \beta^3\right\}\right)\right]$$
$$= 10110100\ 11011101.$$

(c)

$$[\chi(\alpha U), \chi(\alpha V)] = \left[\chi\left(\left\{\beta^4, \beta^5, \beta, 0\right\}\right), \chi\left(\left\{\beta^3, \beta^4, \beta^5, \beta^6, \beta^2, 0\right\}\right)\right]$$
$$= 01001101\ 00111111.$$

Lemma 3.4.1 yksinkertaistaa koodin $P(r)$ minimietäisyyttä koskevan tuloksen osoittamista. Ennen minimietäisyyttä koskevaa tulosta tarvitaan vielä kaksi lemmaa.

Lemma 3.4.3.

(a) Olkoon r pariton luku. Tällöin $2^r - 1 \equiv 1$ (mod 3).

(b) Olkoon r parillinen luku. Tällöin $2^r - 1 \equiv 0$ (mod 3).

Todistus. Käytetään induktiota.

(a) Perusaskel $r = 1$: Nyt $2^1 - 1 = 1 \equiv 1 \pmod 3$ pätee.

Induktio-oletus $r = k$: Oletetaan, että $2^k - 1 \equiv 1 \pmod 3$, ts. $2^k - 1 = 3x + 1$ jollekin luvulle x. Tällöin $2^k = 3x + 2$.

Induktioväite: Väite on voimassa, kun $r = k + 2$. Nyt

$$2^{(k+2)} - 1 = 4 \cdot 2^k - 1.$$

Induktio-oletuksen perusteella

$$4 \cdot 2^k - 1 = 4 \cdot (3x + 2) - 1 = 12x + 7 = 3(4x + 2) + 1,$$

eli

$$2^{(k+2)} - 1 \equiv 1 \pmod 3.$$

Induktioperiaatteen nojalla väite on tosi.

(b) Perusaskel $r = 2$: Nyt $2^2 - 1 = 3 \equiv 0 \pmod 3$ pätee.

Induktio-oletus $r = k$: Oletetaan, että $2^k - 1 \equiv 0 \pmod 3$, ts. $2^k - 1 = 3x$ jollekin luvulle x. Tällöin $2^k = 3x + 1$.

Induktioväite: Väite on voimassa, kun $r = k + 2$. Nyt

$$2^{(k+2)} - 1 = 4 \cdot 2^k - 1.$$

Induktio-oletuksen perusteella

$$4 \cdot 2^k - 1 = 4 \cdot (3x + 1) - 1 = 12x + 3 = 3(4x + 1),$$

eli

$$2^{(k+2)} - 1 \equiv 0 \pmod 3.$$

Induktioperiaatteen nojalla väite on tosi.

□

Seuraava lemma perustelee syyn sille, että luvun r on oltava pariton.

Lemma 3.4.4. *Olkoon β kunnan $\mathbb{F}_{2^r}$ primitiivialkio. Tällöin myös β^3 on kunnan $\mathbb{F}_{2^r}$ primitiivialkio, jos luku r on pariton. Alkio β^3 ei ole kunnan $\mathbb{F}_{2^r}$ primitiivialkio, jos luku r on parillinen.*

Todistus. Lauseen 1.4.4 perusteella tiedetään, että alkio β^i on kunnan primitiivialkio jos ja vain jos $\text{syt}(i, 2^r - 1) = 1$.

Lemman 3.4.3 perusteella tiedetään, että jos luku r on pariton, niin $2^r - 1 \equiv 1 \pmod 3$ ja jos luku r on parillinen, niin $2^r - 1 \equiv 0 \pmod 3$.

Jos siis luku r on parillinen, on $2^r - 1 = 3x$ jollekin kokonaisluvulle x, joten β^3 ei ole primitiivialkio. Jos taas luku r on pariton, niin $2^r - 1 = 3x + 1$, joten β^3 on primitiivialkio. □

Seuraus 3.4.5. *Jos luku r on pariton, niin tällöin jokaista nolla-alkiosta eroavaa alkiota $x \in \mathbb{F}_{2^r}$ kohden on olemassa yksikäsitteinen alkio y, jolle $y^3 = x$.*

Lause 3.4.6. *Koodin $P(r)$ minimietäisyys on 6.*

Todistus. Jos koodin $P(r)$ sisältämän koodisanan $[\chi(U), \chi(V)]$ paino on d, niin

$$d = \text{wt}(\chi(U)) + \text{wt}(\chi(V)) = |U| + |V|.$$

Koodin $P(r)$ määritelmästä seuraa, että d ei voi olla pariton. Koodi $P(r)$ on etäisyysinvariantti. Tällöin riittää osoittaa, että $d \neq 2$, $d \neq 4$ ja että on olemassa koodisana, jonka paino on 6.

Oletetaan, että $d = 2$. Lemman 3.4.1 kohdan (a) perusteella voidaan olettaa, että $|U| = 2$ ja $|V| = 0$. Lemman 3.4.1 kohdan (b) perusteella voidaan olettaa, että $U = \{0, x\}$ jollain $x \in \mathbb{F}_{2^r}, x \neq 0$. Tällöin kuitenkin

$$\sum_{u \in U} u = 0 + x = x.$$

Koska $V = \emptyset$, ei määritelmän 3.2.2 ehto (ii) voi toteutua, joten $d \neq 2$.

Oletetaan nyt, että $d = 4$. Lemman 3.4.1 kohdan (a) perusteella voidaan olettaa, että joko $|U| = 4$ ja $|V| = 0$ tai $|U| = 2$ ja $|V| = 2$.

Oletetaan aluksi, että $|U| = 4$ ja $|V| = 0$. Tällöin voidaan Lemman 3.4.1 kohdan (b) perusteella olettaa, että $U = \{0, x, y, z\}$, missä $x, y, z \in \mathbb{F}_{2^r}$ ovat kaikki erisuuria ja nolla-alkiosta eroavia. Määritelmän 3.2.2 kohdan (iii) perusteella

$$0^3 + x^3 + y^3 + z^3 + (0 + x + y + z)^3 = 0. \tag{3.1}$$

Yhtälön (2.1) jälkimmäinen osa voidaan saattaa muotoon

$$\begin{aligned}
&(0 + x + y + z)^3 \\
&= x^3 + y^3 + z^3 + 3x^2y + 3x^2z + 3xy^2 + 3y^2z + 3xz^2 + 3yz^2 + 6xyz \\
&= x^3 + y^3 + z^3 + x^2y + x^2z + xy^2 + y^2z + xz^2 + yz^2 + 2xyz \\
&+ 2(x^2y + x^2z + xy^2 + y^2z + xz^2 + yz^2 + 2xyz) \\
&= x^3 + y^3 + z^3 + (x + y)(x + z)(y + z).
\end{aligned}$$

Sijoitetaan tämä tulos yhtälöön (2.1), jolloin saadaan

$$0^3 + x^3 + y^3 + z^3 + (0 + x + y + z)^3 = 0,$$

eli

$$x^3 + y^3 + z^3 + x^3 + y^3 + z^3 + (x + y)(x + z)(y + z) = 0,$$

joten

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

mikä on mahdotonta, koska x, y ja z ovat keskenään erisuuria ja nolla-alkiosta eroavia.

