Szegedi Tudományegyetem

Bolyai Intézet

Geometria Tanszék

Reed-Solomon-féle hibajavító kódok

BSc szakdolgozat

Készítette:
Táborosi Andor Zsolt
matematika szakos
hallgató

Témavezető:
Dr. Nagy Gábor Péter
egyetemi docens

Szeged
2013

Tartalomjegyzék

Bevezetés

A kódelmélet a következő kommunikációs modellel foglalkozik: egy feladó valamilyen csatornán keresztül adatokat akar továbbítani egy címzettnek, a továbbítás során pedig az adatok egy része megváltozik. A kérdés az, hogy hogyan tudja a címzett kiválasztani, hogy mely adatok változtak meg, és hogyan tudja a megváltoztatott adatokat kijavítani. Ebben az üzenetek különböző kódolásai segíthetnek.

A Reed-Solomon-kódokat (a következőkben RS-kódok) Irving S. Reed és Gustave Solomon találták fel 1960-ban, akik akkor éppen az MIT Lincoln Laboratóriumnak dolgoztak. A szemináriumi cikküknek a "Polinomkódok bizonyos véges testek felett" ("Polynomial Codes over Certain Finite Fields") címet adták, de ebben a cikkben még nem találtak hatékony dekódoló algoritmust.

A későbbiekben kiderül, hogy az RS-kód az egyik legjobb hibajavító kód, mert a kód elemei a lehető "legtávolabb" vannak egymástól, ami a dekódolás lehetőségeit növeli. Az ilyen kódokat MDS (maximal distance separable) kódoknak nevezzük. Dolgozatomban Peterson 1960-ban kifejlesztett tünet-alapú dekódolását mutatom be. Ezt Elwyn Berlekamp és James Massey továbbfejlesztette 1969-ben, és ezért ezt a változatot Berlekamp - Massey-féle dekódoló algoritmusnak nevezik, de dolgozatomban erre a módszerre nem térek ki részletesen. A RS-kódokat 1977-ben a Voyager-programban, illetve manapság több területen is hasznosítják, többek között a digitális háttértárolók, a digitális kommunikációs szerkezetek vagy a digitális videók területén.

1. Alapfogalmak

1.1. Algebrai alapfogalmak

1.1. Definíció. *Egy (G,∘) algebrai struktúrát csoportnak nevezünk, ha a következők teljesülnek:*

a) $G(\neq \emptyset)$ *zárt* $a \circ: G^2 \to G$ *műveletre, azaz* $\forall a, b \in G$*-re* $a \circ b \in G$*.*

b) $A \circ$ *művelet asszociatív, azaz* $\forall a, b, c \in G : a \circ (b \circ c) = (a \circ b) \circ c$*.*

c) Létezik egységelem, azaz $\exists e \in G$*, melyre teljesül, hogy* $\forall g \in G$*-re* $e \circ g = g \circ e = g$*.*

d) Minden elemnek van inverze, azaz $\forall g \in G : \exists g^{-1}$*, melyre teljesül, hogy* $g^{-1} \circ g = g \circ g^{-1} = e$*.*

1.2. Definíció. *A (G,∘) csoportot Abel-csoportnak hívjuk, ha a ∘ művelet kommutatív, azaz:* $\forall a, b \in G : a \circ b = b \circ a$.

1.3. Definíció. *Egy (R,+,·) algebrai struktúrát gyűrűnek nevezünk, ha a következők teljesülnek:*

a) (R,+) Abel-csoport.

b) A szorzás művelet asszociatív.

c) Az összeadás disztributív a szorzásra nézve, azaz $\forall a, b, c \in R$*-re* $a \cdot (b + c) = (a \cdot b) + (a \cdot c), (a + b) \cdot c = (a \cdot c) + (b \cdot c)$.

1.4. Definíció. *Egy (T, +, ·) algebrai struktúrát testnek nevezünk, ha a következők teljesülnek:*

a) (T,+) Abel-csoport és $(T\setminus\{0\}, \cdot)$ *csoport, ahol 0 a (T,+) csoport egységeleme, és zéruselemnek nevezzük.*

b) Az összes disztributív a szorzásra nézve.

(T,+,·)-t szokás csak T-vel jelölni.

1.5. Definíció. *A (T,+,·) test esetén (T,+)-ot T additív csoportjának,* $(T\setminus\{0\}, \cdot)$*-t T multiplikatív csoportjának nevezzük.*

Jelölések (T,+,·) test esetén:

a) Az additív csoport egységelemét (mint fentebb is írtuk) 0-val, a multiplikatív csoport egységelemét 1-gyel jelöljük.

b) T multiplikatív csoportját T^*-gal is jelölhetjük.

c) Adott $t \in T$ esetén t additív inverzét $-t$-vel, $t \in T^*$ multiplikatív inverzét pedig $\frac{1}{t}$-vel jelöljük.

1.6. Definíció. *Egy T testet véges testnek nevezünk, ha* $|T| < \infty$.

1.7. Definíció. $p \in \mathbb{Z}$ *prímszám esetén* $\mathbb{F}_p$*-t a következőképp definiáljuk.*

A modulo p kongruenciareláció egy ekvivalenciareláció ($a \equiv b \pmod{p} \Leftrightarrow p|b - a$)*, és így meghatároz egy osztályozást* $\mathbb{Z}$*-n. Továbbá ez a reláció kompatibilis az alapműveletekkel, azaz:*

$$a \equiv b \text{ és } c \equiv d \Longrightarrow a + c \equiv b + d \text{ és } a \cdot c \equiv b \cdot d.$$

Ezért a műveletek jól értelmezettek az ekvivalenciaosztályok halmazán. Az ekvivalenciaosztályokat maradékosztályoknak nevezzük, és mivel elég egy reprezentánst választani, adott p esetén a halmazukat a következőképp definiálhatjuk:

$$\mathbb{F}_p = \{0, 1, \ldots, p - 1\}.$$

Belátható, hogyha p prím, akkor ez test a modulo p összeadásra és szorzásra $(\mathbb{F}_p, +_p, \cdot_p)$, és látszik, hogy a rendje p, ami véges. Továbbá az is belátható, hogy a multiplikatív csoportja ciklikus. Minden véges test rendje prímhatvány. Ha a rend $q = p^n$, p prím, akkor $\mathbb{F}_q$-t az $\mathbb{F}_p$ magasabb fokú algebrai bővítményeként kapjuk meg. Bármely véges testben a multiplikatív csoport ciklikus.

