EÖTVÖS LORÁND TUDOMÁNYEGYETEM
TERMÉSZETTUDOMÁNYI KAR

Nagy Viktor

VÉGES TESTEK

BSc szakdolgozat

Témavezető:

Fialowski Alice

Algebra és Számelmélet Tanszék

Budapest, 2014

Köszönetnyilvánítás

Ezúton szeretném megköszönni témavezetőmnek, Fialowski Alice-nak, hogy időt szakított rám, tanácsaival és útmutatásával segítette a munkám.

Köszönöm a családomnak és a barátaimnak, akik mindvégig támogattak, jóban s rosszban egyaránt.

Tartalomjegyzék

Bevezetés

A véges testek elmélete sokféle alkalmazási lehetősége révén az elmúlt évszázadban különösen fontossá vált. Ilyen alkalmazás például a kódelmélet és a titkosírás, de különféle kombinatorikai problémák megoldása során is felmerülnek véges testek.

Az egyszerűbb, prím elemszámú testekkel már a 17-18. században is foglalkoztak, azonban a véges testek általános elméletének kezdete csak a 19. század elejére tehető. Ekkor élt és alkotott Évariste Galois, a modern algebra egyik megalapítója. Ugyanakkor a véges testek jelentősége csak a 20. század közepén nőtt meg. Claude Shannon 1948-ban megjelent, *A kommunikáció matematikai elmélete* című műve az információelmélet megalakulását jelentette.

Az információelmélet fontos részterülete a kódelmélet, amely mindennapjaink része lett. Néhány példát említenék a kódok fontosságának szemléltetésére. Kódokat használnak banki átutalások során titkosításra, műholdról történő televíziós adás sugárzásakor hibajavításra, illetve zenefájlok mp3 formátumba tömörítéséhez.

Szakdolgozatom első fejezetében néhány algebrai fogalmat és tételt foglalok össze, a gyűrűk és a testbővítések témaköréből. A második fejezetben a véges testek elméletével foglalkozom. Itt ejtek szót a véges testek szerkezetéről. Ehhez elengedhetetlen a véges test feletti polinomok vizsgálata, ugyanis ezekkel lehet prímhatványrendű testeket konstruálni, illetve ezekben számolni. Különösen fontos a 2^8 elemű test, mivel a számítástechnikában, illetve a távközlésben általánosan használt tárolókapacitás-mértékegység a bájt.

A harmadik fejezeben a véges testek egyik legfontosabb alkalmazásáról lesz szó, a kódelméletről. A fejezet a kódelmélet algebrai hátteréről, azon belül is a hibajelzésről és -javításról szól. Az első szakaszban ismertetem az alapvető fogalmakat, melyek jó része Richard Hamming 1950 körüli munkásságához köthető. A második szakaszban ciklikus kódokkal, azon belül is a BCH-kódokkal foglalkozom. Itt teszek említést ezek speciális osztályáról, a Reed–Solomon kódokról. Megjegyzem azonban, hogy ezek külön-külön alakultak ki 1959–1960-ban és a kettő között lévő kapcsolatot csak később fedezték fel.

Ezek a kódok a mai napig is széles körben elterjedtek. Ez főként annak kö-

szönhető, hogy többszörös hibákat is képesek javítani, és dekódolásukra hatékony algoritmusok vannak. Alkalmazhatóságukat és hatékonyságukat jól jellemzi, hogy BCH, illetve Reed–Solomon kódot használnak a műholdas kommunikáció során, CD és DVD lemezek hibajavításához és kétdimenziós vonalkódok, mint például a QR-kódok hibajavítására is.

Szakdolgozatom zárásaként a BCH-kódok dekódolására használatos Peterson–Gorenstein–Zierler algoritmust mutatom be. Bár nem ez a leghatékonyabb dekódolási eljárás, ez is jól jelzi a véges testek elméletének fontosságát.

1. fejezet

Algebrai alapfogalmak

A fejezet célja a későbbiek során használt algebrai fogalmak és összefüggések összefoglalása. Ezeket az alapképzés során tanultuk, így bizonyítások itt nem szerepelnek. A fejezet megírása során saját kézzel írt jegyzeteimet, valamint a [3] irodalmat használtam fel.

1.1. Csoportok, gyűrűk, testek

1.1.1. Definíció. Egy G halmazt a G-n értelmezett $*$ művelettel együtt csoportnak hívunk, ha az alábbi három tulajdonság teljesül.

- $*$ asszociatív, azaz $\forall\, a, b, c \in G$-re $a * (b * c) = (a * b) * c$
- létezik neutrális elem, azaz $\exists\, e \in G$, hogy $\forall\, g \in g$-re $e * g = g * e = g$.
- minden elemnek létezik inverze, azaz $\forall\, g \in G$-hez $\exists\, g^{-1} \in G$, hogy $g * g^{-1} = g^{-1} * g = e$

Ha a $*$ művelet kommutatív is, akkor G-t kommutatív, vagy Abel-csoportnak nevezzük.

1.1.2. Definíció. Legyen R nemüres halmaz, $+$ és $\cdot$ binér műveletek R-en, ekkor $(R, +, \cdot)$ gyűrű, ha

- $(R, +)$ Abel-csoport
- $\cdot$ asszociatív
- a szorzás mindkét oldalról disztributív az összeadásra nézve, azaz $\forall\, a, b, c \in R$-re teljesülnek a következő egyenlőségek $c(a + b) = ca + cb$ és $(a + b)c = ac + bc$

Ha $a, b \in R \setminus \{0\}$ esetén $ab = 0$ teljesül, akkor a-t baloldali, b-t jobboldali *nullosztónak* nevezzük. Egy gyűrű *nullosztómentes*, ha nincsenek benne nullosztók, azaz egy szorzat értéke akkor és csak akkor nulla, ha valamelyik tényezője nulla. Azt mondjuk, hogy egy gyűrű *kommutatív*, ha a szorzás kommutatív, ha pedig a szorzásnak létezik egységeleme, akkor *egységelemes* gyűrűről beszélünk. A legalább kételemű, kommutatív, egységelemes, nullosztómentes gyűrűt *integritási tartománynak* nevezzük. Ha egy gyűrű nemnulla elemei a szorzásra nézve csoportot alkotnak, akkor *ferde testnek* nevezzük. Ha ez a multiplikatív csoport kommutatív is, akkor *testnek* nevezzük. Minden test egyben integritási tartomány is. Fordítva nem igaz, de ha egy integritási tartomány véges, akkor szükségképpen test.

1.1.3. Példa. (i) Az egész számok halmaza integritási tartományt alkot.

(ii) A páros számok halmaza kommutatív gyűrűt alkot, amelyben nincs egységelem.

(iii) $\mathbb{Z}_n$ a modulo n összeadással és szorzással együtt egységelemes, kommutatív gyűrűt alkot, amely pontosan akkor test, ha n prím.

(iv) A 2×2-es valós számokból álló mátrixok egységelemes gyűrűt alkotnak, amely nem kommutatív.

(v) A 2×2-es valós számokból álló invertálható mátrixok ferde testet alkotnak.

(vi) A racionális és a valós számok halmaza is testet alkot.

(vii) A valós együtthatós polinomok a szokásos polinomok közötti összeadással és szorzással integritási tartományt alkotnak, ezt a gyűrűt $\mathbb{R}[x]$-el jelöljük.

(viii) A valós-valós függvények a pontonkénti összadás és szorzás műveleteivel kommutatív, egységelemes gyűrűt alkotnak, amely nem nullosztómentes.

Ha az R gyűrű S részhalmaza maga is gyűrű az R-beli műveletekkel, akkor azt mondjuk, hogy S *részgyűrű*. Ha I olyan részgyűrűje R-nek, hogy minden $r \in R$ és minden $i \in I$ esetén az $ri \in I$ és $ir \in I$, akkor azt mondjuk, hogy I *ideál*. Az I ideált *főideálnak* nevezzük, ha van olyan $r \in R$, hogy $I = (r)$. Ha I ideál R-ben, akkor $(I, +)$ részcsoportja $(R, +)$-nak, amely a kommutativitás miatt normális is. Tehát I az R egy osztályozását adja, az osztályokat modulo I maradékosztályoknak nevezzük. Egy $r \in R$ elem maradékosztályát modulo I jelölje $r + I = [r]$. Az a és b elem pontosan akkor van egy maradékosztályban, ha $a - b \in I$; ekkor azt mondjuk, hogy a kongruens b-vel modulo I és $a \equiv b \bmod I$-vel jelöljük.

1.1.4. Definíció. Legyen I az R gyűrű ideálja. Ekkor a modulo I maradékosztályokon értelmezett $(a+I)+(b+I)=(a+b)+I$ és $(a+I)(b+I)=(ab)+I$ műveletekkel a maradékosztályok gyűrűt alkotnak. Ezt a gyűrűt az R-nek I szerinti maradékoszály- vagy faktorgyűrűjének hívjuk, és R/I-vel jelöljük.

A fent definiált műveletek értelmesek, nem függnek az a és a b reprezentáló elemek megválasztásától, csak a maradékosztályoktól. A művelettartó leképezések és az ideálok között hasonló kapcsolat van, mint a normális részcsoportok és a csoport-homomorfizmusok között.

1.1.5. Definíció. Legyen R és S gyűrű. Egy $\varphi : R \to S$ leképezést *homomorfizmusnak* nevezünk, ha minden $a, b \in R$-re $\varphi(a+b)=\varphi(a)+\varphi(b)$ és $\varphi(ab)=\varphi(a)\varphi(b)$ teljesül. A φ homomorfizmus magja $\ker\varphi = \{r \in R : \varphi(r) = 0 \in S\}$. A szürjektív homomorfizmust *endomorfizmusnak*, a bijektív homomorfizmust *izomorfizmusnak* nevezzük.

1.1.6. Tétel. *Legyen $\varphi : R \to S$ endomorfizmus. Ekkor $\ker\varphi$ ideál R-ben és $R/\ker\varphi$ izomorf S-sel. Megfordítva, ha I az R ideálja, akkor $\psi : R \to R/I$, $\psi(a) = a + I$ leképezés endomorfizmus, melynek magja I.*

1.1.7. Példa. (i) Legyen $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ olyan homomorfizmus, mely egy egész számhoz az n-nel vett osztási maradékát rendeli. Ekkor $\ker\varphi = (n)$, tehát $\mathbb{Z}/(n)$ izomorf $\mathbb{Z}_n$-nel.

(ii) Legyen $\varphi : \mathbb{R}[x] \to \mathbb{C}$ olyan homomorfizmus, melyre $\varphi(f) = f(i)$. Ekkor φ endomorfizmus, és $\varphi(f) = 0$ pontosan akkor teljesül, ha x^2+1 osztja f-et, azaz $\ker\varphi = (x^2+1)$, tehát $\mathbb{R}[x]/(x^2+1)$ izomorf $\mathbb{C}$-vel.

Ha R gyűrű, és van olyan $n \in \mathbb{N}\setminus\{0\}$, hogy $nr = 0$ minden $r \in R$-re, akkor a legkisebb ilyen n-et az R gyűrű *karakterisztikájának* nevezzük, és $\mathrm{char}(R)$-rel jelöljük. Ha nincs ilyen n, akkor azt modjuk, hogy az R gyűrű karakterisztikája 0. Ha $R \neq 0$ olyan egységelemes, nullosztómentes gyűrű, amelynek nem 0 a karakterisztikája, akkor $\mathrm{char}(R)$ prímszám. Következésképpen minden véges test karakterisztikája prím. Ha S az R nullosztómentes gyűrű legalább kételemű részgyűrűje, akkor $\mathrm{char}(R)=\mathrm{char}(S)$. Ha R kommutatív gyűrű, és $\mathrm{char}(R) = p$, akkor minden $a, b \in R$-re teljesül, hogy tetszőleges $n \in \mathbb{N}$ esetén $(a+b)^{p^n} = a^{p^n}+b^{p^n}$ és $(a-b)^{p^n} = a^{p^n}-b^{p^n}$.

1.2. Testbővítések

Legyen L test és K olyan részhalmaza L-nek, hogy K maga is test a L-beli műveletekkel. Ekkor azt mondjuk, hogy K *részteste* L-nek, vagy L a K test *bővítése*;

ezt $L|K$-val jelöljük. Ha $K \neq L$, akkor azt mondjuk, hogy K valódi részteste L-nek. Tekintsük az $\mathbb{F}_p$ résztesteit. Mivel egy ilyen résztestnek tartalmaznia kell a 0 és 1 elemeket, ezért tartalmaznia kell az egész $\mathbb{F}_p$-t, tehát $\mathbb{F}_p$-nek nincs valódi részteste. Egy adott K test néhány résztestének metszete szintén résztest, így K összes résztestének metszete is test; ezt K *prímtestének* nevezzük.

1.2.1. Tétel. *Egy K test prímteste vagy izomorf $\mathbb{F}_p$-vel, vagy $\mathbb{Q}$-val, attól függően, hogy $char(K) = p$ prím vagy $char(K) = 0$.*

Legyen L a K test bővítése, ekkor L egy K feletti vektortér, amelynek a dimenzióját a *bővítés fokának* nevezünk és $|L : K|$-val jelöljük. Ha $|L : K|$ véges, akkor *véges bővítésről* beszélünk, és ekkor igaz, hogy $|L| = |K|^n$, ahol $n = |L : K|$.

1.2.2. Következmény. *Legyen K véges test, ekkor $char(K) = p$ prím és K prímteste $\mathbb{F}_p$, így $|K| = p^n$, ahol $n = |K : \mathbb{F}_p|$.*

Egy M test az $L|K$ bővítés *közbülső teste*, ha fennáll $K \subseteq M \subseteq L$. Ha $L|K$ véges bővítés közbülső teste M, akkor $K|M$ és $M|L$ is véges, és $|K : L| = |K : M||M : L|$.

1.2.3. Definíció. Legyen L test, K egy részteste, A pedig tetszőleges részhalmaza L-nek. Ekkor K-nak A-val való bővítése, $K(A)$ az L olyan résztesteinek metszete, amelyek tartalmazzák K-t és A-t is. Ha $A = \{\alpha_1, \ldots, \alpha_n\}$ véges, akkor $K(A) = K(\alpha_1, \ldots, \alpha_n)$ jelölést használjuk. Az egy elemmel való bővítést *egyszerű bővítésnek* nevezzük.

1.2.4. Definíció. Legyen $L|K$, $\alpha \in L$. Ekkor α *algebrai* elem K fölött, ha létezik olyan nemnulla $f \in K[x]$ polinom, hogy $f(\alpha) = 0$. Ha nincs ilyen polinom, akkor α *transzcendens* K fölött. Az $L|K$ bővítés *algebrai*, ha minden $\alpha \in L$ algebrai K fölött.