Oletetaan seuraavaksi, että $|U| = 2$ ja $|V| = 2$. Tällöin voidaan edelleen Lemman 3.4.1 kohdan (b) perusteella olettaa, että $U = \{0, x\}$ ja $V = \{y, z\}$, $y \neq z$. Tällöin määritelmän 3.2.2 kohdan (iii) perusteella

$$0^3 + x^3 + (0 + x)^3 = y^3 + z^3,$$

eli

$$y^3 + z^3 = 0.$$

Seurauksen 3.4.5 perusteella tiedetään, että jos $y^3 = z^3$, niin $y = z$, mikä on ristiriita. Näin ollen $d \neq 4$.

Etsitään seuraavaksi koodisana, jonka paino on 6. Olkoon $x, y, z \in \mathbb{F}_{2^r}$, missä x, y ja z ovat kaikki erisuuria ja nolla-alkiosta eroavia. Seurauksen 3.4.5 perusteella on olemassa yksikäsitteinen $w \in \mathbb{F}_{2^r}$, jolle $w^3 = x^3 + y^3 + z^3$. Alkiolle w pätee $w \neq x$, $w \neq y$ ja $w \neq z$, koska jos olisi esimerkiksi $w = x$, niin $w^3 = x^3$, jolloin olisi $0 = y^3 + z^3$ ja seurauksen 3.4.5 perusteella edelleen $y = z$, mikä on ristiriita.

Määritellään seuraavaksi alkio $u = w + x + y + z$. Koska summa

$$\begin{aligned} w^3 + (x + y + z)^3 &= x^3 + y^3 + z^3 + (x + y + z)^3 \\ &= x^3 + y^3 + z^3 + x^3 + y^3 + z^3 + (x + y)(x + z)(y + z) \\ &= (x + y)(x + z)(y + z) \neq 0, \end{aligned}$$

niin $w^3 \neq (x + y + z)^3$ ja seurauksen 3.4.5 perusteella myös $w \neq x + y + z$. Näin ollen $u \neq 0$.

Olkoon nyt $U = \{0, u\}$ ja $V = \{w, x, y, z\}$. Osoitetaan, että sana $[\chi(U), \chi(V)]$ on koodin $P(r)$ koodisana. Määritelmän 3.2.2 ehdot (i) ja (iv) ovat selvästi voimassa.

Tarkatellaan ehdon (ii) mukaista summaa:

$$\sum_{a \in U} a = u = w + x + y + z = \sum_{b \in V} b.$$

Näin ollen ehto (ii) on voimassa.

Tarkastellaan ehdon (iii) vasenta puolta:

$$\sum_{a\in U} a^3 + \left(\sum_{a\in U}\right)^3 = u^3 + u^3 = 0.$$

Tarkastellaan seuraavaksi ehdon (iii) oikeata puolta:

$$\sum_{b\in V} b^3 = w^3 + x^3 + y^3 + z^3 = w^3 + w^3 = 0.$$

Näin ollen

$$\sum_{a\in U} a^3 + \left(\sum_{a\in U} a\right)^3 = \sum_{b\in V} b^3,$$

ja $[\chi(U), \chi(V)]$ on koodin $P(r)$ koodisana, jonka paino on 6.

□

Esimerkki 3.4.7. Olkoon $\mathbb{F}_8$ konstruoitu kuten esimerkissä 1.4.6. Olkoot $x = \beta$, $y = \beta^3$ ja $z = \beta^5$ kunnan $\mathbb{F}_8$ alkioita. Määritellään tämän jälkeen alkio $w \in \mathbb{F}_8$ siten, että

$$\begin{aligned} w^3 = x^3 + y^3 + z^3 = \beta^3 + \beta^9 + \beta^{15} = \beta^3 + \beta^2 + \beta \\ =110 + 001 + 010 = 101 = \beta^6 = \left(\beta^2\right)^3, \end{aligned}$$

joten $w = \beta^2$. Olkoon

$$\begin{aligned} u = w + x + y + z = \beta^2 + \beta + \beta^3 + \beta^5 \\ =001 + 010 + 110 + 111 = 010 = \beta. \end{aligned}$$

Määritellään joukot $U = \{0, \beta\}$ ja $V = \left\{\beta^2, \beta, \beta^3, \beta^5\right\}$. Tällöin sana $[\chi(U), \chi(V)] =$ 01000001 01110100 on koodin $P(3)$ koodisana, jonka paino on 6.

Lause 3.4.8. *Koodi $P(r)$ ei ole lineaarinen.*

Todistus. Lineaarinen koodi on lineaariavaruus, jolloin kaikki koodisanojen lineaarikombinaatiot ovat myös koodisanoja.

Aiemmin on todettu, että $[\chi(U), \chi(V)] + [\chi(A), \chi(B)] = [\chi(U \Delta A), \chi(V \Delta B)]$. Lauseen 3.4.6 avulla voidaan konstruoida koodin $P(r)$ koodisanat $[\chi(U), \chi(V)]$ ja $[\chi(A), \chi(B)]$ siten, että $U = \{0, u_1\}$, $V = \{w_1, x_1, y_1, z_1\}$, $A = \{0, u_2\}$ ja $B = \{w_2, x_2, y_2, z_2\}$. Lemman 3.3.1 perusteella sana $[\chi(U \Delta A + u_1), \chi(V \Delta B)]$ on koodin $P(r)$ koodisana.

Koska $|U \Delta A + u_1| \leq 2$, niin

$$d\left([\chi(U \Delta A + u_1), \chi(V \Delta B)], [\chi(U \Delta A), \chi(V \Delta B)]\right) \leq 2|U \Delta A + u_1| \leq 4.$$

Koodin $P(r)$ minimietäisyys on 6, joten sana $[\chi(U \Delta A), \chi(V \Delta B)]$ ei ole koodin $P(r)$ koodisana.