1.8. Definíció. *Tetszőleges $(G, \cdot)$ csoport és $g \in G$ esetén a következők közül egy teljesül:*

a) $\forall m \neq n \in \mathbb{Z} : g^m \neq g^n$,

b) $\exists m \neq n \in \mathbb{Z} : g^m = g^n$.

Az a) esetben azt mondjuk, hogy G végtelen rendű, a b) esetben pedig feltehető, hogy $m < n$, így teljesül, hogy

$$1 = g^m \cdot g^{-m} = g^{n-m} \Rightarrow \exists k \in \mathbb{N} : g^k = 1.$$

Ekkor G-t véges rendűnek, a legkisebb ilyen k-t pedig g rendjének nevezzük és $o(g)$-vel jelöljük.

1.9. Definíció. *$H \subseteq G$ a G csoport részcsoportja, ha $1 \in H$ és $\forall h_1, h_2 \in H : h_1 \cdot h_2, h_1^{-1} \in H$.*

1.10. Definíció. *$A \subseteq G$ esetén az A által generált részcsoporton azt a legszűkebb részcsoportot értjük, ami tartalmazza A-t. Ezt $[A]$-val jelöljük. Továbbá ha $A = \{g_1, g_2, \ldots, g_k\}$, akkor $[A] = [g_1, g_2, \ldots, g_k]$.*

1.11. Definíció. *Legyen G, H csoport. Azt mondjuk, hogy G és H izomorfak, ha $\exists \varphi : G \to H$, melyre teljesül, hogy $\forall g \in G, h \in H : (gh)\varphi = (g\varphi)(h\varphi)$, tovább φ bijektív. Jelölés: $G \cong H$.*

1.12. Definíció. *Az egy elem által generált részcsoportokat ciklikus csoportoknak nevezzük, és belátható, hogy $\forall g \in G : [g] \cong (C_{o(g)}, +)$. Továbbá ekkor g-t generáló elemnek nevezzük, egy véges test rendjén pedig az elemszámát értjük, azaz itt $[g]$ rendje $o(g)$.*

Korábban már említettük, hogy $\mathbb{F}_q$ multiplikatív csoportja ciklikus.

1.13. Definíció. *α-t $\mathbb{F}_q$ primitív elemének nevezzük, ha F_q^* generáló eleme.*

1.14. Definíció. *Az $\mathbb{F}_q$ test multiplikatív csoportjának generáló eleme az az $\alpha \in \mathbb{F}_q \setminus \{0\}$, melyre teljesül, hogy $\alpha^{q-1} = 1. \Longrightarrow \alpha^q = \alpha$.*

1.15. Definíció. *Tetszőleges T test esetén a*

$$T[x] = \{a_0 + a_1x + a_2x^2 + a_3x^3 + \ldots + a_nx^n | n \in \mathbb{N}, a_i \in T \ \ \forall i = 0, \ldots, n\}$$

halmazt a T test feletti polinomgyűrűnek, elemeit pedig polinomoknak nevezzük. Egy $p \in T[x]$ polinomot a következőképp jelölünk:

$$p(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n = \sum_{i=0}^{n} a_ix^i.$$

Ekkor $n \in \mathbb{N}$-et p fokának nevezzük és azt mondjuk, hogy $\deg p = n$; továbbá a_i-ket p együtthatóinak hívjuk.

1.16. Definíció. *Legyen $(T, +, \cdot)$ test, $p(x) = \sum_{i=0}^{n} a_ix^i$, $q(x) = \sum_{j=0}^{m} b_jx^j \in T[x]$ és $\lambda \in T$. Ekkor a polinomok közötti összeadást, illetve a polinomok skalárral való szorzását a következőképp definiáljuk:*

a) $(p + q)(x) = \sum_{k=0}^{\max\{n,m\}} (a_k + b_k)x^k$.
Ha $n < m$, akkor $a_k := 0 \ \forall k > n$; ha $n > m$, akkor $b_k := 0 \ \forall k > m$.

b) $\lambda p(x) = \sum_{i=0}^{n} \lambda a_ix^i$.

Megjegyzés: Természetesen a fenti $(p + q)(x)$ és $\lambda p(x)$ is $T[x]$ eleme.

1.17. Definíció. *Egy T test, $\omega \in T$ és $p \in T[x]$ polinom esetén a p kiértékelése az ω helyen:*

$$p(\omega) = \sum_{i=0}^{n} a_i\omega^i, \text{ ahol } n = \deg p, \ a_i\text{-k pedig } p \text{ együtthatói.}$$

1.2. Kódelméleti alapfogalmak

1.18. Definíció. *$(V,+,\cdot)$ vektortér egy T test felett, ha $a + : V^2 \to V, \cdot : T \times V \to V$ leképezések a következő axiómákat teljesítik $\forall \lambda, \mu \in T$, és $\forall \ u, v \in V$ esetén:*

a) $(V,+)$ Abel-csoport

b) $\lambda \cdot (u + v) = (\lambda \cdot u) + (\lambda \cdot v)$,

c) $(\lambda + \mu) \cdot u = (\lambda \cdot u) + (\mu \cdot u)$,

d) $\lambda \cdot (\mu \cdot v) = (\lambda \cdot \mu) \cdot v$,

e) $1 \cdot v = v$, *ahol 1 a T-beli multiplikatív egységelem.*

1.19. Definíció. *Egy V vektortér esetén $U \subseteq V$ lineáris altér V-ben, ha U nem üres és zárt a V-ben definiált összeadásra és szorzásra. Jelölés: $U \leq V$.*

Pl.: Legyen $m, n \in \mathbb{N}$, p prím és $q = p^m$. Ekkor $\mathbb{F}_q^n$ vektortér $\mathbb{F}_q$ felett, ahol

$$\mathbb{F}_q^n = \{(x_1, x_2, \ldots, x_n) | \forall i = 1, \ldots, n : x_i \in \mathbb{F}_q\}.$$

A továbbiakban q-ra és n-re mindig az előzőek szerint hivatkozunk.