Legyen $L|K$, és $\alpha \in L$ algebrai K felett. Ekkor egyértelműen létezik egy olyan $m_\alpha \in K[x]$ legalacsonyabb fokú, normált polinom, amelynek α gyöke. Ezt hívjuk az α K feletti *minimálpolinomjának*. Az α K feletti *fokán* a minimálpolinom fokát értjük, és $\deg_K \alpha$-val jelöljük. Tetszőleges $f \in K[x]$-re $f(\alpha) = 0 \Leftrightarrow m_\alpha \mid f$. Továbbá, m_α irreducibilis $K[x]$-ben és ha $f \in K[x]$ olyan, hogy $f(\alpha) = 0$ és f irreducibilis, akkor $f = cm_\alpha$ valamely $c \in K$-ra.

1.2.5. Tétel. *Legyen $\alpha \in L$ algebrai K felett és m_α minimálpolinomja n-ed fokú. Ekkor teljesül, hogy $|K(\alpha) : K| = n$ és az $\{1, \alpha, \ldots \alpha^{n-1}\}$ bázis a K feletti $K(\alpha)$ vektortérben.*

Ha $L|K$ bővítés véges, akkor algebrai, és minden $\alpha \in L$-re $\deg_K \alpha$ osztja $|L : K|$-t.

1.2.6. Tétel. *Legyen K test, $f \in K[x]$ irreducibilis polinom. Legyen $L = K[x]/(f)$ és $\alpha \in L$ olyan, hogy $\alpha \equiv x \bmod (f)$. Ekkor:*

(i) *L test;*

(ii) *$L|K$ egyszerű algebrai bővítés;*

(iii) *$L = K(\alpha)$;*

(iv) *$m_\alpha = cf$ alkalmas $c \in K$-val.*

1.2.7. Tétel. *Legyen $f \in K[x]$ irreducibilis polinom K felett, és $f(\alpha) = f(\beta) = 0$. Ekkor van olyan $\varphi : K(\alpha) \to K(\beta)$ izomorfizmus, amelyre $\varphi(\alpha) = \beta$ és minden $k \in K$-ra $\varphi(k) = k$.*

1.2.8. Példa. Legyen a test $\mathbb{F}_2$, amely felett az $x^3 + x + 1$ polinom irreducibilis. Legyen $\alpha \equiv x \bmod (x^3 + x + 1)$, ekkor $\mathbb{F}_2/(x^3 + x + 1) = \mathbb{F}_2(\alpha)$. A test elemei $0, 1, \alpha, \alpha + 1, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1$.

1.2.9. Definíció. Legyen $L|K$ és $0 \neq f \in K[x]$. Azt mondjuk, hogy L az f egy *felbontási teste K felett*, ha $\exists\, c \in K$ és $\exists\, \alpha_1, \ldots, \alpha_n$, hogy $f = \prod_{i=1}^{n} c(x - \alpha_i)$ és $L = K(\alpha_1, \ldots, \alpha_n)$.

1.2.10. Tétel. *Ha K test és $0 \neq f \in K[x]$, akkor létezik az f-nek felbontási teste K felett. Továbbá f-nek bármely két K feletti felbontási teste között megadható olyan izomorfizmus, amely K-t fixen hagyja, és f gyökeit egymásba képezi.*

Mivel a felbontási testek izomorfak, ezért beszélhetünk az f felbontási testéről K felett. Mivel f K feletti felbontási teste véges bővítése K-nak, ezért algebrai bővítés is.

2. fejezet

Véges testek

Jelen fejezetben részletesebben is megismerkedünk a véges testek struktúrájával. A fejezet megírásában segítségemre volt az [1] és a [2] irodalom.

Az első szakaszban a véges testek létezéséről és egyértelműségéről lesz szó. Egy véges test konstruálása során irreducibilis polinomokat használunk, így ezek néhány fontos tulajdonságát is tárgyaljuk. A második szakaszban körosztási testekről lesz szó, melyek segítségével szintén alkothatunk véges testeket. A harmadik szakaszban összefoglalom és példákkal illusztrálom a véges testek szerkezetéről szóló ismereteket. A negyedik szakaszban a véges testek feletti polinomok néhány tulajdonságáról lesz szó, ami segít a véges testek struktúrájának tanulmányozásában.

2.1. Véges testek alaptulajdonságai

Egy testet - mint ahogy csoportoknál és gyűrűknél - *végesnek* nevezünk, ha elemszáma véges. Wedderburn tétele szerint minden véges ferde test kommutatív is, tehát test. Véges testekre korábban végtelen sok példát láttunk, minden p prímre a $\mathbb{Z}/(p)$ maradékosztály gyűrű test. Legyen most F véges test, ekkor F prímteste $\mathbb{F}_p$, és így $|F| = p^n$ valamely p prímre és n pozitív egészre. Azt is láttuk, hogy ha $f \in \mathbb{F}_p[x]$ egy n-ed fokú irreducibilis polinom, akkor $\mathbb{F}_p[x]/(f)$ at $\mathbb{F}_p$ n-ed fokú bővítése, és így p^n elemszámú test. Kérdés, hogy van-e minden n-re n-ed fokú irreducibilis polinom $\mathbb{F}_p$ felett. Ehhez előbb másként konstruálunk véges testeket.

2.1.1. Állítás. *Ha F egy q elemszámú test, akkor minden $a \in F$-re $a^q = a$ teljesül.*

2.1.2. Állítás. *Ha F egy q elemszámú test, K részteste F-nek, akkor $K[x]$-beli $x^q - x$ polinom elsőfokú polinomok szorzatára bomlik, méghozzá $x^q - x = \prod_{a \in F}(x - a)$. Sőt az is igaz, hogy F az $x^q - x$ polinom felbontási teste K felett.*

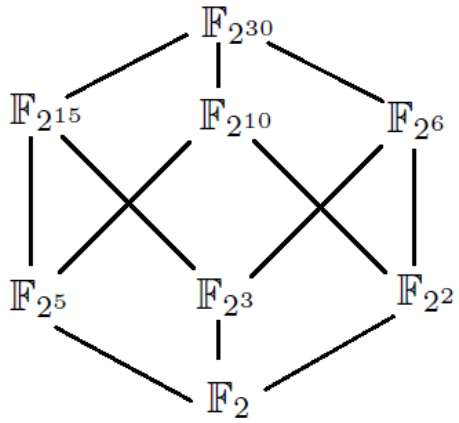
2.1.3. Tétel. *Minden p prímre és minden n pozitív egészre létezik p^n elemszámú test. Bármely $q = p^n$ elemszámú test izomorf az $x^q - x$ polinom $\mathbb{F}_p$ feletti felbontási testével.*

Tehát beszélhetünk a q elemű testről. Ezeket $\mathbb{F}_q$-val jelöljük és q rendű *Galois-testnek* nevezzük.

2.1.4. Tétel. *Legyen $q = p^n$ és K az $\mathbb{F}_q$ test részteste. Ekkor van olyan m, hogy m osztja n-et és $|K| = p^m$. Megfordítva, ha $m \mid n$, akkor $\mathbb{F}_q$-nak pontosan egy p^m elemű részteste van.*

Bizonyítás. A K prímteste szintén $\mathbb{F}_p$, így $|K| = p^m$ alkamas m-mel. Megfordítva ha m osztja n-et, akkor p^{m-1} osztja p^{n-1}-et, így $x^{p^{m-1}} - 1$ osztja $x^{p^{n-1}} - 1$-et, tehát $x^{p^m} - x$ osztja $x^{p^n} - x$-et $\mathbb{F}_p[x]$-ben. Így $x^{p^m} - x$ minden gyöke, $x^q - x$-nek is gyöke, azaz $x^{p^n} - x$ $\mathbb{F}_p$ feletti felbontási teste része $\mathbb{F}_q$-nak, tehát $\mathbb{F}_{p^n} | \mathbb{F}_{p^m}$. Az egyértelműséget indirekt bizonyíthatjuk. Ha lenne az $\mathbb{F}_q$-nak két különböző részteste amiknek az elemszáma p^m, akkor ebben a két testben az $x^{p^m} - x \in \mathbb{F}_q[x]$ polinomnak p^m-nél több gyöke lenne, ami ellentmondás. □

2.1.5. Példa. Az alábbi ábrán a $\mathbb{F}_{2^{30}}$ résztestei láthatók.



Az $\mathbb{F}_q$ test nemnulla elemeinek multiplikatív csoportját jelölje $\mathbb{F}_q^*$.

2.1.6. Állítás. *Minden véges $\mathbb{F}_q$ testnek $\mathbb{F}_q^*$ multiplikatív csoportja ciklikus.*

Az $\mathbb{F}_q^*$ csoport egy generátorát az $\mathbb{F}_q$ *primitív elemének* nevezzük. Tudjuk, hogy $\mathbb{F}_q$-nak $\varphi(q-1)$ primitív eleme van. A primitív elem segítségével beláthatjuk, hogy minden véges test bármely résztestének egyszerű bővítése. Ugyanis legyen $\mathbb{F}_r$ az $\mathbb{F}_q$ bővítése. Ekkor $\mathbb{F}_r$ tetszőleges α primitív elemével $\mathbb{F}_r = \mathbb{F}_q(\alpha)$. Ha $r = q^n$, akkor m_α egy n-ed fokú irreducibilis polinom, így minden véges $\mathbb{F}_q$ testre és minden pozitív egész n-re létezik $f \in \mathbb{F}_q[x]$ n-ed fokú irreducibilis polinom.

A továbbiakban véges test feletti irreducibilis polinomok gyökeiről lesz szó. Legyen f irreduciblis polinom, és legyen α az f tetszőleges gyöke. Ekkor α minimálpolinomja konstansszorosa f-nek, így igaz a következő állítás:

2.1.7. Lemma. *Legyen f az $\mathbb{F}_q$ véges test felett irreducibilis polinom és legyen α olyan, hogy $f(\alpha) = 0$. Ekkor tetszőleges $h \in \mathbb{F}_q[x]$ esetén $h(\alpha) = 0$ pontosan akkor teljesül, ha f osztja h-t.*

2.1.8. Lemma. *Legyen f m-ed fokú irreducibilis polinom $\mathbb{F}_q$ felett. Ekkor f pontosan akkor osztja az $x^{q^n} - x$ polinomot, ha m osztja n-et.*

Bizonyítás. Tegyük fel, hogy f osztja az $x^{q^n} - x$ polinomot, és legyen α at f gyöke. Ekkor α gyöke az $x^{q^n} - x$-nek is, így $\alpha \in \mathbb{F}_{q^n}$. Ekkor viszont $\mathbb{F}_q(\alpha) \subseteq \mathbb{F}_{q^n}$, és mivel $|\mathbb{F}_q(\alpha) : \mathbb{F}_q| = m$ és $|\mathbb{F}_{q^n}| = n$, így m osztja n-et. Most tegyük fel, hogy m osztja n-et. Ekkor $\mathbb{F}_{q^n}$ a 2.1.4 tétel szerint résztestként tartalmazza $\mathbb{F}_{q^m}$-et. Legyen α az f gyöke, ekkor $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$, így $\alpha \in \mathbb{F}_{q^n}$. Következésképpen α gyöke $x^{q^n} - x$-nek, ezért a 2.1.7 alapján f osztja $x^{q^n} - x$-et. □

2.1.9. Tétel. *Legyen f egy m-ed fokú irreducibilis polinom $\mathbb{F}_q$ felett és $f(\alpha) = 0$. Ekkor f minden gyöke egyszeres, és gyökei az $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$, m darab különböző elem.*

Bizonyítás. Legyen $f(x) = \sum_{i=1}^{m} a_i x^i$, ahol $a_i \in \mathbb{F}_q$, és legyen $\beta \in \mathbb{F}_{q^m}$ gyöke f-nek. Felhasználva, hogy $a_i^q = a_i$, és egy p karakterisztikájú testben lehet egy összeget tagonként p^s-edik hatványra emelni, kapjuk, hogy $f(\beta^q) = \sum_{i=1}^{m} a_i \beta^{qi} = \sum_{i=1}^{m} (a_i \beta^i)^q = (\sum_{i=1}^{m} a_i \beta^i)^q = f(\beta)^q = 0$. Tehát az $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ elemek mindegyike gyöke f-nek. Azt kell már csak belátni, hogy különbözőek. Ehhez indirekt tegyük fel, hogy $\alpha^{q^j} = \alpha^{q^k}$ teljesül $0 \leq j < k \leq m-1$-re. Az egyenletet $q^m - k$-adik hatványra emelve adódik, hogy $\alpha^{q^m - k + j} = \alpha^{q^m} = \alpha$, ezért a 2.1.7 szerint f osztja az $x^{m-k+j} - x$ polinomot, de ekkor a 2.1.8 miatt m osztja az $m - k + j$ számot. Viszont $0 < m - k + j < m$, így ellentmondásra jutottunk. □

2.1.10. Definíció. Legyen $\mathbb{F}_{q^m}$ az $\mathbb{F}_q$ bővítése, és $\alpha \in \mathbb{F}_{q^m}$. Az $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ elemeket az α elem $\mathbb{F}_q$-ra vonatkozó *konjugáltjainak* nevezzük.

Az $\alpha \in \mathbb{F}_{q^m}$ elem $\mathbb{F}_q$-ra vonatkozó konjugáltjai pontosan akkor különbözők, ha α minimálpolinomjának foka m. Különben, ha m_α foka d, akkor az $\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}$ elemek különbözők és mindegyik $\frac{m}{d}$-szer szerepel. Könnyen láthahtó, hogy a konjugáltság az ekvivalencia reláció, így beszélhetünk a véges test *konjugáltosztályairól*. Egy osztályban pontosan azok az elemek szerepelnek, amelyek minimálpolinomja közös.

2.1.11. Tétel. *Az $\alpha \in \mathbb{F}_q^*$ elem az $\mathbb{F}_q$ bármely résztestére vonatkozó konjugátjai azonos rendűek.*

Bizonyítás. Az állítás abból következik, hogy $\mathbb{F}_q^*$ ciklikus csoport, melynek rendje $q-1$, ami relatív prím az $\mathbb{F}_q$ test karakterisztikájához. $\square$

2.1.12. Következmény. *Ha α az $\mathbb{F}_q$ test primitív eleme, akkor az $\mathbb{F}_q$ bármely résztestére vonatkozó konjugátjainak a rendje megegyezik.*

2.1.13. Példa. Legyen $\alpha \in \mathbb{F}_{27}$ az $f(x) = x^3 + 2x + 1 \in \mathbb{F}_3[x]$ irreducibilis polinom gyöke. Ekkor az α elem $\mathbb{F}_3$-ra vonatkozó konjugáltjai α, $\alpha^3 = \alpha + 2$ és $\alpha^9 = \alpha + 1$, és mindegyik az $\mathbb{F}_{27}$ test primitív eleme. Az α elem $\mathbb{F}_9$-re vonatkozó konjugáltjai α és $\alpha^9 = \alpha + 1$.

2.2. Egységgyökök és körosztási polinomok

Ebben a szakaszban az $x^n - 1$ polinom felbontási testét vizsgáljuk egy tetszőleges K test felett.

2.2.1. Definíció. Legyen n pozitív egész, K test. Az $x^n - 1$ polinom K feletti felbontási testét K feletti n-edik *körosztási testnek* nevezzük, és $K^{(n)}$-nel jelöljük. Az $x^n - 1$ gyökeit K feletti *n-edik egységgyöknek* nevezzük, ezek halmazát $E^{(n)}$-nel jelöljük.

