POLINOMOK VÉGES TESTEK FELETT

SZAKDOLGOZAT

Készítette: Csohány Dóra

Matematika BSc - elemző szakirány

Témavezető: Ágoston István, egyetemi docens

ELTE TTK, Algebra és Számelmélet Tanszék

Eötvös Loránd Tudományegyetem

Természettudományi Kar

Budapest, 2014

Tartalomjegyzék

Táblázatok jegyzéke

Bevezetés

A dolgozatom témája véges testek felett értelmezett polinomok, ezen belül is ezek faktorizációja és az irreducibilitás vizsgálata. Ha egy nagy fokú egész együtthatós polinomot szeretnénk irreducibilis tényezőkre bontani $\mathbb{Z}$ felett (vagy akár $\mathbb{Q}$ felett), akkor ez gyakran nem is olyan egyszerű feladat. Ezért érdemes lehet visszavezetni a problémát egy viszonylag egyszerűbbre, azaz faktorizáljuk a polinomot modulo q, az így kapott felbontásból pedig következtethetünk a $\mathbb{Z}$ feletti felbontására.

Az első fejezetben a véges testekről, azok felépítéséről és néhány érdekes tuladjonságáról lesz szó.

A második fejezetben először megpróbálom felírni az alacsony fokú polinomokat a kételemű és a háromelemű test felett. Ezután ezek megszámolása lesz a feladat, először egy rekurzív módszerrel majd egy hatékonyabb képlet segítségével fogom ezt megtenni.

A harmadik fejezetben Berlekamp algoritmusát szeretném ismertetni. Ez az eljárás véges test feletti polinomok faktorizációját határozza meg. Hatákonyságát az adja leginkább, hogy egyszerű maradékos osztást, és legnagyobb közös osztó számolást igényel, ezek a műveletek pedig gyorsan elvégezhetők.

Az utolsó, azaz negyedik fejezetben egy kódelméleti alkalmazást mutatok be. A teljesség igénye nélkül csak nagyvonalakban vezetném be ezt a területet azokra a definíciókra és tételekre koncentrálva, amelyek szükségesek ahhoz, hogy egy konkrét kódon szemléltetni tudjam a véges testek feletti polinomok egy alkalmazását. Tehát a kódelméleti bevezetés után a Reed-Solomon kódról lesz szó, és hogy hogyan tudunk létrehozni ilyen kódokat.

1. fejezet

Definíciók és alaptulajdonságok

Hogy véges testek felett tudjunk dolgozni, először meg kell vizsgálnunk azok szerkezetét. Ezt különböző definíciók, állítások és tételek alapján fogom ismertetni.

1.0.1. Állítás. *Legyen K tetszőleges test. Ekkor $\forall\ \alpha \in K,\ \alpha \neq 0$ elemre, az α additív rendje ugyanaz a szám, és ez vagy ∞ vagy egy p prímszám.*

Bizonyítás. Tegyük fel, hogy valamely $r \neq 0$ K-beli elem rendje véges, azaz létezik olyan $n > 0$ természetes szám, hogy $n \cdot r = 0$.
Ekkor tetszőleges $s \in K$-ra igaz a következő:

$$0 = (n \cdot r) \cdot s = \underbrace{(r + r + \cdots + r)}_{n\ db} \cdot s = \underbrace{rs + rs + \cdots rs}_{n\ db} = r \cdot \underbrace{(s + s + \cdots s)}_{n\ db} = r \cdot (n \cdot s).$$

Mivel $r \neq 0$ és K nullosztómentes (mivel test), ez csak úgy lehet 0, ha $n \cdot s = 0$, így ha r és s szerepét megcseréljük, akkor kapjuk, hogy r és s rendje megegyezik, azaz $o(r) = o(s),\ \forall\ r, s \in K^+,\ \ r, s \neq 0$-ra.

Most megmutatjuk, hogy a nem nulla elemek közös rendje, n prímszám.
Legyen tehát $o(r) = n < \infty$, és vegyük n egy felbontását $n = n_1 \cdot n_2$. Ekkor:

$$0 = n \cdot r = n_1 \cdot (n_2 \cdot r).$$

Ha $n_2 < n$, akkor $n_1 \cdot (n_2 \cdot r) = 0$-ban $n_2 \cdot r \neq 0$, vagyis $o(n_2 r) = n$ miatt $n_1 \geq n$-nek teljesülnie kell, vagyis $n = n_1$, és $n_2 = 1$, tehát n prím. $\square$

1.0.2. Definíció. *Legyen K tetszőleges test, ekkor a test karakterisztkáján a következőt értjük:*

$$char\ R = \begin{cases} p, & ha\ o(r) = p,\ \forall\ r \in K,\ r \neq 0 \\ 0, & ha\ o(r) = \infty,\ \forall\ r \in K,\ r \neq 0. \end{cases}$$

1.0.3. Állítás. *Legyen K kommutatív test. Ekkor ha char $K = p$, akkor $\mathbb{Z}_p$ részteste K-nak, és ez a legszűkebb résztest K-ban.*

Bizonyítás. Jelöljük K egységelemét e-vel, és tekintsük az alábbi halmazt:

$$L = \{0, \quad e, \quad e + e = 2 \cdot e, \quad e + e + e = 3 \cdot e, \ldots, (p-1) \cdot e\}.$$

Ha char $K = p$, akkor $\underbrace{e + e + \cdots + e}_{p \ db} = 0$, mivel $o(e) = p$. Ezért L részcsoport K^+-ban. Könnyen belátható, hogy az $m \mapsto m \cdot e$ megfeleltetés egy bijektív csoporthomomorfizmus $\mathbb{Z}_p^+$-ból L-be, és az is világos, hogy ez a megfeleltetés megőrzi a szorzást is:

$$(m \cdot e) \cdot (n \cdot e) = (m \cdot n) \cdot e^2 = (m \cdot n) \cdot e.$$

Így L résztest, és $L \cong \mathbb{Z}_p$.