1.20. Definíció. *Ha F egy véges test, akkor a $C \subset V = F^n$ részhalmazt n hosszú **kódnak** nevezzük. V egy lineáris alterét egy n hosszú **lineáris kódnak** nevezzük. Ha $F = \mathbb{F}_2$, akkor pedig C-t bináris kódnak hívjuk.*

*A C kód elemeit **kódszavaknak** vagy kódvektoroknak nevezzük.*

A következőekben definiált fogalmakat egy általános F véges test esetén is lehetne definiálni, de mivel most az $\mathbb{F}_q^n$ véges testre koncentrálódik a témánk, így a fogalmak során erre a véges testre fogunk hivatkozni.

1.21. Definíció. *Legyen $\boldsymbol{v} = (v_1, v_2, \ldots, v_n), \boldsymbol{u} = (u_1, u_2, \ldots, u_n) \in \mathbb{F}_q^n = V$. A két vektor Hamming-távolságán azon koordináták számát értjük, amelyekben $\boldsymbol{v}$ és $\boldsymbol{u}$ eltér, azaz:*

$$d(\boldsymbol{u}, \boldsymbol{v}) = |\{i : 1 \leq i \leq n, v_i \neq u_i\}|.$$

*A $d\colon V \times V \to \mathbb{N}$ függvényt Hamming-metrikának nevezzük, a $\boldsymbol{v} \in V$ vektor **súlyán** pedig a $d(\boldsymbol{v}, \boldsymbol{0})$ távolságot értjük, és $|\boldsymbol{v}|$-vel jelöljük.*

Vegyük észre, hogy $\forall \boldsymbol{v}, \boldsymbol{u} \in \mathbb{F}_q^n$ vektor esetén

$$d(\boldsymbol{v}, \boldsymbol{u}) = |\{i | 1 \leq i \leq n, v_i - u_i \neq 0\}| = d(\boldsymbol{v} - \boldsymbol{u}, \boldsymbol{0}) = |\boldsymbol{v} - \boldsymbol{u}|.$$

Ezt a tulajdonságot felhasználva könnyen belátható a következő lemma.

1.22. Lemma. *Az $\mathbb{F}_q^n$ vektortéren a d leképezés metrika, azaz a következők teljesülnek $\forall \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z} \in \mathbb{F}_q^n$ esetén:*

a) $d(\boldsymbol{x}, \boldsymbol{y}) \geq 0$ *és* $d(\boldsymbol{x}, \boldsymbol{y}) = 0 \Leftrightarrow \boldsymbol{x} = \boldsymbol{y}$,

b) $d(\boldsymbol{x}, \boldsymbol{y}) = d(\boldsymbol{y}, \boldsymbol{x})$,

c) $d(\boldsymbol{x}, \boldsymbol{y}) \leq d(\boldsymbol{x}, \boldsymbol{z}) + d(\boldsymbol{z}, \boldsymbol{y})$.

1.23. Definíció. *A $\boldsymbol{c} \in \mathbb{F}_q^n$ középpontú $r \in \mathbb{R}_+$ sugarú gömbnek nevezzük a következő halmazt:*

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

Mivel $\mathbb{F}_q^n$ véges, ezért ez a gömb is véges sok elemet tartalmaz, és ezt az elemszámot egy kis kombinatorikával kiszámolhatjuk. Észrevehető, hogyha $r \geq n$, akkor a $\mathbb{B}_r(\boldsymbol{c})$ gömb bármely $c \in \mathbb{F}_q^n$ esetén $\mathbb{F}_q^n$ összes elemét tartalmazza, mivel a gömbben azok az elemek vannak, amelyek legfeljebb r koordinátában térnek el a középponttól, és triviális, hogy bármely elemre igaz, hogy egy másik elemtől legfeljebb az összes koordinátában különbözik. Másrészt ha $r = 0$, akkor a gömbnek csak a középpont az eleme.

Tehát feltehető, hogy $1 \leq r \leq n$. A $\mathbb{B}_r(\boldsymbol{c})$ gömb elemszámának meghatározásához definiáljuk a következő i-sugarú gömbhéjakat a $\boldsymbol{c}$ középpont körül ($0 \leq i \leq r$):

$$\mathbb{B}(i, \boldsymbol{c}) = \{\boldsymbol{x} \in \mathbb{F}_q^n | d(\boldsymbol{c}, \boldsymbol{x}) = i\}.$$

Ezekben a gömbhéjakban azok az elemei vannak $\mathbb{F}_q$-nak, amik pontosan i távolságra vannak $\boldsymbol{c}$-től. Világos, hogy:

$$|\mathbb{B}_r(\boldsymbol{c})| = \sum_{i=0}^{\lfloor r \rfloor} |\mathbb{B}(i, \boldsymbol{c})|.$$

Egy ilyen gömbhéj elemszáma pedig adott i-re $\binom{n}{i}(q-1)^i$. Ez onnan adódik, hogy $\binom{n}{i}$ választás van arra, hogy melyik koordinátákban különbözzön az adott elem $\boldsymbol{c}$-től, egy koordináta esetén pedig $q-1$ lehetőség van egy különböző koordinátát találni, mivel $|\mathbb{F}_q| = q$; és i darab koordinátaválasztás van, amik függetlenek, ezért a koordináták értékeinek kiválasztására $(q-1)^i$ lehetőség van. Tehát:

$$|\mathbb{B}_r(\boldsymbol{c})| = \sum_{i=0}^{\lfloor r \rfloor} |\mathbb{B}(i, \boldsymbol{c})| = \sum_{i=0}^{\lfloor r \rfloor} \binom{n}{i}(q-1)^i.$$

1.24. Definíció. *A*

$$d(C) = \min\{d(\boldsymbol{x}, \boldsymbol{y}) | \boldsymbol{x}, \boldsymbol{y} \in C, \boldsymbol{x} \neq \boldsymbol{y}\}$$

számot ***a C kód minimális távolságának*** *nevezzük.*

1.25. Tétel. *Ha C egy lineáris kód és* $\boldsymbol{d}$*=d(C), akkor*

$$\boldsymbol{d} = \min\{d(\boldsymbol{v}, \boldsymbol{0}) | \boldsymbol{v} \in C \setminus \{\boldsymbol{0}\}\}$$

Vagyis egy lineáris kód minimális távolsága megegyezik a legkisebb súlyú nem-zéró kódvektor súlyával.

