Eötvös Loránd Tudományegyetem
Természettudományi Kar

Tabi Anikó

MRD kódok

BSc alkalmazott matematikus szakdolgozat

Témavezető:

Csajbók Bence

Geometria tanszék

Budapest, 2019

Tartalomjegyzék

Bevezetés

Információs társadalmunkban egyre nagyobb értéket képvisel az adat. Adatot tárolunk, megosztunk, kiolvasunk. Az adatot szeretnénk megóvni sérüléstől, vagy hogy illetéktelen kezekbe kerüljön. Ezen kívül az adattárolás, adatátvitel költségét is csökkenteni szeretnénk. A tárolandó vagy továbbítandó adatot digitalizáljuk, majd a célnak megfelelően kódoljuk, ill. dekódoljuk.

Az információ rögzítés és továbbítás matematikai alapjául a kódelmélet szolgál. Az kezelendő adatokhoz vektorokat, mátrixokat vagy más algebrai objektumokat rendelünk. Definiálunk egy ábécét, ami egy véges halmaz, például vektorok halmaza. Ennek egy részhalmaza lesz a kód. A kódon értelmezhetünk távolságot. Pl. a Hamming-távolság két vektor különböző koordinátáinak száma. Ezen távolság segítségével definiálhatunk hibajavító kódokat, illetve adhatunk felső korlátot a kód elemszámára.

Az MRD kódok az algebrai kódok egy speciális csoportja, melyek a kódszavak minimális távolságának függvényében maximális elemszámúak. A kommunikációs hálózatok és a kriptográfia témakörében van jelentőségük.

Ebben a dolgozatban a legfőbb tulajdonságaikat foglalom össze, egy-egy tételre új bizonyítást adok, illetve említést teszek az alkalmazásukról a lineáris hálózati kódolásban.

Az első fejezetben összegyűjtöm azokat az algebrai definíciókat és tételeket, elsősorban a véges testek témaköréből, melyek szükségesek a kódokhoz kapcsolódó tételek, lemmák bizonyításához.

A második fejezetben ismertetem a linearizált, vagy más néven q-polinomok fogalmát, valamint egy fontos és a későbbiekben hasznos tételt ismertetek, mely a q-polinomok (és egyúttal a legismertebb MRD kód, a Gabidulin-kód polinomjai) és az ún. Dickson-mátrix közötti kapcsolatot írja le.

A harmadik fejezetben több ismert MRD kódot is bemutatok, köztük a Gabidulin-kódot, valamint annak általánosítását, és szó lesz az MRD kódok által definiált altér kódokról (amelyek kódszavai vektorterek) is.

Ez utóbbiak a negyedik fejezetben is előkerülnek, ahol a hálózatok alkalmazási területről lesz szó. Ennek a fejezetnek alapjául Kötter és Kschischang *Coding for Errors and Erasures in Random Network Coding* cikke szolgált.

1. fejezet

Szükséges algebrai definíciók és tételek

Ebben a fejezetben a dolgozatban felhasznált, alapvető algebrai definíciókat és tételeket mutatom be.

1.1. Véges testek

1.1.1. Állítás. *Véges test ($\mathbb{F}$) elemszáma prímhatvány: p^k.*

1.1.2. Állítás. *Ha $\mathbb{F}$ véges test elemszáma p^k, akkor a test egységelemét p-szer összeadva a 0 elemet kapjuk.*

1.1.3. Definíció. Ha $|\mathbb{F}| = p^k$, akkor $\mathbb{F}$ *karakterisztikája*: p.

1.1.4. Definíció. Legkisebb résztest: *prímtest*, elemszáma: p.

1.1.5. Állítás. $|\mathbb{F}| = p^k = q$, $a \in \mathbb{F}$: $a^q = a$.

1.1.6. Állítás. *Minden q prímhatványra izomorfia erejéig egyetlen q elemű test létezik: a $x^q - x$ polinom felbontási teste.*

1.1.7. Állítás. *Egy p karakterisztikájú véges testben $(a+b)^p = a^p + b^p$.*

Bizonyítás. $(a+b)^p = a^p + \binom{p}{1}a^{p-1}b + ... + \binom{p}{p-1}ab^{p-1} + b^p$
Mivel a binomiális együtthatók p többszörösei, és minden $\mathbb{F}_q$-beli elem p-szerese 0, ebből következik az állítás. □

1.1.8. Állítás. *Egy p karakterisztikájú véges testben $(a+b)^{p^k} = a^{p^k} + b^{p^k}$.*

Bizonyítás. Bizonyítás indukcióval:
Láttuk, hogy $(a+b)^p = a^p + b^p$. Tegyük fel, hogy $(a+b)^{p^{k-1}} = a^{p^{k-1}} + b^{p^{k-1}}$.
Az állítás p^k-ra egyszerű átalakításokkal következik:
$(a+b)^{p^k} = ((a+b)^{p^{k-1}})^p = (a^{p^{k-1}} + b^{p^{k-1}})^p = (a^{p^{k-1}})^p + (b^{p^{k-1}})^p = a^{p^k} + b^{p^k}$. □

1.1.9. Állítás. $\mathbb{F}_{q^n}$ $\mathbb{F}_q$ *felett* n *dimenziós vektortér.*

Bizonyítás.

1. $\mathbb{F}_{q^n}$ vektortér. A vektortér axiómák a test axiómákból következnek:
   $\forall\ a, b, c \in \mathbb{F}_{q^n},\ \lambda, \mu \in \mathbb{F}_q\ (\Rightarrow \lambda, \mu \in \mathbb{F}_{q^n})$
   (a) $a + b \in \mathbb{F}_{q^n}$
   (b) $\lambda a \in \mathbb{F}_{q^n}$
   (c) $a + b = b + a$
   (d) $a + (b + c) = (a + b) + c$
   (e) $\exists 0 \in \mathbb{F}_{q^n},\ a + 0 = a$
   (f) $\exists - a \in \mathbb{F}_{q^n},\ a + (-a) = 0$
   (g) $(\lambda + \mu)a = \lambda a + \mu a$
   (h) $\lambda(a + b) = \lambda a + \lambda b$
   (i) $(\lambda\mu)a = \lambda(\mu a)$
   (j) $1a = a$ $(1 \in \mathbb{F}_q)$ ($\mathbb{F}_q$ egységeleme $\mathbb{F}_{q^n}$-nek is egységeleme)
2. Legyen $\mathbb{F}_{q^n}$ bázisa $\mathbb{F}_q$ felett $\{\beta_1, ..., \beta_m\}$, elemszáma m. Ekkor $\mathbb{F}_{q^n} = \{\sum_{i=1}^{m} \lambda_i \beta_i : \lambda_i \in \mathbb{F}_q\}$. $\mathbb{F}_q$ elemszáma q, így $\mathbb{F}_{q^n}$ elemszáma q^m, azaz $m = n$. Tehát a bázis elemszáma, azaz $\mathbb{F}_{q^n}$ mint $\mathbb{F}_q$ feletti vektortér dimenziója: n.

□

1.1.10. Állítás. *Minden testben egy* k*-ad fokú, nem nulla polinomnak legfeljebb* k *gyöke van.*

Bizonyítás. Egy $p(x)$ nem nulla polinomnak x_0 pontosan akkor gyöke, ha $p = (x - x_0)q(x)$ alakba írható, ahol $q(x)$ eggyel kisebb fokú polinom. Így egy k-ad fokú polinom legfeljebb k db elsőfokú polinom szorzatára bomlik, azaz legfeljebb k gyöke lehet. Ez nullosztómentes gyűrű feletti polinomokra igaz, így test felettiekre is. □

1.1.11. Lemma. $\gcd(a^m - 1, a^n - 1) = a^{\gcd(m,n)} - 1$ $(a \in \mathbb{Z}^+, a > 1)$.

Bizonyítás. Legyen $m, n \in \mathbb{Z}^+$ és d a legnagyobb közös osztójuk: $d := \gcd(m, n)$. Ekkor $m = qn + r$ $(0 \leq r < n)$ valamint $m = dm'$ és $n = dn'$. d a következő alakba írható (Bézout-azonosság): $d = u_0 m + v_0 n$ $(u_0, v_0 \in \mathbb{Z})$. Ezt tovább alakítva: $d = u_0 m + v_0 n + kn'dm' - km'dn' = u_0 m + v_0 n + kn'm - km'n = (u_0 + kn')m + (v_0 - km')n$ $(k \in \mathbb{Z})$. k-t megfelelően választva $v_0 - km' < 0$, ezért $\exists u, v \in \mathbb{Z}^+$ $d = um - vn,\ um > vn$.

1. $x^m - 1 = (x^n - 1)(x^{m-n} + x^{m-2n} + ... + x^{m-qn}) + x^r - 1$. Ezért $n|m \Rightarrow r = 0 \Rightarrow (x^n - 1)|(x^m - 1)$, továbbá ha $(x^n - 1)|(x^m - 1) \Rightarrow (x^n - 1)|(x^r - 1)$, amiből következik, hogy $r = 0$ (mivel $0 \leq r < n$). Azaz $x^n - 1|x^m - 1 \Leftrightarrow n|m$. Ebből következik, hogy

$$x^d - 1| \gcd(x^m - 1, x^n - 1).$$

2. $(x^n-1)(-x^{um-vn} - x^{um-(v-1)n} - ... - x^{um-n}) + (x^m - 1)(x^{m(u-1)} + ... + x^m + 1) = x^{um-vn} - 1 = x^d - 1$
$\Rightarrow x^d - 1 = (x^n - 1)a(x) + (x^m - 1)b(x)$, amiből következik:

$$\gcd(x^n - 1, x^m - 1)|x^d - 1.$$

A fentiekből következik, hogy $\gcd(x^m - 1, x^n - 1) = x^{\gcd(m,n)} - 1$.
Egy 1-nél nagyobb a egész számot behelyettesítve: $\gcd(a^m - 1, a^n - 1) = a^{\gcd(m,n)} - 1$ $(a \in \mathbb{Z}^+, a > 1)$. $\square$

Forrás: [7, Chapter 20.18, Theorem 20.18.5.]

1.1.12. Lemma. $\mathbb{F}_{q^k} \cap \mathbb{F}_{q^n} = \mathbb{F}_{q^{\gcd(k,n)}}$

Bizonyítás.

1. $\mathbb{F}_{q^{\gcd(k,n)}} \subseteq \mathbb{F}_{q^k} \cap \mathbb{F}_{q^n}$
$a \in \mathbb{F}_{q^{\gcd(k,n)}}$ pontosan akkor, ha $a^{q^{\gcd(k,n)}} = a$.
$a \in \mathbb{F}_{q^k}$ pontosan akkor, ha $a^{q^k} = a$.
$a \in \mathbb{F}_{q^n}$ pontosan akkor, ha $a^{q^n} = a$.
Mivel $\gcd(k, n)|k$ és $\gcd(k, n)|n$, ezért $\forall a \in \mathbb{F}_{q^{\gcd(k,n)}}$ $a^{q^k} = a$ és $a^{q^n} = a \Rightarrow \mathbb{F}_{q^{\gcd(k,n)}} \subseteq \mathbb{F}_{q^k}$ és $\mathbb{F}_{q^{\gcd(k,n)}} \subseteq \mathbb{F}_{q^n}$.

2. $\mathbb{F}_{q^k} \cap \mathbb{F}_{q^n} \subseteq \mathbb{F}_{q^{\gcd(k,n)}}$
$\alpha \in \mathbb{F}_{q^k} \Rightarrow \alpha^{q^k-1} = 1$, $\alpha \in \mathbb{F}_{q^n} \Rightarrow \alpha^{q^n-1} = 1$
$\Rightarrow 1 = (\alpha^{q^k-1})^a(\alpha^{q^n-1})^b = \alpha^{a(q^k-1)+b(q^n-1)}$ $(\forall a, b \in \mathbb{Z})$
A fentiekből következik, hogy $\alpha^{\gcd(q^k-1,q^n-1)} = 1$. Az előző lemmából (1.1.11) tudjuk, hogy $\gcd(q^k - 1, q^n - 1) = q^{\gcd(k,n)} - 1$, ezért $\alpha^{\gcd(q^k-1,q^n-1)} = 1 \Rightarrow \alpha^{q^{\gcd(k,n)}-1} = 1$. Ez pedig azt jelenti, hogy $\alpha \in \mathbb{F}_{q^{\gcd(k,n)}}$, $\forall \alpha \in \mathbb{F}_{q^k} \cap \mathbb{F}_{q^n}$. Tehát $\mathbb{F}_{q^k} \cap \mathbb{F}_{q^n} \subseteq \mathbb{F}_{q^{\gcd(k,n)}}$.

A fentiekből következik, hogy $\mathbb{F}_{q^k} \cap \mathbb{F}_{q^n} = \mathbb{F}_{q^{\gcd(k,n)}}$. $\square$

1.1.13. Következmény. Ha $k|n$, akkor $\mathbb{F}_{q^k} \subseteq \mathbb{F}_{q^n}$.

1.1.14. Definíció. Legyen $k|n$. Ekkor a *test norma:* $\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^k}}(x) = x^{(q^n-1)/(q^k-1)}$.

1.1.15. Állítás. $\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^k}}$ *test norma* $\mathbb{F}_{q^n}$*-ból* $\mathbb{F}_{q^k}$*-ba képez.*

Bizonyítás. Ha $x = 0$, akkor $\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^k}}(0) = 0 \in \mathbb{F}_q$.
$x \in \mathbb{F}_{q^n} \backslash \{0\}$-ra $(\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^k}}(x))^{q^k-1} = x^{q^n-1} = 1$, azaz $\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^k}}(x) \in \mathbb{F}_{q^k}$. □

1.1.16. Állítás. *A test norma multiplikatív:* $\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^k}}(xy) = \mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^k}}(x)\,\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^k}}(y)$.

Bizonyítás.
$\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^k}}(xy) = (xy)^{(q^n-1)/(q^k-1)} = x^{(q^n-1)/(q^k-1)} y^{(q^n-1)/(q^k-1)} = \mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^k}}(x)\,\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^k}}(y)$.
□

1.1.17. Következmény. $\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^k}}(x^t) = (\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^k}}(x))^t$.

1.1.18. Következmény. $\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^k}}(x^{q^k}) = (\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^k}}(x))^{q^k} = \mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^k}}(x)$.

1.1.19. Állítás. *Ha* $x \in \mathbb{F}_q$*, akkor* $\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x) = x^n$.

Bizonyítás. $\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x) = x^{(q^n-1)/(q-1)} = x^{(1+q+q^2+\ldots+q^{n-1})} = x \cdot x^q \cdot x^{q^2} \cdot \ldots \cdot x^{q^{n-1}} = x^n$.
□

1.2. További definíciók és tételek

1.2.1. Definíció. *Trace:* $x \in \mathbb{F}_{q^n}$, $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x) = x + x^q + x^{q^2} + \ldots + x^{q^{n-1}} \in \mathbb{F}_q$.

1.2.2. Definíció. *Duális bázis:* Ha $\{\beta_i\}_{i=0}^{n-1}$ $\mathbb{F}_{q^n}$-nek egy $\mathbb{F}_q$ feletti bázisa, akkor a $\{\beta_i^*\}_{i=0}^{n-1}$ bázis *duális bázisa*, ha $\forall i,j$-re $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\beta_i\beta_j^*) = \delta_{ij}$, ahol $\delta_{ij} = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}$ (Kronecker delta).

1.2.3. Állítás. *Sylvester-egyenlőtlenség:*

$$\mathrm{rk}\, A + \mathrm{rk}\, B - n \leq \mathrm{rk}(AB) \leq \min(\mathrm{rk}\, A, \mathrm{rk}\, B),$$

ahol $A \in \mathbb{K}^{m\times n}$, $B \in \mathbb{K}^{n\times k}$ *valamely* $\mathbb{K}$ *test felett.*

Bizonyítás.