Ha $K = \mathbb{Q}$, akkor $K^{(n)}$ éppen a már jól ismert komplex n-edik egységgyökök halmaza. A továbbiakban főleg véges testek feletti egységgyököket vizsgálunk.

2.2.2. Tétel. *Legyen n pozitív egész, K p karakterisztikájú test. Ekkor:*

(i) Ha p nem osztja n-et, akkor $E^{(n)}$ a $K^{(n)}$-beli szorzással n-ed rendű ciklikus csoport.

(ii) Ha p osztja n-et, akkor $n = mp^k$, ahol m és k pozitív egészek és p nem osztja m-et. Ekkor $K^{(n)} = K^{(m)}$, $E^{(n)} = E^{(m)}$ és $x^n - 1$ gyökei az $E^{(m)}$ elemei, p^k multiplicitással.

Bizonyítás.

(i) Ha $n = 1$, akkor $E^{(n)} = \{1\}$, ami nyilván ciklikus csoport. Legyen tehát $n \geq 2$, ekkor $x^n - 1$-nek nincs többszörös gyöke, ugyanis a deriváltjának, nx^{n-1}-nek, csak a 0 a gyöke, ami $x^n - 1$-nek nem gyöke. Így $E^{(n)}$-nek n különböző eleme van. Az $E^{(n)}$ csoport, ugyanis $1 \in E^{(n)}$, és ha ε, $\eta \in E^{(n)}$, akkor $(\varepsilon\eta^{-1})^n =$

$\varepsilon^n(\eta^n)^{-1} = 1$, tehát $E^{(n)}$ zárt a szorzásra és az inverz képzésre. Továbbá $E^{(n)}$ ciklikus, mert a $K^{(n)}$ multiplikatív csoportjának részcsoportja, ami véges test lévén ciklikus.

(ii) Rögtön következik (i)-ből és az $x^n - 1 = x^{mp^k} - 1 = (x^m - 1)^{p^k}$ egyenlőségből.

□

2.2.3. Definíció. Legyen K egy p karakterisztikájú test, és n olyan pozitív egész, ami nem osztható p-vel. Ekkor az $E^{(n)}$ ciklikus csoport egy generátorát K feletti *primitív n-edik egységgyöknek* nevezzük.

A primitív n-edik egységgyökök száma $\varphi(n)$ és ha ε primitív n-edik egységgyök, akkor a primitív n-edik egységgyökök halmaza $\{\varepsilon^k | 1 \leq k \leq n, \text{lnko}(k,n) = 1\}$.

2.2.4. Definíció. Legyen K egy p karakterisztikájú test, és n olyan pozitív egész, ami nem osztható p-vel, és ε egy K feletti primitív n-edik egységgyök. Ekkor a

$$\Phi_n(x) = \prod_{\substack{k=1 \\ \text{lnko}(n,k)}}^{n} (x - \varepsilon^k)$$

polinomot *n-edik körosztási polinomnak* nevezzük.

A definícióból rögtön adódik, hogy $\Phi_n(x) \in K^{(n)}[x]$ gyökei a primitív n-edik egységgyökök egyszeres multiplicitással, így a foka $\varphi(n)$. De ennél több is igaz:

2.2.5. Tétel. *Legyen K egy p prím karakterisztikájú test, és n olyan pozitív egész, ami nem osztható p-vel.Ekkor:*

(i) $x^n - 1 = \prod_{d|n} \Phi_d(x)$;

(ii) $\Phi_n(x)$ *normált polinom, és az együtthatói a K prímtestéből valók, sőt, ha K 0 karakterisztikájú test, akkor az együtthatók egészek.*

Bizonyítás.

(i) Legyen ε n-edik egységgyök K felett, és legyen $d = \frac{n}{\text{lnko(k,n)}}$, ahol $1 \leq k \leq n$. Ekkor egyrészt $d \mid n$, másrészt ε^k primitív d-edik egységgyök. Az $x^n - 1 = \prod_{k=1}^{n}(x - \varepsilon^k)$, itt pontosan a d-edik egységgyökök szerepelnek a szorzatban, és mindegyik pontosan egyszer, vagyis igaz az állítás.

(ii) Teljes indukcióval bizonyítunk. Az $n = 1$ eset igaz, hiszen $\Phi_1(x) = x - 1$. Tegyük fel, hogy $k < n$-re igaz az állítás. Ekkor $\Phi_n(x) = \frac{x^n - 1}{f(x)}$, ahol $f(x) = \prod_{d|n, d<n} \Phi_d(x)$. Az indukciós feltevés miatt f egy-főegyüttható és az együtthatói K prímtestéből, illetve $\mathbb{Z}$-ből valók. Az osztást elvégezve kapjuk, hogy $\Phi_n(x)$-re is teljesül a tétel.

□

2.2.6. Példa. Legyen p prím, k pozitív egész. Ekkor:

$$\Phi_{p^k}(x) = \frac{x^{p^k}-1}{\prod\limits_{d|p^k,\ d<p^k} \Phi_d(x)} = \frac{x^{p^k}-1}{\Phi_1(x)\Phi_p(x)\dots\Phi_{p^{k-1}}(x)} =$$

$$= \frac{x^{p^k}-1}{x^{p^{k-1}}-1} = 1 + x^{p^{k-1}} + x^{2p^{k-1}} + \ldots + x^{(p-1)p^{k-1}}.$$

2.2.7. Tétel. *A $K^{(n)}$ körosztási test egyszerű algebrai bővítése K-nak, sőt:*

(i) Ha $K = \mathbb{Q}$, akkor Φ_n körosztási polinom irreducibilis K felett és $|K^{(n)} : K| = \varphi(n)$.

(ii) Ha $K = \mathbb{F}_q$ és $\mathrm{lnko}(q, n) = 1$, akkor Φ_n $\frac{\varphi(n)}{d}$ különböző d-ed fokú irreducibilis normált polinomok szorzatára bomlik $\mathbb{F}_q[x]$-ben. Az $\mathbb{F}_q^{(n)}$ bármelyik ilyen irreducibilis tényező $\mathbb{F}_q$ feletti felbontási teste, és $|\mathbb{F}_q^{(n)} : \mathbb{F}_q| = d$, ahol d a legkisebb olyan pozitív egész, amire $q^d \equiv 1 \bmod n$ teljesül.

Bizonyítás. Ha létezik ε primitív n-edik egyéggyök K felett, akkor $K^{(n)} = K(\varepsilon)$, egyébként a 2.2.2 tétel szerint $K^{(n)} = K^{(m)}$, így ez az eset visszavezetődik az előzőre. A tétel második feléből csak (ii)-t bizonyítjuk. Mivel $\mathrm{lnko}(q, n) = 1$, ezért létezik ε primitív n-edik egységgyök $\mathbb{F}_q$ felett. Az $\varepsilon \in \mathbb{F}_{q^k}$ pontosan akkor teljesül, ha gyöke az $x^{q^k} - x$ polinomnak, azaz $\varepsilon^{q^k} = \varepsilon$, ami azzal ekvivalens, hogy $q^k \equiv 1 \bmod n$, mert ε primitív n-edik egységgyök. A legkisebb ilyen k, amire teljesül az állítás, éppen d, tehát $\varepsilon \in \mathbb{F}_{q^d}$, de $\mathbb{F}_{q^d}$ semelyik valódi résztestében nincs benne. Tehát ε minimálpolinomja $\mathbb{F}_q$ felett d-ed fokú, és mivel ε tetszőleges gyöke volt $\Phi_n(x)$-nek, ezért m_ε osztja $\Phi_n(x)$-et. □

2.2.8. Példa. Legyen $K = \mathbb{F}_{11}$ és $\Phi_{12}(x) = x^4 - x^2 + 1 \in \mathbb{F}_{11}[x]$. Az előző tétel jelöléseit használva $d = 2$, és $\mathbb{F}_{11}$ felett a következőképpen bomlik irreducibilis polinomok szorzatára: $\Phi_{12}(x) = (x^2 + 5x + 1)(x^2 - 5x + 1)$. Továbbá a $\mathbb{F}_{11}^{(12)}$ körosztási test izomorf $\mathbb{F}_{121}$-gyel.

2.2.9. Tétel. *Az $\mathbb{F}_q$ véges test előáll bármely részteste feletti $q-1$-edik körosztási testeként.*

Bizonyítás. Az $x^{q-1} - 1$ polinom gyökei éppen az $\mathbb{F}_q$ nemnulla elemei, így felbomlik elsőfokúak szorzatára $\mathbb{F}_q$-ban, viszont bármely valódi résztestében biztosan nem bomlik fel. □

Az $\mathbb{F}_q^*$ egy $q-1$ rendű ciklikus csoport, így $q-1$ minden pozitív n osztójára egyértelműen létezik $\mathbb{F}_q^*$-nak n rendű ciklikus részcsoportja. Ennek a ciklikus részcsoportnak az elemei pont az n-edik egységgyökök $\mathbb{F}_q$ bármely részteste felett, generátorai pedig a primitív n-edik egységgyökök $\mathbb{F}_q$ bármely részteste felett.

2.2.10. Lemma. *Ha d az n pozitív egész olyan osztója, amire teljesül, hogy $1 \leq d < n$, akkor $\Phi_n(x)$ osztja az $\frac{x^n-1}{x^d-1}$ polinomot, amennyiben $\Phi_n(x)$ definiálva van.*

Bizonyítás. A 2.2.5 tétel (i) részéből tudjuk, hogy $\Phi_n(x) \mid x^n-1$, továbbá $x^n-1 = (x^d-1) \cdot \frac{x^n-1}{x^d-1}$. Viszont az x^d-1 és a $\Phi_n(x)$ polinomoknak nincs közös gyöke, ugyanis előbbi gyökei a d-edik egységgyökök, utóbbi gyökei pedig a primitív n-edik egységgyökök, így $\Phi_n(x)$ feltétlenül osztja $\frac{x^n-1}{x^d-1}$-et. □

2.3. Véges test elemeinek reprezentálása

Most a véges testek elemeinek reprezentálására három különböző módot mutatunk. A továbbiakban feltesszük, hogy p prím, n pozitív egész és $q = p^n$.

Az első – már említett – módszer, hogy $\mathbb{F}_q$ egyszerű algebrai bővítése $\mathbb{F}_p$-nek. Ha $f \in \mathbb{F}_p[x]$ egy n-ed fokú irreducibilis polinom, amelynek gyöke α, akkor $\mathbb{F}_q = \mathbb{F}_p(\alpha)$. Ekkor $\mathbb{F}_q$ elemei pontosan az $a_0 + a_1\alpha + a_2\alpha^2 + \ldots + a_{n-1}\alpha^{n-1}$ alakú számok, ahol $a_i \in \mathbb{F}_p$. Illetve tekinthetjük $\mathbb{F}_q$-t, mint az $\mathbb{F}_p[x]/(f)$ maradékosztály gyűrűt.

2.3.1. Példa. Az $\mathbb{F}_9$ elemeit tekinthetjük, mint az $\mathbb{F}_3$ egyszerű algebrai bővítését az x^2+1 irreducibilis polinom egy α gyökével. Így $\mathbb{F}_9 = \{0, 1, 2, \alpha, 1+\alpha, 2+\alpha, 2\alpha, 1+2\alpha, 2+2\alpha\}$. A számolásoknál figyelembe veszzük, hogy $\alpha^2+1 = 0$, így például $(2+2\alpha)(2+\alpha) = 1+2\alpha^2 = 2$.

A második lehetőség a véges testek reprezentálásásra a 2.2.7 és a 2.2.9 tételeken alapul. Az $\mathbb{F}_q$ test az $\mathbb{F}_p$ test $q-1$-edik körosztási teste, amit megkonstruálhatunk a $\Phi_{q-1}(x) \in \mathbb{F}_p[x]$ körosztási polinom azonos fokú irreducilis polinomok szorzatára bontásával. Bármely ilyen tényező egy tetszőleges gyöke $q-1$-edik primitív egységgyök $\mathbb{F}_p$ felett, így primitív eleme $\mathbb{F}_q$-nak. Tehát $\mathbb{F}_q$ ezen elem hatványaiból és a 0-ból áll.

2.3.2. Példa. Tehát $\mathbb{F}_9 = \mathbb{F}_3^{(8)}$, a nyolcadik körosztási test $\mathbb{F}_3$ felett. A 2.2.6 példa alapján $\Phi_8(x) = x^4+1$ irreducibils tényezőkre bontása $\Phi_8(x) = (x^2+x+2)(x^2+2x+2)$. Legyen ε az x^2+2x+2 polinom gyöke, ekkor ε primitív nyolcadik egységgyök $\mathbb{F}_3$ felett. Tehát $\mathbb{F}_9 = \{0, \varepsilon, \varepsilon^2, \varepsilon^3, \varepsilon^4, \varepsilon^5, \varepsilon^6, \varepsilon^7, \varepsilon^8\}$. Ezt az előző példával összevetve, azt kapjuk, hogy az x^2+2x+2 polinom egy gyöke az $\varepsilon = \alpha+2$. Így $\mathbb{F}_9$ nemnulla elemei a következők:

i	ε^i	i	ε^i
1	$\alpha+2$	5	$2\alpha+1$
2	α	6	2α
3	$2\alpha+2$	7	$\alpha+1$
4	2	8	1

Természetesen ugyanazokat az elemeket kapjuk vissza, csak más sorrendben. Az is látszik, hogy az α elem rendje 4, tehát nem primitív nyolcadik egységgyök, de $\mathbb{F}_3(\alpha) = \mathbb{F}_3(\varepsilon)$.

A harmadik lehetőség a véges test elemeinek mátrixokkal való reprezentálása. Ha $f = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ normált polinom, akkor a kísérő mátrixa a következő $n \times n$-es mátrix:

$$\mathbf{A} = \begin{pmatrix} 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & \ldots & 0 & -a_1 \\ 0 & 1 & \ldots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & -a_0 \end{pmatrix}$$

Ekkor lineáris algebrából ismert, hogy $f(\mathbf{A}) = a_0\mathbf{I} + a_1\mathbf{A} + a_2\mathbf{A}^2 + \ldots + a_{n-1}\mathbf{A}^{n-1} + \mathbf{A}^n = 0$. Így, ha $\mathbf{A}$ egy f n-ed fokú, normált, $\mathbb{F}_p$ felett irreducibilis polinom kísérő mátrixa, akkor $\mathbf{A}$-t tekinthetjük f egy gyökének. Az $\mathbf{A}$ legfeljebb $n-1$-ed fokú polinomjai pedig az $\mathbb{F}_q$ test elemei.