1.26. Definíció. *Egy $t \in \mathbb{N}$ esetén a $C \subseteq \mathbb{F}_q^n$ kódot* ***t-hibajavító kódnak*** *nevezzük, ha $\forall$ különböző $\boldsymbol{u}, \boldsymbol{v} \in C$ esetén*

$$d(\boldsymbol{u}, \boldsymbol{v}) \geq 2t + 1.$$

Megjegyzés. Világos, hogy $\forall$ C t-hibajavító kód esetén $d(C) \geq 2t + 1$, ebből pedig az következik, hogy a t sugarú gömbök diszjunktak, amit a következő lemma is megfogalmaz.

1.27. Lemma. *Ha C t-hibajavító kód, akkor tetszőleges $\boldsymbol{v} \in \mathbb{F}_q^n$ vektorhoz legfeljebb egy olyan $\boldsymbol{c} \in C$ kódszó létezik, amelyre $d(\boldsymbol{c}, \boldsymbol{v}) \leq t$.*

Ez könnyen belátható indirekt módon. Tegyük fel, hogy 2 különböző ilyen kódszó létezik egy adott $\boldsymbol{v}$-re: $\boldsymbol{c_1}$ és $\boldsymbol{c_2}$, azaz $d(\boldsymbol{c_1}, \boldsymbol{v}) \leq t$ és $d(\boldsymbol{c_2}, \boldsymbol{v}) \leq t$. Ekkor a háromszög-egyenlőtlenség alapján:

$$2t \geq d(\boldsymbol{c_1}, \boldsymbol{v}) + d(\boldsymbol{c_2}, \boldsymbol{v}) \geq d(\boldsymbol{c_1}, \boldsymbol{c_2}) \geq 2t + 1, \text{ mivel } C \text{ t-javító kód.}$$

Ezzel azt kaptuk, hogy $2t \geq 2t + 1$, ami ellentmondás, tehát a lemma igaz.

1.28. Definíció. *Ha a $C \subseteq \mathbb{F}_q^n$ lineáris kód dimenziója k, akkor* ***lineáris*** *$[n, k]$* ***kódnak*** *nevezzük.*

1.29. Definíció. *Ha $\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_k$ a C lineáris $[n, k]$ kód egy bázisa, akkor azt a $k \times n$-es $\boldsymbol{G}$ mátrixot, melynek i-edik sora a $\boldsymbol{c}_i$ vektor ($i = 1, \ldots, k$), C* ***generátor mátrixának*** *nevezzük.*

1.30. Tétel (Singleton-korlát)**.** *Ha valamely C lineáris $[n, k]$-kód minimális távolsága d, akkor*

$$d \leq (n - k) + 1.$$

1.31. Definíció. *Ha egy lineáris $[n, k]$-kód minimális távolsága d, és teljesül a*

$$d = n - k + 1$$

egyenlőség, akkor a kódot ***MDS-kódnak*** *nevezzük.*

Megjegyzés. Az MDS a 'Maximal distance separable code' angol kifejezés rövidítése, ami magyarul maximális elválasztási távolságú kódot jelent. Ezt azért hívjuk így, mert az adott vektortér lineáris kódjai között erre (is) teljesül, hogy a kódszavak a lehető legtávolabb vannak egymástól, ez pedig a dekódolásnál bizonyul hasznosnak, ugyanis mivel a kijavítható hibák a kódszavak távolságától függenek ($d \geq 2t + 1$), így az MDS-kódok a lehető legtöbb hibát ki tudják javítani. Más szóval nincs olyan kód az adott vektortérben adott dimenzióval, ami több hibát tudna kijavítani.

1.3. Fourier-transzformált

1.32. Definíció. *Legyen α az $\mathbb{F}_q$ test primitív eleme. Ekkor a*

$$p(x) = \sum_{k=0}^{\deg p} a_k x^k \in \mathbb{F}_q[x]$$

polinom Fourier-transzformáltján a következő $q(x) \in \mathbb{F}_q[x]$ polinomot értjük:

$$r(x) = \sum_{k=0}^{q-2} p(\alpha^k) x^k.$$

Megj.: $p(x)$ Fourier-transzformáltját szokás $p^{\#}$-tel is jelölni.

Tekintsük azon $p \in \mathbb{F}_q[x]$-eket, melyeknek a foka kisebb $q-1$-nél, és a halmazukon vegyük a következő leképezést:

$$\text{eval} : \widehat{D} = \{p \in \mathbb{F}_q[x] : \deg p < q-1\} \to \mathbb{F}_q^{q-1},$$

$$p \mapsto (p(\alpha^0), p(\alpha^1), p(\alpha^2), \ldots, p(\alpha^{q-2})),$$

ahol α az $\mathbb{F}_q$ multiplikatív csoportjának a generáló eleme. α ezen tulajdonságából következik, hogy itt tulajdonképp a p polinom grafikonját kapjuk meg egy $q-1$ komponensű vektorként, mivel $\mathbb{F}_q$ összes nem nulla elemében vesszük a kiértékelését.

Most vegyünk egy másik leképezést, ami egy $p \in \widehat{D}$ polinomhoz az együtthatóit rendeli hozzá:

$$f : p(x) = \sum_{i=0}^{q-2} a_i x^i \mapsto (a_0, a_1, \ldots, a_{q-2}).$$

Látszik, hogy ha az utóbbi leképezést végrehajtjuk a $p \in \widehat{D}$ polinom Fourier - transzformáltjára, akkor ugyanazt kapjuk, mintha az eval-t hajtottuk volna végre a p-re ($f(p^{\#}) = eval(p)$). Kérdés, hogy adott p esetén a két reprezentáció ($f(p)$ és eval(p)) között van-e valamilyen közvetlen kapcsolat.