1. Az A és B lineáris leképezések kompozíciójának mátrixa, $AB \in \mathbb{K}^{m\times k}$. Mivel minden, amit B 0-ba képez, AB is 0-ba képez, ezért $\mathrm{Ker}\, B \subseteq \mathrm{Ker}(AB)$. Jelölje $\bar{B}$ a B leképezés megszorítását $\mathrm{Ker}(AB)$-re. Ekkor $\mathrm{Ker}\, \bar{B} = \mathrm{Ker}\, B$. Mivel $\mathrm{Ker}(AB)$ képéről A a 0-ba képez, ezért $\mathrm{Im}\, \bar{B} \subseteq \mathrm{Ker}\, A$. A $\bar{B}$ leképezésre alkalmazva a dimenziótételt:

$$\dim \mathrm{Ker}(AB) = \dim \mathrm{Ker}\, \bar{B} + \dim \mathrm{Im}\, \bar{B} \;\leq\; \dim \mathrm{Ker}\, B + \dim \mathrm{Ker}\, A.$$

A dimenziótételből következik:
$\dim \mathrm{Ker}(AB) = k - \dim \mathrm{Im}(AB)$,
$\dim \mathrm{Ker}\, B = k - \dim \mathrm{Im}\, B$,
$\dim \mathrm{Ker}\, A = n - \dim \mathrm{Im}\, A$.
Ezeket behelyettesítve: $k - \dim \mathrm{Im}(AB) \leq k - \dim \mathrm{Im}\, B + n - \dim \mathrm{Im}\, A$.
Az egyenlőtlenséget átrendezve: $\dim \mathrm{Im}\, A + \dim \mathrm{Im}\, B - n \leq \dim \mathrm{Im}(AB)$.
Azaz $\mathrm{rk}\, A + \mathrm{rk}\, B - n \leq \mathrm{rk}(AB)$.

2. $\mathrm{Im}(AB) \subseteq \mathrm{Im}\, A \;\Rightarrow\; \mathrm{rk}(AB) \leq \mathrm{rk}\, A$.
$\mathrm{Ker}\, B \subseteq \mathrm{Ker}(AB) \;\Rightarrow\; k - \mathrm{rk}\, B \leq k - \mathrm{rk}(AB) \;\Rightarrow\; \mathrm{rk}(AB) \leq \mathrm{rk}\, B$.
Azaz $\mathrm{rk}(AB) \leq \min(\mathrm{rk}\, A, \mathrm{rk}\, B)$.

□

Forrás: [2, Chapter III., Section 5.]

1.2.4. Lemma. *Legyen* $\{a_1, a_2, ..., a_n\} \subseteq \mathbb{F}_{q^n}$. *Ekkor* $\{a_1, a_2, ..., a_n\}$ *pontosan akkor* $\mathbb{F}_q$*-lineárisan függetlenek, ha* $\forall i \geq 0$*-ra* $\{a_1^{q^i}, a_2^{q^i}, ..., a_n^{q^i}\}$ *is* $\mathbb{F}_q$*-lineárisan függetlenek.*

Bizonyítás. Legyen $\{\alpha_1, ..., \alpha_n\} \subseteq \mathbb{F}_q$. Ekkor igaz a következő:
$\sum_{j=1}^n \alpha_j a_j = 0 \Leftrightarrow (\sum_{j=1}^n \alpha_j a_j)^{q^i} = 0$. Mivel $(\sum_{j=1}^n \alpha_j a_j)^{q^i} = \sum_{j=1}^n \alpha_j a_j^{q^i}$, így következik, hogy $\sum_{j=1}^n \alpha_j a_j = 0 \Leftrightarrow \sum_{j=1}^n \alpha_j a_j^{q^i} = 0$. □

Forrás: [3, Lemma 1.3.1.]

1.2.5. Definíció. *Moore-determináns:* $\Delta(a_1, ..., a_n) := \det \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_1^q & a_2^q & \dots & a_n^q \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{q^{n-1}} & a_2^{q^{n-1}} & \dots & a_n^{q^{n-1}} \end{pmatrix}$.

Forrás: [3, Definition 1.3.2.]

1.2.6. Lemma. $\{a_1, ..., a_k\} \subseteq \mathbb{F}_{q^n}$ $(k \leq n)$ *pontosan akkor* $\mathbb{F}_q$*-lineárisan függetlenek, ha* $\Delta(a_1, ..., a_k) \neq 0$.

Bizonyítás.

1. $\Leftarrow$:
Legyen $\Delta(a_1, ..., a_k) \neq 0$, és indirekten tegyük fel, hogy $\exists \{\alpha_i\}_{i=1}^k \subseteq \mathbb{F}_q$ nem mind 0, hogy $\sum \alpha_i a_i = 0$. Ekkor (1.2.4 lemma miatt) $\sum \alpha_i a_i = 0, \sum \alpha_i a_i^q = 0, ..., \sum \alpha_i a_i^{q^{k-1}} = 0$, azaz

$$\sum_{i=1}^{k} \alpha_i \begin{pmatrix} a_i \\ a_i^q \\ \vdots \\ a_i^{q^{k-1}} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Mivel azonban $\Delta(a_1, ..., a_k) \neq 0$, ez csak úgy lehetséges, ha $\alpha_i = 0, \forall i$-re. Ellentmondásra jutottunk.

2. $\Rightarrow$:
Legyenek $\{a_1, ..., a_k\}$ lineárisan függetlenek $\mathbb{F}_q$ felett. Teljes indukcióval bizonyítható, hogy ekkor $\Delta(a_1, ..., a_k) \neq 0$.
Ez $l = 1$-re könnyen látható, hiszen az egy elemű (a_1) mátrix determinánsa nem 0, ha $a_1 \neq 0$.
Tegyük fel, hogy az állítás igaz $l < k$-ra. Indirekten tegyük fel, hogy $l+1$-re nem igaz, azaz $\Delta(a_1, ..., a_{l+1}) = 0$. Ezért $\exists\ \{\alpha_1, ..., \alpha_{l+1}\} \subseteq \mathbb{F}_{q^n}$ nem mind 0, hogy $\sum_{i=1}^{l+1} \alpha_i a_i = 0, \sum_{i=1}^{l+1} \alpha_i a_i^q = 0, ..., \sum_{i=1}^{l+1} \alpha_i a_i^{q^l} = 0$. Feltételezhető, hogy $\alpha_1 = 1$. Emeljük a j. egyenlőséget q-adik hatványra, és vonjuk ki a $j+1$-edik egyenlőségből $(1 \leq j \leq l)$. Az a_1 tagok kiesnek: $\alpha_1 a_1^{q^j} - \alpha_1^q a_1^{q^j} = a_1^{q^j} - a_1^{q^j} = 0$. Azt kapjuk, hogy $\sum_{i=2}^{l+1} (\alpha_i - \alpha_i^q) a_i^q = 0, ..., \sum_{i=2}^{l+1} (\alpha_i - \alpha_i^q) a_i^{q^l} = 0$, ami egyúttal azt is jelenti, hogy a $\{a_2^q, ..., a_{l+1}^q\}$ elemekhez rendelt Moore-mátrix determinánsa 0, ha $(\alpha_i - \alpha_i^q)$ nem mind 0.
Mivel $\{a_1, ..., a_k\}$ $\mathbb{F}_q$-lineárisan függetlenek, ezért (1.2.4 lemma miatt) $\{a_2^q, ..., a_{l+1}^q\}$ is $\mathbb{F}_q$-lineárisan függetlenek. Az indukciós feltevés (l elemre igaz az állítás) miatt következik, hogy ekkor $\Delta(a_2^q, ..., a_{l+1}^q) \neq 0$. Az előzőek miatt $\alpha_i - \alpha_i^q = 0$, azaz $\alpha_i = \alpha_i^q\ \forall i$-re, ebből következik, hogy $\alpha_i \in \mathbb{F}_q, \forall i$. Mivel feltettük, hogy α_i nem mind 0, és $\sum_{i=1}^{l+1} \alpha_i a_i = 0$, ezért $\{a_1, ..., a_{l+1}\}$ lineárisan összefüggők $\mathbb{F}_q$ felett, vagyis ellentmondásra jutottunk, hiszen az eredeti feltevés szerint $\{a_1, ..., a_k\}$ lineárisan függetlenek $\mathbb{F}_q$ felett. Így tehát $\Delta(a_1, ..., a_{l+1}) \neq 0$.

□

Forrás: [3, Lemma 1.3.3.]

1.2.7. Következmény. $\{a_1, ..., a_n\} \subseteq \mathbb{F}_{q^n}$ pontosan akkor $\mathbb{F}_q$-lineárisan függetlenek, azaz bázis $\mathbb{F}_{q^n}$-ben, ha $\Delta(a_1, ..., a_n) \neq 0$.

Forrás: [3, Corollary 1.3.4.]

1.2.8. Állítás. *$\{a_1, ..., a_k\} \subseteq \mathbb{F}_{q^n}$ $(k \leq n)$ pontosan akkor $\mathbb{F}_q$-lineárisan függetlenek, ha a következő („Moore-szerű") mátrix determinánsa (jelölje Δ_s) nem 0, ahol s, n relatív prímek:*

$$\begin{pmatrix} a_1 & a_2 & \dots & a_k \\ a_1^{q^s} & a_2^{q^s} & \dots & a_k^{q^s} \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{q^{(k-1)s}} & a_2^{q^{(k-1)s}} & \dots & a_k^{q^{(k-1)s}} \end{pmatrix}$$

Bizonyítás. Az 1.2.6 lemmabeli bizonyítás alkalmazható erre az esetre is.

1. $\Leftarrow$:
   Tegyük fel, hogy $\Delta_s(a_1, ..., a_k) \neq 0$ és $\{a_1, ..., a_k\}$ lineárisan összefüggő $\mathbb{F}_q$ felett, azaz $\exists\{\alpha_i\}_{i=1}^k \subseteq \mathbb{F}_q$ nem mind 0, hogy $\sum \alpha_i a_i = 0$. Ekkor (1.2.4 lemma miatt) $\sum \alpha_i a_i^{q^s} = 0, \sum \alpha_i a_i^{q^{2s}} = 0, ..., \sum \alpha_i a_i^{q^{(k-1)s}} = 0$, azaz $\exists\{\alpha_i\}_{i=1}^k$:

   $$\sum_{i=1}^k \alpha_i \begin{pmatrix} a_i \\ a_i^{q^s} \\ \vdots \\ a_i^{q^{(k-1)s}} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

   amiből következik, hogy $\Delta_s(a_1, ..., a_k) = 0$. Ellentmondás.

2. $\Rightarrow$:
   Tegyük fel, hogy $\{a_1, ..., a_k\}$ $\mathbb{F}_q$-lineárisan függetlenek. Teljes indukcióval bizonyítható, hogy ekkor $\Delta_s \neq 0$. Tegyük fel, hogy $k-1$-re igaz, és (indirekten) k-ra nem.
   Ekkor $\exists\ \{\alpha_1, ..., \alpha_k\} \subseteq \mathbb{F}_{q^n}$ nem mind 0, hogy $\sum_{i=1}^k \alpha_i a_i = 0$, $\sum_{i=1}^k \alpha_i a_i^{q^s} = 0$, ..., $\sum_{i=1}^k \alpha_i a_i^{q^{(k-1)s}} = 0$.
   Az előző bizonyítás lépéseit alkalmazzuk annyi változtatással, hogy a j. egyenlőséget a q^s-edik hatványra emeljük, és azt vonjuk ki a $j+1$. egyenlőségből. Így kapjuk, hogy $\sum_{i=2}^k (\alpha_i - \alpha_i^{q^s}) a_i^{q^s} = 0$, ..., $\sum_{i=2}^k (\alpha_i - \alpha_i^{q^s}) a_i^{q^{(k-1)s}} = 0$.
   Mivel $\{a_1, ..., a_k\}$ $\mathbb{F}_q$-lineárisan független, ezért $\{a_2^{q^s}, ..., a_k^{q^s}\}$ is az. Indukcióból következik, hogy $\Delta_s(a_2^{q^s}, ..., a_k^{q^s}) \neq 0$. Az előzőek miatt ekkor $\alpha_i - \alpha_i^{q^s} = 0$, azaz $\alpha_i = \alpha_i^{q^s}\ \forall i$. Amiből következik, hogy $\alpha_i \in \mathbb{F}_{q^s}$. Mivel $\alpha_i \in \mathbb{F}_{q^n}$, ezért $\alpha_i \in \mathbb{F}_{q^n} \cap \mathbb{F}_{q^s}$. Az 1.1.12 lemmából következik, hogy ekkor $\alpha_i \in \mathbb{F}_{q^{\gcd(s,n)}}$. Mivel s és n relatív prímek, ezért $\alpha_i \in \mathbb{F}_q\ \forall i$. Ekkor azonban $\{a_1, ..., a_k\}$ lineárisan összefüggőek lennének $\mathbb{F}_q$ felett. Ellentmondás.

□

2. fejezet

Véges test résztest felett lineáris függvényei

2.1. Lineáris függvények és polinomok

Véges testek egyéb tulajdonságain túl érdekes kérdés lehet, hogy mit mondhatunk el a függvényeikről, ezen belül pedig egy adott résztest felett lineáris függvényeikről. Ezekre a kérdésekre az alábbi két állítás ad választ.

Az utóbbihoz be kell vezetnünk a linearizált, vagy más néven ($\mathbb{F}_q$ véges test esetén) q-polinomok fogalmát.

2.1.1. Állítás. *Véges test függvényei polinomok.*

Bizonyítás.

1. Egy q elemű test ($\mathbb{F}_q$) különböző függvényeinek száma: q^q (elemek száma q, mindegyiknek q-féle képe lehet).

2. $\mathbb{F}_q[x]$-beli $\sum_{i=0}^{q-1} a_i x^i$ ($a_i \in \mathbb{F}_q$) alakú polinomok száma: q^q. Mivel minden a_i együttható q különböző értéket vehet fel, ez összesen q^q polinomot jelent.

3. Különböző $\sum_{i=0}^{q-1} a_i x^i$ alakú polinomok különböző függvénynek felelnek meg. Ha nem így lenne, létezne két különböző polinom, amelyek minden $\mathbb{F}_q$-beli x-re egyenlőek:

$$\sum_{i=0}^{q-1} a_i x^i = \sum_{i=0}^{q-1} b_i x^i \quad \Longleftrightarrow \quad \sum_{i=0}^{q-1} (a_i - b_i) x^i = 0 \quad \forall x \in \mathbb{F}_q$$

   Ekkor azonban a polinomnak q darab gyöke lenne. Mivel egy (nem 0) $q-1$ fokú polinomnak (egy test felett) legfeljebb $q-1$ gyöke lehet, a fenti egyenlőség csak úgy teljesülhet, ha ez a nulla polinom. Tehát $a_i - b_i = 0$, azaz $a_i = b_i \ \ \forall i$.

Mivel éppen annyi ($\sum_{i=0}^{q-1} a_i x^i$ alakú) polinom létezik, mint ahány függvény, és különböző (ilyen alakú) polinom különböző függvénynek felel meg, ezért nem létezik olyan függvény $\mathbb{F}_q$-ban, ami nem polinom. Azaz következik az állítás. □

2.1.2. Állítás. *Minden $\mathbb{F}_{q^n}[x]$-beli, $f(x) = \sum_{i=0}^{t} a_i x^{q^i} (t \in \mathbb{N})$ alakú polinomnak megfelelő függvény megegyezik egy $g(x) = \sum_{i=0}^{n-1} b_i x^{q^i}$ alakú polinomhoz tartozó függvénnyel: $\forall f(x)\ \exists g(x)$, hogy $f(a) = g(a)\ \forall a \in \mathbb{F}_{q^n}$.*

Bizonyítás. $i \geq n$-re, ahol $i = bn + r$, $a^{q^i} = a^{q^{bn+r}} = (a^{q^n})^{q^{(b-1)n}q^r} = a^{q^{(b-1)n}q^r}$, mivel $a \in \mathbb{F}_{q^n}$, így $a^{q^n} = a$. Indukció miatt $a^{q^{(b-1)n}q^r} = a^{q^r}$, azaz minden a^{q^i} tag egyenlő egy a^{q^r} taggal, ahol $r \leq n-1$. □

2.1.3. Definíció. q-polinomnak nevezzük a következő alakban előálló $\mathbb{F}_{q^n}[x]$-beli polinomokat:

$$\sum_{i=0}^{n-1} a_i x^{q^i},\ a_i \in \mathbb{F}_{q^n}.$$

2.1.4. Definíció. Azt mondjuk, hogy egy $\sum_{i=0}^{k} a_i x^{q^i}$ polinom q-foka k, ha $a_k \neq 0$.

2.1.5. Definíció. *$\mathbb{F}_q$-lineáris függvény:* egy $f : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ függvény $\mathbb{F}_q$-lineáris, ha $\forall\ x, y \in \mathbb{F}_{q^n}$:
$f(x+y) = f(x) + f(y)$,
$f(\lambda x) = \lambda f(x),\ \forall\ \lambda \in \mathbb{F}_q$.