Legyen most T a K-nak egy tetszőleges részeste. Ekkor $T \neq 0$, így T multiplikatív csoportja ($T^\times$) részcsoportja K multiplikatív csoportjának ($K^\times$-nek). Ezért K egységeleme, $e \in T$. Így $L \subseteq T$, vagyis L része K összes résztestének. Ilyenkor azt mondjuk, hogy L a K prímteste. □

1.0.4. Állítás. *Ha K egy véges test és elemszámát $|K|$-val jelöljük, akkor a K feletti n-dimenziós vektortérnek $|K|^n$ eleme van.*

Bizonyítás. A V vektortér elemei egyértelműen felírhatók $k_1 v_1 + \ldots k_n v_n$ alakban, ahol $v_1, \ldots v_n$ V egy bázisa. Ekkor minden $k_i \in K$ elem $|K|$-féleképpen választható ki egymástól függetlenül, vagyis $|K| \cdot |K| \cdots |K| = |K|^n$ féle elem van V-ben. □

1.0.5. Állítás. *Ha $\mathbb{F}$ véges test, akkor az elemszáma prímhatvány, azaz $|\mathbb{F}| = p^n$, ahol $p =$char $\mathbb{F}$.*

Bizonyítás. Mivel $\mathbb{F}$ véges, ezért tudjuk, hogy az elemek rendje véges, így a karakterisztikája, nem lehet 0. Az előbbiek szerint $\mathbb{F}$-nek van egy $\mathbb{Z}_p$-vel izomorf részteste (a prímtest). Ebből következik, hogy $\mathbb{F}$ vektortér $\mathbb{Z}_p$ felett. Ennek a dimenziója legyen $n = dim_{\mathbb{Z}_p}\mathbb{F}$. Ebből adódik, hogy $\mathbb{F} \cong (\mathbb{Z}_p)^n$, vagyis $\mathbb{F}$ elemszáma p^n, $|\mathbb{F}| = p^n$ □

Azt, hogy $\forall$ p^n-re $\exists$ p^n elemű test, és ez egyértelmű, az alábbi definíció és állítások mutatják.

1.0.6. Definíció. *Egy tetszőleges K test feletti f polinom felbontási testének nevezzük, azt a legszűkebb K-t tartalmazó L testet, amelyben f lineáris tényezők szorzatára bomlik.*

1.0.7. Tétel. *Egy K test felett bármely nem konstans polinomnak léteik felbontási teste és ez izomorfia erejéig egyértelműen meghatározott.*

1.0.8. Tétel. *Ha $q = p^n$, akkor minden p prímszámra és minden n természetes számra létezik q elemű véges test, továbbá minden $q = p^n$ elemű véges test izomorf az $\mathbb{Z}_p$ test feletti $x^q - x$ polinom felbontási testével (sőt az elemei pontosan $x^q - x$ gyökei lesznek és mind egyszeres).*

Bizonyítás. 1.) Először mutassuk meg, hogy ha K p^n elemű test, akkor minden eleme gyöke $x^q - x$-nek. Legyen p prím és $p^n = q$. Mivel K-nak q eleme van, a multiplikatív csoportja $q - 1$ elemű. A csoportelméleti Lagrange-tétel miatt (mely szerint egy véges csoport bármely részcsoportjának rendje osztója a csoport rendjének) e csoport minden elemének $q - 1$-edik hatványa a test egységeleme, azaz 1. Vagyis a K nem nulla elemei gyökei az $x^{q-1}-1$ polinomnak. Ezt x-szel szorozva kapjuk, hogy K minden eleme (beleértve a 0-t is) gyöke az $x^q - x$ polinomnak.

2.) Ezután belátjuk, hogy bármely két p^n elemű test izomorf. Ez előbb kapott $x^q - x$ polinomnak az együtthatói $1, -1$ és 0, ezek benne vannak a K test P prímtestében. Ekkor az $x^q - x \in P[x]$ polinom felbontási teste $P \cong \mathbb{Z}_p$ fölött éppen K, mivel gyökei pontosan K elemei, vagyis K a legszűkebb test, amely a polinom összes gyökét tartalmazza. Ez minden p^n elemű testre igaz, így a felbontási test egyértelműsége miatt bármely két p^n elemű test izomorf.

3.) Végezetül legyen K az $x^q - x \in \mathbb{Z}_p[x]$ polinom felbontási teste $\mathbb{Z}_p$ felett. Megmutatjuk hogy K elemszáma p^n, és hogy $x^q - x$ gyökei résztestek alkotnak, és így K az $x^q - x$ gyökeinek halmaza. Ez közvetlenül adódik abból, hogy mivel q hatványa K karakterisztikájának, ezért igaz a következő azonosság:

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

Ez nyilván a szorzásra is teljesül:

$$(x \cdot y)^q = x^q \cdot y^q.$$

Tehát $x^q - x$ gyökei résztestet alkotnak.

Ahhoz, hogy K elemszáma q, már csak azt kell belátni, hogy $x^q - x$ gyökei mind különbözők. Ha lenne többszörös gyöke, akkor az gyöke lenne a deriváltjának is. De a derivált:

$$(x^q - x)' = qx^{q-1} - 1 = p^n x^{q-1} - 1 = -1.$$

Hiszen $K[x]$ karakterisztikája is p. Ekkor a -1 konstans polinomnak nincs gyöke, tehát $x^q - x$-nek nincs többszörös gyöke K-ban. $\square$

Megjegyzés. A továbbiakban $\mathbb{F}_q$ jelöli az egyetlen q elemű testet.