Az nyilvánvaló, hogy mindkét reprezentációval egy $q-1$ skalárból álló vektort kapunk. Az is látszik, hogy eval bijekció $\widehat{D}$ és $\mathbb{F}_q^{q-1}$ között, mivel $\ker(\text{eval}) \cap \widehat{D} = \{0\}$ és a számosságuk megegyezik.

Ezen észrevételek is megerősíteni látszanak, hogy a Fourier - transzformáció a két halmaz között egy kapcsolatot állít fel. Vegyük a következő polinomokat:

$$p = \sum_{k=0}^{q-2} a_k x^k \in \widehat{D}, r = p^{\#}$$

Most nézzük meg, mi történik, ha az eval-t végrehajtjuk r-re, azaz p Fourier - transzformáltjára. Ehhez szükségünk van r-nek az α^i helyeken felvett értékeire.

$$r(\alpha^i) = v_0 + v_1\alpha^i + v_2\alpha^{2i} + \ldots + v_{q-2}\alpha^{i(q-2)} = \sum_{j=0}^{q-2} v_j\alpha^{ij} =$$

$$= \sum_j p(\alpha^j)\alpha^{ij} = \sum_j (\sum_{k=0}^{q-2} a_k\alpha^{jk})\alpha^{ij} = \sum_{j,k} a_k\alpha^{(i+k)j} = \sum_k a_k(\sum_{j=0}^{q-2}(\alpha^{i+k})^j).$$

Vezessük be a következő jelölést: $\beta = \alpha^{i+k}$. Ekkor a következő vehető észre:

$$\sum_{j=0}^{q-2}\beta^j = 1 + \beta + \ldots + \beta^{q-2} = \begin{cases} \frac{\beta^{q-1}-1}{\beta-1} = 0 & \text{, ha } \beta \neq 1 \\ q-1 = -1 & \text{, ha } \beta = 1. \end{cases}$$

Az első esetben azért 0 az eredmény, mert $\beta^{q-1} = \alpha^{(q-1)(i+k)}$ és $\alpha^{q-1} = 1$, mivel α generáló elem, ill. $q \equiv 0$ modulo a test karakterisztikája, ezért teljesül, hogy $q - 1 = -1$.

Az eredményt felhasználva a következőt kapjuk:

$$\sum_{j=0}^{q-2}(\alpha^{i+k})^j = \begin{cases} 0 & \text{, ha } i+k \neq q-1 \\ -1 & \text{, ha } i+k = q-1 \end{cases}$$

Adott k esetén ezen utóbbi összeget jelöljük γ_k-val. Tehát

$$r(\alpha^i) = \sum_k a_k\gamma_k = -a_{q-1-i} =: w_i.$$

Megjegyzés: Az $i = 0$ esetben $w_0 = -a_0$.

Most hajtsuk végre r-re a Fourier-transzformációt:

$$r^{\#}(x) = w_0 + w_1x + w_2x^2 + \ldots + w_{q-2}x^{q-2} =$$

$$-(a_0 + a_{q-2}x + a_{q-3}x^2 + \ldots + a_1x^{q-2}).$$

Ebből azt a következtetést vonhatjuk le, hogy egy adott $p(x)$ polinom Fourier-transzformáltjának Fourier-transzformáltjának az együtthatói szinte ugyanazok, mint p együtthatói, tehát ez a Fourier-transzformáció egy bizonyos módon önmagának az inverze.

2. Reed-Solomon-féle hibajavító kódok

A kommunikáció során továbbított üzenetről feltesszük, hogy egy n - dimenziós véges test feletti vektortér (jelöljük F^n-nel) egy eleme, azaz egy F^n-beli vektor, pl.: $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ az üzenet, ahol minden a_i F eleme. Ezt a vektort nevezzük kódszónak. A továbbítás közben hibák hatására a címzett az $\mathbf{a}$ helyett a $\mathbf{b} = \mathbf{a} + \mathbf{e}$ vektort kapja meg; itt $\mathbf{e}$-t hibavektornak nevezzük. Ezeknek a hibáknak a kijavítására találták fel a hibajavító kódokat, amiknek a Reed-Solomon-kódok egy speciális fajtája.

2.1. Felépítés

Legyen q prímhatvány és α az $\mathbb{F}_q$ primitív eleme, azaz:

$$\mathbb{F}_q = \{0\} \cup \{\alpha^0, \alpha^1, \alpha^2, \ldots, \alpha^{q-2}\}.$$

Rögzített $k \in \mathbb{N}$ esetén a $C \leq \mathbb{F}_q^{q-1}$ Reed-Solomon-kódot a következőképp definiáljuk:

$$C = \{(p(\alpha^0), p(\alpha^1), p(\alpha^2), \ldots, p(\alpha^{q-2})) | p \in \mathbb{F}_q[x], \deg p < k \in \mathbb{N}\},$$

azaz vesszük az összes $\mathbb{F}_q[x]$-beli, legfeljebb k-ad fokú polinom kiértékelését az $\alpha^0 = 1, \alpha^1 = \alpha, \alpha^2, \ldots, \alpha^{q-2}$ helyeken. Ezt a kiértékelést nevezzük a p grafikonjának, mivel az összes $\mathbb{F}_q^*$-beli elemben vettük az értékét. Világos, hogy $C \leq \mathbb{F}_q^{q-1}$, azaz C lineáris kód $\mathbb{F}_q^{q-1}$-ben.