Näin ollen koodi $P(r)$ ei ole lineaarinen.

□

Luku 4

Koodausalgoritmi laajennetuille Preparata-koodeille

4.1 Yleistä

Tässä luvussa esitellään algoritmi, jonka avulla viestivektoreita koodataan laajennettujen Preparata-koodien koodisanoiksi. Algoritmissa hyödynnetään aikaisemmin esiteltyjä BCH-koodeja koskevia tuloksia sekä aiemmin esitettyä kaksi virhettä korjaavan BCH-koodin tarkistusmatriisia H.

Koska laajennetut Preparata-koodit eivät ole lineaarisia, ei niillä ole dimensiota. Tämä tarkoittaa myös sitä, että koodin $P(r)$ koodisanojen lukumäärää ei vielä tiedetä. Sanojen lukumäärä saadaan kuitenkin määriteltyä koodausalgoritmia käsittelevän teorian yhteydessä.

4.2 Koodin $P(r)$ koodisanojen lukumäärä

Olkoon matriisi H lemman 2.3.9 mukainen kaksi virhettä korjaavan BCH-koodin tarkistusmatriisi, eli

$$H = \begin{bmatrix} \beta^0 & \beta^0 \\ \beta^1 & \beta^3 \\ \beta^2 & \beta^6 \\ \vdots & \vdots \\ \beta^i & \beta^{3i} \\ \vdots & \vdots \\ \beta^{2^r-2} & \beta^{3(2^r-2)} \end{bmatrix}.$$

Olkoon A matriisin H alimatriisi, joka muodostuu matriisin H viimeisistä $2r$ rivistä. Olkoon H' matriisin H alimatriisi, joka muodostuu poistamalla matriisista H sen $2r$ alinta riviä. Lemman 2.3.11 perusteella matriisin A aste on $2r$, joten käänteismatriisi A^{-1} on olemassa.

Olkoon $m = [m_L, m_R]$ mikä tahansa binäärinen sana, jonka pituus on $2^{r+1} - 2r - 2$, $r \geq 1$, ja missä sanan m_L pituus on $2^r - 1$ ja sanan m_R pituus on $2^r - 2r - 1$.

Tulkitaan sen jälkeen sanat m_L ja m_R polynomeiksi sillä tavalla, että

$$m_L(x) = \sum_{i=0}^{2^r-1} a_i x^i, \text{ missä } a_i = m_{L_i}$$

ja

$$m_R(x) = \sum_{i=0}^{2^r-2r-1} b_i x^i, \text{ missä } b_i = m_{R_i}.$$

Tällä tavalla tulkittuna saadaan muodostettua seuraavat sanat, jotka muodostuvat kahdesta kunnan $\mathbb{F}_{2^r}$ alkiosta:

$$[m_L(\beta), m_L(\beta^3)] = m_L H$$

ja

$$[m_R(\beta), m_R(\beta^3)] = m_R H',$$

Määritellään lisäksi pituudeltaan $2r$ oleva sana

$$v_R = [m_L(\beta) + m_R(\beta), m_L(\beta^3) + (m_L(\beta))^3 + m_R(\beta^3)]A^{-1},$$

missä ensimmäinen osa $m_L(\beta) + m_R(\beta)$ tulkitaan binäärivektoriksi sillä tavalla, että yhteenlaskun jälkeen alkio $m_L(\beta) + m_R(\beta)$ muutetaan binäärivektoriksi, jonka pituus on r. Jälkimmäinen osa $m_L(\beta^3) + (m_L(\beta))^3 + m_R(\beta^3)$ tulkitaan vastaavalla tavalla binäärivektoriksi, jonka pituus on r.

Lause 4.2.1. *Olkoon r pariton luku ja $m = [m_L, m_R]$ binäärinen sana, jonka pituus on $2^{r+1} - 2r - 2$. Olkoot $\chi(U) = [m_L, p_L]$, missä $p_L \in \{0, 1\}$ siten, että* $\mathrm{wt}([m_L, p_L])$ *on parillinen ja $\chi(V) = [m_R, v_R, p_R]$, missä $p_R \in \{0, 1\}$ siten, että* $\mathrm{wt}([m_R, v_R, p_R])$ *on parillinen. Alkioita p_L ja p_R kutsutaan pariteetintarkistusbiteiksi. Tällöin sana $[\chi(U), \chi(V)] = [m_L, p_L, m_R, v_R, p_R]$ on koodin $P(r)$ koodisana.*

Todistus. Olkoot matriisit H, H' ja A määritelty samalla tavalla kuin aikaisemmin. Tällöin

$$\begin{aligned}
[m_R, v_R]H &= [m_R]H' + [v_R]A \\
&= [m_R(\beta), m_R(\beta^3)] + [m_L(\beta) + m_R(\beta), m_L(\beta^3) + (m_L(\beta))^3 + m_R(\beta^3)]A^{-1}A \\
&= [m_R(\beta) + m_L(\beta) + m_R(\beta), m_R(\beta^3) + m_L(\beta^3) + (m_L(\beta))^3 + m_R(\beta^3)] \\
&= [m_L(\beta), m_L(\beta^3) + (m_L(\beta))^3].
\end{aligned}$$

Joukko U on nyt

$$U = \{b^i \mid \text{ sanan } \chi(U) \text{ kohdassa } i \text{ on } 1,\ 0 \le i \le 2^r - 2\} \cup \{0 \mid \text{, jos } p_L = 1\}$$

ja joukko V on

$$V = \{b^i \mid \text{ sanan } \chi(V) \text{ kohdassa } i \text{ on } 1,\ 0 \le i \le 2^r - 2\} \cup \{0 \mid \text{, jos } p_R = 1\}$$

Näin ollen

$$[m_R, v_R]H = \left[\sum_{v \in V} v, \sum_{v \in V} v^3\right].$$

Vastaavasti

$$m_L(\beta) = \sum_{u \in U} u$$

ja

$$m_L(\beta^3) + (m_L(\beta))^3 = \sum_{u \in U} u^3 + \left(\sum_{u \in U} u \right)^3 .$$