1.0.9. Definíció. *Azt mondjuk, hogy egy $f(x) \in \mathbb{F}_q[x]$ polinom irreducibilis az $\mathbb{F}_q$ test felett, ha $f(x)$ bármely $f(x) = g(x)h(x)$ felbontásában az egyik tényező n-edfokú a másik pedig konstans polinom.*

1.0.10. Definíció. *Legyen $f \in \mathbb{F}_q[x]$ irreducibilis polinom, L pedig f felbontási test K felett. Ekkor, ha L felett az f mindegyik gyöke generálja az L multipikatív csoportját, akkor ezt az f polinomot primitív polinomnak nevezzük.*

1.0.11. Definíció. *Legyen $f = a_0 + a_1x + \cdots + a_nx^n$, $(a_0, a_n \neq 0)$ egy T test feletti polinom, és g legyen:*

$$a_n + a_{n-1}x + \cdots + a_0x^n.$$

Ekkor $g(x)$-et az f-hez tartozó reciprok polinomnak nevezzük.

1.0.12. Definíció. *Legyen F egy p karakterisztikájú véges test és α eleme $\mathbb{F}_{p^k}$ testnek. Ekkor α minimálpolinomja (m_α) az a legalacsonyabbfokú $\mathbb{F}_p$ együtthatós normált polinom, melynek gyöke α.*

1.0.13. Definíció. *Az $\mathbb{F}_q$ véges test egy $\alpha \neq 0$ elemét prmitívnek nevezzük, ha az $\mathbb{F}_q$ test minden nem nulla eleme egyértelműen felírható α^n alakban, ahol n egy pozitív egész szám.*

Megjegyzés. Ez azt jelenti, hogy α generálja az $\mathbb{F}_q^\times$ multiplikatív csoportot. (Meg lehet mutatni, hogy minden véges test multiplikatív csoportja ciklikus, tehát van benne primitív elem.)

2. fejezet

Irreducibilis polinomok

Polinomok vizsgálata során fontos feladat a polinomok faktorizálása alacsonyabb fokúak szorzatára. Ehhez el kell tudnunk dönteni, hogy mikor irreducibilis egy polinom. Végtelen testek esetén általában nincs értelme az irreducibilisek felsorolását tervezni, de véges testek felett könnyedén megadhatók, illetve megszámolhatók.

2.1. Irreducibilisek felsorolása

Kezdjük el felírni a normált irreducibilis polinomokat $\mathbb{F}_p$ felett (ahol p prím) Eratoszthenész módszerével. Azaz az összes polinom közül húzzuk ki azokat, amelyek valamely alacsonyabb fokú normált irreducibilisek többszörösei.

$\mathbb{F}_2$ felett az *elsőfokúak*:

$$\underline{x}, \quad \underline{x+1}$$

és ezek irreducibilisek.

A *másodfokúak*:

$$x^2, \quad x^2+1, \quad x^2+x, \quad \underline{x^2+x+1}.$$

Az elsőfokúak többszörösei x^2, $(x+1)\cdot(x+1) = x^2+1$, $x\cdot(x+1) = x^2+x$, ezeket ki is húzhatjuk, és mivel más módon nem állhat elő reducibilis másodfokú, így x^2+x+1 az egyetlen irreducibilis.

Harmadfokúak:

$$x^3, \quad x^3+1, \quad x^3+x, \quad \underline{x^3+x+1}, \quad x^3+x^2, \quad \underline{x^3+x^2+1}, \quad x^3+x^2+x, \quad x^3+x^2+x+1.$$

Állítsunk elő harmadfokú polinomokat x, $x+1$, x^2+x+1 segítségével az összes lehetséges módon:

$$\begin{aligned} x \cdot x \cdot x &= x^3 \\ x \cdot x \cdot (x+1) &= x^3 + x^2 \\ x \cdot (x+1) \cdot (x+1) &= x^3 + x \\ (x+1) \cdot (x+1) \cdot (x+1) &= x^3 + x^2 + x + 1 \\ (x^2+x+1) \cdot x &= x^3 + x^2 + x \\ (x^2+x+1) \cdot (x+1) &= x^3 + 1 \end{aligned}$$

Ha ezeket kihúzzuk, amik maradnak azok az irreducibilisek: x^3+x^2+1, x^3+x+1. Ezek az aláhúzottak a korábbi listában.

Vegyük észre, hogy az eljárást gyorsíthatjuk. Az elsőfokúak többszörösei pontosan azok, amelyeknek van gyöke $\mathbb{F}_2$ felett. Tehát ahelyett, hogy felsorolnánk az összes negyedfokú polinomot, hagyjuk ki a 0 konstans tagúakat, vagyis amelyeknek a 0 gyöke, valamint amelyeknek páros sok tagja van, azaz gyök az 1 (az utóbbi csak 2 karakterisztika esetén).

Így már csak az alábbi *negyedfokúak* közül kerülhetnek ki az irreduciblisek:

$$\underline{x^4+x+1}, \quad x^4+x^2+1, \quad \underline{x^4+x^3+1}, \quad \underline{x^4+x^3+x^2+x+1}$$

Ebből már csak a másodfokú irreducibilis négyzetét, azaz $(x^2+x+1)^2$-et kell kihúznunk, ami x^4+x^2+1-el egyenlő. Tehát a fent aláhúzottak maradnak.

Az így kapott polinomok a hatodfokúakig a következő táblázatban láthatóak.

Fokszám	$\mathbb{F}_2$ feletti irreducibilisek			Számuk
$n=1$	x,	$x+1$		2
$n=2$	x^2+x+1			1
$n=3$	x^3+x+1,	x^3+x^2+1		2
$n=4$	x^4+x+1,	x^4+x^3+1,	$x^4+x^3+x^2+x+1$	3
$n=5$	x^5+x^2+1,	$x^5+x^4+x^3+x+1$,	$x^5+x^4+x^3+x^2+1$,	6
	x^5+x^3+1,	$x^5+x^4+x^2+x+1$,	$x^5+x^3+x^2+x+1$	
$n=6$	x^6+x+1,	$x^6+x^5+x^4+x^2+1$,	$x^6+x^5+x^2+x+1$,	9
	x^6+x^3+1,	$x^6+x^5+x^4+x+1$,	$x^6+x^4+x^3+x+1$,	
	x^6+x^5+1,	$x^6+x^5+x^3+x^2+1$,	$x^6+x^4+x^2+x+1$	

2.1. táblázat. Irreducibilisek $\mathbb{F}_2$ felett

Hasonlóan a 3 elemű testre, a negyedfokúakig.