2.3.3. Példa. (i) Ahogyan a 2.3.1 példában, legyen $f(x) = x^2+1 \in \mathbb{F}_3[x]$, Ekkor f kísérő mátrixa:

$$\mathbf{A} = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$$

Az $\mathbb{F}_9$ test elemeit a következőképpen reprezentálhatjuk $\mathbb{F}_9 = \{\mathbf{0}, \mathbf{I}, 2\mathbf{I}, \mathbf{A}, \mathbf{I}+\mathbf{A}, 2\mathbf{I}+\mathbf{A}, 2\mathbf{A}2\mathbf{I}+2\mathbf{A}, 2\mathbf{I}+2\mathbf{A}\}$. A számolási szabályok megegyeznek az $\mathbb{F}_3$ test feletti mátrixok szokásos számolási szabályaival, például:

$$(2\mathbf{I}+2\mathbf{A})(2\mathbf{I}+\mathbf{A}) = \begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix}\begin{pmatrix} 2 & 2 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = 2\mathbf{I}.$$

(ii) A számolást megkönnyíti, ha nem az x^2+1, hanem az x^2+2x+2 irreducibilis polinom kísérő mátrixát tekintjük, ugyanis ennek tetszőleges gyöke primitív eleme $\mathbb{F}_9$-nek, így a kisérő mátrix hatványai lesznek a nemnulla elemek. Tehát a kísérő mátrix a következő:

$$\mathbf{C} = \begin{pmatrix} 0 & 2 \\ 1 & 2 \end{pmatrix}$$

és $\mathbb{F}_9 = \{0, \mathbf{C}, \mathbf{C}^2, \mathbf{C}^3, \mathbf{C}^4, \mathbf{C}^5, \mathbf{C}^6, \mathbf{C}^7, \mathbf{C}^8\}$

Az eddigi eredmények összefoglalásaként nézzünk meg egy példát!

2.3.4. Példa. Konstruáljuk meg a 16 elemű testet, majd határozzuk meg az $\mathbb{F}_2$ feletti konjugált osztályokat, illetve a minimálpolinomokat is!

Először meghatározzuk $\Phi_{15}(x)$-et.

$$x^{15} - 1 = \Phi_{15}(x)\Phi_5(x)\Phi_3(x)\Phi_1(x) = \Phi_{15}(x)\frac{\Phi_5(x)\Phi_1(x)}{\Phi_1(x)}\Phi_3(x)\Phi_1(x)$$

, tehát

$$\Phi_{15}(x) = \frac{(x^{15}-1)(x-1)}{(x^5-1)(x^3-1)} = x^8 + x^7 + x^5 + x^4 + x^3 + x + 1.$$

Ez két negyedfokú, $\mathbb{F}_2$ felett irreducibilis polinom szorzatára bomlik, méghozzá $(x^4 + x + 1)(x^4 + x^3 + 1)$ alakban. Tekintsük az $x^4 + x + 1$ polinomot, amelynek legyen α gyöke. Ekkor α primitív tizenötödik egységgyök. Figyelembe véve, hogy $\alpha^4 = \alpha + 1$, $\mathbb{F}_{16}^*$ elemei a következőképpen reprezentálhatók:

i	1	2	3	4	5	6	7	8
α^i	α	α^2	α^3	$\alpha+1$	$\alpha^2+\alpha$	$\alpha^3+\alpha^2$	$\alpha^3+\alpha+1$	α^2+1

i	9	10	11	12	13	14	15
α^i	$\alpha^3+\alpha$	$\alpha^2+\alpha+1$	$\alpha^+\alpha^2+\alpha$	$\alpha^3+\alpha^2+\alpha+1$	$\alpha^3+\alpha^2+1$	α^3+1	1

A konjugáltosztályok a következők: $C_1 = \{\alpha, \alpha^2, \alpha^4, \alpha^8\}$, $C_3 = \{\alpha^3, \alpha^6, \alpha^{12}, \alpha^9\}$, $C_5 = \{\alpha^5, \alpha^{10}\}$, $C_7 = \{\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}\}$.

Most számoljuk ki a megfelelő minimálpolinomokat!

Azt tudjuk, hogy $m_1(x) = x^4 + x + 1$.

$$m_3(x) = (x-\alpha^3)(x-\alpha^6)(x-\alpha^9)(x-\alpha^{12}) = x^4 + (\alpha^3+\alpha^6+\alpha^9+\alpha^{12})x^3 + (\alpha^3\alpha^6+$$

$$+\alpha^3\alpha^9+\alpha^3\alpha^{12}+\alpha^6\alpha^9+\alpha^6\alpha^{12}+\alpha^9\alpha^{12})x^2+(\alpha^3\alpha^6\alpha^9+\alpha^3\alpha^6\alpha^{12}+\alpha^3\alpha^9\alpha^{12}+\alpha^6\alpha^9\alpha^{12})x+$$

$$+\alpha^3\alpha^6\alpha^9\alpha^{12} = x^4 + (\alpha^3+\alpha^6+\alpha^9+\alpha^{12})x^3 + (\alpha^9+\alpha^{12}+1+1+\alpha^3+\alpha^6)x^2+$$

$$+(\alpha^3+\alpha^6+\alpha^9+\alpha^{12})x + 1 = x^4 + x^3 + x^2 + x + 1$$

Hasonló számolással adódik, hogy $m_5(x) = x^2 + x + 1$ és $m_7(x) = x^4 + x^3 + 1$.

2.4. Véges test feletti polinomok

A véges testek feletti polinomok elmélete fontos szerepet játszik a véges testek struktúrájának vizsgálatában, és számos egyéb alkalmazásban is. Az irreducibilis

polinomok véges testek konstruálásához alapvető fontosságúak. A fejezet jelen szakaszában bevezetjük a polinom rendjének fogalmát. A szakasz végén a primitív elemek minimálpolinomjainak és az adott fokú lehető legmagasabb rendű polinomok kapcsolatát vizsgáljuk.

Egy polinom rendjének definíciója a következő lemmán alapul.

2.4.1. Lemma. *Legyen $f \in \mathbb{F}_q[x]$ $m \geq 1$ fokú polinom és $f(0) \neq 0$. Ekkor létezik egy $e \leq q^m - 1$ pozitív egész, mellyel $f(x)$ osztja $x^e - 1$-et.*

Bizonyítás. Az $\mathbb{F}_q[x]/(f)$ maradékosztály-gyűrű q^m-1 nemnulla elemet tartalmaz. Ha $0 \leq j \leq q^m - 1$, az $x^j + (f)$ maradékoszályok mindegyike nemnulla, és számuk q^m. A skatulya–elv szerint vannak olyan r, s egészek, hogy $0 \leq r < s \leq q^m - 1$, és $x^r \equiv x^s \bmod f(x)$. Mivel x és $f(x)$ relatív prímek, ezért $x^{s-r} \equiv 1 \bmod f(x)$, tehát $f(x)$ osztja $(x^{s-r} - 1)$-et és $0 < s - r \leq q^m - 1$. □

2.4.2. Definíció. Legyen $f \in \mathbb{F}_q[x]$ nemnulla polinom. Ha $f(0) \neq 0$, akkor a legkisebb pozitív egész e számot, amelyre teljesül, hogy $f(x)$ osztja $x^e - 1$-et, az f polinom *rendjének* nevezzük és $\mathrm{ord}(f)$-fel jelöljük. Ha $f(0) = 0$, akkor f egyértelműen felírható $f(x) = x^k g(x)$ alakban, ahol $g(0) \neq 0$. Ekkor definíció szerint legyen $\mathrm{ord}(f) = \mathrm{ord}(g)$.

Az irreducibilis polinomok rendjét a következő módon jellemezhetjük.

2.4.3. Tétel. *Legyen $f \in \mathbb{F}_q[x]$ egy m-ed fokú irreducibilis polinom $\mathbb{F}_q$ felett és $f(0) \neq 0$. Ekkor* $\mathrm{ord}(f)$ *megegyezik f bármely gyökének az $\mathbb{F}_{q^m}^*$ csoportban vett multiplikatív rendjével.*

Bizonyítás. A 2.1.9 és a 2.1.11 tételek szerint az $\mathbb{F}_{q^m}^*$ csoportban az f bármely gyökének rendje megegyezik. Legyen $\alpha \in \mathbb{F}_{q^m}^*$ az f egy gyöke. Ekkor a 2.1.7 lemma miatt $\alpha^e = 1$ akkor és csak akkor, ha $f(x)$ osztja az $x^e - 1$ polinomot. A definíciók alapján a legkisebb ilyen e az f, és az α rendje. □

2.4.4. Következmény. *Ha $f \in \mathbb{F}_q[x]$ m-ed fokú irreducibilis polinom $\mathbb{F}_q$ felett, akkor* $\mathrm{ord}(f)$ *osztja $(q^m - 1)$-et.*

Bizonyítás. Ha $f(x) = cx$, ahol $c \in \mathbb{F}_q^*$, akkor $\mathrm{ord}(f) = 1$. Különben a 2.4.3 tétel és $|\mathbb{F}_{q^m}^*| = q^m - 1$ miatt igaz az állítás. □

Később látunk rá példát, hogy reducibilis polinomokra a következmény nem szükségképpen igaz. Az előző tétel alapján megszámolhatjuk egy adott fokú és adott rendű normált irreducibilis polinomok számát. Használjuk a következő elnevezést. Ha n pozitív egész és b egész, továbbá n és b relatív prímek, akkor a legkisebb olyan k-t, amire teljesül, hogy $b^k \equiv 1 \bmod n$, a b *multiplikatív rendjének* hívjuk modulo n.

2.4.5. Tétel. *Az $\mathbb{F}_q$ feletti m fokú, e rendű, normált, irreducibilis polinomok száma:*

(i) $\frac{\varphi(e)}{m}$, *ha* $e \geq 2$ *és* m *a* q *multiplikatív rendje modulo* e;

(ii) 2, *ha* $m = e = 1$;

(iii) 0 *minden más esetben.*

Bizonyítás. Legyen $f \in \mathbb{F}_q[x]$ irreducibilis polinom és $f(0) \neq 0$. Ekkor a 2.4.3 tétel szerint $\mathrm{ord}(f) = e$ akkor és csak akkor, ha f minden gyöke primitív e-edik egységgyök $\mathbb{F}_q$ felett. Tehát $\mathrm{ord}(f) = e$ pontosan akkor teljesül, ha f osztja a Φ_e körosztási polinomot. A 2.2.7 tétel (ii) része miatt Φ_e bármely irreducibilis tényezőjének a foka m, ahol m a q multiplikatív rendje modulo e, és a különböző irreducibilis tényezők száma pontosan $\frac{\varphi(e)}{m}$. Az $m = e = 1$ esethez hozzá kell még venni az $f(x) = x$ polinomot is. □

Mivel minden pozitív fokú polinomot felírhatunk irreducibilis polinomok szorzataként, egy polinom rendjét kiszámíthatjuk, ha tudjuk egy irreducibilis polinom bármely hatványának rendjét, és a páronként relatív prím polinomok szorzatának rendjét.

2.4.6. Lemma. *Legyen c pozitív egész, $f \in \mathbb{F}_q[x]$, melyre $f(0) \neq 0$. Ekkor f pontosan akkor osztja az $x^c - 1$ polinomot, ha* $\mathrm{ord}(f)$ *osztja c-t.*

Bizonyítás. Tegyük fel, hogy $\mathrm{ord}(f) = e$ osztja c-t. Ekkor, mivel f osztja $(x^e - 1)$-et és $x^e - 1$ osztja $(x^c - 1)$-et, ezért f osztja $(x^c - 1)$-et. Megfordítva, ha f osztja $(x^c - 1)$-et, akkor $c \geq e$, így $c = me + r$ alakba írható, ahol $m \in \mathbb{N}$ és $0 \leq r < e$. Az $x^c - 1 = (x^{me} - 1)x^r + (x^r - 1)$ egyenlőségből következik, hogy f osztja $(x^r - 1)$-et, ez viszont csak $r = 0$ esetén lehetséges, tehát e osztja c-t. □

2.4.7. Következmény. *Ha e_1 és e_2 pozitív egész számok és* $\mathrm{lnko}(e_1, e_2) = d$, *akkor az $x^{e_1} - 1$ és az $x^{e_2} - 1$ polinomok legnagyobb közös osztója $x^d - 1$.*

Bizonyítás. Legyen $f(x)$ az $x^{e_1} - 1$ és az $x^{e_2} - 1$ polinomok legnagyobb közös osztója. Mivel az $x^{e_1} - 1$ és az $x^{e_2} - 1$ polinomok osztják az $x^d - 1$ polinomot, ezért $x^d - 1$ osztja f-et. Másrészt f az $x^{e_1} - 1$ és az $x^{e_2} - 1$ polinomok közös osztója, így a 2.4.6 lemma miatt $\mathrm{ord}(f)$ osztja e_1-et és e_2-t, így osztja d-t is. Ekkor, ugyancsak a 2.4.6 lemma miatt, f osztja $(x^d - 1)$-et, tehát $f(x) = x^d - 1$. □

2.4.8. Tétel. *Legyen $g \in \mathbb{F}_q[x]$ irreducibilis polinom $\mathbb{F}_q$ felett és $g(0) \neq 0$, továbbá legyen* $\mathrm{ord}(g) = e$ *és $f = g^k$ valamilyen k pozitív egészre. Legyen t a legkisebb olyan egész, amelyre $p^t \geq k$, ahol p a test karakterisztikája. Ekkor* $\mathrm{ord}(f) = ep^t$.

Bizonyítás. Legyen $c = \mathrm{ord}(f)$. Ekkor definíció szerint f osztja $(x^c - 1)$-et, így g is osztja azt, mert $g \mid f$. Ekkor a 2.4.6 lemma szerint e osztja c-t. Mivel g osztja az $x^e - 1$ polinomot, ezért f osztja az $(x^e - 1)^k$ polinomot, sőt $p^t \geq k$ miatt, osztja a $(x^e - 1)^{p^t} = x^{ep^t} - 1$ polinomot is. Ezért ugyancsak a 2.4.6 lemma miatt c osztja ep^t-t. Korábban láttuk, hogy $e \mid c$, így $c = ep^u$ alakú, ahol $0 \leq u \leq t$. A 2.4.4 következmény miatt p nem osztja e-t, így $x^e - 1$-nek csak egyszeres gyökei vannak. Ekkor az $x^{ep^u} - 1 = (x^e - 1)^{p^u}$ polinom minden gyöke p^u multiplicitású. De $g(x)^k$ osztja $(x^{ep^u} - 1)$-et, ezért a gyökök multiplicitása miatt $p^u \geq k$ és így $u \geq t$. Tehát $u = t$ és $c = ep^t$. □

2.4.9. Tétel. *Legyenek $g_1, \ldots, g_k$ páronként relatív prím nemnulla polinomok $\mathbb{F}_q$ felett, és legyen $f = g_1 \ldots g_k$. Ekkor* $\mathrm{ord}(f)$ *megegyezik az* $\mathrm{ord}(g_1), \ldots, \mathrm{ord}(g_k)$ *számok legkisebb közös többszörösével.*

Bizonyítás. Elegendő csak azt az esetet vizsgálni, amikor $g_i(0) \neq 0$ semelyik i-re sem. Legyen $e = \mathrm{ord}(f)$, $e_i = \mathrm{ord}(g_i)$ és az $\mathrm{ord}(g_1), \ldots, \mathrm{ord}(g_k)$ számok legkisebb közös többszöröse c. Mivel minden i-re a g_i osztja $(x^{e_i} - 1)$-et, így mindegyik osztja az $x^c - 1$ polinomot is. Azonban a g_i-k páronként relatív prím polinomok, így f is osztja az $(x^c - 1)$-et. A 2.4.6 lemma miatt kapjuk, hogy e osztja c-t. Másrészt f osztja az $x^e - 1$ polinomot, így mindegyik g_i is osztja azt. Ekkor megint a 2.4.6 lemma miatt mindegyik e_i osztja e-t, így c is osztja e-t. Következésképpen $e = c$. □

2.4.10. Példa. Határozzuk meg az $f(x) = x^{10} + 2x^8 + 2x^7 + x^5 + 2x^4 + x^3 + 2x + 1$ $\mathbb{F}_3$ feletti polinom rendjét!