Nyt

$$\left[\sum_{v \in V} v, \sum_{v \in V} v^3 \right] = [m_R, v_R]H$$

$$= [m_L(\beta), m_L(\beta^3) + (m_L(\beta))^3] = \left[\sum_{u \in U} u, \sum_{u \in U} u^3 + \left(\sum_{u \in U} u \right)^3 \right],$$

joten

$$\left[\sum_{v \in V} v, \sum_{v \in V} v^3 \right] = \left[\sum_{u \in U} u, \sum_{u \in U} u^3 + \left(\sum_{u \in U} u \right)^3 \right],$$

eli

$$\sum_{u \in U} u = \sum_{v \in V} v$$

ja

$$\sum_{u \in U} u^3 + \left(\sum_{u \in U} u \right)^3 = \sum_{v \in V} v^3 .$$

Näin ollen määritelmän 3.2.2 ehdot (ii) ja (iii) ovat voimassa. Myös määritelmän 3.2.2 ehdot (i) ja (iv) ovat selvästi voimassa. Tämä tarkoittaa, että sana $[\chi(U), \chi(V)]$ on koodin $P(r)$ koodisana. □

Seuraus 4.2.2. *Koodissa $P(r)$ on $2^{2^{r+1}-2r-2}$ koodisanaa.*

Todistus. Lauseessa 4.2.1 on $2^{2^{r+1}-2r-2}$ eri tapaa valita sana $m = [m_L, m_R]$. Jokaisesta erilaisesta valinnasta saadaan erilainen koodisana, jonka osat p_L, v_R ja p_R määrittyvät yksikäsitteisesti sanan m perusteella. Näin ollen koodissa $P(r)$ on yhteensä $2^{2^{r+1}-2r-2}$ koodisanaa. □

4.3 Koodin $P(r)$ koodausalgoritmi

Algoritmi 4.3.1. [Laajennetun Preparata-koodin $P(r)$ koodaus] Olkoon m_L binäärinen sana, jonka pituus on $2^r - 1$ ja olkoon m_R binäärinen sana, jonka pituus on $2^r - 2r - 1$. Määritellään v_R samalla tavalla kuin lauseessa 4.2.1. Tällöin sana $[m_L, p_L, m_R, v_R, p_R]$ on viestiä $m = [m_L, m_R]$ vastaava koodisana.

Esimerkki 4.3.2. Olkoot $r = 3$, $m_L = 0110010$ ja $m_R = 1$. Tällöin

$$m_L(\beta) = \beta + \beta^2 + \beta^5 = \beta^0 \text{ ja } m_R(\beta) = \beta^0,$$

$$m_L(\beta^3) = \beta^3 + \beta^6 + \beta^{15} = \beta^2 \text{ ja } m_R(\beta^3) = \beta^0.$$

Olkoon matriisi A^{-1} muodostettu samalla tavoin kuin esimerkissä 2.3.12. Tällöin saadaan muodostettua

$$\begin{aligned} v_R &= [\beta^0 + \beta^0, \beta^2 + \beta^0 + \beta^0]A^{-1} \\ &= [0, \beta^2]A^{-1} \\ &= [000001] \begin{bmatrix} 001 & 011 \\ 111 & 010 \\ 011 & 101 \\ 110 & 100 \\ 101 & 110 \\ 111 & 001 \end{bmatrix} \\ &= 111001. \end{aligned}$$

Nyt voidaan koodata viestisana $m = [0110010, 1] = 01100101$ koodisanaksi

$$c = [m_L, p_L, m_R, v_R, p_R] = [0110010, 1, 1, 111001, 1] = 01100101\ 11110011.$$

Sanaa muodostettaessa pariteetintarkistusbitit p_L ja p_R saavat molemmat arvon 1, jolloin määritelmän 3.2.2 ehto (i) täyttyy.

Luvun 2 merkintöjen avulla ilmaistuna koodisana $c = [\chi(U), \chi(V)]$, missä $\chi(U) = 01100101$ ja $\chi(V) = 11110011$.

Luku 5

Dekoodausalgoritmi laajennetuille Preparata-koodeille

5.1 Yleistä

Edellisessä luvussa esitellyn koodin $P(r)$ koodausalgoritmin jälkeen käsitellään vielä koodin $P(r)$ dekoodausalgoritmi. Lauseen 3.4.6 perusteella koodin $P(r)$ minimietäisyys on 6 riippumatta luvun r arvosta. Huomautuksen 1.2.7 perusteella voidaan määrittää koodin virheenkorjauskyky e epäyhtälöstä $d_{\min}C \geq 2e + 1$. Nyt $d_{\min}C = 6$, joten

$$d_{\min}C \geq 2e + 1 \Leftrightarrow 2e \leq 6 - 1 \Leftrightarrow e \leq \frac{5}{2}.$$

Koska virheiden määrä on aina kokonaisluku, pystyy koodi $P(r)$ korjaamaan maksimissaan 2 virhettä. Lähdetään määrittämään erilaiset mahdollisuudet sille, missä kohtaa vastaanotettua viestisanaa virheet voivat sijaita, jonka jälkeen muodostetaan dekoodausalgoritmi koodille $P(r)$.

5.2 Vastaanotetussa sanassa esiintyvien virheiden sijainneista

Olkoon w vastaanotettu sana muotoa $w = [w_L, p_L, w_R, p_R]$, missä w_L ja w_R ovat pituudeltaan $2^r - 1$ olevia sanoja ja p_L sekä p_R ovat pariteetintarkistusbittejä, joilla

varmistetaan määritelmän 3.2.2 ehdon (i) toteutuminen. Näiden perusteella voidaan määrittää

$$[w_L(\beta), w_L(\beta^3)] = w_L H \text{ ja } [w_R(\beta), w_R(\beta^3)] = w_R H.$$

Käydään seuraavaksi läpi kaikki vaihtoehdot sille, miten vastaanotetussa sanassa esiintyvät virheet voivat sijaita.

1. Oletetaan, että kaikki virheet esiintyvät vain vastaanotetun sanan pariteetintarkistusbiteissä p_L ja p_R, niin tällöin määritelmän 3.2.2 perusteella

   $$w_L(\beta) = w_R(\beta)$$

   ja

   $$w_L(\beta^3) + (w_L(\beta))^3 = w_R(\beta^3).$$

   On siis helppo tarkastaa, esiintyykö virheitä vain pariteetintarkistusbiteissä. Dekoodaus onnistuu muuttamalla tarvittavat pariteetintarkistusbitit.