Fokszám	$\mathbb{F}_3$ feletti normált irreducibilisek			Számuk
$n=1$	x,	$x+1$,	$x+2$	3
$n=2$	x^2+1,	x^2+x+2,	x^2+2x+2	3
$n=3$	x^3+2x+1,	x^3+2x^2+1,	x^3+x^2+x+2,	8
	x^3+2x+2,	x^3+2x^2+x+1,	x^3+2x^2+2x+2	
	x^3+x^2+2,	x^3+x^2+2x+1,		
$n=4$	x^4+x+2,	x^4+x^2+x+1,	$x^4+2x^3+x^2+1$,	18
	x^4+2x+2,	x^4+x^2+2x+1,	$x^4+x^3+x^2+x+1$,	
	x^4+x^2+2,	x^4+2x^2+2x+2,	$x^4+2x^3+x^2+x+2$,	
	x^4+2x^2+2,	x^4+2x^3+x+1,	$x^4+x^3+x^2+2x+2$,	
	x^4+x^3+2,	x^4+x^3+2x+1,	$x^4+2x^3+2x^2+x+2$,	
	x^4+2x^3+2,	$x^4+x^3+x^2+1$,	$x^4+2x^3+x^2+2x+1$	

2.2. táblázat. Normált irreducibilisek $\mathbb{F}_3$ felett

2.2. Irreducibilisek száma

Ez a módszer nagy fokszám esetén, illetve az alaptest elemszámának növekedésével hosszadalmassá válhat. Már az $\mathbb{F}_3$ feletti ötödfokú normált irreducibilisek felsorolásától

is eltekintek, mert túl sok helyet venne igénybe, (48 különböző polinomot kellett volna a táblázatban feltüntetni). A következő lépésben pedig a normált hatodfokú polinomok száma a 3 elemű test felett 729, ezeket már felírni is hosszadalmas lenne, még akkor is, ha kihagyjuk azokat amelyeknek gyöke a 0, és ráadásul ebből még ki kellene válogatni az irreducibiliseket. Ehelyett inkább számoljuk meg őket.

A polinomok össz számából vonjuk ki a reducibiliseket, amelyek úgy állhatnak elő, mint alacsonyabb fokú irreducibilisek szorzatai. Ezt egyszerű kombinatorikai eszközökkel megkaphatjuk. Jelölje $N_{n,p}$ az n-edfokú normált irreducibilisek számát $\mathbb{F}_p$ felett.

$\mathbb{F}_5$ felett a normált *elsőfokú* polinomok száma 5, ezek irreducibilisek is egyben így $\boxed{5} = N_{1,5}$.

A normált *másodfokúak* száma 25. Reducibilist úgy kaphatunk, hogy vesszük 2 különböző elsőfokú szorzatát: ezt $\binom{5}{2} = 10$ féleképpen tehetjük meg, vagy vesszük 1 elsőfokú négyzetét: ez $\binom{5}{1} = 5$-féleképpen tehető meg. Tehát a másodfokú normált irreducibilisek száma: $25 - 15 = \boxed{10} = N_{2,5}$.

Normált *harmadfokú* polinomból van 125 ($= 5^3$). A reducibilisek számát a következőképpen kapjuk:

- egy másodfokú és egy elsőfokú normált irreducibilis szorzata: $\binom{N_{2,5}}{1} \cdot \binom{N_{1,5}}{1} = \binom{10}{1} \cdot \binom{5}{1} = 50$ féle,
- három elsőfokú szorzata: $\binom{N_{1,5}}{3} = \binom{5}{3} = 10$ féle,
- egy elsőfokú négyzetének és egy másik elsőfokú szorzata: $\binom{N_{1,5}}{1} \cdot \binom{N_{1,5}-1}{1} = \binom{5}{1} \cdot \binom{4}{1} = 20$ féle,
- egy elsőfokú köbe: $\binom{N_{1,5}}{1} = \binom{5}{1} = 5$ féle lehet.

Tehát a normált irreducibilisek száma: $125 - (50 + 10 + 20 + 5) = \boxed{40} = N_{3,5}$.

A normált *negyedfokúak* száma 625. Annyival egyszerűsíthetjük a számolást, hogy pl. a csupa elsőfokú szorzatot, ahelyett hogy esetekre bontanánk aszerint, hogy

- 1 normált elsőfokú irreducibilis negyedik hatványát,
- 1 elsőfokú köbének és 1 tőle különbözőnek a szorzatát,
- 1 elsőfokú négyzetének és 2 tőle különbözőnek a szorzatát,
- 2 különböző elsőfokú négyzetét,

- 4 különböző elsőfokú szorzatát vesszük,

egy egyszerű visszatevéses mintavétellel számoljuk, így a számukra: $\binom{n+k-1}{k}$ adódik, ha n lehetőség közül visszatevéssel választunk k darabot.
A *negyedfokú* normált reducibilisek száma:

- egy harmadfokú és egy elsőfokú szorzata: $\binom{N_{3,5}}{1} \cdot \binom{N_{1,5}}{1} = \binom{40}{1} \cdot \binom{5}{1} = 200$ féle,
- két másodfokú szorzata: $\binom{N_{2,5}+2+1}{2} = \binom{11}{2} = 55$ féle,
- egy másodfokú és két elsőfokú szorzata: $\binom{N_{2,5}}{1} \cdot \binom{N_{1,5}+2-1}{2} = \binom{10}{1} \cdot \binom{6}{2} = 150$ féle,
- 4 elsőfokú szorzata: $\binom{N_{1,5}+4-1}{4} = \binom{5+4-1}{4} = \binom{8}{4} = 70$ féle lehet.