2.1.6. Állítás. *Egy $\mathbb{F}_{q^n}$ véges test $\mathbb{F}_q$-lineáris függvényei pontosan a q-polinomok.*

Bizonyítás.

1. $\mathbb{F}_q$-lineáris leképezések száma $\mathbb{F}_{q^n}$-en: q^{n^2}

   Tudjuk, hogy $\mathbb{F}_{q^n}$ egy n dimenziós vektortér $\mathbb{F}_q$ felett. Így egy $\mathbb{F}_q$-lineáris leképezés mátrixa egy $n \times n$-es mátrix, melynek elemei $\mathbb{F}_q$-beliek. Mivel a mátrix minden eleme q-féle lehet, így összesen q^{n^2} különböző $n \times n$-es mátrix, így q^{n^2} $\mathbb{F}_q$-lineáris leképezés létezik $\mathbb{F}_{q^n}$-en.

2. q-polinomok száma $\mathbb{F}_{q^n}[x]$-ben: q^{n^2}

   Egy q-polinom n tagból áll, az együtthatói $\mathbb{F}_{q^n}$-beliek, azaz q^n különböző értéket vehetnek fel. Ebből következik, hogy a q-polinomok száma $(q^n)^n$, azaz q^{n^2}.

3. Minden q-polinom $\mathbb{F}_q$-lineáris függvényt határoz meg.

   Ehhez a 2.1.5 definícióbeli tulajdonságnak kell teljesülnie:

   (a) $f(x_1 + x_2) = \sum a_i (x_1 + x_2)^{q^i} = \sum a_i ({x_1}^{q^i} + {x_2}^{q^i}) = \sum a_i {x_1}^{q^i} + \sum a_i {x_2}^{q^i} = f(x_1) + f(x_2)$

   (b) $f(\lambda x) = \sum a_i (\lambda x)^{q^i} = \sum a_i \lambda^{q^i} x^{q^i} = \sum a_i \lambda x^{q^i} = \lambda \sum a_i x^{q^i} = \lambda f(x)$
   (Mivel $\lambda \in \mathbb{F}_q$, ezért $\lambda^{q^i} = \lambda$.)

4. Különböző q-polinomok különböző $\mathbb{F}_q$-lineáris függvénynek felelnek meg.

   Az előző bizonyításban láttuk, hogy különböző polinomok különböző függvényt határoznak meg, így ez különböző q-polinomokra is igaz. Az előző pontban pedig, hogy minden q-polinom $\mathbb{F}_q$-lineáris függvény.

Az 1-4. pontokból következik az állítás. □

2.2. Linearizált polinomok jellemzése

Véges test $\mathbb{F}_q$-lineáris függvényei, azaz a q-polinomok mátrix segítségével jellemezhetőek. Ehhez bevezetek néhány jelölést (melyek megegyeznek a [11]-ben szereplő jelöléssel), valamint egy lemmára is szükség lesz.

Jelölje $\mathscr{L}_n(\mathbb{F}_{q^n})$ a q-polinomok gyűrűjét $\mathbb{F}_{q^n}[x]/(x^{q^n}-x)$-ben, $L(x)$ pedig egy elemét:

$$L(x) \in \mathscr{L}_n(\mathbb{F}_{q^n}) \quad \Longleftrightarrow \quad L(x) = \textstyle\sum_{i=0}^{n-1} a_i x^{q^i} \in \mathbb{F}_{q^n}[x]/(x^{q^n}-x).$$

Jelölje $\mathscr{M}_n(\mathbb{F}_q)$ az $\mathbb{F}_q$ feletti $n \times n$-es mátrixokat, $\mathscr{D}_n(\mathbb{F}_{q^n})$ pedig az $\mathbb{F}_{q^n}$ feletti *Dickson-mátrix*ok halmazát:

$$D \in \mathscr{D}_n(\mathbb{F}_{q^n}) \quad \Longleftrightarrow \quad D = \begin{pmatrix} a_0 & a_1 & \dots & a_{n-1} \\ a_{n-1}^q & a_0^q & \dots & a_{n-2}^q \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{q^{n-1}} & a_2^{q^{n-1}} & \dots & a_0^{q^{n-1}} \end{pmatrix} (a_i \in \mathbb{F}_{q^n}).$$

Rögzítsünk egy $\mathbb{F}_q$-bázist $\mathbb{F}_{q^n}$-ben: $\{\beta_i\}_{i=0}^{n-1}$; jelölje $\{\beta_i^*\}_{i=0}^{n-1}$ a duális bázist, melyre $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\beta_i\beta_j^*) = \delta_{ij}$, $0 \le i,j \le n-1$, ahol $\delta_{ij} = \begin{cases} 1, & i=j \\ 0, & i \neq j \end{cases}$ (Kronecker delta).

Mátrixok további jelölése: (a_{ij}).

Például a Dickson-mátrix: $(a_{j-i}^{q^i})$, ahol az (i,j). elem $a_{j-i \ (mod\ n)}^{q^i}$ $(i,j = 0..n-1)$.

Legyen $D_L \in \mathscr{D}_n(\mathbb{F}_{q^n})$ az a Dickson-mátrix, amely első (azaz 0.) sorának elemei az $L(x) \in \mathscr{L}_n(\mathbb{F}_{q^n})$ q-polinom együtthatói. A következő lemma szerint az $L(x)$-hez tartozó lineáris transzformáció mátrixa (M_L) leírható D_L és egy rögzített bázis segítségével.

2.2.1. Lemma. *Legyen $L(x) = \sum_{i=0}^{n-1} a_i x^{q^i} \in \mathscr{L}_n(\mathbb{F}_{q^n})$, jelölje $M_L \in \mathscr{M}_n(\mathbb{F}_q)$ az $L(x)$ lineáris transzformáció mátrixát a $\{\beta_i\}_0^{n-1}$ bázisban. Ekkor*

$$M_L = (\beta_j^{q^i})^{-1} D_L (\beta_j^{q^i}). \tag{2.1}$$

Bizonyítás. Mivel M_L az $L(x)$-hez tartozó lineáris transzformáció mátrixa a $\{\beta_j\}$ bázisban, ezért:

$$(L(\beta_0), ..., L(\beta_{n-1})) = (\beta_0, ..., \beta_{n-1}) M_L.$$

Jelölje m_{kj} az M_L k-adik sorának j-edik elemét. A fentiek alapján: $L(\beta_j) = \sum_{k=0}^{n-1} m_{kj}\beta_k$ $(\forall\, 0 \le j \le n-1)$. A következő egyenlőség adódik (a továbbiakban Tr jelölje az $\mathbb{F}_{q^n}$-ből $\mathbb{F}_q$-ba képező *trace* függvényt):

$$\mathrm{Tr}(\beta_i^* L(\beta_j)) = \mathrm{Tr}(\beta_i^* (\textstyle\sum_{k=0}^{n-1} m_{kj}\beta_k)).$$

A *trace*-t kifejtve kapjuk (a szumma továbbra is $k = 0$-tól $n-1$-ig megy, ezt az egyszerűség és az átláthatóság kedvéért most elhagyjuk):

$$\mathrm{Tr}(\beta_i^*(\sum m_{kj}\beta_k)) = \mathrm{Tr}(\sum m_{kj}\beta_i^*\beta_k) =$$
$$\sum m_{kj}\beta_i^*\beta_k + (\sum m_{kj}\beta_i^*\beta_k)^q + (\sum m_{kj}\beta_i^*\beta_k)^{q^2} + ... + (\sum m_{kj}\beta_i^*\beta_k)^{q^{n-1}}.$$

Kihasználva a tagonkénti hatványozás lehetőségét, valamint, hogy mivel $m_{kj} \in \mathbb{F}_q$, ezért $m_{kj}^q = m_{kj}$, kapjuk a további egyenlőséget:

$$... = \sum m_{kj}\beta_i^*\beta_k + \sum m_{kj}(\beta_i^*\beta_k)^q + \sum m_{kj}(\beta_i^*\beta_k)^{q^2} + ... + \sum m_{kj}(\beta_i^*\beta_k)^{q^{n-1}} =$$
$$\sum m_{kj}(\beta_i^*\beta_k + (\beta_i^*\beta_k)^q + (\beta_i^*\beta_k)^{q^2} + ... + (\beta_i^*\beta_k)^{q^{n-1}}) = \sum m_{kj}\,\mathrm{Tr}(\beta_i^*\beta_k).$$

Mivel $\mathrm{Tr}(\beta_i^*\beta_k) = \delta_{ik}$, ezért $\sum_{k=0}^{n-1} m_{kj}\,\mathrm{Tr}(\beta_i^*\beta_k) = m_{ij}$.

A fentiekből a következő egyenlőség adódik:

$$\mathrm{Tr}(\beta_i^* L(\beta_j)) = m_{ij},\ \forall\ 0 \le i,j \le n-1.$$

Tehát M_L minden eleme előáll ilyen alakban: $M_L = (m_{ij}) = (\mathrm{Tr}(\beta_i^* L(\beta_j)))$.

A $(\beta_i^{*q^j})$ és $(L(\beta_j)^{q^i})$ mátrixokat, valamint a szorzatuk mátrixát felírva jutunk a további egyenlőségre:

$$(\beta_i^{*q^j}) = \begin{pmatrix} \beta_0^* & \beta_0^{*q} & \dots & \beta_0^{*q^{n-1}} \\ \beta_1^* & \beta_1^{*q} & \dots & \beta_1^{*q^{n-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \beta_{n-1}^* & {\beta_{n-1}^*}^q & \dots & {\beta_{n-1}^*}^{q^{n-1}} \end{pmatrix},$$

$$(L(\beta_j)^{q^i}) = \begin{pmatrix} L(\beta_0) & L(\beta_1) & \dots & L(\beta_{n-1}) \\ L(\beta_0)^q & L(\beta_1)^q & \dots & L(\beta_{n-1})^q \\ \vdots & \vdots & \ddots & \vdots \\ L(\beta_0)^{q^{n-1}} & L(\beta_1)^{q^{n-1}} & \dots & L(\beta_{n-1})^{q^{n-1}} \end{pmatrix},$$

$$(\beta_i^{*q^j})(L(\beta_j)^{q^i}) = \begin{pmatrix} \mathrm{Tr}(\beta_0^* L(\beta_0)) & \mathrm{Tr}(\beta_0^* L(\beta_1)) & \dots & \mathrm{Tr}(\beta_0^* L(\beta_{n-1})) \\ \mathrm{Tr}(\beta_1^* L(\beta_0)) & \mathrm{Tr}(\beta_1^* L(\beta_1)) & \dots & \mathrm{Tr}(\beta_1^* L(\beta_{n-1})) \\ \vdots & \vdots & \ddots & \vdots \\ \mathrm{Tr}(\beta_{n-1}^* L(\beta_0)) & \mathrm{Tr}(\beta_{n-1}^* L(\beta_1)) & \dots & \mathrm{Tr}(\beta_{n-1}^* L(\beta_{n-1})) \end{pmatrix},$$

ahol az i. sor j. eleme éppen $\mathrm{Tr}(\beta_i^* L(\beta_j))$.

Tehát adódik a következő:

$$M_L = (\mathrm{Tr}(\beta_i^* L(\beta_j))) = (\beta_i^{*q^j})(L(\beta_j)^{q^i}).$$

A továbbiakban az $(L(\beta_j)^{q^i})$ mátrixot vizsgáljuk. Mivel $L(x) \in \mathbb{F}_{q^n}[x]/(x^{q^n} - x)$, ezért az $L(\beta_j)$-kkel mod $x^{q^n} - x$ számolunk. $L(x)^{q^i}$-t kifejtve és az indexet átalakítva ($k := j + i\ (mod\ n)$) kapjuk:

$$L(x)^{q^i} = (\sum_{j=0}^{n-1} a_j x^{q^j})^{q^i} = \sum_{j=0}^{n-1} a_j^{q^i} x^{q^{j+i}} = \sum_{k=i}^{n-1+i} a_{k-i}^{q^i} x^{q^k} = \sum_{k=0}^{n-1} a_{k-i}^{q^i} x^{q^k},$$
$$0 \le i \le n-1.$$

Itt az együtthatók éppen D_L i. sorának elemei, így a következő egyenlőség adódik az $\{L(x)^{q^i}\}_{i=0}^{n-1}$-kből alkotott n-dimenziós vektorra:

$$\begin{pmatrix} L(x) \\ L(x)^q \\ \vdots \\ L(x)^{q^{n-1}} \end{pmatrix} = D_L \begin{pmatrix} x \\ x^q \\ \vdots \\ x^{q^{n-1}} \end{pmatrix}.$$

β_j-ket behelyettesítve: $(L(\beta_j)^{q^i}) = D_L(\beta_j^{q^i})$.

Most nézzük a $(\beta_i^{*q^j})$ mátrixot. Mivel $\mathrm{Tr}(\beta_i^*\beta_j) = \delta_{ij}$, ezért $(\beta_i^{*q^j})(\beta_j^{q^i}) = (\mathrm{Tr}(\beta_i^*\beta_j)) = I_n$, azaz az $n \times n$-es egységmátrix. Tehát $(\beta_i^{*q^j}) = (\beta_j^{q^i})^{-1}$.

Láttuk, hogy $M_L = (\beta_i^{*q^j})(L(\beta_j)^{q^i})$, továbbá $(L(\beta_j)^{q^i}) = D_L(\beta_j^{q^i})$ és $(\beta_i^{*q^j}) = (\beta_j^{q^i})^{-1}$, így ezeket behelyettesítve: $M_L = (\beta_j^{q^i})^{-1} D_L(\beta_j^{q^i})$. Ami éppen (2.1). $\square$

Forrás: [11, Lemma 4.1.]

2.2.2. Állítás. *Legyen $A \in \mathbb{K}^{n\times n}$ valamely $\mathbb{K}$ test felett. Ekkor* $\mathrm{rk}\, A = k \Leftrightarrow \exists\, P, Q \in \mathbb{K}^{n\times n}$ *invertálható mátrixok, hogy $A = PEQ$, ahol E egy diagonális mátrix, melynek átlójában a felső k elem 1, a többi 0:* $E = \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix}$.

Bizonyítás.

1. $\Leftarrow$:
   A *Sylvester-egyenlőtlenség*ből következik, hogy

   $$\mathrm{rk}\, P + \mathrm{rk}(EQ) - n \leq \mathrm{rk}(PEQ) \leq \min(\mathrm{rk}\, P, \mathrm{rk}(EQ)),$$

   továbbá

   $$\mathrm{rk}\, E + \mathrm{rk}\, Q - n \leq \mathrm{rk}(EQ) \leq \min(\mathrm{rk}\, E, \mathrm{rk}\, Q).$$

   Mivel P és Q invertálhatóak, ezért $\mathrm{rk}\, P = \mathrm{rk}\, Q = n$, továbbá $\mathrm{rk}\, E = k \leq n$. Azt kapjuk, hogy

   $$k + n - n \leq \mathrm{rk}(EQ) \leq k, \text{ azaz } \mathrm{rk}(EQ) = k.$$

   Ebből pedig

   $$n + k - n \leq \mathrm{rk}(PEQ) \leq k,$$

   azaz $\mathrm{rk}\, A = \mathrm{rk}(PEQ) = k$.

2. $\Rightarrow$:
Az A mátrix megfeleltethető egy lineáris leképezés mátrixának két n-dimenziós vektortér között: $V_1 \to V_2$. Legyenek $\{p_i\}_{i=1}^n$ és $\{q_i\}_{i=1}^n$ bázisok V_1-ben ill. V_2-ben. Legyen r az $\{Ap_i\}_{i=1}^n$ vektorok között a függetlenek maximális száma. Feltehető, hogy a lineárisan független vektorok: $\{Ap_i\}_{i=1}^r$. A maradék $n-r$ vektor előáll ezek lineáris kombinációjaként: $Ap_i = \sum_{j=1}^r \lambda_{ij} Ap_j$, $i = r+1, ..., n$.
Térjünk át új bázisokra V_1 ill. V_2-ben a következőképp:
$p'_i = \begin{cases} p_i, & i = 1, ..., r \\ p_i - \sum_{j=1}^r \lambda_{ij} p_j, & i = r+1, ..., n \end{cases}$,
$q'_i = Ap'_i$, $i = 1, ..., r$, ezt kiegészítjük bázissá további $n-r$ db $q'_{r+1}, ..., q'_n$ vektorral.
Ekkor $Ap'_i = A(p_i - \sum_{j=1}^r \lambda_{ij} p_j) = Ap_i - \sum_{j=1}^r \lambda_{ij} Ap_j = Ap_i - Ap_i = 0$, $i = r+1, ..., n$.
Ebből, és az új $\{q'_i\}_{i=1}^n$ bázis definíciójából következik, hogy a leképezés mátrixa az új bázisokban:

$$\begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix}$$, melynek r db eleme 1, a többi 0.