Az $f(x)$ kanonikus alakja $\mathbb{F}_3$ felett $(x^3 + 2x + 1)^2(x^4 + x^2 + x + 1)$. Az $x^3 + 2x + 1$ polinom rendje 26, így a 2.4.8 tétel szerint $(x^3 + 2x + 1)^2$ rendje $26 \cdot 3^1 = 78$. Az $x^4 + x^2 + x + 1$ polinom rendje 40, így a 2.4.9 tétel alapján $\mathrm{ord}(f) = \mathrm{lkkt}(26, 40) = 1560$. Ez nem osztja a $3^{10} - 1$-et, ami bizonyítja a 2.4.4 következmény utáni megjegyzést.

Hasonló érveléssel adódik, hogy véges sok nemnulla polinom legkisebb közös többszörösének rendje egyenlő a polinomok rendjének legkisebb közös többszörösével. A fentiek segítségével igazolható a következő általános formula a polinomok rendjére:

2.4.11. Tétel. *Legyen $\mathbb{F}_q$ egy p karakterisztikájú test, és $f \in \mathbb{F}_q[x]$ pozitív fokú polinom, melyre $f(0) \neq 0$. Legyen $f = af_1^{b_1} \ldots f_k^{b_k}$, ahol $a \in \mathbb{F}_q$, $b_1, \ldots, b_k \in \mathbb{N}$, és $f_1, \ldots, f_k$ különböző normált irreducibilis polinomok $\mathbb{F}_q[x]$-ben. Ekkor* $\mathrm{ord}(f) = ep^t$, *ahol e az* $\mathrm{ord}(f_1), \ldots, \mathrm{ord}(f_k)$ *számok legkisebb közös többszöröse, és t a legkisebb olyan egész, amire $p^t \geq \max(b_1, \ldots, b_k)$.*

A 2.4.1 lemma és a 2.4.2 definíció alapján egy $m \geq 1$ fokú $\mathbb{F}_q$ feletti polinom rendje legfeljebb $q^m - 1$. A polinomok egy fontos osztályát alkotják azok a polinomok, melyeknek a rendje pontosan $q^m - 1$.

2.4.12. Definíció. Egy $m \geq 1$ fokú $f \in \mathbb{F}_q[x]$ polinomot $\mathbb{F}_q$ feletti *primitív polinomnak* nevezünk, ha az $\mathbb{F}_{q^m}$ test egy primitív elemének az $\mathbb{F}_q$ feletti minimálpolinomja.

A primitív polinomokat a következőképpen jellemezhetjük.

2.4.13. Tétel. *Egy $f \in \mathbb{F}_q[x]$ m-ed fokú polinom akkor és csakis akkor primitív $\mathbb{F}_q$ felett, ha normált, $f(0) \neq 0$ és* $\mathrm{ord}(f) = q^m - 1$.

Bizonyítás. Ha f primitív polinom $\mathbb{F}_q$ felett, akkor normált és $f(0) \neq 0$. Továbbá f irreducibilis, és gyöke $\mathbb{F}_{q^m}$ egyik primitív eleme, így a 2.4.3 tétel szerint $\mathrm{ord}(f) = q^m - 1$.

Megfordítva, mivel $\mathrm{ord}(f) = q^m - 1$, ezért $m \geq 1$. Most megmutatjuk, hogy f irreducibilis $\mathbb{F}_q$ felett. Indirekt tegyük fel, hogy f reducibilis $\mathbb{F}_q$ felett. Ekkor f vagy felírható egy irreducibilis polinom hatványaként, vagy két legalább elsőfokú relatív prím polinom szorzata. Az első esetben $f = g^k$, ahol g irreducibilis $\mathbb{F}_q$ felett és $k \geq 2$. Ekkor a 2.4.8 tétel miatt f rendjét osztja az $\mathbb{F}_q$ test karakterisztikája, ami ellentmondás, mert $(q^m - 1)$-et nem osztja. A második esetben $f = g_1 g_2$, ahol g_1 és g_2 relatív prím normált polinomok $\mathbb{F}_q$ felett m_1 és m_2 pozitív fokokkal. Ha $i = 1$, 2-re $e_i = \mathrm{g_i}$, akkor $\mathrm{ord}(f) \leq e_1 e_2$ a 2.4.9 tétel szerint. Továbbá a 2.4.1 miatt $e_i \leq q^m - 1$, így

$$\mathrm{ord}(f) \leq (q^{m_1} - 1)(q^{m_2} - 1) < q^{m_1 + m_2} - 1 = q^m - 1,$$

ami ellentmondás. Tehát f irreducibilis $\mathbb{F}_q$ felett, ezért a 2.4.3 tételből következik, hogy f primitív polinom $\mathbb{F}_q$ felett. $\square$

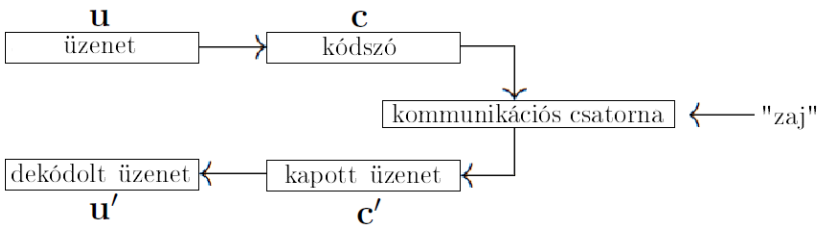
3. fejezet

Kódelmélet

A véges testek egyik legfontosabb alkalmazása a kódelmélet. A fejezetben ismertetem az algebrai kódelmélet alapjait, főként hibajelző és hibajavító kódolásokról lesz szó. Ezek célja az információ hibázó csatornákon történő megbízható átvitele, illetve a hibázó adattárolókon történő megbízható tárolása. Az első szakaszban a lineáris kódokról lesz szó. A második szakasz a lineáris kódok egy fontos osztályáról, a ciklikus kódokról szól. Itt ismertetem a BCH-kódokat és ezek speciális változatát, a Reed–Solomon kódokat. A fejezet megírásához az az [1], a [4], a [6], [7], [5] irodalmat használtam fel.

3.1. Lineáris kódok

A kódelmélet egyik fő feladata, hogy a hibák valószínűségét a lehető legkisebbé tegye. E célból az üzenetet redundáns információval együtt küldjük el. A redundancia teszi lehetővé a hibák észlelését és javítást, így biztosítva az információ védelmét esetleges hibák fellépése esetén. A kommunikációs rendszer egy egyszerű modellje látható az ábrán.



Az üzenet egy k hosszú $\mathbf{u}$ vektor, melynek elemei az F véges forrásábécéből valók. A kódoló az üzenetet egy n hosszú $\mathbf{c}$ vektorba, a kódszóba képezi, melynek elemei a K véges kódábécéből valók. A "zajos" kommunikációs csatornán történő

átvitel során a kódszóban hiba keletkezhet. Az így kapott üzenet egy $\mathbf{c}'$, amelyből a dekódoló egy $\mathbf{u}'$ dekódolt üzenetet kap.

Kódolási sémának nevezünk egy $f : F^k \to K^n$ injektív függvényt. Az $f^{-1} : K^n \to F^k$ függvényt *dekódolási sémának* hívjuk. *Kódon* a kódszavak halmazát értjük, és arra a C, vagy ha a paramétereket is ki akarjuk emelni, akkor a $C(n, k)$ jelölést használjuk. Tehát egy $C(n, k)$ kód nem más, mint K^n egy részhalmaza. A kód átvitele során esetlegesen fellépő hiba azt eredményezheti, hogy a kapott üzenet nem kódszó lesz. A hibajavítás célja, hogy ekkor is ki tudjuk találni az eredeti kódszót, amire a dekódolási sémát alkalmazva megkapjuk az üzenetet. A továbbiakban a dekódolás alatt csak a hibajavítást értjük, ugyanis a kódolási séma egyértelműen meghatározza a dekódolási sémát. Az algebrai hibajavító kódolás alapvető fogalma a következő.

3.1.1. Definíció. Legyen $\mathbf{u}, \mathbf{v} \in K^n$, ekkor $\mathbf{u}$ és $\mathbf{v}$ *Hamming-távolságán* azon i koordináták számát értjük, amelyekre $u_i \neq v_i$. A két vektor Hamming-távolságát $\mathrm{d}(\mathbf{u}, \mathbf{v})$ jelöli.

Könnyen igazolható, hogy a Hamming-távolság valóban metrika, azaz:

3.1.2. Tétel.

- $\mathrm{d}(\mathbf{u}, \mathbf{v}) \geq 0$
- $\mathrm{d}(\mathbf{u}, \mathbf{v}) = 0 \Leftrightarrow \mathbf{u} = \mathbf{v}$
- $\mathrm{d}(\mathbf{u}, \mathbf{v}) = \mathrm{d}(\mathbf{v}, \mathbf{u})$
- $\mathrm{d}(\mathbf{u}, \mathbf{v}) \leq \mathrm{d}(\mathbf{u}, \mathbf{w}) + \mathrm{d}(\mathbf{w}, \mathbf{v})$

Az így kapott metrikus téren a szokásos módon értelmezhetjük a gömb fogalmát. Egy $\mathbf{u}$ körüli t *sugarú gömbön* a $\{\mathbf{v} \in \mathbb{F}_q^n : \mathrm{d}(\mathbf{u}, \mathbf{v}) \leq t\}$ halmazt értjük.

A hibajavításhoz a következő módszert használjuk. A kapott c' üzenet dekódolása során olyan c kódszót keresünk, amire a $\mathrm{d}(\mathbf{c}, \mathbf{c}')$ minimális, ugyanis kevesebb hiba előfordulásának valószínűsége sokkal nagyobb. A minimális távolság meghatározása általában nem egyszerű feladat, ezért speciális alakú kódokat használunk. Egy kód fontos jellemzője, hogy hány hibát tud jelezni, illetve javítani.

3.1.3. Definíció. Egy kód:

- *t-hibajelző*, ha bármely kódszavának legalább egy, de legfeljebb t tetszőleges komponensét megváltoztatva nem kapunk kódszót;
- *t-hibajavító*, ha bármely két különböző kódszó legfeljebb t helyen történő megváltoztatása esetén nem kapjuk ugyanazt a két kódszót.

3.1.4. Definíció. Egy C kód minimális távolságán a $\mathrm{d}_C = \min\limits_{\substack{\mathbf{c}\neq\mathbf{c}'\\ \mathbf{c},\mathbf{c}'\in C}} \mathrm{d}(\mathbf{c},\mathbf{c}')$ számot értjük.

Mind a t-hibajelzés, mind a t-hibajavítás szoros kapcsolatban áll a minimális kódtávolsággal.

3.1.5. Tétel. *Egy C kód pontosan akkor t-hibajelző, ha $\mathrm{d}_C \geq t+1$, és pontosan akkor t-hibajavító, ha $\mathrm{d}_C \geq 2t+1$.*

Bizonyítás. A 3.1.3 definíció alapján a C kód pontosan akkor t-hibajelző, ha bármely kódszótól legfeljebb t távolságra lévő vektorok egyike sem kódszó, így $\mathrm{d}_C \geq t+1$. Hasonlóan C pontosan akkor t hibajavító, ha a kódszavak körüli t sugarú gömbök diszjunktak, így, felhasználva a háromszög-egyenlőtlenséget, kapjuk, hogy $\mathrm{d}_C \geq 2t+1$. $\square$

3.1.6. Példa. (paritásellenőrző kód) Legyen $a_i \in \mathbb{F}_2$ és az elküldendő üzenet $a_1, \ldots, a_k$. Ha $1 \leq i \leq k$, akkor $b_i = a_i$ és legyen b_{k+1} 1, ha $\sum_{i=1}^{k} a_i$ páratlan, és 0, ha páros. A minimális kódtávolság 2, így a kód 1-hibajelző, ezért tegyük fel, hogy legfeljebb csak egy hiba történt. Ha a $b_1, \ldots, b_{k+1}$ kódszóra $\sum_{i=1}^{k+1} b_i$ páros, akkor nem történt hiba, ha páratlan, akkor egy hiba történt. A hibajavítás ezzel a kóddal nem lehetséges.

3.1.7. Példa. (ismétléses kód) Most az elküldendő üzenet egyetlen bit legyen, a hozzá tartozó kódszó pedig az, hogy ezt n-szer megismételjük. Így a minimális kódtávolság n, tehát $n-1$ hibát képes jelezni, és $\left\lfloor \frac{n-1}{2} \right\rfloor$ hibát képes javítani. A dekódolás a következő módon történik: Megkeressük a leggyakrabban előforduló elemet a kódszóban, ez lesz a küldött üzenet. Ha legfeljebb $\left\lfloor \frac{n-1}{2} \right\rfloor$ hiba történt, akkor az elküldendő bit több, mint $\frac{n}{2}$-ször szerepel, így ez a leggyakoribb.

Legtöbbször a forrás- és a kódábécét is ugyanazon az $\mathbb{F}_q$ véges testnek választjuk. Ekkor tekinthetjük a kódszavakat $\mathbb{F}_q^n$-beli n-dimenziós sorvektornak. Ahogy korábban láttuk, a C kód nem más, mint $\mathbb{F}_q^n$ egy részhalmaza. A hibajavítás algebrai módszereit az teszi lehetővé, hogy C-ről azt is megköveteljük, hogy az $\mathbb{F}_q^n$ vektortér lineáris altere legyen. Ez vezet a következő definícióhoz.

3.1.8. Definíció. Legyen $\mathbf{H}$ tetszőleges olyan $\mathbb{F}_q$ feletti $(n-k)\times n$-es mátrix, melynek rangja $n-k$. Definiáljuk C-t a következőképpen: $C := \{\mathbf{c} \in \mathbb{F}_q^n : \mathbf{H}\mathbf{c}^T = 0\}$. Ekkor C-t *lineáris* (n,k) *kódnak* nevezzük, n a *kód hossza*, k pedig a *kód dimenziója*. A C elemei a *kódszavak*, $\mathbf{H}$ a kód *paritásellenőrző mátrixa*. A $q=2$ esetben C-t *bináris kódnak* nevezzük. Ha $\mathbf{H} = (\mathbf{A}, \mathbf{I}_{n-k})$ alakú, akkor C-t *szisztematikus kódnak* nevezzük.