Így az irreducibilisek száma: $625 - (200 + 55 + 150 + 70) = \boxed{150} = N_{4,5}$.

Összesítés a következő táblázatban látható, mindenütt a normált polinomok számát, illetve a normált irreducibilisek számát tüntettük fel.

	$\mathbb{F}_2$		$\mathbb{F}_3$		$\mathbb{F}_5$		$\mathbb{F}_7$	
n	Normált polinomok száma	Irreducibilisek száma	Normált polinomok száma	Irreducibilisek száma	Normált polinomok száma	Irreducibilisek száma	Normált polinomok száma	Irreducibilisek száma
1	2	2	3	3	5	5	7	7
2	4	1	9	3	25	10	49	21
3	8	2	27	8	125	40	343	112
4	16	3	81	18	625	150	2401	588
5	32	6	243	48	3125	624	16807	3360
6	64	9	729	116	15625	2580	117649	19544

2.3. táblázat. Normált irreducibilisek száma

Elárulom, hogy a 7 elemű test feletti hatodfokú normált irreducibilisek számát már nem ezzel a módszerrel számoltam, hanem a következő fejezetben ismertetendő módszerrel.

2.3. Képlet az irreducibilisek számára

Az előbbi egy rekurzív módszer, azaz ahhoz, hogy például a tizedfokú irreducibilisek számát megkapjuk, ismernünk kell az összes nála alacsonyabb fokú irreducibilisek számát. Létezik egy egyszerűbb képlet, de ehhez definiálnunk kell a Möbius függvényt,

illetve használnunk kell a Möbius-féle megfordítási formulát. Ez utóbbinak a bizonyítása megtalálható [4]-ben, itt most nem bizonyítjuk.

2.3.1. Definíció. *A $\mu(n)$ Möbius függvényt mint számelméleti függvényt a következőképpen értelmezzük:*

$$\mu(n) = \begin{cases} 1, & \text{ha } n = 1 \\ 0, & \text{ha létezik } p \text{ prím, hogy } p^2 \mid n \\ (-1)^k, & \text{ha } n = p_1 \cdot p_2 \dots p_k, \text{ ahol } p_i \text{ -k különböző prímek.} \end{cases}$$

2.3.2. Tétel. *Legyen f egy számelméleti függvény, és f összegezési függvénye pedig: $F(n) = \sum_{d|n} f(d)$. Így, ha F adott, akkor f a következő módon határozható meg:*

$$f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) \cdot F(d). \tag{2.1}$$

A fenti formulát nevezzük Möbius-féle megfordítási formulának.

2.3.3. Állítás. *Jelölje $F_d(x)$ azon $\mathbb{F}_p[x]$-beli polinomok szorzatát, melyek normált d-edfokú irreducibilisek $\mathbb{F}_p$ felett. Ekkor $x^{p^n} - x = \prod_{d|n} F_d(x)$.*

Bizonyítás. Tudjuk, hogy $f(x) = x^{p^n} - x$ gyökei egyszeresek, hiszem $f'(x) = -1$, így $(f, f') = 1$. Az is világos, hogy a $q = p^n$ elemű testnek, $\mathbb{F}_q$-nak minden eleme gyöke f-nek, hiszen ha α eleme $\mathbb{F}_q^\times$-nek, akkor a Lagrange-tételből következik, hogy $\alpha^{p^n-1} = 1$, és a 0 is nyilvánvalóan gyöke ($f(0) = 0$). (Valójában éppen ezzel a gondolatmenettel igazoltuk az $\mathbb{F}_q$-nak mint f felbontási testének létezését a 1.0.8. Tételben.)

Azt kell megmutatnunk, hogy $\prod_{d|n} F_d(x)$ gyökei is egyszeresek és megegyeznek az $\mathbb{F}_q$ elemeivel. Világos, hogy különböző irreducibilis polinomoknak nem lehet közös gyökük, hiszen, ha lenne, akkor a legalább elsőfokú $\mathbb{F}_q$-beli legnagyobb közös osztójuk, osztaná mind a két polinomot. Másrészt ha egy $\mathbb{F}_p$ feletti $g(x)$ polinom irreducibilis, akkor többszörös gyöke csak úgy lehetne, ha a deriváltjára $g(x)' = 0$ teljesülne, ez esetben pedig $g(x) = h(x^p) = h(x)^p$, ami ellentmondana g irreducibilitásának.

Ezután már csak azt kell belátnunk, hogy $\prod_{d|n} F_d(x)$ gyökei megegyeznek $\mathbb{F}_p$ elemeivel. Vegyünk először egy $g(x) \in \mathbb{F}_p[x]$ d-edfokú normált irreducibilis polinomot, melynek jelöljük egy gyökét α-val, azaz $g(\alpha) = 0$. Ekkor $\mathbb{F}_p(\alpha)$ az $\mathbb{F}_p$ d-ed fokú bővítése, így α gyöke lesz az $x^{p^d} - x$ polinomnak, sőt $\alpha \neq 0$ esetén az $x^{p^d-1} - 1$ polinomnak is. De ha d osztója n-nek, akkor $n = l \cdot d$ miatt

$$p^n - 1 = p^{l \cdot d} - 1 = (p^d - 1)(p^{(l-1)d} + p^{(l-2)d} + \dots + p^d + 1),$$

azaz $t = p^d - 1 | p^n - 1 = s$. Ekkor $s = t \cdot u$ miatt

$$x^{p^n-1}-1 = x^s-1 = x^{t\cdot u}-1 = (x^t-1)(x^{(n-1)t}+x^{(n-2)t}\cdots+1) = (x^{p^d-1}-1)(x^{(n-1)t}+\cdots+1),$$

vagyis α gyöke az $f(x) = x^{p^n} - x$ polinomnak. Mivel ez nyilván akkor is igaz, ha $\alpha = 0$, ezzel beláttuk, hogy $\prod_{d|n} F_d(x)$ gyökei az $\mathbb{F}_q$ elemei közül kerülnek ki.