Legyenek P' és Q az áttérési mátrixok az új bázisokra, E pedig jelölje a fenti mátrixot. Ekkor $E = P'AQ^{-1}$, amiből $A = P'^{-1}EQ$. Legyen $P = P'^{-1}$, így $A = PEQ$, ahol P és Q invertálhatóak. A bizonyítás első feléből következik, hogy ekkor A és E rangja megegyezik, tehát $r = k$.

□

Forrás: [2, Chapter III., Section 5.]

2.2.3. Állítás. *Minden $L(x) \in \mathscr{L}_n(\mathbb{F}_{q^n})$ lineáris transzformáció mátrixának (L) rangja ill. determinánsa egyenlő a megfelelő Dickson-mátrix (D_L) rangjával ill. determinánsával, azaz* $\operatorname{rk} L = \operatorname{rk} D_L$ *és* $\det L = \det D_L$.

Bizonyítás.

1. Egy lineáris transzformáció bármely bázisban felírt mátrixának ugyanakkora a rangja ill. determinánsa. Ezért $\operatorname{rk} L = \operatorname{rk} M_L$ és $\det L = \det M_L$ (ahol M_L az L lineáris transzformáció mátrixa az $\mathbb{F}_q$ feletti $\{\beta_i\}_{i=0}^{n-1}$ bázisban felírva). Továbbá az előző lemmából és a determinánsok szorzástételéből következik, hogy

$$\det M_L = \det((\beta_j^{q^i})^{-1} D_L(\beta_j^{q^i})) = \det(\beta_j^{q^i})^{-1} \det D_L \det(\beta_j^{q^i}) = \det D_L \det\left((\beta_j^{q^i})^{-1}(\beta_j^{q^i})\right) = \det D_L \det I_n = \det D_L$$

(ahol I_n az $n \times n$-es egységmátrix). Tehát $\det L = \det M_L = \det D_L$.

2. Az előző állításból tudjuk, hogy léteznek olyan invertálható $P,\ Q \in \mathbb{F}_q^{n\times n}$ mátrixok, hogy $M_L = PEQ$, ahol E egy olyan diagonális mátrix, amelynek felső $\operatorname{rk} M_L$ db eleme 1, a többi 0. Ekkor

$$M_L = (\beta_j^{q^i})^{-1} D_L (\beta_j^{q^i}) \iff D_L = (\beta_j^{q^i}) M_L (\beta_j^{q^i})^{-1} = (\beta_j^{q^i}) PEQ (\beta_j^{q^i})^{-1}.$$

Legyen $R = (\beta_j^{q^i})P$ és $S = Q(\beta_j^{q^i})^{-1} \in \mathbb{F}_{q^n}^{n\times n}$. Mivel $(\beta_j^{q^i})$, P és Q is invertálható, ezért R és S is invertálhatóak. Azaz $\exists R,\ S \in \mathbb{F}_{q^n}^{n\times n}$ invertálható mátrixok, hogy $D_L = RES$. Az előző állítást ezúttal D_L-re alkalmazva kapjuk, hogy $\operatorname{rk} D_L = \operatorname{rk} M_L = \operatorname{rk} L$.

□

Forrás: [11, Proposition 4.4.]

3. fejezet

MRD kódok

3.1. Rank metric kód korlátja

Legyen $\mathcal{C} \subseteq \mathbb{F}_q^{m\times n}$, azaz a q elemű test feletti $m \times n$-es mátrixok egy részhalmaza.

Jelölje $d(A,B) = \mathrm{rk}(A-B)$ az $\mathbb{F}_q^{m\times n}$-beli mátrixok különbségének rangját.

3.1.1. Állítás. *Ekkor $d(A,B) = \mathrm{rk}(A-B)$ egy metrika $\mathbb{F}_q^{m\times n}$-en („rank distance").*

Bizonyítás.

1. $\mathrm{rk}(A-B) \geq 0$ a mátrix rang definíciójából következik.
2. $\mathrm{rk}(A-B) = 0 \iff A = B$, mivel egyedül a null mátrix rangja 0.
3. $\mathrm{rk}(A-B) = \mathrm{rk}(B-A)$ következik abból, hogy a mátrix (-1)-gyel való szorzása nem változtat a rangján.
4. $\mathrm{rk}(A-B) + \mathrm{rk}(B-C) \geq \mathrm{rk}(A-C)$ (háromszög egyenlőtlenség)
   U, V vektorterekre $dim(U)+dim(V) \geq dim(U+V)$. Mátrix rangja egyenlő az oszlopterének dimenziójával, ezért $\mathrm{rk}(A)+\mathrm{rk}(B) \geq \mathrm{rk}(A+B)$. A megfelelő helyekre $A-B$-t ill. $B-C$-t helyettesítve: $\mathrm{rk}(A-B)+\mathrm{rk}(B-C) \geq \mathrm{rk}(A-B+B-C) = \mathrm{rk}(A-C)$.

□

3.1.2. Definíció. $\mathcal{C} \subseteq \mathbb{F}_q^{m\times n}$ részhalmazt a $d(A,B) = \mathrm{rk}(A-B)$ $(A,B \in \mathcal{C})$ metrikával *rank metric kód*nak nevezzük.

3.1.3. Állítás. *Legyen d a minimális rang távolság $\mathcal{C}$-n:*

$$d := \min\{\mathrm{rk}(A-B) : A,B \in \mathcal{C}\}.$$

Ekkor

$$|\mathcal{C}| \leq q^{max\{n,m\}(min\{n,m\}-d+1)}. \tag{3.1}$$

Bizonyítás. Legyen $m \leq n$. Indirekten tegyük fel, hogy $|\mathcal{C}| > q^{n(m-d+1)}$. Tekintsük az ${\mathbb{F}_q}^{m\times n}$-beli $m \times n$-es mátrixok felső $m-d+1$ sorát. Mivel a test q elemű, ezért összesen $q^{n(m-d+1)}$ különböző $(m-d+1)\times n$-es részmátrix létezik. Feltettük, hogy $\mathcal{C}$ ennél több elemű, így létezik legalább kettő, amelyik felső $m-d+1$ sorában megegyezik. Ebből következik, hogy a különbségük rangja legfeljebb $m-(m-d+1) = d-1$, azaz $\exists A,\ B \in \mathcal{C}$, $\mathrm{rk}(A-B) \leq d-1$. Azonban d-t a különbségmátrixok rangjának minimumaként definiáltuk, tehát ellentmondásra jutottunk. □

3.1.4. Következmény. A korlát négyzetes mátrixokra:

$$|\mathcal{C}| \leq q^{n(n-d+1)}. \tag{3.2}$$

3.1.5. Definíció. $\mathcal{C}$-t MRD („Maximum Rank Distance") kódnak nevezzük, ha maximális elemszámú, azaz

$$|\mathcal{C}| = q^{max\{n,m\}(min\{n,m\}-d+1)}.$$

3.1.6. Definíció. Ha $\mathcal{C}$ MRD kód és altér $\mathbb{F}_q^{m\times n}$-ben, akkor $\mathcal{C}$-t *lineáris MRD kód*nak nevezzük.

3.2. Kódok reprezentációja

Rank metric kódok mátrixokon túl tekinthetőek vektorok, vagy q-polinomok halmazának is.

Egy $\mathcal{C} \subseteq \mathbb{F}_q^{m\times n}$ kód megfeleltethető egy $\mathcal{C}' \subseteq \mathbb{F}_{q^n}^m$ kódnak (a mátrix egy-egy sorát $\mathbb{F}_q$-beli koordinátáknak tekintve $\mathbb{F}_{q^n}$ valamely $\mathbb{F}_q$-bázisához, azok megfeleltethetőek egy $\mathbb{F}_{q^n}$-beli elemnek), valamint egy $\mathcal{C} \subseteq \mathbb{F}_q^{n\times n}$ kód egy $\mathcal{C}'' \subseteq \mathbb{F}_{q^n}[x]$ linearizált polinomokkal definiált kódnak, amelyben a polinomok maximum $n-1$ q-fokúak.

A mátrix reprezentációban a távolság a mátrixok különbségének a rangja. A vektor reprezentációban a távolság annak a térnek az $\mathbb{F}_q$ feletti dimenziója, amelyet a két vektor különbségének koordinátái feszítenek, másképpen a különbségvektor $\mathbb{F}_q$ felett független koordinátáinak maximális száma. Két mátrix különbségének a rangja egyenlő a nekik megfelelő vektorok különbsége által feszített tér dimenziójával. Linearizált polinomokkal definiált kód egy polinomjának rangja $n-$(a polinom gyökeinek száma), ami egyenlő a hozzá tartozó lineáris leképezés mátrixának rangjával, így két q-polinom rang távolsága a megfelelő mátrixok különbségének rangja.

Forrás: [1, Section 1.1], [9, 9 Appendix]

3.3. Altér kódok

Altér kódok elemei vektorterek. A következőkben az MRD kódokkal való kapcsolatukról lesz szó.

3.3.1. Definíció. Legyen $\mathcal{S}$ egy véges dimenziós vektortér altereinek egy nemüres halmaza. Ezen definiáljuk a következő távolság-függvényt:

$$d_S(U,V) = \dim U + \dim V - 2\dim(U \cap V).$$

$\mathcal{S}$-t altér kódnak nevezzük („subspace code"). Ha $\mathcal{S}$ minden eleme azonos dimenziójú, akkor $\mathcal{S}$ konstans dimenziójú kód („constant dimension code").

Egy MRD kód meghatároz egy konstans dimenziójú altér kódot.
Legyen $X \in \mathcal{C}$, ahol $\mathcal{C} \subseteq \mathbb{F}_q^{m\times n}$ egy MRD kód d minimum rang távolsággal. Definiáljuk $\mathcal{S}$ elemeit a következőképpen:

$$S = \{S_X : X \in \mathcal{C}\},$$
$$S_X := \{(u, Xu) : u \in \mathbb{F}_q^n\} \subseteq \mathbb{F}_q^{n+m}.$$

Ekkor $\mathcal{S}$ egy konstans dimenziójú altér kód $2d$ minimális távolsággal.

3.3.2. Állítás. *$\mathcal{S}$ elemei n-dimenziós alterek $\mathbb{F}_q$ felett. Az $\mathcal{S}$-en értelmezett távolság-függvényre a következő teljesül:*

$$d_S(S_X, S_Y) = 2\,\mathrm{rk}(X - Y),$$

$S_X, S_Y \in \mathcal{S},\ X, Y \in \mathcal{C}$. d_S metrika $\mathcal{S}$-en.

Bizonyítás.

1. S_X altér:
   (a) $(u, Xu) \in S_X,\ \lambda \in \mathbb{F}_q \ \Rightarrow\ \lambda(u, Xu) \in S_X$
   Ez következik abból, hogy $\lambda(u, Xu) = (\lambda u, \lambda X u) = (\lambda u, X(\lambda u)) \in S_X$, mivel $\lambda u \in \mathbb{F}_q^n$.
   (b) $(u_1, Xu_1), (u_2, Xu_2) \in S_X \ \Rightarrow\ (u_1, Xu_1) + (u_2, Xu_2) \in S_X$
   $(u_1, Xu_1) + (u_2, Xu_2) = (u_1 + u_2, Xu_1 + Xu_2) = (u_1 + u_2, X(u_1 + u_2)) \in S_X$, mert $u_1 + u_2 \in \mathbb{F}_q^n$.

2. S_X n-dimenziós:
   Mivel $u \in \mathbb{F}_q^n$, és $\mathbb{F}_q^n$ n-dimenziós $\mathbb{F}_q$ felett, valamint $(u, Xu) = (v, Xv) \Leftrightarrow u = v$, ezért S_X is n-dimenziós.

3. $d_S(S_X, S_Y) = 2\,\mathrm{rk}(X - Y)$:
   Definíció szerint $d_S(S_X, S_Y) = \dim S_X + \dim S_Y - 2\dim(S_X \cap S_Y)$.
   $S_X \cap S_Y = \{(u, Xu) : u \in \mathbb{F}_q^n,\ Xu = Yu\}$, vagyis azon $(u, Xu) \in \mathbb{F}_q^{n+m}$ vektorok halmaza, ahol $Xu - Yu = (X - Y)u = 0$. Azaz $u \in \mathrm{Ker}(X - Y)$.
   Tehát $\dim(S_X \cap S_Y) = \dim \mathrm{Ker}(X - Y) = n - \dim \mathrm{Im}(X - Y) = n - \mathrm{rk}(X - Y)$.
   Behelyettesítve:
   $d_S(S_X, S_Y) = \dim S_X + \dim S_Y - 2\dim(S_X \cap S_Y) = n + n - 2(n - \mathrm{rk}(X - Y)) = 2n - 2n + 2\,\mathrm{rk}(X - Y) = 2\,\mathrm{rk}(X - Y)$.

4. d_S metrika:
   Tudjuk, hogy $d_S(S_X, S_Y) = 2\,\mathrm{rk}(X - Y)$ és hogy $\mathrm{rk}(X - Y)$ metrika.
   (a) $d_S(S_X, S_Y) \geq 0$, mert $rk(X - Y) \geq 0$

(b) $d_S(S_X, S_Y) = 0 \Leftrightarrow S_X = S_Y$, mert $rk(X - Y) = 0 \Leftrightarrow X = Y$

(c) $d_S(S_X, S_Y) = d_S(S_Y, S_X)$, mert $rk(X - Y) = rk(Y - X)$

(d) $d_S(S_X, S_Y) + d_S(S_Y, S_Z) \geq d_S(S_X, S_Z)$, mert $2\,\mathrm{rk}(X - Y) + 2\,\mathrm{rk}(Y - Z) \geq 2\,\mathrm{rk}(X - Z) \Leftrightarrow \mathrm{rk}(X - Y) + \mathrm{rk}(Y - Z) \geq \mathrm{rk}(X - Z)$, ezt pedig már láttuk.

□

3.3.3. Következmény. $\min d_S = \min\{d_S(S_X, S_Y) : S_X, S_Y \in \mathcal{S}\} = \min\{2\,\mathrm{rk}(X - Y) : X, Y \in \mathcal{C}\} = 2\min\{\mathrm{rk}(X - Y) : X, Y \in \mathcal{C}\} = 2d$.

Forrás: [8, Section 1.4]

3.4. Gabidulin-kód

Ernst Gabidulin egy általános definíciót adott MRD kódok egy csoportjára.

2.1.6 állításban láttuk, hogy egy $\mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ $\mathbb{F}_q$-lineáris leképezés előáll q-polinom alakban:

$$\sum_{i=0}^{n-1} a_i x^{q^i},\ a_i,\ x \in \mathbb{F}_{q^n}.$$

Valamint minden q-polinom $\mathbb{F}_q$-lineáris leképezés.

3.4.1. Definíció. *Gabidulin-kód:*
Legyen $\gcd(n, s) = 1$, $k \leq n$.

$$\mathcal{G}_{k,s,n} := \{a_0 x + a_1 x^{q^s} + ... + a_{k-1} x^{q^{s(k-1)}} : a_0, a_1, ..., a_{k-1} \in \mathbb{F}_{q^n}\}$$

Ha $s = 1$:

$$\mathcal{G}_k = \{a_0 x + a_1 x^q + ... + a_{k-1} x^{q^{(k-1)}} : a_0, a_1, ..., a_{k-1} \in \mathbb{F}_{q^n}\}$$

Forrás: [8, Section 2]

Ahhoz, hogy lássuk, hogy ez tényleg MRD kód, két állítást kell bizonyítanunk a q-polinomok, majd a Gabidulin-kód polinomjainak rangjáról.