Legyen $D = \{p \in \mathbb{F}_q[x] | \deg p < k\}$, és tekintsük az

$$\text{eval}: D \to C, p \mapsto (p(\alpha^0), p(\alpha^1), p(\alpha^2), \ldots, p(\alpha^{q-2}))$$

leképezést. Belátható, hogy ez egy lineáris leképezés, és így bázist bázisba visz. A D-beli természetes bázis: $\{1, x, x^2, \ldots, x^{k-1}\}$, így az 1.29 definíció és D bázisainak eval melletti képei alapján a C bázisaiból alkotott generáló mátrix a következőképp áll elő:

$$G = \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & \alpha & \alpha^2 & \ldots & \alpha^{q-2} \\ 1 & \alpha^2 & \alpha^4 & \ldots & \alpha^{2q-4} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{k-1} & \alpha^{2k-2} & \ldots & \alpha^{(q-2)(k-1)} \end{pmatrix}$$

Ezenkívül látszik, hogy az i-edik sorának j-edik eleme:

$$G_{ij} = \alpha^{(i-1)(j-1)}, \ (i = 1, \ldots, k, j = 1, \ldots, q-1),$$

és így $G \in \mathbb{F}_q^{k\times(q-1)}$ és C k-dimenziós.

Tehát C egy lineáris $[q-1,k]$ kód, és a Singleton-korlát miatt (ld. 1.30 tétel) $d(C) \leq (q-1-k)+1 = q-k$. Ezen kívül még további észrevételek tehetők C minimális távolságát illetően.

C tehát a következő halmaz:

$$\{(p(\alpha^0),\ldots,p(\alpha^{q-2}))|\deg p < k\}.$$

Egy adott p polinomhoz tartozó elemét C-nek jelöljük w_p-vel. Legyen p és $\widetilde{p}$ két tetszőleges, legfeljebb k-adfokú polinom, és tegyük fel, hogy $d(w_p, w_{\widetilde{p}}) = l$. Ekkor a következők vehetők észre:

$$l = |w_p - w_{\widetilde{p}}| = |w_{p-\widetilde{p}}|, \text{ mivel}$$

$$(p(\alpha^0), p(\alpha^1),\ldots) - (\widetilde{p}(\alpha^0), \widetilde{p}(\alpha^1),\ldots) = (p(\alpha^0) - \widetilde{p}(\alpha^0),\ldots)$$
$$= ((p-\widetilde{p})(\alpha^0),\ldots) = w_{p-\widetilde{p}}.$$

Az egyszerűség kedvéért jelöljük $p-\widetilde{p}$-ot P-vel.

$$\begin{aligned} w_P \text{ súlya } l &\iff l \text{ helyen lesz } P \neq 0 \\ &\iff \text{legalább } q-1-l \text{ helyen } 0 \\ &\iff P\text{-nek legalább } q-1-l \text{ gyöke van.} \end{aligned}$$

Mivel P foka is kisebb, mint k, így teljesülnek a következők is:

$$\begin{aligned} q-1-l \leq \deg P < k\,, \\ q-1-l \leq k-1\,, \\ l \geq q-k \end{aligned}$$

Ezekből látszik, hogy ha két kódvektor távolsága l, akkor $l \geq q-k$, így C minimális távolságára is teljesül, hogy nagyobb $q-k$-nál. Ezt az eredményt és a Singleton-korlátból kapott eredményt egybevetve kapjuk a következő tételt:

2.1. Tétel. *Bármely $C \leq \mathbb{F}_q^{q-1}$, k-dimenziós Reed-Solomon-kódra teljesül, hogy*

$$d(C) = q-k.$$

Ennek egyenes következménye, hogy C MDS-kód, azaz a lehető legnagyobb távolságra vannak egymástól a kódszavai, és így C az egyik legtöbb hibát kijavítani képes kód. Felhasználva a t-hibajavító kód definícióját (1.26) és azt, hogy $d(C) = q-k$, a következő eredményekre juthatunk:

$$\begin{aligned} d(C) = q-k \geq 2t+1\,, \\ q-k-1 \geq 2t\,, \\ \frac{q-k-1}{2} \geq t \end{aligned}$$

Tehát C $\lfloor \frac{q-k-1}{2} \rfloor$ hibát még biztos ki tud javítani, és nincs olyan lineáris kód $\mathbb{F}_q^{q-1}$-ben, ami k dimenziós és több hibát tudna kijavítani, mint C.

Visszatérve a feladatunkhoz: egy ember üzenetet küld egy másiknak, azaz választ egy $w \in C$-t és elküldi egy zajos csatornán. Megérkezik egy $w' = w + e \in \mathbb{F}_q^{q-1}$, ahol e-vel a hibavektort jelöltük. Ekkor ha $w' \in C$, azaz $e = \mathbf{0}$, akkor nem volt hiba és készen vagyunk, ha viszont ez nem teljesül, meg kell találnunk a w'-höz legközelebb eső C-beli elemet. A $w' \in C$ eldöntésében segít a fent definiált G mátrix, mivel C elemei G sorvektorainak lineáris kombinációiból állnak. Tehát $w' = (y_0, y_1, \ldots, y_{q-2})$ akkor eleme C-nek, ha $\exists \boldsymbol{x} = (x_0, x_1, \ldots, x_{k-1})$, melyre $G^{\mathrm{T}}\boldsymbol{x} = w'$, azaz:

$$G^{\mathrm{T}}\boldsymbol{x} = \begin{pmatrix} x_0 + x_1 + x_2 + \ldots + x_{k-1} \\ x_0 + x_1\alpha + x_2\alpha^2 + \ldots + x_{k-1}\alpha^{k-1} \\ x_0 + x_1\alpha^2 + x_2\alpha^4 + \ldots + x_{k-1}\alpha^{2k-2} \\ \vdots \\ x_0 + x_1\alpha^{q-2} + x_2\alpha^{2q-4} + \ldots + x_{k-1}\alpha^{(q-2)(k-1)} \end{pmatrix} = \begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ \vdots \\ y_{q-2} \end{pmatrix} = w'$$

Ebből α és y_i-k ismeretében egy olyan lineáris egyenletrendszert kapunk, amiben k ismeretlen és $q-1$ egyenlet van, azaz ha van megoldás, azt Gauss-eliminációval megkaphatjuk. Ha viszont nincs megoldás, akkor meg kell keresnünk a w'-höz legközelebb eső C-beli elemet, ami a dekódolás feladatához vezet.