Végezetül vegyük most $\mathbb{F}_q$ egy tetszőleges α elemét, és nézzük α-nak az $\mathbb{F}_q$ feletti minimálpolinomját, melynek a fokát jelöljük d-vel. Mivel $\mathbb{F}_p(\alpha) \subseteq \mathbb{F}_q$, ezért $\mathbb{F}_{p^d}$ részteste $\mathbb{F}_q$-nak, azaz létezik olyan l, hogy $(p^d)^l = p^n$. Így $d|n$, vagyis $\mathbb{F}_q$ minden eleme gyöke egy d-edfokú irreducibilis polinomnak, valamely $d|n$-re. Ezzel az állítást bebizonyítottuk. □

2.3.4. Tétel. *Legyen $N_{n,p}$ az n-edfokú irreducibilisek száma $\mathbb{F}_p$ felett, és $\mu()$ a Möbius függvény.*
Ekkor

$$N_{n,p} = \frac{1}{n} \cdot \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d \tag{2.2}$$

képlet adódik az irreducibilisek számára.

Bizonyítás. Legyen $N_{d,p}$ a d-ed fokú normált irreducibilis polinomok száma $\mathbb{F}_p$ felett, ahol d pozitív egész. Ekkor az előző tételben bebizonyított $x^{p^n} - x = \prod_{d|n} F_d$ egyenlőség mindkét oldalának fokát meg kell viszgálnunk. $x^{p^n} - x$ foka nyilván p^n, a $\prod_{d|n} F_d$ kifejezésben pedig F_d foka $d \cdot N_{d,p}$, $\forall$ d-re, ezért

$$p^n = \sum_{d|n} d \cdot N_{d,p}.$$

Ekkor p^n az $n \cdot N_{n,p}$ függvény összegezési függvényének felel meg. Azaz ha alkamazzuk a Möbius-féle megfordítási formulát $n \cdot N_{n,p}$-re, akkor:

$$n \cdot N_{n,p} = \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d.$$

A keresett képlet pedig n-nel való osztás után rögtön adódik.

Vegyük észre, hogy $N_{n,p} \neq 0$, mivel

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) p^d \;=\; p^{d_1} \pm p^{d_2} \pm \cdots \pm p^{d_k}$$

alakban írható fel, ahol d_i-k különbözőek. □

Alkalmazzuk már kiszámolt értékekre (a 2.3. táblázat alapján).
$\mathbb{F}_3$ esetén a negyedfokú normált irreducibilisek száma:

$$N_{4,3} = \frac{1}{4} \cdot \left[\mu\left(\frac{4}{1}\right) \cdot 3 + \mu\left(\frac{4}{2}\right) \cdot 3^2 + \mu\left(\frac{4}{4}\right) \cdot 3^4 \right] = \frac{1}{4} \cdot [0 + (-1) \cdot 9 + 81] = 18$$

$\mathbb{F}_7$ felett az ötödfokú normált irreducibilisek száma:

$$N_{5,7} = \frac{1}{5} \cdot \left[\mu\left(\frac{5}{1}\right) \cdot 7 + \mu\left(\frac{5}{5}\right) \cdot 7^5 \right] = \frac{1}{5} \cdot [(-1) \cdot 7 + 16807] = 3360.$$

Ez a számolás testbővítésen alapul. Legyen a test, ami felett számolni szeretnénk $\mathbb{F}_p$. Ha az m-ed fokú irreducibilisek számát keressük, akkor ehhez vegyük $\mathbb{F}_p$ m-ed fokú bővítését $L = \mathbb{F}_{p^m}$-t, amely p^m elemű. Itt már van gyöke minden m-ed fokú $\mathbb{F}_p$ felett irreducibilis polinomnak. Ekkor már csak az a feladatunk, hogy $\mathbb{F}_{p^m}$ elemei között megtaláljuk ezeket. A gyökök számát megkaphatjuk egy egyszerű logikai szita segítségével, majd ha a kapott értéket elosztjuk m-mel pontosan az $\mathbb{F}_p$ feletti irreducibilisek számát kapjuk (mivel minden polinomhoz m darab gyök tartozik). A logikai szitára azért van szükség, hogy minden elemet egyszer vonjunk le p^m-ből, mivel számos elem az L több résztestének is eleme lehet. L résztestei azok a p^d elemű testek, ahol $d|m$. Tehát p^m-ből vonjuk le minden résztest elemszámát, ekkor lehetnek olyan résztestek, amelyeket többször is levontunk, ez abban az esetben fordul elő, ha $\mathbb{F}_{p^{d_1}} \subseteq \mathbb{F}_{p^{d_2}}$ $(d_1 \neq d_2)$ tartalmazás áll fenn.

Nézzük meg néhány konkrét esetre is az előbbi gondolatmenetet.

$\mathbb{F}_3$ feletti negyedfokú irreducibilisek száma:
$\mathbb{F}_{3^4}$ résztestei $\mathbb{F}_3$, és $\mathbb{F}_{3^2}$. Mivel a 3 elemű test részteste $\mathbb{F}_{3^2}$-nek is, így az elemszámát kétszer is levontuk, ezt korrigálva a számolás a következő:

$$N_{4,3} \;=\; \frac{3^4 - (3 + (3^2)) + 3}{4} \;=\; 18.$$

$\mathbb{F}_5$ feletti hatodfokú irreducibilisek száma:
$\mathbb{F}_{5^6}$ résztestei: $\mathbb{F}_{5^3}$, $\mathbb{F}_{5^2}$ és $\mathbb{F}_5$. Az utóbbi mindkét nála nagyobb résztestnek eleme, tehát az elemszámát háromszor vontuk ki, ezért hozzá kell adni kétszer, hogy helyesen kapjuk meg a gyökök számát. Tehát:

$$N_{6,5} \;=\; \frac{5^6 - ((5^3) + (5^2) + 5) + 10}{6} \;=\; 2580.$$

3. fejezet

Berlekamp algoritmusa

Ez a fejezet Prasolov-Polynomials című könyve alapján került feldolgozásra [1] , amely Elwyn Berlakamp 1967-es cikkén alapul [3].