3.4.2. Állítás. *k q-fokú q-polinomok rangja legalább $n - k$.*

Bizonyítás. Egy k q-fokú polinomnak legfeljebb q^k gyöke lehet. Ezért a hozzá tartozó lineáris transzformáció magterének a dimenziója legfeljebb k, amiből következik, hogy a rangja legalább $n - k$. □

Forrás: [8, Theorem 2]

Legyen $A = \{\alpha_0, \alpha_1, ..., \alpha_{k-1}\} \subseteq \mathbb{F}_{q^n}$, $\gcd(n, s) = 1$ és $k \leq n$. Definiáljuk a következő mátrixot:

$$M_{A,s} = \begin{pmatrix} \alpha_0 & \alpha_1 & \dots & \alpha_{k-1} \\ \alpha_0^{q^s} & \alpha_1^{q^s} & \dots & \alpha_{k-1}^{q^s} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_0^{q^{s(k-1)}} & \alpha_1^{q^{s(k-1)}} & \dots & \alpha_{k-1}^{q^{s(k-1)}} \end{pmatrix},$$

jelölje $\Delta_{A,s}$ a determinánsát.

3.4.3. Állítás. *Egy $\mathcal{G}_{k,s,n}$-beli polinomhoz tartozó lineáris transzformáció rangja legalább $n-k+1$.*

Bizonyítás. Indirekten tegyük fel, hogy $f(x) = \sum_{i=0}^{k-1} a_i x^{q^{si}} \in \mathcal{G}_{k,s,n}$ rangja $\leq n-k$, azaz a magtér dimenziója $\geq k$. Válasszunk ki k db $\mathbb{F}_q$-lineárisan független $\mathbb{F}_{q^n}$-beli elemet (jelölje őket B), melyet a $f(x)$ a 0-ba képez. Ekkor a belőlük képzett $M_{B,s}$ mátrix determinánsa nem lehet 0 (1.2.8 állítás miatt). Mivel a mátrixot magtérbeli elemekből képeztük, azt balról szorozva a polinom együtthatóiból képzett vektorral a 0 vektort kapjuk. Ez azonban ellentmond annak, hogy a determináns nem nulla. Tehát nem létezhet k lineárisan független elem a magtérben, vagyis a polinomfüggvény rangja legalább $n-k+1$. □

Bizonyítás Dickson-mátrixszal

Bizonyítás. 2.2.3 állításban láttuk, hogy egy q-polinom rangja megegyezik a hozzá tartozó Dickson-mátrix rangjával.

A mátrix rangja nem változik, ha invertálható mátrixokkal szorozzuk. Válasszunk egy megfelelő permutáció-mátrixot (P), és szorozzuk be vele D-t balról, és annak inverzével (azaz transzponáltjával) jobbról úgy, hogy a kapott mátrixban szerepeljen egy megfelelő nagyságú felsőháromszög mátrix. Ez az alkalmas P permutáció-mátrix a következő sorrendbe rendezi a mátrix sorait ill. oszlopait, azokat 0-tól indexelve:
0., s., $2s$., ..., $(n-1)s$. sor/oszlop (modulo n számolva).

Egy példán szemléltetve, ahol $n=5,\ k=3,\ s=2$, a polinom $a_0x + a_1x^{q^2} + a_2x^{q^4}$, a hozzá tartozó Dickson-mátrix: $D = \begin{pmatrix} a_0 & 0 & a_1 & 0 & a_2 \\ a_2^q & a_0^q & 0 & a_1^q & 0 \\ 0 & a_2^{q^2} & a_0^{q^2} & 0 & a_1^{q^2} \\ a_1^{q^3} & 0 & a_2^{q^3} & a_0^{q^3} & 0 \\ 0 & a_1^{q^4} & 0 & a_2^{q^4} & a_0^{q^4} \end{pmatrix}$.

A megfelelő permutáció-mátrix: $P = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$.

$$D' = PDP^{-1} = \begin{pmatrix} a_0 & a_1 & a_2 & 0 & 0 \\ 0 & a_0^{q^2} & a_1^{q^2} & a_2^{q^2} & 0 \\ 0 & 0 & a_0^{q^4} & a_1^{q^4} & a_2^{q^4} \\ a_2^q & 0 & 0 & a_0^q & a_1^q \\ a_1^{q^3} & a_2^{q^3} & 0 & 0 & a_0^{q^3} \end{pmatrix}$$

Látható, hogy az új D' mátrix (i,j) indexű eleme az eredeti D mátrix (is, js) indexű elemével egyenlő (az indexeket mindig modulo n tekintjük). Ha feltesszük, hogy a polinom együtthatói nem 0-k, akkor a D mátrix egy is. sorának (ami a 0. sor is elemmel való eltoltja, elemenként a q^{is}. hatványra emelve) *nem 0 elemei* a következő oszlopindexű elemek: $is, (i+1)s, (i+2)s, ..., (i+k-1)s \pmod n$.

A D' mátrix i. sorának 0 - $(i-1)$. elemei: a D mátrix is. sorának következő oszlopindexű elemei: $0, s, 2s, ..., (i-1)s \pmod n$.

Mivel $(n,s) = 1$, ezért $\{0, s, 2s, ..., (n-1)s \pmod n\} = \{0, 1, 2, ..., n-1\}$. Ebből következik, hogy az új D' mátrix i. sorának első i (0.,...,$i-1$. indexű) eleme között akkor lehet nem 0 elem (a polinom valamely együtthatójának hatványa), ha $\{0, s, 2s, ..., (i-1)s\}$ $\cup$ $\{is, (i+1)s, (i+2)s, ..., (i+k-1)s\}$ elemszáma $> n$. Azaz, ha $i+k-1 > n-1 \Leftrightarrow i+k > n \Leftrightarrow i > n-k$.

Ha viszont $i \in \{0, 1, ..., n-k\}$, akkor az első i elem nem 0, ami azt jelenti, hogy D'-ben szerepel egy $(n-k+1) \times (n-k+1)$-es felsőháromszög mátrix (a D' mátrix bal fölső sarkában, átlójában a_0 hatványaival), amely determinánsa nem 0, ha $a_0 \neq 0$. Tehát D, és így a q-polinom rangja $\geq n-k+1$.

Hasonlóan bizonyítható, hogy a D' mátrix jobb fölső sarkában pedig szerepel egy $(n-k+1) \times (n-k+1)$-es alsóháromszög mátrix.

A D' mátrix i. sorának nem nulla elemei (amennyiben a polinom együtthatói nem 0-k) tehát a D mátrix is. sorának következő oszlopindexű elemei: $0, s, 2s, ..., (i-1)s \pmod n$.

$i < n-k$ esetén D' i. sorának utolsó $n-k-i$ (>0) eleme ($(i+k)$ - $(n-1)$. indexszel) pedig az eredeti D mátrix következő oszlopindexű elemei: $(i+k)s, (i+k+1)s, ..., (n-1)s \pmod n$.

Mivel $\{0, s, 2s, ..., (n-1)s \pmod n\} = \{0, 1, 2, ..., n-1\}$, ezért a két halmaz metszete üres:
$\{0, s, 2s, ..., (i-1)s \pmod n\} \cap \{(i+k)s, (i+k+1)s, ..., (n-1)s \pmod n\} = \emptyset$.

Tehát $i \in \{0, ..., n-k-1\}$ esetén a D' mátrix i. sorának utolsó $n-k-i$ eleme 0. Azaz valóban található D'-ben (annak jobb fölső sarkában, átlójában a_{k-1} hatványaival) egy $(n-k+1) \times (n-k+1)$-es alsóháromszög mátrix, amely determinánsa nem 0, ha $a_{k-1} \neq 0$.

Az $a_{k-1} = 0$ esetet k szerinti indukcióval bizonyítjuk.

$k = 1$-re a polinom: $a_0 x$, a Dickson-mátrix pedig így néz ki:

$$\begin{pmatrix} a_0 & 0 & 0 & \dots & 0 \\ 0 & a_0^q & 0 & \dots & 0 \\ 0 & 0 & a_0^{q^2} & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & a_0^{q^{n-1}} \end{pmatrix}.$$

A mátrix és a polinom rangja n, ha $a_0 \neq 0$.

$k = 2$-re a polinom: $a_0x + a_1x^{q^s}$. Ha $a_1 = 0$, akkor ez azonos az előző polinommal, tehát a rangja szintén n, ami nagyobb, mint $n - k + 1 = n - 2 + 1 = n - 1$, tehát a $k = 2$ esetre igaz a 3.4.3-beli állítás.

Tegyük fel, hogy $k - 1$-re igaz, hogy a rang $\geq n - (k - 1) + 1$ (az $a_{k-2} \neq 0$ és az $a_{k-2} = 0$ esetben is). Azt az előzőekben láttuk, hogy $a_{k-1} \neq 0$ esetén a rang $\geq n-k+1$. Ha $a_{k-1} = 0$, akkor a polinom: $a_0x + a_1x^{q^s} + ... + a_{k-2}x^{q^{(k-2)s}}$. Indukciós feltevés miatt ennek rangja $\geq n - (k - 1) + 1 = n - k + 2 > n - k + 1$.

Tehát az állítás igaz erre az esetre is. □

3.4.4. Tétel. *$\mathcal{G}_{k,s,n}$ MRD-kód.*

Bizonyítás. 3.4.3 állításban láttuk, hogy minden $\mathcal{G}_{k,s,n}$-beli polinomhoz tartozó lineáris transzformáció rangja $\geq n-k+1$. Mivel két $\mathcal{G}_{k,s,n}$-beli polinom különbsége is $\mathcal{G}_{k,s,n}$-beli, ezért a különbség-rangok is legalább $n-k+1$. Legyen d ezek közül a minimális. Így $d \geq n-k+1$. (3.2)-ból tudjuk, hogy $|\mathcal{G}_{k,s,n}| \leq q^{n(n-d+1)}$. Mivel $d \geq n-k+1$, ezért $|\mathcal{G}_{k,s,n}| \leq q^{n(n-(n-k+1)+1)} = q^{nk}$.
$\mathcal{G}_{k,s,n}$ elemszáma $(q^n)^k = q^{nk}$. Tehát $\mathcal{G}_{k,s,n}$ maximális elemszámú, azaz MRD-kód. □

3.5. Kódok ekvivalenciája

A következő, lineáris MRD kódok elemein végzett műveletek *ekvivalens kódok*at eredményeznek:

1. transzponálás ($n \times n$-es mátrixokon),
2. invertálható mátrixokkal való (balról/jobbról) szorzás,
3. mátrix elemeinek azonos p^k. hatványra emelése (ahol p a test karakterisztikája).

Jelölés: $\mathcal{M}$ MRD kód
$\mathcal{M}^T = \{M^T : M \in \mathcal{M}\}$
$A\mathcal{M}B = \{AMB : M \in \mathcal{M}\}$, ahol A és B invertálhatóak
$\mathcal{M}^{p^k} = \{M^{p^k} : M \in \mathcal{M}\}$, ahol M^{p^k} az elemenkénti hatványozást jelöli

3.5.1. Állítás. *A fenti műveletek nem változtatnak a rang-távolságon.*

Bizonyítás. A műveletek egyike sem változtat a mátrix rangján. Továbbá:

1. $M_1, M_2 \in \mathcal{M}$, $M_1^T, M_2^T \in \mathcal{M}^T$: $\mathrm{rk}(M_1^T - M_2^T) = \mathrm{rk}((M_1 - M_2)^T) = \mathrm{rk}(M_1 - M_2)$,
2. $M_1, M_2 \in \mathcal{M}$, $AM_1B, AM_2B \in A\mathcal{M}B$: $\mathrm{rk}(AM_1B - AM_2B) = \mathrm{rk}(A(M_1 - M_2)B) = \mathrm{rk}(M_1 - M_2)$,
3. $M_1, M_2 \in \mathcal{M}$, $M_1^{p^k}, M_2^{p^k} \in \mathcal{M}^{p^k}$: $\mathrm{rk}(M_1^{p^k} - M_2^{p^k}) = \mathrm{rk}((M_1 - M_2)^{p^k}) = \mathrm{rk}(M_1 - M_2)$.

□

3.5.2. Definíció. $\mathcal{C}$ és $\mathcal{C}' \subseteq \mathbb{F}_q^{m\times n}$ lineáris kódok *ekvivalensek*, ha a fenti műveletek segítségével megkaphatóak egymásból: $\exists$ A, B invertálható mátrixok, hogy $A\mathcal{C}^\sigma B = \mathcal{C}'$, ahol σ testautomorfizmus, azaz $\sigma : x \mapsto x^{p^k}$.

3.5.3. Megjegyzés. A kód-ekvivalenciát általában a transzponálás nélkül definiálják.

3.5.4. Tétel. *Legyen $\mathbb{F}$ egy test. Ekkor az alábbiak ekvivalensek:*
a) $\mathcal{A}$: $\mathbb{F}^{m\times n} \to \mathbb{F}^{m\times n}$ bijekció, valamint $\mathcal{A}$ és $\mathcal{A}^{-1}$ is megőrzi a rang-távolságot
b) $m \neq n$ esetben: $\mathcal{A}(X) = PX^\sigma Q + R$,
$m = n$ esetben: $\mathcal{A}(X) = PX^\sigma Q + R$ vagy $\mathcal{A}(X) = P(X^T)^\sigma Q + R$,
$\forall X \in \mathbb{F}^{m\times n}$, ahol P és Q invertálhatóak, σ automorfizmus $\mathbb{F}$-en.

Forrás: [10, Theorem 3.4]

3.5.5. Következmény. A 3.5.4 tétel alapján ahhoz, hogy kódok közötti megfeleltetés bijektív legyen, és megőrizze a rangtávolságot, szükséges, hogy a leképezés $PX^\sigma Q + R$ alakú legyen.
Lineáris kódok esetén (amikor $\mathcal{C}$ és $\mathcal{C}'$ is altér), a $+R$ elhagyható, ugyanis ha $\mathcal{C}$ altér, akkor $P\mathcal{C}Q$ is az, továbbá $P\mathcal{C}Q + R = \mathcal{C}' \Leftrightarrow P\mathcal{C}Q = \mathcal{C}' - R$. Mivel $P\mathcal{C}Q$ altér, tehát tartalmazza a null mátrixot, ezért $\mathcal{C}' - R$ is, azaz $R \in \mathcal{C}' \Rightarrow P\mathcal{C}Q = \mathcal{C}' - R = \mathcal{C}'$.
Így pontosan a 3.5.1 állításbeli átalakítások azok, amelyek egymásutánjai lineáris kódok esetén biztosítják a bijektív leképezést és a rangtávolság megőrzését.

Forrás: [10, Chapter 3], [6, Section 3]

Kód-ekvivalencia polinomkompozícióval

Ha a kódokat polinomhalmazként definiáljuk, akkor az ekvivalens kódot eredményező műveletek közül az invertálható mátrixszal való szorzás a polinomkompozíciónak felel meg (az f q-polinomhoz tartozó mátrix jobbról szorzásának megfelel az $f \circ g$, míg balról szorzásának a $h \circ f$ kompozíció, g és h invertálhatóak).

Kódok ekvivalenciáját az idealizátoraik segítségével is eldönthetjük.

3.5.6. Definíció. Egy kód jobb oldali idealizátora a következő halmaz:

$$RI_{\mathcal{C}} = \{R \in GL(m, \mathbb{F}_q) : MR \in \mathcal{C}, \forall M \in \mathcal{C}\}.$$

Hasonlóan, a bal oldali idealizátor:

$$LI_{\mathcal{C}} = \{L \in GL(n, \mathbb{F}_q) : LM \in \mathcal{C}, \forall M \in \mathcal{C}\}.$$

3.5.7. Tétel. *Ekvivalens kódok jobb ill. bal oldali idealizátora ekvivalens.*

Bizonyítás. Tegyük fel, hogy $\mathcal{C}_1$ és $\mathcal{C}_2$ ekvivalens kódok. Legyen A és B két invertálható mátrix, σ automorfizmus, melyekre $A\mathcal{C}_1^\sigma B = \mathcal{C}_2$.

Ha $R \in RI_{\mathcal{C}}$, akkor $R^\sigma \in RI_{\mathcal{C}^\sigma}$ ($\mathcal{C}R \in \mathcal{C} \Rightarrow \mathcal{C}^\sigma R^\sigma \in \mathcal{C}^\sigma$). Hasonlóan ha $L \in LI_{\mathcal{C}}$, akkor $L^\sigma \in LI_{\mathcal{C}^\sigma}$ ($L\mathcal{C} \in \mathcal{C} \Rightarrow L^\sigma \mathcal{C}^\sigma \in \mathcal{C}^\sigma$).