2. Oletetaan, että vastaanotetun sanan osassa w_L ei ole virheitä, osassa w_R on yksi virhe kohdassa i ja enintään yksi virhe pariteetintarkistusbiteissä p_L ja p_R. Tällöin määritelmän 3.2.2 perusteella

   $$w_L(\beta) = w_R(\beta) + \beta^i$$

   ja

   $$w_L(\beta^3) + (w_L(\beta))^3 = w_R(\beta^3) + \beta^{3i}.$$

   Koska

   $$w_L(\beta) + w_R(\beta) = \beta^i$$

   niin

   $$(w_L(\beta) + w_R(\beta))^3 = \beta^{3i}.$$

Lisäksi

$$w_L(\beta^3) + (w_L(\beta))^3 + w_R(\beta^3) = \beta^{3i},$$

joten

$$(w_L(\beta) + w_R(\beta))^3 = w_L(\beta^3) + (w_L(\beta))^3 + w_R(\beta^3).$$

Jos viimeinen yhtälö toteutuu, niin tällöin $\beta^i = w_L(\beta) + w_R(\beta)$. Dekoodaus onnistuu tällöin muuttamalla osan w_R kohdassa i sijaitseva bitti, sekä enintään yksi pariteetintarkistusbitti.

3. Oletetaan, että vastaanotetun sanan osassa w_R ei ole virheitä, osassa w_L on yksi virhe kohdassa i ja enintään yksi virhe pariteetintarkistusbiteissä p_L ja p_R. Tällöin voidaan soveltaa lemman 3.4.1 kohtaa (a) ja toistaa vaihtoehdossa 2 esiintyvät askeleet, jolloin saadaan yhtälö

$$(w_R(\beta) + w_L(\beta))^3 = w_R(\beta^3) + (w_R(\beta))^3 + w_L(\beta^3).$$

Jos yhtälö toteutuu, niin tällöin $\beta^i = w_R(\beta) + w_L(\beta)$. Dekoodaus onnistuu tällöin muuttamalla osan w_L kohdassa i sijaitseva bitti, sekä enintään yksi pariteetintarkistusbitti.

4. Oletetaan, että vastaanotetun sanan osassa w_R esiintyy kaksi virhettä kohdissa i ja j. Tällöin määritelmän 3.2.2 perusteella

$$w_L(\beta) = w_R(\beta) + \beta^i + \beta^j$$

ja

$$w_L(\beta^3) + (w_L(\beta))^3 = w_R(\beta^3) + \beta^{3i} + \beta^{3j}.$$

Näin ollen summien $\beta^i + \beta^j$ ja $\beta^{3i} + \beta^{3j}$ arvot tiedetään, mutta eksponenttien i ja j arvoja ei tiedetä. Olkoot $s_1 = \beta^i + \beta^j$ ja $s_3 = \beta^{3i} + \beta^{3j}$.

Lähdetään tarkastelemaan yhtälöparia

$$\begin{cases} \beta^i + \beta^j = s_1 \\ \beta^{3i} + \beta^{3j} = s_3 \end{cases}.$$

Kirjoitetaan jälkimmäisen yhtälön vasen puoli tekijämuodossa

$$\beta^{3i} + \beta^{3j} = (\beta^i + \beta^j)(\beta^{2i} + \beta^{i+j} + \beta^{2j}).$$

Lisäksi huomioidaan, että

$$s_1^2 = (\beta^i + \beta^j)^2 = \beta^{2i} + \beta^{2j},$$

koska β^i ja β^j ovat sellaisen kunnan alkioita, jonka karakteristika on 2.

Näin ollen

$$\begin{aligned} s_3 &= \beta^{3i} + \beta^{3j} \\ &= (\beta^i + \beta^j)(\beta^{2i} + \beta^{i+j} + \beta^{2j}) \\ &= s_1(\beta^{2i} + \beta^{2j} + \beta^{i+j}) \\ &= s_1(s_1^2 + \beta^{i+j}). \end{aligned}$$

Tästä saadaan, että

$$\frac{s_3}{s_1} = s_1^2 + \beta^{i+j},$$

eli

$$\beta^{i+j} = \frac{s_3}{s_1} + s_1^2.$$

Tarkastellaan seuraavaksi toisen asteen yhtälöä $(x + \beta^i)(x + \beta^j) = 0$, jonka juuret ovat β^i ja β^j. Auki kerrottuna yhtälö on

$$x^2 + (\beta^i + \beta^j)x + \beta^{i+j} = 0.$$

Aiemman tarkastelun perusteella yhtälö saadaan muotoon

$$x^2 + s_1 x + \left(\frac{s_3}{s_1} + s_1^2\right) = 0.$$

Ratkaisemalla tämän yhtälön juuret β^i ja β^j saadaan selville vastaanotetussa koodisanan w osassa w_R esiintyvien virheiden sijainnit i ja j. Dekoodaus onnistuu tällöin muuttamalla sanassa w_R kohdissa i ja j olevien bittien arvot.

5. Oletetaan, että vastaanotetun sanan osassa w_L esiintyy kaksi virhettä kohdissa i ja j. Tällöin voidaan soveltaa lemman 3.4.1 kohtaa (a), jonka jälkeen määritelmän 3.2.2 perusteella

$$w_R(\beta) = w_L(\beta) + \beta^i + \beta^j$$

ja

$$w_R(\beta^3) + (w_R(\beta))^3 = w_L(\beta^3) + \beta^{3i} + \beta^{3j}.$$

Myös tässä tapauksessa summien $\beta^i + \beta^j$ ja $\beta^{3i} + \beta^{3j}$ arvot tiedetään, mutta eksponenttien i ja j arvoja ei tiedetä. Suorittamalla sama päättely kuin kohdassa 4, saadaan sanan w osassa w_L esiintyvien virheiden sijainnit i ja j selvitettyä ratkaisemalla yhtälö

$$x^2 + s_1 x + \left(\frac{s_3}{s_1} + s_1^2\right) = 0,$$

missä $s_1 = \beta^i + \beta^j$ ja $s_3 = \beta^{3i} + \beta^{3j}$.

Dekoodaus onnistuu tällöin muuttamalla osan w_L kohdissa i ja j olevien bittien arvot.