Az egyik legismertebb módszer véges test feletti polinomok irreducibilis faktorokra bontására Berlekamp algoritmusa. Ezt fogjuk részletesen megviszgálni. Az algoritmus fontosságát az adja elsősorban, hogy az $\mathbb{F}_p[x]$-beli faktorizációt a $\mathbb{Z}[x]$ (azaz $\mathbb{Q}[x]$-beli) gyors faktorizációra is alkalmazhatjuk.

3.1. Többszörös irreducibilis faktorok

Legyen $f = f_1^{\alpha_1} \cdot f_2^{\alpha_2} \cdots f_k^{\alpha_k} \in \mathbb{F}_p[x]$, ahol $f_i^{\alpha_i}$ $(1 \leq i \leq k)$ különböző irreducibilis normált polinomok $\alpha_i \in \mathbb{N}^+$ multiplicitással. Az algoritmus csak olyan polinomokra működik, melyben nincsenek többszörös irreducibilis faktorok, ezért az f polinom faktorizációját először visszavezetjük egy ilyen polinom fölbontására. Ezt a következő módon tehetjük meg.

Tegyük fel, hogy $\alpha_1 > 1$, és deriváljuk f-et.
A szorzat deriválási szabályának megfelelően:

$$f' = \alpha_1 \cdot f_1^{\alpha_1 - 1} \cdot f' \cdot (\underbrace{f_2^{\alpha_2} \cdot f_3^{\alpha_3} \cdots f_k^{\alpha_k}}_{g}) + f_1^{\alpha_1} \cdot \underbrace{(f_2^{\alpha_2} \cdot f_3^{\alpha_3} \cdots f_k^{\alpha_k})'}_{g'}, \text{ ahol } f_1 \nmid g.$$

Ebből, ha kiemeljük $f^{\alpha_1 - 1}$-et, a következőt kapjuk:

$$f' = f_1^{\alpha_1 - 1} \cdot (\underbrace{f_1' \cdot \alpha_1 \cdot g + f_1 \cdot g'}_{h + f_1 \cdot g'}).$$

Vegyük észre, hogy mivel f_1 irreducibilis, ezért $f_1' \neq 0$, mert $f_1' = 0$ esetén f_1-ben minden nem mulla együtthatójú tag kitevője osztható p-vel, azaz

$$f_i(x) = a_{t\cdot p}x^{t\cdot p} + a_{(t-1)\cdot p}x^{(t-1)\cdot p} + \cdots a_{1\cdot p}x^{1\cdot p} + a_{0\cdot p}x^{0\cdot p} = l_i(x^p) = l_i(x)^p.$$

Ez pedig ellentmond f_1 irreducibilitásának.
Ha tehát $\alpha_1 \neq 0$ $\mathbb{F}_p$-ben, akkor

$$f' = f_1^{\alpha_1 - 1}(h + f_1 \cdot g'), \text{ ahol } f_1 \nmid h,$$

következésképpen $f_1 \nmid h + f_1 \cdot g'$. Feltéve tehát, hogy semelyik $\alpha_i \neq 0$-val $\mathbb{F}_p$-ben, azt kapjuk, hogy:

$$f' = f_1^{\alpha_1 - 1} \cdot f_2^{\alpha_2 - 1} \cdots f_k^{\alpha_k - 1} \cdot G, \text{ ahol } f_i \nmid G, \ \forall \ i\text{-re}.$$

Ezután vegyük f és f' legnagyobb közös osztóját:

$$(f, f') = f_1^{\alpha_1 - 1} \cdot f_2^{\alpha_2 - 1} \cdots f_k^{\alpha_k - 1}.$$

Ezzel megkaptuk a faktorokat eggyel kisebb kitevőn. Így ha f-et elosztjuk az (f, f') legnagyobb közös osztóval, pontosan f faktorait kapjuk, méghozzá mindegyiket pontosan egyszer.

Vegyük észre, hogy mivel véges test felett vagyunk ez nem minden esetben működik. Előfordulhat, hogy $f' = f^{\alpha_1 - 1} \cdot (f_1' \cdot \alpha_1 \cdot g + f_1 \cdot g')$-ban az eddig kitevőként szereplő $\alpha_1 \in \mathbb{N}^+$ az $\mathbb{F}_p$ test felett mint szorzó 0-vá válik, vagyis $\alpha_1 \equiv 0 \ (mod\ p)$.
Ekkor

$$f' = f_1^{\alpha_1} \cdot g' \ \Rightarrow \ (f, f') = f_1^{\alpha_1} \cdot (f_2^{\alpha_2 - 1} \cdots f_k^{\alpha_k - 1}).$$

Vagyis f_1 kitevője nem fog csökkenni.
Nézzük meg mit tehetünk ebben az esetben. Ha például: $p|\alpha_1$ de $p \nmid \alpha_2, \ldots, \alpha_k$.
Ekkor

$$f' = f_1^{\alpha_1} \cdot (f_2^{\alpha_2} \cdot f_3^{\alpha_3} \cdots f_k^{\alpha_k})'.$$

Általában tehát, ha $\alpha_i \equiv 0 \ (\text{mod } p)$, akkor:

$$\frac{f}{(f, f')} = \prod_{j \neq i} f_j.$$

Így $(f, f') = d$ általános alakja a fentiek szerint a következő:

$$d = (f, f') = \prod_{p \nmid \alpha_i} f_i^{\alpha_i - 1} \prod_{p | \alpha_i} f_i^{\alpha_i}.$$

Osszuk le f-fet d-vel:

$$\frac{f}{d} = \prod_{p \nmid \alpha_i} f_i.$$

Így megkaptuk f néhány faktorának szorzatát.