2.2. Dekódolás

A dekódoláshoz az úgynevezett **tünet-dekódolást** (syndrome decoding) fogjuk majd használni, amit Peterson fejlesztett ki 1960-ban. Ennél a módszernél az üzenetekre a következő módon tekintünk: amit a feladó küld, az egy legfeljebb k-ad fokú $p(x)$ polinom $\mathbb{F}_q^{q-1}$-beli grafikonja; amit a címzett megkap, az egy legfeljebb $(q-2)$-ed fokú $\mathbb{F}_q^{q-1}$ feletti $s(x)$ polinom együtthatóiból alkotott vektor. Tehát a küldött üzenet $(c_0, c_1, \ldots, c_{q-2})$, azaz ezek a c_i-k a p adott α^i helyen vett értékei, és ha feltételezzük, hogy nem történt hiba a továbbítás során, akkor a kapott üzenet az $r(x)$ polinom együtthatói, ahol $r = p^{\#}$, azaz

$$r(x) = \sum_{i=0}^{q-2} c_i x^i.$$

Korábban levezettük, hogy a Fourier-transzformáltra a következő teljesül: $\forall i = 0, \ldots, q-2 : r(\alpha^i) = -a_{q-1-i}$, ezen kívül tudjuk, hogy $\deg p < k$,

tehát $a_k = a_{k+1} = \ldots = a_{q-1} = 0$, így kapjuk azt, hogy $r(\alpha^i) = 0$, ha:

$$k \leq q-1-i \leq q-1$$

$$k-q+1 \leq -i \leq 0$$

$$-k+q-1 \geq i \geq 0,$$

azaz $r(\alpha^i) = 0 \forall i = 0, \ldots, q-k-1$ esetén.

Tehát $r(\alpha^0) = r(\alpha) = r(\alpha^2) = \ldots = r(\alpha^{q-k-1}) = 0$, és így $r(x)$ osztható a $g(x) = \prod_{j=0}^{q-k-1}(x-\alpha^j)$ polinommal. Az üzenetküldés során ez az r polinom sérül, és a kapott üzenet az $s(x) = r(x) + e(x)$ polinom együtthatói, ahol

$$e(x) = \sum_{i=0}^{q-2} e_i x^i.$$

Az x i-edik hatványánál akkor kapunk hibát, ha $e_i \neq 0$. A C kód konstrukciója miatt feltehető, hogy a hiba mérete legfeljebb $\widehat{t} := \lfloor \frac{q-k-1}{2} \rfloor$, mert ennyi hibát még a kód ki tud javítani.

Ha tudjuk, hogy v hiba van az x különböző i_k hatványaiban ($v \leq \widehat{t}$), akkor

$$e(x) = \sum_{k=1}^{v} e_{i_k} x^{i_k}.$$

A dekódolás célja, hogy megtaláljuk a hibák helyeit (i_k) és értékeit (e_{i_k}). Ha ezek megvannak, akkor $e(x)$-et ki tudjuk számolni és le tudjuk vonni $s(x)$-ből, így megkapva az eredeti üzenetet. Ezekhez a számításokhoz kell definiálnunk az S_j tüneteket.

2.2. Definíció.

$$S_j = s(\alpha^j) = \underbrace{r(\alpha^j)}_{0} + e(\alpha^j) = e(\alpha^j) = \sum_{k=1}^{v} e_{i_k}(\alpha^j)^{i_k},\ j = 1, 2, \ldots, q-1-k$$

Ebből látszik, hogy azért előnyös a tünetekkel foglalkozni, mert az elküldött polinomtól függetlenek.

2.3. Hibahelyek és hibaértékek

A kényelmesség kedvéért bevezetjük a következő jelöléseket a **hibahelyekre (X_k)** és a **hibaértékekre (Y_k)**:

$$X_k := \alpha^{i_k},\ Y_k := e_{i_k}.$$

Így a tünetek a következő módon egyszerűsödnek:

$$S_j = \sum_{k=1}^{v} Y_k X_k^j.$$

Ezek egy $q - k - 1 \geq 2v$ egyenletből álló egyenletrendszert adnak meg $2v$ ismeretlennel, de ez az egyenletrendszer az X_k-kban nemlineáris, így nincs egyértelmű megoldása. Viszont ha az X_k-kat ismernénk (lásd a következőkben), akkor a tünetek által adott egyenletek olyan lineáris egyenletrendszert adnának meg, amikből egyszerűen megkaphatók az Y_k hibaértékek.

Mátrixokkal felírva az egyenletrendszert:

$$\begin{pmatrix} X_1^1 & X_2^1 & \dots & X_v^1 \\ X_1^2 & X_2^2 & \dots & X_v^2 \\ \vdots & \vdots & \ddots & \vdots \\ X_1^{q-1-k} & X_2^{q-1-k} & \dots & X_v^{q-1-k} \end{pmatrix} \begin{pmatrix} Y_1 \\ Y_2 \\ \vdots \\ Y_v \end{pmatrix} = \begin{pmatrix} S_1 \\ S_2 \\ \vdots \\ S_v \end{pmatrix}$$

Ebből pedig az adódik, hogy már csak az X_k-k megkeresése a probléma.

2.4. Hibakereső polinom

Peterson talált egy rekurzív összefüggést, ami egy lineáris egyenletrendszer kialakulásához vezetett. Ezeket megoldva megkapjuk a hibák helyeit.