Legyen L a $\mathcal{C}_1$ bal idealizátorának egy eleme. Ekkor $\mathcal{C}_2 = A\mathcal{C}_1^\sigma B = AL^\sigma \mathcal{C}_1^\sigma B = AL^\sigma A^{-1} A\mathcal{C}_1^\sigma B = AL^\sigma A^{-1}\mathcal{C}_2$, azaz $AL^\sigma A^{-1} \in LI_{\mathcal{C}_2}$.

Hasonlóan, ha $R \in RI_{\mathcal{C}_1}$, akkor $\mathcal{C}_2 = A\mathcal{C}_1^\sigma B = A\mathcal{C}_1^\sigma R^\sigma B = A\mathcal{C}_1^\sigma B B^{-1} R^\sigma B = \mathcal{C}_2 B^{-1} R^\sigma B$, így $B^{-1}R^\sigma B \in RI_{\mathcal{C}_2}$.

Ugyanez nyilvánvalóan igaz $\mathcal{C}_2$ idealizátoraira is, tehát ekvivalens kódok bal / jobb idealizátorai valóban ekvivalensek. □

3.6. További MRD kódok

Egy másik MRD kód, az úgynevezett „Twisted Gabidulin-kód" a Gabidulin-kódhoz hasonló, de azzal nem ekvivalens.

A következőkben $\mathrm{N}(x)$ az $\mathbb{F}_{q^n}$-ból $\mathbb{F}_q$-ba képző test normát jelöli, azaz $\mathrm{N}(x) = \mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x) = x^{(q^n-1)/(q-1)}$.

3.6.1. Definíció. Legyen $\mathcal{A}_k(\delta, r)$ q-polinomok halmaza legfeljebb $k < n$ q-fokkal, ahol $a_k = \delta a_0^{q^r}$ és $\mathrm{N}(\delta) \neq (-1)^{nk}$:

$$\mathcal{A}_k(\delta, r) := \{a_0 x + a_1 x^q + ... + a_{k-1} x^{q^{k-1}} + \delta a_0^{q^r} x^{q^k} : a_0, a_1, ..., a_{k-1} \in \mathbb{F}_{q^n}\}$$

Forrás: [8, Theorem 5.]

Annak bizonyításához, hogy ez szintén MRD kód, két lemmára lesz szükség.

3.6.2. Lemma. *Legyen f egy k q-fokú q-polinom: $\sum_{i=0}^{k} a_i x^{q^i}$. Ha f rangja $n-k$* $\implies$ $\mathrm{N}(a_0) = (-1)^{kn}\,\mathrm{N}(a_k)$.

Bizonyítás. Legyen U $\mathbb{F}_{q^n}$-nek egy k-dimenziós $\mathbb{F}_q$-altere. Ekkor egyértelműen létezik egy 1 főegyütthatós, k q-fokú q-polinom, amelynek U elemei gyökei. Ezt U *minimálpolinom*jának nevezzük.
Legyen U bázisa $\mathbb{F}_q$ felett $\{u_0, u_1, ..., u_{k-1}\}$. Legyen $f(x)$ a következő mátrix determinánsa:

$$\begin{pmatrix} x & x^q & \dots & x^{q^k} \\ u_0 & u_0^q & \dots & u_0^{q^k} \\ \vdots & \vdots & \ddots & \vdots \\ u_{k-1} & u_{k-1}^q & \dots & u_{k-1}^{q^k} \end{pmatrix}.$$

Ekkor $f(x) = a_0 x + a_1 x^q + ... + a_k x^{q^k}$ q-polinom, és U elemei a gyökei: $u \in U$, x helyére u-t helyettesítve a mátrix felső sora a többi sorának lineáris kombinációja, mert $u = \sum_{i=0}^{k-1} \lambda_i u_i$, $\lambda_i \in \mathbb{F}_q$ $\Rightarrow$ $u^{q^l} = \sum_{i=0}^{k-1} \lambda_i^{q^l} u_i^{q^l} = \sum_{i=0}^{k-1} \lambda_i u_i^{q^l}$, tehát a determináns 0, így $f(u) = 0$.

A determinánst az első sor szerint kifejtve, x együtthatója: $a_0 = det \begin{pmatrix} u_0^q & \dots & u_0^{q^k} \\ \vdots & \ddots & \vdots \\ u_{k-1}^q & \dots & u_{k-1}^{q^k} \end{pmatrix}$, x^{q^k} együtthatója: $a_k = (-1)^k det \begin{pmatrix} u_0 & \dots & u_0^{q^{k-1}} \\ \vdots & \ddots & \vdots \\ u_{k-1} & \dots & u_{k-1}^{q^{k-1}} \end{pmatrix}$, azaz $a_0 = (-1)^k a_k^q$. Ebből (1.1.16, 1.1.18 és 1.1.19 állítások miatt) következik: $\mathrm{N}(a_0) = \mathrm{N}((-1)^k a_k^q) = \mathrm{N}((-1)^k)\,\mathrm{N}(a_k^q) = (-1)^{kn}\,\mathrm{N}(a_k)$.
Ha létezne másik 1 főegyütthatós, q^k fokú $g(x)$ polinom, amelynek U elemei gyökei, akkor $(f(x)/a_k - g(x))$ polinom foka $< q^k$ és U elemei gyökei, de mivel U elemszáma q^k, ezért ez csak úgy lehetséges, ha ez az azonosan 0 polinom, azaz $g(x) = f(x)/a_k$.
Azonos q^k gyökkel és q^k fokkal rendelkező q-polinomok tehát egymás konstansszorosai, ezért az állítás igaz minden $n-k$ rangú, k q-fokú q-polinomra is: $\lambda f(x) = \lambda \sum_{i=0}^{k} a_i x^{q^i} = \sum_{i=0}^{k} \lambda a_i x^{q^i}$, $\lambda \in \mathbb{F}_{q^n} \Rightarrow \mathrm{N}(\lambda a_0) = \mathrm{N}(\lambda)\,\mathrm{N}(a_0) = \mathrm{N}(\lambda)(-1)^{kn}\,\mathrm{N}(a_k) = (-1)^{kn}\,\mathrm{N}(\lambda a_k)$. □

Forrás: [8, Lemma 3.]

3.6.3. Lemma. *Az* $\mathrm{N}: \mathbb{F}_{q^n} \to \mathbb{F}_q$ *leképezés szürjektív.*

Bizonyítás.

1. $\mathbb{F}_{q^n}$ multiplikatív csoportja ciklikus, azaz egy elemmel generálható: $\mathbb{F}_{q^n} \setminus \{0\} = < g > = \{1, g, g^2, ..., g^{q^n-2}\}$.

2. Az 1 normájú elemek (ciklikus) részcsoportot alkotnak:
   $\mathrm{N}(1) = 1$; ha $\mathrm{N}(a) = 1$ és $\mathrm{N}(b) = 1$, akkor $\mathrm{N}(ab) = \mathrm{N}(a)\,\mathrm{N}(b) = 1$; ha $\mathrm{N}(a) = 1$, akkor $\mathrm{N}(a^{-1}) = \mathrm{N}(a^{-1})\,\mathrm{N}(a) = \mathrm{N}(a^{-1}a) = \mathrm{N}(1) = 1$;
   Jelölje G az 1 normájú elemek részcsoportját: $G = \{g^i : \mathrm{N}(g^i) = 1\}$.
   $\mathrm{N}(g^i) = (g^i)^{(q^n-1)/(q-1)} = g^{i(q^n-1)/(q-1)} = 1$ ($g^i \in G$). Mivel g rendje $q^n - 1$, ezért $q^n - 1 | i(q^n-1)/(q-1)$. Ebből következik, hogy $i \in \{0, q-1, 2(q-1), ...\}$ és $i \le q^n - 2 \Rightarrow G = \{1, g^{q-1}, g^{2(q-1)}, ..., g^{((q^n-1)/(q-1)-1)(q-1)} = g^{q^n-q}\}$, egy $(q^n-1)/(q-1)$ elemű részcsoport.

3. A G szerinti mellékosztályok: $G, gG, g^2G, ..., g^{q^n-2}G$. Ha ezek közül kettő megegyezik, pl $g^kG = g^lG$, akkor $g^k/g^lG = G \Rightarrow g^{k-l} \in G \Rightarrow (q-1) | (k-l) \Rightarrow$ a különböző mellékosztályok: $G, gG, g^2G, ..., g^{q-2}G$ ($g^{q-1}G = G$-től ismétlődnek). Ez $q-1$ db különböző mellékosztály.

4. **3.6.4. Állítás.** *Különböző mellékosztályok elemeinek normája különböző.*

   Bizonyítás. A norma g^iG-n: $\mathrm{N}(g^i) = \mathrm{N}(g)^i$.
   Indirekten tegyük fel, hogy $\exists i, j : \mathrm{N}(g)^i = \mathrm{N}(g)^j$ $(0 \le j < i \le q-2)$. Ekkor $\mathrm{N}(g)^{i-j} = g^{(i-j)(q^n-1)/(q-1)} = 1$. $0 < (i-j)(q^n-1)/(q-1) \le (q-2)(q^n-1)/(q-1) < q^n - 1$. De

mivel g generátorelem és a rendje q^n-1, nem lehet ennél kisebb kitevőjű hatványa 1, tehát ellentmondásra jutottunk. □

Mivel a különböző mellékosztályok száma $q-1$, ebből következik, hogy a norma ezeken $q-1$ különböző értéket vesz fel. Továbbá $\mathrm{N}(a)=0 \Leftrightarrow a=0$. N $\mathbb{F}_q$-ba képez, ami q elemű, tehát annak minden értékét felveszi.

□

3.6.5. Tétel. *$\mathcal{A}_k(\delta,r)$ MRD kód.*

Bizonyítás. 3.6.3 lemma miatt ilyen δ biztosan létezik.
$\mathcal{A}_k(\delta,r)$ $\mathbb{F}_q$ felett nk dimenziós. Mivel az $\mathcal{A}_k(\delta,r)$-beli polinomok foka $\leq q^k$, ezért a rangjuk $\geq n-k$. A 3.6.2 lemma alapján, ha valamely polinom rangja egyenlő lenne $n-k$-val, akkor $\mathrm{N}(a_0)=(-1)^{kn}\mathrm{N}(a_k)$ teljesülne. Mivel $a_k=\delta a_0^{q^r}$, ezért $\mathrm{N}(a_k)=\mathrm{N}(\delta)\,\mathrm{N}(a_0^{q^r})=\mathrm{N}(\delta)\,\mathrm{N}(a_0)^{q^r}=\mathrm{N}(\delta)\,\mathrm{N}(a_0)$, mert $\mathrm{N}(a_0)\in\mathbb{F}_q$. De δ-t úgy választottuk, hogy $\mathrm{N}(\delta)\neq(-1)^{nk}$. Tehát $\mathcal{A}_k(\delta,r)$-beli polinomok rangja $\geq n-k+1$.
$\mathcal{A}_k(\delta,r)$ elemszáma $(q^n)^k=q^{nk}$, mivel a polinomok együtthatói $\mathbb{F}_{q^n}$-beliek.
Legyen d a polinom rangok közül a minimális. (3.2)-ből tudjuk, hogy $|\mathcal{A}_k(\delta,r)|\leq q^{n(n-d+1)}$. Mivel a $\mathcal{A}_k(\delta,r)$-beli (nem 0) polinomok rangja $\geq n-k+1$, ezért $|\mathcal{A}_k(\delta,r)|\leq q^{n(n-d+1)}\leq q^{n(n-(n-k+1)+1)}=q^{nk}$. Láttuk, hogy $|\mathcal{A}_k(\delta,r)|=q^{nk}$, így az előző egyenlőtlenségben egyenlőség áll, azaz $\mathcal{A}_k(\delta,r)$ (definíció szerint) MRD kód. □

Forrás: [8, Theorem 5.]

3.6.6. Állítás. *A fenti kód $1<k<n-1$ esetben nem ekvivalens a Gabidulin-kóddal.*

Bizonyítás. A 3.5.7 tétel szerint ehhez elég belátni, hogy az idealizátoraik nem ekvivalensek, ehhez pedig elég az, hogy valamely idealizátoruk elemszáma nem azonos.

$\mathcal{A}_k(0,r)=\{a_0x+a_1x^q+...+a_{k-1}x^{q^{k-1}} : a_0,...,a_{k-1}\in\mathbb{F}_{q^n}\}$, ami éppen $\mathcal{G}_{k,1,n}$, így tegyük fel, hogy $\delta\neq 0$.

1. *A Gabidulin-kód idealizátorainak elemszáma q^n.*

   A Gabidulin-kód ($\mathcal{G}_{k,s,n}=\{\sum_{i=0}^{k-1}a_ix^{q^{is}}, a_i\in\mathbb{F}_{q^n}\}$) jobb és bal idealizátora:
   $RI(\mathcal{G}_{k,s,n})\supseteq\{ax : a\in\mathbb{F}_{q^n}\}$, mivel $f(x)\in\mathcal{G}_{k,s,n}$ és $g(x)=ax$ esetén $(f\circ g)(x)=\sum_{i=0}^{k-1}a_i(ax)^{q^{is}}=\sum_{i=0}^{k-1}a_ia^{q^{is}}x^{q^{is}}\in\mathcal{G}_{k,s,n}$.
   $LI(\mathcal{G}_{k,s,n})\supseteq\{bx : b\in\mathbb{F}_{q^n}\}$, mivel $f(x)\in\mathcal{G}_{k,s,n}$ és $h(x)=bx$ esetén $(h\circ f)(x)=b\sum_{i=0}^{k-1}a_ix^{q^{is}}=\sum_{i=0}^{k-1}ba_ix^{q^{is}}\in\mathcal{G}_{k,s,n}$.
   Tehát a Gabidulin-kód jobb ill. bal oldali idealizátora legalább q^n elemű.

   $\mathcal{G}_{k,s,n}$ $\mathbb{F}_q$-lineáris altér, és így $RI(\mathcal{G}_{k,s,n})$ is az, hiszen ha $\mathcal{C}$ egy $\mathbb{F}_q$-lineáris kód, akkor: $A,B\in RI_{\mathcal{C}}$, $\lambda,\mu\in\mathbb{F}_q$, $\mathcal{C}(\lambda A+\mu B)=\mathcal{C}\lambda A+\mathcal{C}\mu B=\lambda\mathcal{C}A+\mu\mathcal{C}B=\lambda\mathcal{C}+\mu\mathcal{C}=\mathcal{C}\ \Rightarrow$ $\lambda A+\mu B\in RI_{\mathcal{C}}$, tehát $RI_{\mathcal{C}}$ $\mathbb{F}_q$-lineáris.

   Mivel $RI(\mathcal{G}_{k,s,n})$ nem nulla elemei invertálhatóak, ezért rangjuk n, és mivel altér, ezért bármelyik két $RI(\mathcal{G}_{k,s,n})$-beli különbsége is $RI(\mathcal{G}_{k,s,n})$-beli, azaz n-rangú. Tehát

$RI(\mathcal{G}_{k,s,n})$-ban a minimális rang távolság $= n$. A (3.1)-beli korlátot $RI(\mathcal{G}_{k,s,n})$-ra felírva: $|RI(\mathcal{G}_{k,s,n})| \leq q^{n(n-d+1)} = q^{n(n-n+1)} = q^n$.

Ugyanez igaz $LI(\mathcal{G}_{k,s,n})$-ra is. Következik, hogy a Gabidulin-kód idealizátorai pontosan q^n eleműek.

2. Vizsgáljuk meg az $\mathcal{A}_k(\delta, r)$ jobb idealizátorát.

Állítás. *$\mathcal{A}_k(\delta, r)$ jobb idealizátorának elemei $f(x) = bx$ alakúak, ahol $b \in \mathbb{F}_{q^{gcd(r-k,n)}}$.*

Bizonyítás. Legyen $f(x) = b_0x + b_1x^q + b_2x^{q^2} + ... + b_{n-1}x^{q^{n-1}} \in RI(\mathcal{A}_k(\delta, r))$.