6. Oletetaan, että vastaanotetun sanan w osassa w_L on tasan yksi virhe kohdassa i ja osassa w_R on tasan yksi virhe kohdassa j. Tällöin määritelmän 3.2.2 perusteella

$$w_L(\beta) + \beta^i = w_R(\beta) + \beta^j,$$

ja

$$w_L(\beta^3) + \beta^{3i} + \left(w_L(\beta) + \beta^i\right)^3 = w_R(\beta^3) + \beta^{3j}.$$

Ratkaistaan ensimmäinen yhtälö alkion β^j suhteen, jolloin saadaan

$$\beta^j = w_L(\beta) + \beta^i + w_R(\beta).$$

Sijoitetaan tämä jälkimmäiseen yhtälöön, jolloin saadaan

$$\begin{aligned}
w_L(\beta^3) + \beta^{3i} + \left(w_L(\beta) + \beta^i\right)^3 &= w_R(\beta^3) + \left(w_L(\beta) + \beta^i + w_R(\beta)\right)^3 \\
&= w_R(\beta^3) + \left(w_L(\beta) + \beta^i\right)^3 \\
&+ \left(w_L(\beta) + \beta^i\right)^2 w_R(\beta) \\
&+ \left(w_L(\beta) + \beta^i\right) (w_R(\beta))^2 + (w_R(\beta))^3 \\
&= w_R(\beta^3) + \left(w_L(\beta) + \beta^i\right)^3 \\
&+ \left((w_L(\beta))^2 + \beta^{2i}\right) w_R(\beta) \\
&+ \left(w_L(\beta) + \beta^i\right) (w_R(\beta))^2 + (w_R(\beta))^3 \\
&= w_R(\beta^3) + \left(w_L(\beta) + \beta^i\right)^3 + \\
&+ (w_L(\beta))^2 w_R(\beta) + \beta^{2i} w_R(\beta) \\
&+ w_L(\beta) (w_R(\beta))^2 + \beta^i (w_R(\beta))^2 + (w_R(\beta))^3 .
\end{aligned}$$

Yhtälö saadaan sieventämällä muotoon

$$\begin{aligned}
\beta^{3i} + \beta^{2i} w_R(\beta) + \beta^i (w_R(\beta))^2 + (w_R(\beta))^3 \\
= w_L(\beta^3) + w_R(\beta^3) + (w_L(\beta))^2 w_R(\beta) + w_L(\beta)(w_R(\beta))^2,
\end{aligned}$$

eli

$$\begin{aligned}\left(\beta^i + w_R(\beta)\right)^3 &= \left(w_L(\beta^3) + w_R(\beta^3)\right) + (w_L(\beta))^3 + (w_R(\beta))^3 \\ &\quad + (w_L(\beta))^3 + (w_L(\beta))^2 w_R(\beta) + w_L(\beta)(w_R(\beta))^2 + (w_R(\beta))^3 \\ &= \left(w_L(\beta^3) + w_R(\beta^3)\right) \\ &\quad + (w_L(\beta) + w_R(\beta))^3 + (w_L(\beta))^3 + (w_R(\beta))^3.\end{aligned}$$

Merkitään yhtälön oikeaa puolta kirjaimella D, eli

$$D = \left(w_L(\beta^3) + w_R(\beta^3)\right) + (w_L(\beta) + w_R(\beta))^3 + (w_L(\beta))^3 + (w_R(\beta))^3.$$

Tällöin

$$\left(\beta^i + w_R(\beta)\right)^3 = D,$$

eli

$$\beta^i + w_R(\beta) = D^{\frac{1}{3}},$$

joten

$$\beta^i = w_R(\beta) + D^{\frac{1}{3}}.$$

Lisäksi

$$\beta^j = w_L(\beta) + \beta^i + w_R(\beta) = w_L(\beta) + w_R(\beta) + D^{\frac{1}{3}} + w_R(\beta),$$

joten

$$\beta^j = w_L(\beta) + D^{\frac{1}{3}}.$$

Dekoodaus onnistuu tällöin muuttamalla osan w_L kohdassa i ja osan w_R kohdassa j olevien bittien arvot.

Nämä kuusi tapausta kattavat kaikki eri mahdollisuudet, miten kaksi virhettä voivat esiintyä vastaanotetussa sanassa. Virhekohtien sijainnin määrittäminen onnistuu jokaisessa näissä tapauksissa kohtuullisella vaivalla. Lisäksi pariteettiehdot mahdollistavat sen, että oikean tapauksen valinta vastaanotetun sanan w tapauksessa on mahdollista.

5.3 Koodin $P(r)$ dekoodausalgoritmi

Yhdistämällä edellisessä kappaleessa esitetyt tulokset, saadaan muodostettua laajennetulle Preparata-koodille $P(r)$ dekoodausalgoritmi, jonka askeleet vastaavat edellisen kappaleen eri tapauksia, vieläpä samassa järjestyksessä. Jokaisessa askeleessa on ehto, jonka toteutuessa virheet voidaan paikallistaa ja korjata. Mikäli ehto ei toteudu, niin jatketaan algoritmin seuraavaan askeleeseen.

Algoritmi 5.3.1. [Laajennetun Preparata-koodin $P(r)$ dekoodaus] Olkoon $w = [w_L, p_L, w_R, p_R]$ vastaanotettu sana.

0. Lasketaan $L_1 = w_L(\beta)$, $L_3 = w_L(\beta^3)$, $R_1 = w_R(\beta)$ ja $R_3 = w_R(\beta^3)$ käyttäen apuna lemmassa 2.3.9 esitettyä matriisia H.

1. Jos $L_1 + R_1 = 0$ ja $L_3 + L_1^3 + R_3 = 0$, niin virheet esiintyvät ainoastaan pariteetintarkistusbiteissä p_L ja p_R. Tällöin korjataan tarvittaessa näiden bittien arvoa sillä tavalla, että $[w_L, p_L]$ ja $[w_R, p_R]$ ovat molemmat pariteetiltaan parillisia, ts. molempien paino on parillinen.

2. Jos $(L_1 + R_1)^3 + L_3 + L_1^3 + R_3 = 0$, niin $\beta^i = L_1 + R_1$. Tällöin korjataan osan w_R kohdassa i sijaitsevan bitin arvo, sekä tarvittaessa *enintään yhden* pariteetintarkistusbitin arvo. Mikäli molempien pariteetintarkistusbittien arvoa tulisi muuttaa, on vastaanotetussa sanassa kolme virhettä, eikä sitä voida dekoodata. Tällöin on pyydettävä viestin uudelleenlähetys.