2.3. Definíció (Hibakereső polinom)**.**

$$\Lambda(x) = \prod_{k=1}^{v}(1 - xX_k) = 1 + \Lambda_1 x + \Lambda_2 x^2 + \ldots + \Lambda_v x^v.$$

$\Lambda(x)$ gyökei az X_k^{-1}-ek, azaz

$$\Lambda(X_k^{-1}) = 0 \quad \forall k = 1, \ldots, v$$

$$\Lambda(X_k^{-1}) = 1 + \Lambda_1 X_k^{-1} + \Lambda_2 X_k^{-2} + \ldots + \Lambda_v X_k^{-v} = 0.$$

Rögzített k és tetszőleges $1 \leq j \leq v$ esetén ha beszorzunk $Y_k X_k^{j+v}$-nel, akkor még mindig nullát kapunk:

$$Y_k X_k^{j+v} \Lambda(X_k^{-1}) = 0$$

Így

$$Y_k X_k^{j+v} + Y_k X_k^{j+v} \Lambda_1 X_k^{-1} + Y_k X_k^{j+v} \Lambda_2 X_k^{-2} + \ldots + Y_k X_k^{j+v} \Lambda_v X_k^{-v} = 0,$$

tehát

$$Y_k X_k^{j+v} + \Lambda_1 Y_k X_k^{j+v-1} + \Lambda_2 Y_k X_k^{j+v-2} + \ldots + \Lambda_v Y_k X_k^{j} = 0.$$

Ha ezt az összes k-ra végrehajtjuk és szummázunk $k = 1$-től v-ig, a következőt kapjuk:

$$\sum_{k=1}^{v} (Y_k X_k^{j+v} + \Lambda_1 Y_k X_k^{j+v-1} + \Lambda_2 Y_k X_k^{j+v-2} + \ldots + \Lambda_v Y_k X_k^{j}) = 0$$

$$\sum_{k=1}^{v} (Y_k X_k^{j+v}) + \Lambda_1 \sum_{k=1}^{v} (Y_k X_k^{j+v-1}) + \Lambda_2 \sum_{k=1}^{v} (Y_k X_k^{j+v-2}) + \ldots + \Lambda_v \sum_{k=1}^{v} (Y_k X_k^{j}) = 0$$

A tünetekkel felírva (2.2 definíció):

$$S_{j+v} + \Lambda_1 S_{j+v-1} + \ldots + \Lambda_{v-1} S_{j+1} + \Lambda_v S_j = 0 \text{ (mivel } S_i = \sum_{k=1}^{v} Y_k X_k^i)$$

Rövidebben:

$$\sum_{l=0}^{v} S_{l+j} \Lambda_{v-l} = 0 \quad (\Lambda_0 = 1)$$

$$\sum_{l=0}^{v-1} S_{l+j} \Lambda_{v-l} = -S_{j+v} \; (\forall j = 1, \ldots, v)$$

Ezekből kapjuk a következő lineáris egyenletrendszert:

$$\begin{pmatrix} S_1 & S_2 & \ldots & S_v \\ S_2 & S_3 & \ldots & S_{v+1} \\ \vdots & \vdots & \ddots & \vdots \\ S_v & S_{v+1} & \ldots & S_{2v-1} \end{pmatrix} \begin{pmatrix} \Lambda_v \\ \Lambda_{v-1} \\ \vdots \\ \Lambda_1 \end{pmatrix} = \begin{pmatrix} -S_{v+1} \\ -S_{v+2} \\ \vdots \\ -S_{v+v} \end{pmatrix}$$

Mivel az $S_j = s(\alpha^j)$ tüneteket ismerjük, ezt az egyenletrendszert megoldva megkapjuk a hibakereső polinom Λ_i együtthatóit. Tehát ha ismerjük v-t, akkor $\Lambda(x)$ kiszámítható. Bár v-t pontosan nem ismerjük, de egy felső korlátot ismerünk rá, mint fentebb is említettük ($\widehat{t}$), és számolhatunk úgy, mintha elérné ezt a felső korlátot, mivel ha még nem is éri el, akkor néhány utolsó együttható 0 lesz, ez pedig nem okoz gondot.

Ha $\Lambda(x)$-et ismerjük, a gyökeit különböző módszerekkel meg tudjuk találni (ilyen pl. a Chien-keresés), majd a gyökök reciprokait véve megkapjuk X_k-kat. Továbbá

$$X_k = \alpha^{i_k} \Rightarrow i_k = \log_\alpha X_k,$$

így megtudtuk a hibák helyeit. Ezek után mivel X_k-k ismertek, a fenti egyenletrendszert Y_k-kra meg tudjuk oldani. Ekkor a korábbiak alapján gyakorlatilag megkaptuk $e(x)$-et is, és azt $s(x)$-ből levonva megkapjuk $r(x)$-et, aminek az együtthatóit szerették volna elküldeni, és készen vagyunk a dekódolással.

Nyilatkozat

Alulírott Táborosi Andor Zsolt, kijelentem, hogy a dolgozatomat más szakon korábban nem védtem meg, saját munkám eredménye, és csak a hivatkozott forrásokat (szakirodalom, eszközök, stb.) használtam fel.

Tudomásul veszem, hogy szakdolgozatomat a Szegedi Tudományegyetem Bolyai Intézetének könyvtárában a kölcsönözhető könyvek között helyezik el, és az interneten is nyilvánosságra hozhatják.

Szeged, 2013. május 15. .....

aláírás

Köszönetnyilvánítás

Ezúton szeretnék köszönetet mondani **Dr. Nagy Gábor Péternek**, amiért a szakdolgozatom témaválasztásában, illetve a kidolgozásában a kezdetektől fogva segített tanácsaival, útmutatásával, továbbá hogy erre a projektre áldozta az idejét. Ezen felül azt is szeretném megköszönni neki, hogy ráirányította a figyelmem a *Véges geometriák és kódok* című kurzusra. **Prof. Korchmáros Gábornak** pedig azért szeretnék köszönetet mondani, mert ezen kurzus megtartásával segített nekem a véges geometria témáját megismerni, ami szintén hozzájárult a szakdolgozatom témájának megválasztásához.

Hivatkozások

[1] D. Joyner, R. Kreminski, J. Turisco, *Applied Abstract Algebra*, The Johns Hopkins University Press, Baltimore, 2004.

[2] Kiss Gy. - Szőnyi T., *Véges Geometriák*, Polygon Könyvtár, Szeged, 2001.

[3] *http://en.wikipedia.org/wiki/Reed-Solomon_error_correction* 2013.04.16.

[4] Korchmáros Gábor, *Véges geometriák és kódok (előadásjegyzet)*, Szegedi Tudományegyetem, 2012.