3.1.9. Példa. Legyen $\mathbf{H}$ a következő mátrix $\mathbb{F}_2$ felett:

$$\mathbf{H} = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Adott c_1 és c_2 esetén a $\mathbf{Hc}^T = 0$ egyenletrendszert megoldva kapjuk, hogy $c_3 = c_1$, $c_4 = c_1 + c_2$ és $c_5 = c_2$. Így a kódolási séma a következő: $(u_1, u_2) \mapsto (u_1, u_2, u_1, u_1 + u_2, u_2)$.

Ahogy a példán is látszik, szisztematikus kódoknál a kódolási sémát úgy kapjuk, hogy minden $u_1 \dots u_k$ blokkot kiegészítjük egy $c_{k+1} \dots c_n$ blokkal, így kapjuk a kódszót. Az első k koordinátát *üzenet szegmensnek*, a következő $n-k$ koordinátát *paritás szegmensnek* nevezzük.

Mivel a C lineáris (n, k) kód megegyezik a paritásellenőrző mátrixa magterével, így az egy k dimenziós lineáris altér $\mathbb{F}_q^n$-ben. Legyen $\mathbf{g_1}, \dots, \mathbf{g_k}$ C egy bázisa. Ekkor minden $\mathbf{c} \in C$ egyértelműen előáll $\sum_{i=1}^{k} u_i \mathbf{g_i}$ alakban. A $\mathbf{g_i}$-kből, mint sorvektorokból alkotott $k \times n$-es $\mathbf{G}$ mátrixot a C kód egyik *generátormátrixának* nevezzük. A generátormátrix nem egyértelmű, más bázishoz más generátormátrix tartozik. Ezért általában a C kód generátormátrixán olyan G mátrixot értünk, amelynek sortere C.

A $\mathbf{G}$ mátrix segítségével könnyen el tudunk kódolni egy $\mathbf{u} \in \mathbb{F}_q^k$ üzenetet, ugyanis az $\mathbf{u} \mapsto \mathbf{uG}$ függvény bijektív $\mathbb{F}_q^k$-ból C-be. Így minden $\mathbf{u} \in \mathbb{F}_q^k$-ra $\mathbf{HG}^T\mathbf{u}^T = \mathbf{H}(\mathbf{uG})^T = \mathbf{Hc}^T = 0$, tehát $\mathbf{HG}^T = 0$. Speciálisan, ha $\mathbf{H} = (\mathbf{A}, \mathbf{I}_{n-k})$ alakú, akkor $\mathbf{G} = (\mathbf{I}_k, -\mathbf{A}^T)$.

Korábban szó volt a minimális kódtávolság fogalmának fontosságáról. Ezt nem mindig lehet egyszerűen meghatározni, előfordulhat, hogy bármely két kódszónak a távolságát ki kell hozzá számolni. Viszont lineáris kódok esetén kevesebb számolás is elég. Ehhez vezessük be a következő definíciót.

3.1.10. Definíció. Egy $\mathbf{c} \in C$ kódszó *Hamming-súlyán* a $\mathbf{c}$ nemnulla komponenseinek a számát értjük, és $\mathrm{w}(\mathbf{c})$-vel jelöljük. A C *kód minimum súlya* a nemnulla kódszavak Hamming-súlyának minimuma.

Ha C lineáris kód, akkor bármely két $\mathbf{u}$ és $\mathbf{v}$ kódszó különbsége is kódszó, továbbá $\mathrm{d}(\mathbf{u}, \mathbf{v}) = \mathrm{w}(\mathbf{u} - \mathbf{v})$. Ennek az észrevételnek egy fontos következménye, hogy ha C lineáris kód, akkor $\mathrm{d}_C = \mathrm{w}_C$. A minimális kódtávolság meghatározásához hasznos a következő lemma.

3.1.11. Lemma. *Legyen C lineáris kód, melynek paritásellenőrző mátrixa $\mathbf{H}$. Ekkor $\mathrm{d}_c \geq s + 1$ akkor és csak akkor, ha $\mathbf{H}$ bármely s oszlopa lineárisan független.*

Bizonyítás. Indirekt tegyük fel, hogy $\mathbf{H}$-nak van s lineárisan összefüggő oszlopa. Ekkor van olyan $\mathbf{c} \in C \setminus \{0\}$ vektor, ami legfeljebb csak az s oszlopnak megfelelő koordinátákon nem nulla, és $\mathbf{Hc}^T = 0$. Ekkor $\mathrm{w}(\mathbf{c}) \leq s$ és így $\mathrm{d}(\mathbf{c}) \leq s$, ami ellentmond a $\mathrm{d}(\mathbf{c}) \geq s+1$ feltételnek. Hasonlóan látható be, hogy ha $\mathbf{H}$-nak bármely s oszlopa lineárisan független, akkor nincs olyan $\mathbf{c} \in C \setminus \{0\}$, hogy $\mathbf{Hc}^T = 0$ és $\mathrm{w}(\mathbf{c}) \leq s$. □

Most rátérünk a lineáris kódok dekódolására. Legyen C lineáris (n,k) kód az $\mathbb{F}_q$ test felett, és tekintsük az $\mathbb{F}_q/C$ faktorcsoportot, azaz $\mathbb{F}_q/C$ elemei az $\mathbf{u}+C = \{\mathbf{u}+\mathbf{c} : \mathbf{c} \in C, \mathbf{u} \in \mathbb{F}_q^n\}$ mellékosztályok. Ekkor $\mathbb{F}_q^n$ előáll q^{n-k} mellékosztály uniójaként, ahol minden mellékosztály q^k elemű.

Tegyük fel, hogy a $\mathbf{c}$ kódszó továbbítása után az $\mathbf{u}$ vektort kapjuk. Az $\mathbf{e} = \mathbf{u} - \mathbf{c}$ vektort *hibavektornak* nevezzük. Ekkor minden $\mathbf{e}$ lehetséges hibavektor és $\mathbf{u}$ ugyanabban a mellékosztályban szerepel. A legvalószínűbb hibavektor a legkisebb súlyú az $\mathbf{u}$ mellékosztályában. Minden egyes mellékosztályban keressük meg a legkisebb súlyú elemet, ezt, illetve, ha több ilyen van, akkor az egyiket hívjuk *mellékosztály-vezetőnek*. Készítsünk el egy olyan táblázatot, amelynek az első sora a kódszavakból áll, a további sorai pedig a mellékosztályok. Az első oszlopba a mellékosztály-vezetők kerülnek. Ezek után a kapott $\mathbf{u}$ vektorból kivonva a sorában lévő mellékosztály-vezetőt az elküldött $\mathbf{c}$ kódszót nyerjük.

Az $\mathbf{u}$ mellékosztályának megtalálásához nyújt segítséget az úgynevezett szindróma.

3.1.12. Definíció. Legyen $\mathbf{H}$ a C lineáris (n,k) kód paritásellenőrző mátrixa. Ekkor az $\mathrm{S}(\mathbf{u}) = \mathbf{Hu}^T$ vektort az $\mathbf{u}$ vektor *szindrómájának* nevezzük.

A definícióból rögtön adódik, hogy $\mathbf{u}$ szindrómája pontosan akkor 0, ha $\mathbf{u}$ kódszó. Mivel $\mathbf{u}$ és $\mathbf{v}$ pontosan akkor van egy mellékosztályban, ha a különbségük kódszó, ezért két vektor szindrómája pontosan akkor egyenlő, ha azok ugyanabban a mellékosztályban vannak. Tehát ha a táblázatunkat kiegészítjük a mellékoszályoknak megfelelő szindrómák oszlopával, akkor a következő algoritmussal dekódolhatjuk $\mathbf{c}$-t.

Kiszámoljuk az $\mathrm{S}(u)$ szindrómát, megkeressük a hozzá tartozó mellékosztály-vezetőt, ezt kivonjuk $\mathbf{u}$-ból és így visszanyerjük $\mathbf{c}$-t.

3.1.13. Példa. Legyen C egy bináris $(4,2)$ kód generátormátrixa $\mathbf{G}$, paritásellenőrző mátrixa $\mathbf{H}$, ahol $\mathbf{G} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$, $\mathbf{H} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix}$. Ekkor a következő táblázatot kapjuk:

üzenetek	00	01	10	11	
kódszavak	0000	0101	1011	1110	$\binom{0}{0}$
	0001	0100	1010	1111	$\binom{0}{1}$
	0010	0111	1001	1100	$\binom{1}{0}$
	1000	0011	0110	1101	$\binom{1}{1}$
	mellékosztály-vezetők				szindrómák

Ha a kapott üzenet a $\mathbf{u} = 1010$, akkor megkereshetjük $\mathbf{u}$-t a táblázatban, de ez nagy táblázat esetén időigényes. Ilyenkor egyszerűbb csak a $\mathbf{Hu}^T$ szindrómát kiszámolni, ez jelen esetben $\binom{0}{1}$. Ezután megkeressük a hozzá tartozó mellékosztályvezetőt, itt most 0001. A legvalószínűbb az, hogy az eredeti kódszó az $1011 = 1010 - 0001$ volt, az ehhez tartozó üzenet pedig az 10.

Az algoritmus hátránya, hogy nagy lineáris kód esetén a mellékoszály-vezetők megtalálása szinte esélytelen. Ez teszi szükségessé speciális alakú kódok konstrukcióját.

Most 1-hibajavító kódokat fogunk konstruálni. Ehhez az kell, hogy a minimális kódtávolság legalább 3 legyen. A 3.1.11 lemma alapján ennek szükséges és elégséges feltétele, hogy $\mathbf{H}$ bármely két oszlopa lineárisan független legyen. Két $\mathbb{F}_q^m$-beli vektor pontosan akkor összefüggő, ha az egyik a másik skalárszorosa. A 0 vektor önmagában is összefüggő, így a maradék q^{m-1} vektort $q-1$ osztályba sorolhatjuk, ahol az egyes osztályokban az egymással páronként összefüggő vektorok vannak. Minden ilyen osztályból válasszunk ki egy vektort, és ezek legyenek a $\mathbf{H}$ mátrix oszlopai. Ekkor a $\mathbf{H}$ paritásellenőrző mátrixszal adott lineáris $(m, \frac{q^{m-1}}{q-1})$ kódot $\mathbb{F}_q$ feletti m rendű *Hamming-kódnak* nevezzük.

Speciálisan $q = 2$ esetén a bináris Hamming-kódokat kapjuk. Az m rendű bináris Hamming-kód $\mathbf{H}$ paritásellenőrző mátrixa egyértelmű, az oszlopai az $1, 2, \ldots, 2^{m-1}$ számok kettes számrendszerbeli alakjából állnak.

A Hamming-kódokat úgy konstruáltuk meg, hogy 1-hibajavítók legyenek. Most bináris Hamming-kódok esetén egyszerű algoritmust adunk a hibajavításra. Tegyük fel, hogy a $\mathbf{c}$ kód elküldése után a $\mathbf{v}$ vektort kaptuk. Mivel egy hibajavító kódról beszélünk, feltehetjük, hogy az $\mathbf{e}$ hibavektor súlya 1, azaz $\mathbf{e}$ koordinátái közül pontosan egy nemnulla elem van; ez bináris kód esetén 1. A kapott $\mathbf{u}$ vektor szindrómája $\mathbf{Hu}^T = \mathbf{He}^T$. Ekkor tehát a szindróma $\mathbf{H}$ azon oszlopával egyezik meg, ahol a hiba történt. Ha a szindróma kiszámolása után $\mathbf{H}$ i-edik oszlopát kapjuk, akkor $\mathbf{u}$-nak az i-edik koordinátáját módosítva nyerjük az eredeti $\mathbf{c}$ kódszót.

3.1.14. Példa. Tekintsük az $\mathbb{F}_2$ feletti 3 rendű Hamming-kódot. Ez egy lineáris $(7,4)$ kód a $\mathbf{H} = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$ paritásellenőrző mátrixszal. Ha a kapott üzenet $\begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$, akkor a szindróma $\begin{pmatrix} 1 & 1 & 1 \end{pmatrix}^T$, így a hiba az első koordinátában történt, vagyis az elküldött kódszó a $\begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$ volt.

A kódelmélet célja, hogy minél több hibát ki lehessen javítani, ehhez a kódszavak távolságát kell növelni. Másrészt minél több információt akarunk elküldeni, vagyis nem hatékony, ha a kódszavak az elküldendő üzenethez képest túl hosszúak. Ezért a továbbiakban az $\mathbb{F}_q$ test feletti C lineáris (n,k) kód d_C minimum kódtávolsága, n hossza és k dimenziója közötti kapcsolatokat vizsgáljuk.

A $\mathbf{H}$ paritásellenőrző mátrixnak $n-k$ sora van, ezért legfeljebb $n-k$ lineárisan független oszlopa lehet. Így a 3.1.11 lemma alapján $\mathrm{d}_C \leq n-k+1$. Ezt az egyenlőtlenséget nevezzük *Singleton-korlátnak.* Az olyan kódokat, amik ezt az egyenlőtlenséget egyenlőséggel teljesítik, *MDS-kódoknak* nevezzük. Például a 3.1.7 példában szereplő ismétléses kód MDS-kód.

Most tegyük fel, hogy C t-hibajavító, ekkor a kódszavak körüli t sugarú gömbök diszjunktak. Egy $\mathbf{u}$ vektortól k távolságra lévő elemek száma $\binom{n}{k}(q-1)^k$, így egy t sugarú gömbben $\sum_{k=0}^{t}\binom{n}{k}(q-1)^k$ vektor van. Mivel q^k kódszó és q^n vektor van összesen, így $q^k\sum_{k=0}^{t}\binom{n}{k}(q-1)^k \leq q^n$. Ezt az egyenlőtlenséget hívjuk *Hamming-korlátnak.* Ha a kódszavak körüli t sugarú gömbök teljesen lefedik $\mathbb{F}_q^n$-et, azaz a fenti egyenlőtlenség egyenlőséggel teljesül, akkor a kódot *perfektnek* nevezzük. Az 1-hibajavító kódok esetén a Hamming-korlát a következő egyszerűbb alakot ölti: $1+n(q-1) \leq q^{n-k}$. A Hamming-kódok esetén $n-k=m$ és $n=\frac{q^m-1}{q-1}$, így azt kapjuk, hogy minden Hamming-kód perfekt.

3.2. Ciklikus kódok

Eddig a lineáris kódokat az $\mathbb{F}_q^n$ vektortér egy lineáris altereként értelmeztük. Azonban az $\mathbb{F}_q^n$ vektorteret azonosíthatjuk a legfeljebb $n-1$-ed fokú $\mathbb{F}_q$ feletti polinomokkal, az $(u_0,u_1,\ldots u_{n-1}) \leftrightarrow u_0+u_1x+\ldots+u_{n-1}x^{n-1}$ izomorfizmus segítségével. A $\mathbf{c}$ kódszóhoz tartozó $c(x)$ polinomot *kódpolinomnak* nevezzük.