3. Jos $(L_1 + R_1)^3 + R_3 + R_1^3 + L_3 = 0$, niin $\beta^i = L_1 + R_1$. Tällöin korjataan osan w_L kohdassa i sijaitsevan bitin arvo, sekä tarvittaessa *enintään yhden* pariteetintarkistusbitin arvo. Mikäli molempien pariteetintarkistusbittien arvoa tulisi muuttaa, on vastaanotetussa sanassa kolme virhettä, eikä sitä voida dekoodata. Tällöin on pyydettävä viestin uudelleenlähetys.

4. Jos vastaanotetun sanan w molempien osien $[w_L, p_L]$ sekä $[w_R, p_R]$ pariteetti on parillinen, ja yhtälön

$$x^2 + (L_1 + R_1)x + \frac{L_3 + L_1^3 + R_3 + (L_1 + R_1)^3}{L_1 + R_1} = 0$$

ratkaisut ovat β^i ja β^j, niin osassa w_R on kaksi virhettä kohdissa i ja j. Tällöin korjataan osan w_R kohdassa i ja j sijaitsevien bittien arvot.

5. Jos vastaanotetun sanan w molempien osien $[w_L, p_L]$ sekä $[w_R, p_R]$ pariteetti on parillinen, ja yhtälön

$$x^2 + (L_1 + R_1)x + \frac{R_3 + R_1^3 + L_3 + (L_1 + R_1)^3}{L_1 + R_1} = 0$$

ratkaisut ovat β^i ja β^j, niin osassa w_L on kaksi virhettä kohdissa i ja j. Tällöin korjataan osan w_L kohdassa i ja j sijaitsevien bittien arvot.

6. Jos vastaanotetun sanan molempien osien $[w_L, p_L]$ sekä $[w_R, p_R]$ pariteetti on pariton, niin

$$\beta^i = R_1 + \left(L_1^3 + R_1^3 + (L_1 + R_1)^3 + L_3 + R_3\right)^{\frac{1}{3}},$$

ja

$$\beta^j = L_1 + \left(L_1^3 + R_1^3 + (L_1 + R_1)^3 + L_3 + R_3\right)^{\frac{1}{3}}.$$

Tällöin korjataan osan w_L kohdassa i olevan bitin arvo ja osan w_R kohdassa j olevan bitin arvo.

7. Mikäli yksikään aikaisempien askelien tuloksista ei tuottanut vastaanotettua sanaa lähinnä olevaa koodisanaa, voidaan vastaanotetussa sanassa w tulkita olevan vähintään kolme virhettä, eikä sanaa voida dekoodata. Tällöin on pyydettävä viestin uudelleenlähetys.

Katsotaan lopuksi vielä muutama esimerkki dekoodauksesta.

Esimerkki 5.3.2. Olkoon $\mathbb{F}_8$ konstruoitu polynomin $1 + x + x^3$ avulla ja olkoon lähetetyt koodisanat koodattu käyttäen koodia $P(3)$. Oletetaan, että vastaanotetussa sanassa on korkeintaan kaksi virhettä.

(a) Vastaanotetaan sana 10010011 11100111. Suoritetaan dekoodaus algoritmin 5.3.1 avulla.

0.

$$
\begin{aligned}
[L_1, L_3] = w_L H = [1001001] \cdot &\begin{bmatrix} \beta^0 & \beta^0 \\ \beta^1 & \beta^3 \\ \beta^2 & \beta^6 \\ \beta^3 & \beta^2 \\ \beta^4 & \beta^5 \\ \beta^5 & \beta^1 \\ \beta^6 & \beta^4 \end{bmatrix} \\
&= [\beta^0 + \beta^3 + \beta^6, \beta^0 + \beta^2 + \beta^4] \\
&= [100 + 110 + 101, 100 + 001 + 011] \\
&= [111, 110],
\end{aligned}
$$

eli $L_1 = 111 = \beta^5$ ja $L_3 = 110 = \beta^3$.

$$
\begin{aligned}
[R_1, R_3] = w_R H = [1110011] \cdot &\begin{bmatrix} \beta^0 & \beta^0 \\ \beta^1 & \beta^3 \\ \beta^2 & \beta^6 \\ \beta^3 & \beta^2 \\ \beta^4 & \beta^5 \\ \beta^5 & \beta^1 \\ \beta^6 & \beta^4 \end{bmatrix} \\
&= [\beta^0 + \beta^1 + \beta^2 + \beta^5 + \beta^6, \beta^0 + \beta^3 + \beta^6 + \beta^1 + \beta^4] \\
&= [100 + 010 + 001 + 111 + 101, 100 + 110 + 101 + 010 + 011] \\
&= [101, 110],
\end{aligned}
$$

eli $R_1 = 101 = \beta^6$ ja $R_3 = 110 = \beta^3$.

1. $L_1 + R_1 = 111 + 101 = 010 = \beta \neq 0$, joten edetään seuraavaan askeleeseen.
2. $(L_1 + R_1)^3 + L_3 + L_1^3 + R_3 = \beta^3 + \beta^3 + \beta^{15} + \beta^3 = \beta^0 \neq 0$, joten edetään seuraavaan askeleeseen.
3. $(L_1 + R_1)^3 + R_3 + R_1^3 + L_3 = \beta^3 + \beta^3 + \beta^{18} + \beta^3 = \beta^6 \neq 0$, joten edetään

seuraavaan askeleeseen.

4.

$$x^2 + \beta x + \frac{\beta^3 + \beta^{15} + \beta^3 + \beta^3}{\beta} = x^2 + \beta x + \frac{1}{\beta}$$
$$= x^2 + \beta x + \beta^6 = 0.$$

Esimerkiksi kokeilemalla löydetään yhtälölle ratkaisut $x_1 = \beta^2$ ja $x_2 = \beta^4$. Korjataan siis osan $w_R = 11100111$ kohdissa 2 ja 4 olevat bitit, jolloin saadaan oikeaksi koodisanaksi $c = 10010011\ 11001111$.

Jos alkuperäinen viestisana on $m = [m_L, m_R]$, niin sitä vastaava koodisana on algoritmin 4.3.1 mukaan sana $[m_L, p_L, m_R, v_R, p_R]$. Näin ollen alkuperäinen viestisana on

$$m = [1001001, 1] = 10010011.$$

(b) Vastaanotetaan sana 10100100 10001001. Suoritetaan dekoodaus algoritmin 5.3.1 avulla.