$1 < k < n-2$ *eset:*

Vegyük az $\mathcal{A}_k(\delta, r)$-nek egy olyan elemét, ahol az a_1-et kivéve minden együttható 0, és vegyük az $f(x)$-el való kompozícióját:
$a_1(f(x))^q = a_1b_0^qx^q + a_1b_1^qx^{q^2} + ... + a_1b_{n-1}^qx$.
Mivel $f(x) \in RI(\mathcal{A}_k(\delta, r)) \Rightarrow a_1(f(x))^q \in \mathcal{A}_k(\delta, r)$, ezért az $x^{q^{k+1}}, ..., x^{q^{n-1}}$ együtthatói 0-k: $b_k = b_{k+1} = ... = b_{n-2} = 0$.
Tehát $f(x) = b_0x + b_1x^q + b_2x^{q^2} + ...b_{k-1}x^{q^{k-1}} + b_{n-1}x^{q^{n-1}}$.

Ezt a gondolatmenetet folytatva, valamely $a_ix^{q^i}$ monomba (a többi együtthatót 0-nak választva) helyettesítve $f(x)$-et azt kapjuk, hogy $f(x)$ $k-i+1, ..., n-i-1$ indexű együtthatóinak 0-knak kell lenniük. Ha az összes $0 < i < k$-ra elvégezzük a behelyettesítést, azt kapjuk, hogy
$i = 1: \ k, k+1, ..., n-2$,
$\vdots$
$i = k-1: \ 2, 3, ..., n-k$,
összesítve: a $2, ..., n-2$ indexű együtthatók mind 0-k $f(x)$-ben.
Következik, hogy $f(x) = b_0x + b_1x^q + b_{n-1}x^{q^{n-1}}$.

Most helyettesítsük f-et az $a_0x + \delta a_0^{q^r}x^{q^k}$ polinomba:
$a_0f(x) + \delta a_0^{q^r}(f(x))^{q^k} = a_0b_0x + a_0b_1x^q + a_0b_{n-1}x^{q^{n-1}} + \delta a_0^{q^r}b_0^{q^k}x^{q^k} + \delta a_0^{q^r}b_1^{q^k}x^{q^{k+1}} + \delta a_0^{q^r}b_{n-1}^{q^k}x^{q^{k-1}}$.
Az $x^{q^{k+1}}$ és $x^{q^{n-1}}$ tagok nem szerepelnek az $\mathcal{A}_k(\delta, r)$-beli polinomokban, ezért b_1 és b_{n-1} szükségképpen 0-k. Tehát $f(x) = b_0x$.
x és x^{q^k} együtthatói között pedig a következő összefüggés áll fenn:
$\delta a_0^{q^r}b_0^{q^k} = \delta(a_0b_0)^{q^r} \Leftrightarrow b_0^{q^k} = b_0^{q^r} \Leftrightarrow b_0 = b_0^{q^{r-k}}$, amiből az következik, hogy $b_0 \in \mathbb{F}_{q^{r-k}} \cap \mathbb{F}_{q^n}$, amiből 1.1.12 lemma miatt $b \in \mathbb{F}_{q^{gcd(r-k,n)}}$.

$2 < k = n-2$ *eset:*

Az előző gondolatmenethez hasonlóan, ebben az esetben is $f(x) = b_0x + b_1x^q + b_{n-1}x^{q^{n-1}}$.
Ezt helyettesítsük az a_1x^q monomba (ahol $a_1 \neq 0$): $a_1(f(x))^q = a_1b_0^qx^q + a_1b_1^qx^{q^2} + a_1b_{n-1}^qx \in \mathcal{A}_k(\delta, r)$. Mivel $k > 2$, ebből hiányzik az x^{q^k} tag, így szükségképpen (a $\delta \neq 0$ feltevés miatt) x együtthatója is nulla, így (mivel $a_1 \neq 0$) $b_{n-1} = 0$.
Így $f(x) = b_0x + b_1x^q$.
$f(x)$-et $a_0x + \delta a_0^{q^r}x^{q^k}$-ba ($a_0 \neq 0$) helyettesítve kapjuk:
$a_0f(x) + \delta a_0^{q^r}(f(x))^{q^k} = a_0b_0x + a_0b_1x^q + \delta a_0^{q^r}b_0^{q^k}x^{q^k} + \delta a_0^{q^r}b_1^{q^k}x^{q^{k+1}}$.

Az $x^{q^{k+1}} = x^{q^{n-1}}$ tag kiesik ($\mathcal{A}_k(\delta, r)$-beli polinomok max k q-fokúak), így $b_1 = 0$.
Következik, hogy $f(x) = b_0 x$.
Az x és x^{q^k} együtthatóinak összefüggéséből azt kapjuk, hogy $b \in \mathbb{F}_{q^{gcd(r-k,n)}} = \mathbb{F}_{q^{gcd(r+2,n)}}$.

$k = 2, n = 4$ *eset:*

Ekkor $\mathcal{A}_2(\delta, r) = \{a_0 x + a_1 x^q + \delta a_0^{q^r} x^{q^2}\}$.

f pedig ilyen alakú: $f(x) = b_0 x + b_1 x^q + b_3 x^{q^3}$.

$a_1 x^q$-ba ($a_1 \neq 0$) való helyettesítés után: $a_1(f(x))^q = a_1 b_0^q x^q + a_1 b_1^q x^{q^2} + a_1 b_3^q x \in \mathcal{A}_2(\delta, r)$.
x és x^{q^2} együtthatójára a következőnek kell teljesülnie: $\delta a_1^{q^r} b_3^{q^{r+1}} = a_1 b_1^q$.
Azaz: $p(a_1) = \delta b_3^{q^{r+1}} a_1^{q^r} - b_1^q a_1 = 0$. Ez a_1-nek egy q^r fokú polinomja, melynek legfeljebb q^r gyöke lehet. Ez az egyenlet azonban minden $\mathbb{F}_{q^4}$-beli elemre igaz, azaz biztosan van q^4 gyök. Ez csak úgy lehetséges, ha $p(a_1)$ a 0 polinom, vagy ha $r \equiv 0 \pmod 4$.
Ha $p(a_1)$ a 0 polinom, akkor $b_1 = b_3 = 0$. Ez esetben $f(x) = b_0 x$.
$r \equiv 0 \pmod 4$ esetén $a_1^{q^r - 1} = 1$, és így $b_1^q = \delta b_3^q \Leftrightarrow b_1 = \delta^{q^3} b_3$.
Behelyettesíthetjük f-be: $f(x) = b_0 x + \delta^{q^3} b_3 x^q + b_3 x^{q^3}$.
Most f-et helyettesítsük az $a_0 x + \delta a_0^{q^r} x^{q^2} = a_0 x + \delta a_0 x^{q^2}$ polinomba ($a_1 = 0$, $a_0 \neq 0$):
$a_0 f(x) + \delta a_0 (f(x))^{q^2} = a_0 b_0 x + a_0 \delta^{q^3} b_3 x^q + a_0 b_3 x^{q^3} + \delta a_0 b_0^{q^2} x^{q^2} + \delta a_0 \delta^q b_3^{q^2} x^{q^3} + \delta a_0 b_3^{q^2} x^q$.
Mivel ez $\mathcal{A}_2(\delta, r)$-beli, ezért x^{q^3} együtthatója 0: $a_0 b_3 + \delta^{q+1} a_0 b_3^{q^2} = 0 \Leftrightarrow b_3 + \delta^{q+1} b_3^{q^2} = 0$.
Egy újabb q-polinomot kaptunk, ezúttal b_3-ra. Azt szeretnénk belátni, hogy $b_3 = 0$ az egyetlen megoldás.
A 2.2.3 állítás szerint egy q-polinom rangja megegyezik a hozzá tartozó Dickson-mátrix rangjával. A $b_3 + \delta^{q+1} b_3^{q^2}$ polinom Dickson-mátrixa:

$$\begin{pmatrix} 1 & 0 & \delta^{q+1} & 0 \\ 0 & 1 & 0 & \delta^{q(q+1)} \\ \delta^{q^2(q+1)} & 0 & 1 & 0 \\ 0 & \delta^{q^3(q+1)} & 0 & 1 \end{pmatrix}.$$

Felsőháromszög mátrixá alakítás után:

$$\begin{pmatrix} 1 & 0 & \delta^{q+1} & 0 \\ 0 & 1 & 0 & \delta^{q(q+1)} \\ 0 & 0 & 1 - \delta^{q+1+q^2(q+1)} & 0 \\ 0 & 0 & 0 & 1 - \delta^{q(q+1)+q^3(q+1)} \end{pmatrix}.$$

Itt $\delta^{q+1+q^2(q+1)} = \delta^{1+q+q^2+q^3} = \delta^{(q^4-1)/(q-1)} = \mathrm{N}(\delta)$, valamint $\delta^{q(q+1)+q^3(q+1)} = \delta^{1+q+q^2+q^3} = \mathrm{N}(\delta)$. Tehát a mátrix determinánsa: $(1-\mathrm{N}(\delta))^2$. Tudjuk, hogy $\mathrm{N}(\delta) \neq 1$, így a determináns nem nulla. Azaz a mátrix és a polinom teljes rangú, vagyis $b_3 = 0$ az egyetlen megoldás. Így $b_1 = \delta^{q^3} b_3$ is 0. Tehát $f(x) = b_0 x$ az $r = 0$ esetben is.
$f(x) = b_0 x$-et $a_0 x + \delta a_0^{q^r} x^{q^2}$ ($a_0 \neq 0$) polinomba helyettesítve:
$a_0 f(x) + \delta a_0^{q^r} (f(x))^{q^2} = a_0 b_0 x + \delta a_0^{q^r} b_0^{q^2} x^{q^2} \in \mathcal{A}_2(\delta, r)$.
x és x^{q^2} együtthatóiból: $\delta a_0^{q^r} b_0^{q^r} = \delta a_0^{q^r} b_0^{q^2} \Leftrightarrow b_0^{q^r} = b_0^{q^2} \Leftrightarrow b_0 = b_0^{q^{r-2}} \Rightarrow b_0 \in \mathbb{F}_{q^{r-2}} \cap \mathbb{F}_{q^4} = \mathbb{F}_{q^{gcd(r-2,4)}}$.

□

A fentiekből következik, hogy $RI(\mathcal{A}_k(\delta,r))$ elemszáma $< q^n$, ha $r \not\equiv k \pmod n$, azaz ebben az esetben $\mathcal{A}_k(\delta,r)$ nem ekvivalens a Gabidulin-kóddal.

3. Most vizsgáljuk meg $\mathcal{A}_k(\delta,r)$ bal idealizátorát.

Állítás. *$\mathcal{A}_k(\delta,r)$ bal idealizátorának elemei $f(x)=bx$ alakúak, ahol $b \in \mathbb{F}_{q^{gcd(r,n)}}$.*

Bizonyítás. Legyen $f(x)=b_0x+b_1x^q+b_2x^{q^2}+...+b_{n-1}x^{q^{n-1}} \in LI(\mathcal{A}_k(\delta,r))$.

$f(x)$-be valamely $a_ix^{q^i} \in \mathcal{A}_k(\delta,r)$ $(a_i \neq 0)$ monomot helyettesítve kapjuk:
$f(a_ix^{q^i})=b_0(a_ix^{q^i})+b_1(a_ix^{q^i})^q+...+b_{n-1}(a_ix^{q^i})^{q^{n-1}}=b_0a_ix^{q^i}+b_1a_i^qx^{q^{i+1}}+...+b_{n-1}a_i^{q^{n-1}}x^{q^{i-1}} \in \mathcal{A}_k(\delta,r)$.
Itt $x^{q^{k+1}},...,x^{q^{n-1}}$ együtthatója $0 \Rightarrow b_{k+1-i}=b_{k+2-i}=...=b_{n-1-i}=0$. Ezt $i=1,...,k-1$-re összesítve kapjuk, hogy $b_2=b_3=...=b_{n-2}=0$, tehát $f(x)=b_0x+b_1x^q+b_{n-1}x^{q^{n-1}}$.

$1<k<n-2$ *eset:*

Helyettesítsük $f(x)$-be $a_0x+\delta a_0^{q^r}x^{q^k}$-t $(a_0 \neq 0)$:
$f(a_0x+\delta a_0^{q^r}x^{q^k})=b_0a_0x+\delta b_0a_0^{q^r}x^{q^k}+b_1a_0^qx^q+\delta^qb_1a_0^{q^{r+1}}x^{q^{k+1}}+b_{n-1}a_0^{q^{n-1}}x^{q^{n-1}}+\delta^{q^{n-1}}b_{n-1}a_0^{q^{r-1}}x^{q^{k-1}} \in \mathcal{A}_k(\delta,r)$.
Itt $x^{q^{k+1}}$ és $x^{q^{n-1}}$ együtthatója 0, amiből következik, hogy $b_1=0$ és $b_{n-1}=0$. Így $f(x)=b_0x$.
Az x és x^{q^k} együtthatóinak összefüggéséből pedig: $\delta b_0^{q^r}a_0^{q^r}=\delta b_0a_0^{q^r} \Leftrightarrow b_0^{q^r}=b_0$, ebből következik, hogy $b_0 \in \mathbb{F}_{q^r} \cap \mathbb{F}_{q^n}=\mathbb{F}_{q^{gcd(r,n)}}$.

$2<k=n-2$ *eset:*

f-be a_1x^q-t helyettesítve: $f(a_1x^q)=b_0a_1x^q+b_1a_1^qx^{q^2}+b_{n-1}a_1^{q^{n-1}}x$.
Mivel itt $x^{q^k}=x^{q^{n-2}}$ együtthatója 0, ezért szükségképp x együtthatója is $0 \Rightarrow b_{n-1}=0$. Azaz $f(x)=b_0x+b_1x^q$.
$f(a_0x+\delta a_0^{q^r}x^{q^k})=b_0a_0x+\delta b_0a_0^{q^r}x^{q^k}+b_1a_0^qx^q+\delta^qb_1a_0^{q^{r+1}}x^{q^{k+1}} \in \mathcal{A}_k(\delta,r)$.
Itt $x^{q^{k+1}}$ együtthatójának 0-nak kell lennie, ezért $b_1=0$, és így az x^q tag is kiesik. Marad: $b_0a_0x+\delta b_0a_0^{q^r}x^{q^k} \in \mathcal{A}_k(\delta,r)$.
x és x^{q^k} együtthatói közötti összefüggésből ugyanazt kapjuk, mint előbb: $b_0^{q^r}=b_0 \Rightarrow b_0 \in \mathbb{F}_{q^{gcd(r,n)}}$.

$k=2, n=4$ *eset:*

$f(x)=b_0x+b_1x^q+b_3x^{q^3} \in LI(\mathcal{A}_2(\delta,r))$.
$f(a_1x^q)=b_0a_1x^q+b_1a_1^qx^{q^2}+b_3a_1^{q^3}x \in \mathcal{A}_2(\delta,r)$.
x és x^{q^2} együtthatóiból: $\delta b_3^{q^r}a_1^{q^{r+3}}=b_1a_1^q \Leftrightarrow \delta b_3^{q^r}a_1^{q^{r+3}}-b_1a_1^q=0$.
Ez a_1-nek egy q-polinomja, amelynek így tehát q^4 gyöke van (minden $a_1 \in \mathbb{F}_{q^4}$ gyöke). Ez úgy lehetséges, ha ez a 0 polinom, ekkor $b_1=b_3=0$. Vagy pedig $r=2$, ebben az esetben: $a_1^q(\delta b_3^{q^2}-b_1)=0$ $(\forall a_1 \in \mathbb{F}_{q^4}) \Rightarrow b_1=\delta b_3^{q^2}$.
Tehát $f(x)=b_0x+\delta b_3^{q^2}x^q+b_3x^{q^3}$.
Helyettesítsük f-be az $a_0x+\delta a_0^{q^2}x^{q^2}$ polinomot:
$f(a_0x+\delta a_0^{q^2}x^{q^2})=b_0a_0x+\delta b_3^{q^2}a_0^qx^q+b_3a_0^{q^3}x^{q^3}+b_0\delta a_0^{q^2}x^{q^2}+\delta b_3^{q^2}\delta^qa_0^{q^3}x^{q^3}+b_3\delta^{q^3}a_0^qx^q$.
Itt x^{q^3} együtthatója 0: $b_3a_0^{q^3}+\delta^{q+1}b_3^{q^2}a_0^{q^3}=0 \Leftrightarrow b_3+\delta^{q+1}b_3^{q^2}=0$.
Erre pedig már láttuk (a jobb idealizátornál), hogy a $b_3=0$ az egyetlen megoldás,

így pedig b_1 is 0.
Tehát $f(x) = b_0 x$ minden r-re.
$f(a_0 x + \delta a_0^{q^r} x^{q^2}) = b_0 a_0 x + b_0 \delta a_0^{q^r} x^{q^2} \in \mathcal{A}_2(\delta, r) \Rightarrow \delta b_0^{q^r} a_0^{q^r} = b_0 \delta a_0^{q^r} \Leftrightarrow b_0 = b_0^{q^r} \Rightarrow$
$b_0 \in \mathbb{F}_{q^r} \cap \mathbb{F}_{q^n} = \mathbb{F}_{q^{gcd(r,n)}}$.