A továbbiakban tegyük fel, hogy $\mathrm{lnko}(q,n)=1$ és a legfeljebb $n-1$-ed fokú polinomokat tekintsük az $\mathbb{F}_q[x]/(x^n-1)$ maradékosztálygyűrű elemeinek. Ekkor C a maradékoszálygyűrű egy részhalmaza, ezért használható a $c(x)\in C$ jelölés. Értelmezzük két legfeljebb n-ed fokú polinom szorzatát a következő módon: $u(x)v(x) = f(x) \Leftrightarrow u(x)v(x) \equiv f(x) \bmod (x^n-1)$. Természetesen adódik a kérdés, hogy miért

az x^n-1 polinomot választottuk, hiszen bármely n-ed fokú polinommal faktorizálva a legfeljebb $n-1$-ed fokú polinomok halmazát kaptuk volna, és a szorzást hasonlóan értelmezhetnénk. A kérdésre a következő definíció, illetve tétel ad magyarázatot.

3.2.1. Definíció. Az $\mathbb{F}_q$ feletti C lineáris (n,k) kód *ciklikus*, ha $(c_0, c_1, \ldots, c_{n-1}) \in C \Rightarrow (c_{n-1}, c_0, \ldots, c_{n-2}) \in C$.

Legyen C ciklikus kód és a $\mathbf{c}$ kódszónak megfelelő polinom $c_0+c_1x+\ldots+c_{n-1}x^{n-1}$. Ekkor definíció szerint a $\tilde{c}(x) = c_{n-1} + c_0x + \ldots + c_{n-2}x^{n-1}$ polinom is kódpolinom. Mivel $\tilde{c}(x) \equiv xc(x) \bmod (x^n-1)$, így egy C kód pontosan akkor ciklikus, ha $c(x) \in C$-ből következik, hogy $xc(x) \in C$. Ennek az észrevételnek a következménye az alábbi tétel.

3.2.2. Tétel. *Egy C kód pontosan akkor ciklikus, ha az $\mathbb{F}_q/(x^n-1)$ maradékosztálygyűrű ideálja.*

Bizonyítás. Ha C ideál, akkor lineáris altér $\mathbb{F}_q^n$-ben, továbbá ha $c(x) \in C$, akkor $xc(x) \in C$, tehát C ciklikus. A megfordításhoz tegyük fel, hogy C ciklikus. Ekkor ha $c(x) \in C$, akkor $xc(x) \in C$, így $x^2c(x) \in C$, és így tovább, minden $k \in \mathbb{N}$-re $x^kc(x) \in C$. Mivel C lineáris altér, ezért ezek bármely lineáris kombinációja is benne van C-ben, azaz tetszőleges $b(x)$ polinommal $b(x)c(x) \in C$, tehát C ideál. □

3.2.3. Tétel. *Az $\mathbb{F}_q[x]/(x^n-1)$ faktorgyűrű minden I ideálja főideál, sőt I generátora a benne lévő legkisebb fokú normált polinom. Továbbá a generáló polinom osztja az x^n-1 polinomot.*

Bizonyítás. Legyen I az $\mathbb{F}_q[x]/(x^n-1)$ faktorgyűrű ideálja és $g(x)$ a benne lévő legkisebb fokú normált polinom, továbbá legyen $h(x)$ tetszőleges I-beli polinom. Osszuk el maradékosan $h(x)$-et $g(x)$-szel, ekkor $h(x) = q(x)g(x) + r(x)$, ahol $\deg r(x) < \deg g(x)$, vagy $r(x) = 0$. Viszont $h(x)$ és $q(x)h(x)$ is I-ben van, ezért $r(x)$ is, így a $g(x)$ definíciója miatt $r(x) = 0$. Tehát I a $g(x)$ többszöröseiből áll.

Most osszuk el maradékosan x^n-1-et g-vel, azaz $x^n-1 = h(x)g(x)+s(x)$, ahol $s = 0$ vagy $\deg s < \deg g$. Ekkor $s(x) \equiv -h(x)g(x) \pmod{x^n-1}$. Ha $s(x)$ nem 0, akkor lenne egy $g(x)$-nél kisebb fokú normált polinom I-ben, ami ellentmondás. □

3.2.4. Definíció. Legyen $C = \big(g(x)\big)$ ciklikus kód. Ekkor $g(x)$-et a C *generátorpolinomjának* nevezzük, a $h(x) = \frac{x^n-1}{g(x)}$ polinom pedig a C *paritásellenőrző polinomja.*

3.2.5. Tétel. *Legyen a C kód paritásellenőrző polinomja $h(x)$. Egy tetszőleges $u(x)$ polinom pontosan akkor van C-ben, ha $u(x)h(x) = 0$.*

Bizonyítás. A C ciklikus kód a $g(x)$ generáló polinom többszöröseiből áll, így ha $u(x) \in C$, akkor létezik $q(x)$ polinom, hogy $u(x) = q(x)g(x)$. Ekkor $u(x)h(x) = q(x)g(x)h(x) = a(x)(x^n - 1) = 0$.

Másrészt ha $c(x)h(x) = 0$, akkor van olyan $q(x)$ polinom, hogy $c(x)h(x) = q(x)(x^n - 1)$. Ekkor $c(x)h(x)g(x) = a(x)g(x)(x^n - 1)$, így $c(x) = a(x)g(x)$, tehát $c(x)$ kódpolinom. $\square$

Legyen $g(x) = g_0 + g_1x + \ldots + g_{n-k}x^{n-k}$ egy $(n-k)$-ad fokú polinom, ami osztja $x^n - 1$-et. Ekkor a

$$\mathbf{G} = \begin{pmatrix} g_0 & g_1 & \ldots & \ldots & \ldots & \ldots & g_{n-k-1} & g_{n-k} & 0 & 0 & \ldots & 0 \\ 0 & g_0 & g_1 & \ldots & \ldots & \ldots & \ldots & g_{n-k-1} & g_{n-k} & 0 & \ldots & 0 \\ 0 & 0 & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & 0 & \ldots & 0 & g_0 & g_1 & \ldots & \ldots & \ldots & \ldots & g_{n-k-1} & g_{n-k} \end{pmatrix}$$

generátor mátrixszal megadott C lineáris kód ciklikus (n, k) kód, ugyanis $\mathbf{G}$ sorai lineárisan függetlenek, mert $g_0 \neq 0$, és $C = \big(g(x)\big)$. Ha $h(x) = \frac{x^n-1}{g(x)} = h_0 + h_1x + \ldots + h_kx^k$, akkor C paritásellenőrző mátrixa

$$\mathbf{H} = \begin{pmatrix} 0 & 0 & \ldots & 0 & h_k & h_{k-1} & \ldots & \ldots & \ldots & \ldots & h_1 & h_0 \\ 0 & \ldots & 0 & h_k & h_{k-1} & \ldots & \ldots & \ldots & \ldots & h_1 & h_0 & 0 \\ \vdots & \iddots & \iddots & \iddots & \iddots & \iddots & \iddots & \iddots & \iddots & \iddots & \iddots & 0 \\ 0 & \iddots & \iddots & \iddots & \iddots & \iddots & \iddots & \iddots & \iddots & \iddots & \iddots & \vdots \\ h_k & h_{k-1} & \ldots & \ldots & \ldots & \ldots & h_1 & h_0 & 0 & 0 & \ldots & 0 \end{pmatrix}.$$

Legyen C az $\mathbb{F}_q$ test feletti ciklikus kód, és legyen $g(x)$ a generátorpolinomja. Ekkor minden $c(x) \in C$ előáll $c(x) = q(x)g(x)$ alakban. Így az $\mathbb{F}_q$ test egy alkalmas véges bővítéséből való α elemre $g(\alpha) = 0$ pontosan akkor teljesül, ha minden $c(x)$ kódpolinomra $c(\alpha) = 0$. Ennek az észrevételnek a következménye az alábbi tétel.

3.2.6. Tétel. *Legyenek a $C \subseteq \mathbb{F}_q[x]/(x^n - 1)$ ciklikus kód g generátorpolinomjának gyökei $\alpha_1, \alpha_2, \ldots, \alpha_{n-k}$. Ekkor az $f \in \mathbb{F}_q[x]/(x^n - 1)$ polinom pontosan akkor kódpolinom, ha a hozzá tartozó $(f_0, \ldots, f_{n-1})$ együttható vektor a $\mathbf{H}$ mátrix nullterében van, ahol*

$$\mathbf{H} = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \ldots & \alpha_1^{n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha_{n-k} & \alpha_{n-k}^2 & \ldots & \alpha_{n-k}^{n-1} \end{pmatrix}.$$

Ezekután a szindróma szerepét ezzel a $\mathbf{H}$ mátrixszal a $\mathbf{H}\mathbf{v}^T$ játssza. Sőt ez a $\mathbf{H}$ tovább egyszerűsödhet, ugyanis ha $g(x)$-et speciális alakban adjuk meg, akkor elég csak bizonyos gyökeiről megkövetelni, hogy a kódpolinomoknak is gyökei legyenek.

Legyenek $\alpha_1, \alpha_2, \ldots, \alpha_s$ az $\mathbb{F}_q$ test egy véges bővítésének elemei. Az $m_i(x)$ jelölje az α_i elem $\mathbb{F}_q$ test feletti minimálpolinomját $i = 1, 2 \ldots, s$-re. Legyen n olyan természetes szám, hogy $\alpha_i^n = 1$, azaz minden i-re $m_i \mid a\ 2.1.4 szerint x^n - 1$ teljesüljön. Legyen $g(x) = \mathrm{lkkt}\big(m_1(x), \ldots, m_s(x)\big)$, ekkor $g(x)$ osztja az $x^n - 1$ polinomot. Tekintsük a $C \subseteq \mathbb{F}_q^n$ ciklikus kódot, amit a $g(x)$ generál. Ekkor $c(x) \in C$ pontosan akkor, ha $c(x) = q(x)g(x)$ alkalmas $q(x)$ polinommal. Legyen minden i-re $g_i(x) = \frac{g(x)}{m_i(x)}$, így $c(x)$ pontosan akkor kódpolinom, ha $c(x) = q(x)g_i(x)m_i(x)$. Tehát $c(x)$ pontosan akkor kódpolinom, ha minden i-re $m_i(x) \mid c(x)$, ami azzal ekvivalens, hogy $c(\alpha_i) = 0$ minden $i = 1, 2 \ldots, s$-re. Az így konstruált C kódot az $\alpha_1, \ldots \alpha_s$ *elemek által generált kódnak* nevezzük.

3.2.7. Példa. Legyen α primitív n-edik egységgyök $\mathbb{F}_{2^m}$ felett, és C az α által generált kód. A hibajavítás során meg kell határoznunk a kapott $\mathbf{v}$ szó szindrómáját. Általában a szindróma egy $n - k$ hosszú oszlopvektor, de most egyszerűbb módot is találhatunk a hibajavításra. Mivel $c(x)$ pontosan akkor kódszó, ha $c(\alpha) = 0$, ezért a 3.2.6 tételbeli $\mathbf{H}$ mátrix a következő alakú:

$$\mathbf{H} = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \ldots & \alpha_1^{n-1} \end{pmatrix}.$$

Ekkor $v(\alpha) = \mathbf{H}\mathbf{v}^T$. Tegyük fel, hogy az üzenet továbbítása során egy hiba történt. Legyen $\mathbf{e_j}$ az a vektor aminek a j-edik koordinátája 1, a többi 0, így a hozzá tartozó polinom $e_j(x) = x^{j-1}$, ahol $1 \leq j \leq n$. Legyen az elküldött kód $\mathbf{u}$, a kapott pedig $\mathbf{v}$. Ekkor $\mathbf{v} = \mathbf{u} + \mathbf{e_j}$, így $v(\alpha) = u(\alpha) + e_j(\alpha) = \alpha^{j-1}$, ami egyértelműen meghatározza a hiba helyét, ugyanis $\alpha^j \neq \alpha^i$, ha $j \neq i$. Az $e_j(\alpha)$-t *hibajelző számnak* nevezzük.

3.2.8. Tétel. *Legyen α az $\mathbb{F}_q$ test egy véges bővítésének eleme, aminek a rendje n. Továbbá legyen d olyan pozitív egész, amire teljesül, hogy $2 \leq d \leq n$, és legyen a nemnegatív egész. Ekkor az $\alpha^a, \alpha^{a+1}, \ldots, \alpha^{a+d-2}$ által definiált C kód minimumtávolsága d.*

Bizonyítás. Minden $\mathbf{c}$ kódszóra $\mathbf{Q}\mathbf{c}^T = 0$, ahol

$$\mathbf{Q} = \begin{pmatrix} 1 & \alpha^a & \alpha^{2a} & \ldots & \alpha^{(n-1)a} \\ 1 & \alpha^{a+1} & \alpha^{2(a+1)} & \ldots & \alpha^{(n-1)(a+1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{a+d-2} & \alpha^{2(as+d-2)} & \ldots & \alpha(n-1)(a+d-2) \end{pmatrix}.$$

Megmutatjuk, hogy $\mathbf{Q}$ bármely $d-1$ sora lineárisan független, így a 3.1.11 tételhez hasonlóan $d_C \geq d$. Válasszunk ki $\mathbf{Q}$-nak $d-1$ különböző oszlopát. Így a következő determinánst kapjuk:

$$\begin{vmatrix} \alpha^{ai_1} & \alpha^{ai_2} & \dots & \alpha^{ai_{d-1}} \\ \alpha^{(a+1)i_1} & \alpha^{(a+1)i_2} & \dots & \alpha^{(a+1)i_{d-1}} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha^{(a+d-2)i_1} & \alpha^{(a+d-2)i_2} & \dots & \alpha(a+d-2)i_{d-1} \end{vmatrix} =$$

$$= \alpha^{a(i_1+i_2+\dots+i_{d-1})} \begin{vmatrix} 1 & 1 & \dots & 1 \\ \alpha^{i_1} & \alpha^{i_2} & \dots & \alpha^{i_{d-1}} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha^{i_1(d-2)} & \alpha^{i_2(d-2)} & \dots & \alpha i_{d-1}(d-2) \end{vmatrix} \neq 0.$$

□

A továbbiakban speciális ciklikus kódokól, a BCH-kódokról, lesz szó, amit R.C. Bose és D.K. Ray-Chauhuri (1960), valamint tőlük függetlenül A. Hocquengham (1959) fedezett fel.

3.2.9. Definíció. Legyen b nemnegatív egész, α az $\mathbb{F}_{q^m}$ test feletti primitív n-edik egységgyök. Legyen $2 \leq d \leq n$, ekkor az $\mathbb{F}_q$ feletti n hosszú d tervezett távolságú *BCH-kódon* az $\alpha^b, \alpha^{b+1}, \dots, \alpha^{b+d-2}$ által generált ciklikus kódot értjük.

Ha α primitív eleme $\mathbf{F}_{q^m}$-nek, akkor *primitív BCH-kódról* beszélünk, ekkor $n = q^m - 1$. Ha $m = 1$, akkor az $\mathbb{F}_q$ feltti n hosszú BCH-kódot *Reed–Solomon kódnak* nevezzük.