0.

$$[L_1, L_3] = w_L H = [1010010] \cdot \begin{bmatrix} \beta^0 & \beta^0 \\ \beta^1 & \beta^3 \\ \beta^2 & \beta^6 \\ \beta^3 & \beta^2 \\ \beta^4 & \beta^5 \\ \beta^5 & \beta^1 \\ \beta^6 & \beta^4 \end{bmatrix}$$
$$= [\beta^0 + \beta^2 + \beta^5, \beta^0 + \beta^6 + \beta^1]$$
$$= [100 + 001 + 111, 100 + 101 + 010]$$
$$= [010, 011],$$

eli $L_1 = 010 = \beta^1$ ja $L_3 = 011 = \beta^4$.

$$
\begin{aligned}
[R_1, R_3] = w_R H = [1000100] \cdot &\begin{bmatrix} \beta^0 & \beta^0 \\ \beta^1 & \beta^3 \\ \beta^2 & \beta^6 \\ \beta^3 & \beta^2 \\ \beta^4 & \beta^5 \\ \beta^5 & \beta^1 \\ \beta^6 & \beta^4 \end{bmatrix} \\
&= [\beta^0 + \beta^4, \beta^0 + \beta^5] \\
&= [100 + 011, 100 + 111] \\
&= [111, 011],
\end{aligned}
$$

eli $R_1 = 111 = \beta^5$ ja $R_3 = 011 = \beta^4$.

1. $L_1 + R_1 = 010 + 111 = 101 = \beta^6 \neq 0$, joten edetään seuraavaan askeleeseen.
2. $(L_1 + R_1)^3 + L_3 + L_1^3 + R_3 = \beta^{18} + \beta^4 + \beta^3 + \beta^4 = \beta^6 \neq 0$, joten edetään seuraavaan askeleeseen.
3. $(L_1 + R_1)^3 + R_3 + R_1^3 + L_3 = \beta^{18} + \beta^4 + \beta^{15} + \beta^4 = \beta^2 \neq 0$, joten edetään seuraavaan askeleeseen.
4. Vastaanotetun sanan w molempien osien $[w_L, p_L]$ sekä $[w_R, p_R]$ pariteetti on pariton, joten edetään seuraavaan askeleeseen.
5. Vastaanotetun sanan w molempien osien $[w_L, p_L]$ sekä $[w_R, p_R]$ pariteetti on pariton, joten edetään seuraavaan askeleeseen.
6.

$$
\begin{aligned}
\beta^i &= R_1 + \left(L_1^3 + R_1^3 + (L_1 + R_1)^3 + L_3 + R_3\right)^{\frac{1}{3}} \\
&= \beta^5 + (\beta^3 + \beta^{15} + \beta^{18} + \beta^4 + \beta^4)^{\frac{1}{3}} \\
&= \beta^5 + (\beta^5)^{\frac{1}{3}} \\
&= \beta^5 + (\beta^{12})^{\frac{1}{3}} \\
&= \beta^5 + \beta^4 \\
&= \beta^0,
\end{aligned}
$$

joten $i = 0$.

Edelleen

$$\begin{aligned}\beta^j &= L_1 + \left(L_1^3 + R_1^3 + (L_1 + R_1)^3 + L_3 + R_3\right)^{\frac{1}{3}} \\ &= \beta^1 + \beta^4 = \beta^2,\end{aligned}$$

joten $j = 2$.

Korjataan siis osan $w_L = 10100100$ kohdassa 0 oleva bitti ja osan $w_R = 10001001$ kohdassa 2 oleva bitti, jolloin saadaan oikeaksi koodisanaksi $c = 00100100\ 10101001$. Alkuperäinen viestisana on

$$m = [0010010, 1] = 00100101.$$

(c) Vastaanotetaan sana 10001000 11101001. Suoritetaan dekoodaus algoritmin 5.3.1 avulla.

0.

$$\begin{aligned}[L_1, L_3] = w_L H &= [1000100] \cdot \begin{bmatrix} \beta^0 & \beta^0 \\ \beta^1 & \beta^3 \\ \beta^2 & \beta^6 \\ \beta^3 & \beta^2 \\ \beta^4 & \beta^5 \\ \beta^5 & \beta^1 \\ \beta^6 & \beta^4 \end{bmatrix} \\ &= [\beta^0 + \beta^4, \beta^0 + \beta^5] \\ &= [100 + 011, 100 + 111] \\ &= [111, 011],\end{aligned}$$

eli $L_1 = 111 = \beta^5$ ja $L_3 = 011 = \beta^4$.

$$
\begin{aligned}
[R_1, R_3] = w_R H = [1110100] \cdot &\begin{bmatrix} \beta^0 & \beta^0 \\ \beta^1 & \beta^3 \\ \beta^2 & \beta^6 \\ \beta^3 & \beta^2 \\ \beta^4 & \beta^5 \\ \beta^5 & \beta^1 \\ \beta^6 & \beta^4 \end{bmatrix} \\
&= [\beta^0 + \beta^1 + \beta^2 + \beta^4, \beta^0 + \beta^3 + \beta^6 + \beta^5] \\
&= [100 + 010 + 001 + 011, 100 + 110 + 101 + 111] \\
&= [100, 000],
\end{aligned}
$$

eli $R_1 = 100 = \beta^0$ ja $R_3 = 000 = 0$.

1. $L_1 + R_1 = 111 + 100 = 011 = \beta^4 \neq 0$, joten edetään seuraavaan askeleeseen.
2. $(L_1 + R_1)^3 + L_3 + L_1^3 + R_3 = \beta^{12} + \beta^4 + \beta^{15} + 0 = \beta^3 \neq 0$, joten edetään seuraavaan askeleeseen.
3. $(L_1 + R_1)^3 + R_3 + R_1^3 + L_3 = \beta^{12} + 0 + \beta^0 + \beta^4 = 0$.

Tällöin $\beta^i = L_1 + R_1 = \beta^4$, joten $i = 4$. Jos sanan w osan w_L kohdassa $i = 4$ sijaitseva bitti korjataan, pitäisi sen jälkeen myös molemmat pariteetintarkistusbitit p_L ja p_R korjata, joten tässä tapauksessa on pyydettävä viestin uudelleenlähetys.

Kirjallisuutta

[1] D. Hankerson et al.: *Coding Theory and Cryptography - The Essentials (Second Edition, Revised and Expanded)*, Marcel Dekker, Inc., New York 2000.

[2] M. Rinta-aho: *Koodausteoria-kurssin (800667S) luentomoniste*, Oulun yliopisto, 2009