□

Tehát $LI(\mathcal{A}_k(\delta, r))$ elemszáma $< q^n$, ha $r \not\equiv 0 \pmod{n}$, azaz ebben az esetben $\mathcal{A}_k(\delta, r)$ nem ekvivalens a Gabidulin-kóddal.

A 2. és 3. pontokból következik, hogy $\mathcal{A}_k(\delta, r)$ nem ekvivalens a Gabidulin-kóddal, ha $r \not\equiv k$ vagy $r \not\equiv 0 \pmod{n}$. Mivel $1 < k < n - 1$, az egyik feltétel biztosan igaz, így tehát a két kód (r-től függetlenül) nem ekvivalens.

□

4. fejezet

Hálózatok és kódolás

4.1. MRD kódok alkalmazása a hálózati kommunikációban

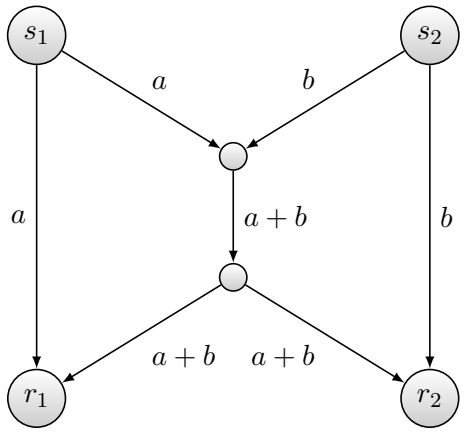
A kommunikációs hálózat egy irányított gráffal ábrázolható. A forráspontok (csak kimenő élekkel) jelölik az információ forrását, a küldőt, a nyelők (csak bemenő élekkel) pedig a fogadót. Az irányított élek a kommunikációs csatornák, a közbülső pontok pedig különböző eszközök, melyeken keresztül áramlik az adat.

A kódolási folyamat során a küldő az üzenetet több csomagra bontva továbbítja különböző pontokba, majd ezek az információs csomagok pontról pontra továbbítódnak a célig. A fogadó pontok a csomagokat összegyűjtik, és visszafejtik az eredeti üzenetet.

Lineáris hálózati kódolás

A hálózati kommunikáció során létrejött információs csomagok kódolásának egyik módja, hogy a közbülső pontok a kapott csomagok különböző lineáris kombinációját küldik tovább. Ezt *lineáris hálózati kódolás*nak nevezik.

A lineáris hálózati kódolásra egy példa az ún. „pillangó hálózat" (*butterfly network*).



Ebben az üzenet két csomagra bontva (a, b) kerül elküldésre. A cél: mindkét csomagot eljuttatni mindkét fogadóhoz (r_1, r_2). Az üzenetküldés 3 csatornán történik: a, b, $a + b$

csomagok kerülnek továbbításra. A két fogadóhoz a és $a+b$ ill. b és $a+b$ csomagok érkeznek, melyekből az eredeti a és b üzenet mindkét fogadó számára visszafejthető.

Random lineáris hálózati kódolás

Random lineáris hálózati kódolás esetén a források véletlenszerűen választják ki a belső pontok paramétereit, ami alapján a lineáris kombináció történik, és ezt az információs csomagokkal együtt továbbítják. Majd ezen paraméterek segítségével kerülnek dekódolásra a kódszavak. A kódolásra rank metric kód alkalmazható, a továbbított kódszavak vektorok, az eredetileg küldött vektorok visszafejthetők. Ez csak *koherens* esetben működik, azaz ha a hálózati struktúra ismert.

Nem koherens esetben azonban se a küldő, se a fogadó által nem ismert a struktúra. A belső pontokon a lineáris kombináció véletlenszerűen történik, nem előre meghatározott paraméterek alapján, így az előző módszer nem alkalmazható. A kapott üzenet itt is az eredetinek lineáris kombinációja, azonban az eredeti vektor nem viszafejthető a lineáris kombinációk ismeretének hiányában. Ezért az információ nem vektorok, hanem vektorterek formájában kerül kódolásra, és ezen vektorterek egy-egy generátorhalmaza lesz a továbbítandó üzenet.

Az információ-átadás a küldő és fogadó között több körben történik. Minden egyes körben fix hosszúságú csomagok kerülnek a hálózatba a küldő által: n hosszú sorvektorok $\mathbb{F}_q$ felett. Egy belső csúcs a rajta áthaladó vektoroknak veszi egy véletlenszerű $\mathbb{F}_q$-lineáris kombinációját, és azt küldi tovább. A fogadó csúcs összegyűjti a hozzá érkező véletlenszerű csomagokat, és abból megpróbálja visszafejteni az eredeti üzenetet.

Anomáliák

Előfordulhat, hogy különböző események, zaj hatására egy-egy csomag hibásan, vagy egyáltalán nem továbbítódik (törlődik), ezzel hibás adatot vagy adatvesztést okozva. A sikeresen továbbított adatcsomagok halmaza egy irányított multigráfot határoz meg, ahol a csúcsok megegyeznek a hálózat csúcshalmazával, az élek pedig a sikeres csomagtovábbításokat jelölik. Az információ-továbbítási arány a gráf küldő és fogadó közötti minimális vágásával jellemezhető.

A következőkben mind a hibamentes, mind a hibás adatot tartalmazó esetet megvizsgáljuk.

Matematikai reprezentáció

Legyen egyetlen küldő és egy fogadó. Jelölje az információs csomagokat $x_1, x_2, ..., x_m \in \mathbb{F}_q^n$, $X \in \mathbb{F}_q^{m \times n}$ a belőlük képzett mátrix. A belső pontok által továbbított lineáris kombinációk legyenek $y_1, y_2, ..., y_l$. Feltehető, hogy lineárisan függetlenek (a nem független elemeket elhagyjuk). Így a belőlük képzett mátrix, $Y \in \mathbb{F}_q^{l \times n}$ rangja l. Azaz Y a hibamentes esetben a következőképp áll elő:

$$Y = HX,$$

ahol X a küldött üzenet, Y a fogadott üzenet, $H \in \mathbb{F}_q^{l \times m}$ a lineáris kombinációk együtthatóiból álló mátrix, amelynek j. sorának elemei az y_j-t eredményül adó lineáris kombináció együtthatói, azaz $y_j = \sum_{i=1}^{m} h_{ji} x_i$, $h_{ji} \in \mathbb{F}_q$.

Ha valahol bekerül egy hibás üzenet a hálózatba, az továbbítódik a következő pontokon keresztül a lineáris kombinációkban. Jelölje a hibás vektorokat $e_1, ..., e_t$, a belőlük képzett mátrix E. A fogadott vektorok mátrixát ebben az esetben a következő képlet írja le:

$$Y = HX + GE,$$

$y_j = \sum_{i=1}^{m} h_{ji} x_i + \sum_{k=1}^{t} g_{jk} e_k$, $h_{ji}, g_{jk} \in \mathbb{F}_q$, $X \in \mathbb{F}_q^{m \times n}$ sorai az üzenet-vektorok, $Y \in \mathbb{F}_q^{l \times n}$ sorai a kapott vektorok, $H \in \mathbb{F}_q^{l \times m}$, $G \in \mathbb{F}_q^{l \times t}$.

A lineáris hálózati kódolás problémája tehát: X-et visszakapni Y-ból.

Koherens hálózati kódolás esetén az Y és H mátrixok is ismertek (GE nem az), ekkor a kódolásra Gabidulin-kód alkalmazható, annak sorait továbbítva. (Gabidulin-kód dekódolására [4]-ban szerepel egy algoritmus.)

Nem-koherens esetben viszont H (és G) is ismeretlen, véletlenszerű mátrix, tehát csak Y adott. X egyetlen, Y-ban is megőrzött tulajdonsága (legalábbis hibamentes esetben) a sortere (vagy annak egy altere). Ekkor a kódolás (konstans dimenziójú) altér kóddal történhet. Így nem az eredetileg küldött vektorokat, hanem az általuk generált vektorteret kell visszakapnunk.

Megjegyzés: HX sorai egy alteret generálnak X sorterében, amelynek dimenziója megegyezik HX rangjával. Csomag törlések miatt előfordulhat, hogy HX rangja, és így az általa generált altér dimenziója kisebb, mint X sorteréé.

A 3.3 fejezetben láttuk, hogy egy MRD kód meghatároz egy konstans dimenziójú altér kódot. Egy tetszőleges rank distance kóddal is definiálhatunk konstans dimenziójú kódot, azonban ha a kód MRD, úgy a legbővebb az altér kód.

Konstans dimenziójú kód előállítása

A következő egy a [12]-ben is alkalmazott módszer konstans dimenziójú altér kód előállítására.

Legyen $\mathcal{C} \subseteq \mathbb{F}_q^{m \times n}$ egy RD kód d minimális távolsággal. Ekkor a $\mathcal{C}$-vel definiált *lifted code* a következő:

$$\mathcal{LC} = \{S_C = \mathrm{rs}\,[I|C^T] \subseteq \mathbb{F}_q^{n+m} : C \in \mathcal{C}\},$$

azaz $\mathcal{LC}$ elemei az $[I|C^T]$ mátrixok sorterei, ahol I az $n \times n$-es egységmátrix. Ekkor

1. $\mathcal{LC}$ konstans dimenziójú, mivel minden eleme n dimenziós altér;
2. ha $\mathcal{C}$ minimum távolsága d, akkor $\mathcal{LC}$ minimum távolsága $2d$: $d_S(S_{C_1}, S_{C_2}) = 2d(C_1, C_2)$;
3. ha $\mathcal{C}$ MRD kód, akkor $\mathcal{LC}$ optimális.

Forrás: [4], [12, Section 5.7.2], [5, Chapter 2]

A fenti definíció tulajdonképpen megegyezik a 3.3-beli definícióval, ugyanis: $[I|C^T]$ sortere $= \{v = \sum_{i=1}^{n} u_i(e_i, c_i) : u_i \in \mathbb{F}_q\}$, ahol (e_i, c_i) az $[I|C^T]$ mátrix i. sorát jelöli ($e_i \in \mathbb{F}_q^n$, $c_i \in \mathbb{F}_q^m$). Továbbá: $v = \sum_{i=1}^{n} u_i(e_i, c_i) = (\sum_{i=1}^{n} u_i e_i, \sum_{i=1}^{n} u_i c_i) = (u^T, u^T C^T) = (u, Cu)^T$, ahol tehát $u \in \mathbb{F}_q^n$. Azaz: rs $[I|C^T]$ transzponálás után $\{(u, Cu) : u \in \mathbb{F}_q^n, C \in \mathcal{C}\}$, ami éppen a 3.3-beli definíció.

4.2. Kódolás altér kóddal

Nem-koherens random lineáris hálózati kódolás esetén az eredeti üzenet a hálózatban előforduló hibás vetorok ill. vektortörlések számának függvényében fejthető vissza.

Hálózati modell

Válasszunk egy n dimenziós vektorteret $\mathbb{F}_q$ felett: W. A küldött csomagok legyenek W vektorai. Az információt W ezen vektorok által generált alterei jelentik. Jelölje $\mathcal{P}(W)$ a W összes alterének halmazát.

Definiáljuk a $\mathcal{H}_k$ operátort a következőképpen:

$$\mathcal{H}_k(V) = \begin{cases} V, \text{ ha } \dim V \leq k \\ V \text{ egy tetszőleges } k\text{-dimenziós altere, ha } \dim V > k \end{cases}.$$

Legyen $U, V \in \mathcal{P}(W)$, V a bemeneti, U a kimeneti vektortér, $\dim(U \cap V) = k$, $\mathcal{H}_k(V) = U \cap V$, $U = \mathcal{H}_k(V) \oplus E$, ahol $E \in \mathcal{P}(W)$ a hibás vektorok tere.

Jelölje $\rho = \dim V - k$ a törölt vektorok számát, $t = \dim E$ pedig a hibás vektorokét.

Kódolás

Vegyük W altereinek egy (nem üres) halmazát, ez lesz a kód: $\mathcal{C} \subseteq \mathcal{P}(W)$. Altér kódok (3.3) fejezetben definiált távolsága a következő: $d(U, V) = \dim U + \dim V - 2\dim(U \cap V)$, konstans dimenziójú kód esetén (minden altér dimenziója k): $d(U, V) = 2k - 2\dim(U \cap V)$. Legyen $d(\mathcal{C})$ a minimális távolság.

Egy minimális távolság dekóder valamely $\mathcal{C}$ kódhoz egy adott U outputhoz legközelebbi V kódszót adja vissza: $d(U, V) \leq d(U, V'), \forall V' \in \mathcal{C}$.

A háromszög-egyenlőtlenségből látható, hogy az alábbi tétel elégséges feltételt ad arra, hogy egy ilyen dekóderrel visszakapjuk U-ból V-t.

4.2.1. Tétel. *Legyen $\mathcal{C}$ kód, $V \in \mathcal{C}$ a küldött üzenet, $U = \mathcal{H}_k(V) \oplus E$ a kapott üzenet, $\dim E = t$. Jelölje $\rho = \max(0, \max_{C \in \mathcal{C}}(\dim C - k))$ a törlések maximális számát. Ha $2(t + \rho) < d(\mathcal{C})$, akkor $\mathcal{C}$ egy minimális távolság dekódere visszaadja V-t U-ból.*

Ha feltesszük, hogy a törlések száma 0 (minden adatcsomag minden pontban továbbításra került), akkor a következőt kapjuk:

4.2.2. Következmény. Ha $U = \mathcal{H}_{\dim W}(V) \oplus E = V \oplus E$ a kapott tér, $\dim E = t$ és $2t < d(\mathcal{C})$, akkor $\mathcal{C}$ egy minimális távolság dekódere visszaadja V-t U-ból.

Forrás: [4], [5, Chapter 2]

Irodalomjegyzék

[1] Ernst M. Gabidulin. Rank-metric codes and applications. `http://iitp.ru/upload/content/839/Gabidulin.pdf`.

[2] F. R. Gantmacher. *The Theory of Matrices.* Chelsea Publishing Company, 2000.

[3] David Goss. *Basic Structures of Function Field Arithmetic.* Springer-Verlag Berlin Heidelberg, 1996.

[4] Ralf Kötter and Frank R. Kschischang. Coding for errors and erasures in random network coding. *IEEE Transactions on Information Theory*, 54(8):3579–3591, 2008.

[5] Lien Lambert. Random network coding and designs over $\mathbb{F}_q$. Master's thesis, Ghent University, Faculty of Sciences, Department of Mathematics, 2013.

[6] Dirk Liebhold and Gabriele Nebe. Automorphism groups of gabidulin-like codes. *Arch. Math.*, 107:355–366, 2016.

[7] S. E. Payne. *Topics in Finite Geometry: Ovals, Ovoids and Generalized Quadrangles.* University of Colorado Denver, 2007.

[8] John Sheekey. A new family of linear maximum rank distance codes. *Advances in Mathematics of Communications*, 10(3):475–488, 2016.

[9] John Sheekey. Mrd codes: Constructions and connections. `https://arxiv.org/pdf/1904.05813.pdf`, 2019.

[10] Zhe-Xian Wan. *Geometry of Matrices.* World Scientific Publishing Co Pte Ltd, 1996.

[11] Baofeng Wu and Zhuojun Liu. Linearized polynomials over finite fields revisited. *Finite Fields and Their Applications*, 22:79–100, 2013.

[12] Ferdinando Zullo. *Linear Codes and Galois Geometries: Between Two Worlds.* PhD thesis, Universita degli studi della Campania „Luigi Vanvitelli", Dipartimento di Matematica e Fisica, 2018.