A BCH-kódok definicíója nem egységes a szakirodalomban. Az $\alpha \in \mathbb{F}_{q^m}$ rendje n, így $n \mid a\ 2.1.4 szerint q^m - 1$, ezért a legkisebb olyan m, amire teljesül, hogy α benne van az $\mathbb{F}_q$ m-ed fokú bővítésében, a q multiplikatív rendje modulo n. Van ahol ezt is felteszik a definícióban; ekkor az $m = 1$ feltétel az $n = q - 1$ feltétellel ekvivalens. Ekkor a Reed–Solomon kódot *primtívnek* nevezzük. Gyakran megkövetelik a definícióban a $b = 1$ teljesülését is.

A BCH-kódok azért hasznosak, mert a 3.2.8 tétel miatt egy d tervezett távolságú BCH-kód minimumtávolsága d. Emiatt gyakran felteszik, hogy $d = 2t + 1$ legyen, ekkor a kód t-hibajavító. Minden pozitív d-hez tudunk konstruálni olyan BCH-kódot, aminek a tervezett távolsága d. Azonban a minimális távolság növeléséhez az n kódhosszt is meg kell növelni. Mivel m a q modulo n rendjének többszöröse, így az m értéke is nő.

Most a BCH-kódok dekódolására adunk egy általános algoritmust. Legyen $u(x)$ az elküldött, $v(x)$ a kapott és $e(x)$ a hibapolinom, tehát $v(x) = u(x) + e(x)$.

Először határozzuk meg a $\mathbf{v}$ szindrómáját. $\mathbf{H}\mathbf{v}^T = (S_b, S_{b+1}, \ldots, S_{b+d-2})^T$, ahol $S_j = v(\alpha^j) = w(\alpha^j) + e(\alpha^j) = e(\alpha^j)$ és $b \leq j \leq b+d-2$. Ha $r \leq t$ hiba történt, akkor $e(x) = \sum_{i=1}^{r} c_i x^{a_i}$, ahol az $a_1, \ldots, a_r$ hibahelyek a $\{0, 1, \ldots, n-1\}$ halmazból valók. Az $\mathbb{F}_{q^m}$-beli $\eta_i = \alpha^{a_i}$ elemeket *hibahely-számoknak*, a $c_i \in \mathbb{F}_q^*$ elemeket *hibaértékeknek* nevezzük. Ekkor $S_j = e(\alpha^j) = \sum_{i=1}^{r} c_i \eta_i^j$ minden $b \leq j \leq b+d-2$-re. Az $\mathbb{F}_{q^m}$ test számolási szabályai miatt

$$S_j^q = \left(\sum_{i=1}^{r} c_i \eta_i^j \right)^q = \sum_{i=1}^{r} c_i^q \eta_i^{jq} = \sum_{i=1}^{r} c_i \eta_i^{jq} = S_{jq}. \tag{3.1}$$

Az (η_i, c_i) párok, ahol $1 \leq i \leq r$, egyértelműen meghatározzák az $e(x)$ hibapolinomot. Bináris esetben a hibaérték csak 1 lehet, így ekkor a hibahely-számok meghatározása is elég.

A következő lépéshez emlékeztetőül szolgál az alábbi definíció.

3.2.10. Definíció. Az $x_1, \ldots, x_n$ változójú k-adik *elemi szimmetrikus polinomot* úgy kapjuk, hogy $x_1, \ldots, x_n$ közül minden lehetséges módon kiválasztunk k darabot, a kiválasztott x_i-ket összeszorozzuk, majd a szorzatokat összeadjuk. Az így kapott polinomot $\sigma_k(x_1, \ldots, x_n)$-nel jelöljük, ahol $1 \leq k \leq n$. Ha a változók egyértelműek, akkor csak σ_k-t írunk. Definíció szerint legyen $\sigma_0 \equiv 1$.

Legyen σ_i az $\eta_1, \ldots, \eta_r$ változók i-edik elemi szimmetrikus polinomja, ahol $0 \leq i \leq r$. Ekkor

$$\prod_{i=1}^{r} (\eta_i - x) = \sum_{i=0}^{r} (-1)^i \sigma_{r-1} x^i = \sigma_r - \sigma_{r-1} x + \ldots + (-1)^r \sigma_0 x^r.$$

Az x helyébe η_i-t írva és $(-1)^r$-rel szorozva kapjuk:

$$0 = (-1)^r \sigma_r + (-1)^{r-1} \sigma_{r-1} \eta_i + \ldots + (-1) \sigma_1 \eta_i^{r-1} + \sigma_0 \eta_i^r \quad 1 \leq i \leq r.$$

Az egyenletet szorozzuk $c_i \eta_i^j$-vel majd adjuk őket össze 1-től r-ig, ekkor kapjuk:

$$(-1)^r \sigma_r S_j + (-1)^{r-1} \sigma_{r-1} S_{j+1} + \ldots + (-1) \sigma_1 S_{j+r-1} + \sigma_0 S_{j+r} \quad b \leq j \leq b+r-1.$$

A továbbiakhoz két lemmát bizonyítunk.

3.2.11. Lemma. *A c_i ismeretlenekkel adott $S_j = \sum_{i=1}^{r} c_i \eta_i^j$, ahol $b \leq j \leq b+d-2$, lineáris egyenletrendszer pontosan akkor oldható meg, ha η_i-k az $\mathbb{F}_{q^m}^*$ multiplikatív csoport különböző elemei.*

Bizonyítás. A lineáris egyenlerenszerhez tartozó együtthatómátrix determinánsa

$$\begin{vmatrix} \eta_1^b & \eta_2^b & \dots & \eta r^b \\ \eta_1^{b+1} & \eta_2^{b+1} & \dots & \eta r^{b+1} \\ \vdots & \vdots & & \vdots \\ \eta_1^{b+r-1} & \eta_2^{b+r-1} & \dots & \eta r^{b+r-1} \end{vmatrix} = \eta_1^b \eta_2^b \dots \eta_r^b \prod_{1 \le i < j \le r} (\eta_j - \eta_i) \neq 0.$$

□

3.2.12. Lemma.

$$(-1)^r \sigma_r S_j + (-1)^{r-1} \sigma_{r-1} S_{j+1} + \ldots + (-1)\sigma_1 S_{j+r-1} + \sigma_0 S_{j+r}, \quad b \le j \le b+r-1,$$

$(-1)^i \sigma_i = \tau_i$ ismeretlenekkel adott lineáris egyenletrendszer pontosan akkor oldható meg egyértelműen, ha r hiba történt.

Bizonyítás. A lineáris egyenletrendszerhez tartozó mátrix a következő:

$$\begin{pmatrix} S_b & S_{b+1} & \dots & S_{b+r-1} \\ S_{b+1} & S_{b+2} & \dots & S_{b+r} \\ \vdots & \vdots & & \vdots \\ S_{b+r-1} & S_{b+r} & \dots & S_{b+2r-2} \end{pmatrix} = V D V^T,$$

ahol

$$V = \begin{pmatrix} 1 & 1 & \dots & 1 \\ \eta_1 & \eta_2 & \dots & \eta_r \\ \vdots & \vdots & & \vdots \\ \eta_1^{r-1} & \eta_2^{r-1} & \dots & \eta_r^{r-1} \end{pmatrix} \text{ és } \quad D = \begin{pmatrix} c_1 \eta_1^b & 0 & \dots & 0 \\ 0 & c_2 \eta_2^b & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & c_r \eta_r^b \end{pmatrix}.$$

A mátrix pontosan akkor nem szinguláris, ha V és D sem az. A V Vandermonde-mátrix pontosan akkor nem szinguláris, ha η_i-k klönbözőek. A D pedig akkor és csak akkor reguláris, ha η_i-k és c_i-k nemnullák. Mindkét feltétel akkor és csak akkor elégíthető ki, ha r hiba történt. □

Az $s(x) = \prod_{i=1}^r (1 - \eta_i x) = \sum_{i=0}^r (-1)^i \sigma_i x^i = \sum_{i=0}^r \tau_i x^i$ polinomot nevezzük *hibajelző polinomnak*. Az $s(x)$ gyökei $\eta_1^{-1}, \eta_2^{-1}, \dots, \eta_r^{-1}$. Az $s(x) = 0$ egyenletet úgy oldjuk meg, hogy behelyettesítjük a test összes elemét. Összefoglalva:

1. lépés Meghatározzuk a $\mathbf{H}\mathbf{v}^T = (S_b, S_{b+1}, \dots, S_{b+d-2})^T$ szindrómát. Írjuk fel a következő egyenletrendszert: $S_j = \sum_{i=1}^r c_i \eta_i^j$, ahol $b \le j \le b+d-2$.

2. lépés Meghatározzuk a legnagyobb olyan $r \leq t$ számot, amelyre igaz, hogy az $S_{j+r} + S_{j+r-1}\tau_1 + \ldots + S_j\tau_r = 0$, $b \leq j \leq b+r-1$ egyenletrendszerhez tartozó együtthatómátrix reguláris, így tudjuk, hogy r hiba történt. Ezután az $s(x) = \prod_{i=1}^{r}(1-\eta_i x) = \sum_{i=0}^{r}\tau_i x^i$ hibajelző polinomban S_j segítségével meghatározzuk a τ_i együtthatókat.

3. lépés Megoldjuk az $s(x) = 0$ egyenletet az α hatványainak behelyettesítésével. Így megkapjuk az η_i hibahely jelző számokat.

4. lépés Az 1. lépésben található egyenletrendszer első r sorába behelyettesítjük η_i-ket és meghatározzuk c_i-ket. Az elküldött $\mathbf{u}$ kódszót az $u(x) = v(x) - e(x)$ egyenletből nyerjük.

3.2.13. Példa. Legyen α az $\mathbb{F}_{16}$ olyan primitív eleme, amelyre teljesül, hogy $\alpha^4 = \alpha + 1$. Továbbá legyen a bináris $(15, 5)$ BCH-kód generátor polinomja $g(x) = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1$. Feltéve, hogy a kapott üzenet a $\mathbf{v} = 010011011100100$, határozzuk meg az eredeti kódszót és az üzenetet!

Mivel $g(x) = (x^4+x+1)(x^4+x^3+x^2+x+1)(x^2+x+1)$, így a 2.3.4 példa alapján g gyökei a következők $\{\alpha, \alpha^2, \alpha^4, \alpha^8, \alpha^3, \alpha^6, \alpha^{12}, \alpha^9, \alpha^5, \alpha^{10}\}$, így a $b = 1$ választással kapjuk, hogy a kód tervezett távolsága $d = 7$, ugyanis 1–6-ig α minden hatványa szerepel a gyökök között. Emiatt a kód 3-hibajavító.

Az első lépésben határozzuk meg a szindrómákat!

A kapott szóból $v(x) = x + x^4 + x^5 + x^7 + x^8 + x^9 + x^{12}$, így ismét a 2.3.4 példa felhasználásával kapjuk, hogy $S_1 = v(\alpha) = \alpha + \alpha^4 + \alpha^5 + \alpha^7 + \alpha^8 + \alpha^9 + \alpha^{12} = \alpha^3 + \alpha^2 = \alpha^6$, $S_3 = v(\alpha^3) = \alpha^3 + \alpha^{12} + 1 + \alpha^6 + \alpha^9 + \alpha^{12} + \alpha^6 = \alpha + 1 = \alpha^4$ és $S_5 = v(\alpha^5) = \alpha^5+\alpha^5+\alpha^{10}+\alpha^5+\alpha^{10}+1+1 = \alpha^5$. A többi szindróma megállapításához felhasználjuk a 3.1 összefüggést, így $S_2 = S_1^2 = \alpha^{12}$, $S_4 = S_2^2 = \alpha^9$ és $S_6 = S_3^2 = \alpha^8$.

A második lépésben meghatározzuk a hibák számát az $S_{j+r} + S_{j+r-1}\tau_1 + \ldots + S_j\tau_r = 0$, $1 \leq j \leq r$ egyenletrendszer segítségével és meg is oldjuk azt. Mivel a kódunk 3-hibajavító, ezért r legfeljebb 3.

Mivel

$$\begin{vmatrix} S_1 & S_2 & S_3 \\ S_2 & S_3 & S_4 \\ S_3 & S_4 & S_5 \end{vmatrix} = \begin{vmatrix} \alpha^6 & \alpha^{12} & \alpha^4 \\ \alpha^{12} & \alpha^4 & \alpha^9 \\ \alpha^4 & \alpha^9 & \alpha^5 \end{vmatrix} = \alpha^{10} \neq 0,$$

így $r = 3$ hiba történt. Az

$$\begin{cases} \alpha^6\tau_3 & + & \alpha^{12}\tau_2 & + & \alpha^4\tau_1 & = & \alpha^9 \\ \alpha^{12}\tau_3 & + & \alpha^4\tau_2 & + & \alpha^9\tau_2 & = & \alpha^5 \\ \alpha^4\tau_3 & + & \alpha^9\tau_2 & + & \alpha^5\tau_1 & = & \alpha^8 \end{cases}$$

egyenletrendszer megoldása a $\tau_1 = \alpha^6$, $\tau_2 = \alpha^{10}$, $\tau_3 = \alpha^{14}$.

A harmadik lépés az $s(x) = \prod_{i=1}^{3}(1 - x\eta_i) = \sum_{i=0}^{3} \tau_i x^i = 1 + \alpha^6 x + \alpha^{10} x^2 + \alpha^1 4$ polinom gyökeinek megkeresése. Próbálgatással kapjuk, hogy $\eta_1^{-1} = \alpha^4$, $\eta_2^{-1} = \alpha^5$ és $\eta_3^{-1} = \alpha^7$, így $\eta_1 = \alpha^{11}$, $\eta_2 = \alpha^{10}$ és $\eta_3 = \alpha^8$. Tehát a hibák a kilencedik, tizenegyedik és tizenkettedik pozícióban történtek.

A negyedik lépés a hibák mértékének kitalálása lenne, de ez bináris kód esetén mindig 1. Így az elküldött kódszó az $\mathbf{u} = 010011010111100$ volt. Az üzenetet az $\frac{u(x)}{g(x)} = x^2 + x$ polinomból visszakódolva kapjuk, ez pedig nem más, mint 01100.

Irodalomjegyzék

[1] Rudolf Lidl – Harald Niederreiter, *Finite Fields* (2nd ed.), Cambridge University Press, 1997.

[2] Lakatos Piroska, *Bevezetés a véges testek elméletébe* Debrecen, Debreceni Egyetem, Matematika Intézet, 2010.

[3] Kiss Emil, *Bevezetés az algebrába*, Typotex, 2007.

[4] J.I.Hall, *Notes on Coding Theory*, Department of Mathematics Michigan State University East Lansing, 2010.

[5] Madhu Sudan, *Essential Coding Theory*, MIT, 2002. online jegyzet
http://people.csail.mit.edu/madhu/FT02/

[6] Lakatos Piroska, *Kódelmélet* Debrecen, Debreceni Egyetem, Matematika Intézet, 2010.

[7] Buttyán L., Györfi L., Győri S., Vajda I.,*Kódolástechnika*, 2006.