Nincs más dolgunk, mint megvizsgálni d fokát. Ha $0 < \deg d = \deg f$, akkor d-ben f összes f_i faktora pontosan α_i-szer szerepel, vagyis $\alpha_i \equiv 0 \ (mod\ p)$, $\forall\ i$-re. Tehát $d = \prod_{p|\alpha_i} f_i^{\alpha_i} = g^p$. Ekkor g foka nyilván kisebb, mint f foka, tehát g-re alkalmazhatjuk az algoritmust.

Ha viszont $\deg d < \deg f$, akkor alkalmazhatjuk a Berlekamp algoritmust $\frac{f}{d}$-re. Az algoritmus megadja azokat az f_i-ket, melyekre $p \nmid \alpha_i$-t. Hogy megkapjuk a többit is, osszuk le az ilyen f_i-knek a lehető legnagyobb hatványával a $d = (f, f')$ polinomot. Az osztás után a $\bar{d} = \prod_{p|\alpha j} f_j^{\alpha_j}$ polinomot kapjuk. Erre alkalmazhatjuk azt a redukciót, hogy $\bar{d} = r(x)^p$, és faktorizálhatjuk a nyilvánvalóan alacsonyabb fokú r-et.

3.2. Szükséges tételek

Mielőtt rátérnénk magára az algoritmusra, be kell látnunk hozzá a következő tételeket.

3.2.1. Tétel. *Legyen $f \in \mathbb{F}_p[x]$ egy $n > 0$ fokú normált polinom.*

i) Ha h egy $\mathbb{F}_p$ beli polinom, amely teljesíti a $h^p \equiv h \ (mod\ f)$ kongruenciát, azaz $h^p - h$ osztható f-fel, akkor f a következő alakban áll elő:

$$f(x) = \prod_{a \in \mathbb{F}_p} (f(x), h(x) - a),$$

ahol $(f(x), h(x) - a)$ a két polinom legnagyobb közös osztóját jelenti.

ii) Legyen $f = f_1 \cdots f_k$, ahol $f_1 \cdots f_k$ különböző normált irreducibilis polinomok. Ekkor $h^p \equiv h \ (mod\ f)$, akkor és csak akkor teljesülhet, ha $h(x) \equiv a_i \ (mod\ f_i)$, ahol $a_i \in \mathbb{F}_p$. Továbbá az is igaz, hogy minden $(a_1, \ldots, a_k) \in \mathbb{F}_p^k$-hoz pontosan egy ilyen normált h polinom tartozik, aminek a foka kisebb, mint f foka.

Bizonyítás. i) Legyen $F(x) = \prod_{a \in \mathbb{F}_p} (f(x), h(x) - a)$. Nyilvánvaló, hogy a $h(x) - a$ polinomok különböző a-kra páronként relatív prímek. Tehát az $(f(x), h(x) - a)$ polinomok egymáshoz relatív prím osztói $f(x)$-nek, vagyis $f(x)$ osztható ezek szorzatával, $F(x)$-szel. Tudjuk továbbá, hogy az $\mathbb{F}_p$ test felett igaz a következő azonosság: $\prod_{a \in \mathbb{F}_p} (y - a) = y^p - y$,

mivel az $y^p - y$-nak az $\mathbb{F}_p$ minden eleme gyöke. Alkalmazva ezt $y = h(x)$-re a következőt kapjuk:

$$\prod_{a \in \mathbb{F}_p} (h(x) - a) = h(x)^p - h(x).$$

h választása miatt $h(x)^p - h(x)$ osztható $f(x)$-szel, vagyis $f(x)$ osztja $\prod_{a \in \mathbb{F}_p}(h(x) - a)$-t is, azaz az $F(x)$ polinomot. Mivel f és F oszthatóak egymással és tudjuk, hogy normáltak, ebből már következik, hogy $f = F$.

ii) Ha $h(x) \equiv a_i \ (mod\ f_i)$, akkor vehetjük a p-edik hatványát, arra is teljesül a kongruencia. Mivel $a_i \in \mathbb{F}_p$-re $a_i^p = a_i$, ezért minden i-re igaz a következő: $h(x)^p \equiv a_i^p = a_i \equiv h(x) \ (mod\ f_i)$, tehát $h(x)^p \equiv h(x) \ (mod\ f_1 \cdot f_2 \cdots f_k)$.

Megfordítva, ha a

$$h(x)^p - h(x) = \prod_{a \in \mathbb{F}_p} (h(x) - a)$$

polinom osztható f-fel, akkor osztható az összes $f_1, \ldots, f_k$ polinommal is. De ha a páronként relatív prím $(h(x) - a)$-k szorzatát osztja egy f_i irreducibilis polinom, akkor ez azt jelenti, hogy osztja valamely faktorát is, azaz $\forall\ i$-re $\exists\ a_i \in \mathbb{F}_p$, hogy $h(x) \equiv a_i \ (mod\ f_i)$.

Még be kell még látnunk, hogy bármely $(a_1, \ldots, a_k)$-hoz egyértelműen létezik ilyen h. Ez rögtön következik a polinomokra vonatkozó kínai maradéktételből.

3.2.2. Lemma. *(Kínai maradéktétel polinomokra)*
Legyenek $f_1, \ldots, f_k$ egymáshoz relatív prím irreducibilis polinomok egy F test felett, valamint $g_1, \ldots g_k$ tetszőleges polinomok ugyanezen test felett. Ekkor létezik olyan h polinom, amelyre igaz, hogy $h(x) \equiv g_i \ (mod\ f_i)$ és ez a polinom egyértelműen meghatározott modulo $f = f_1 \cdots f_k$.

Bizonyítás. Az f_i és $F_i = \frac{f}{f_i}$ relatív prímek. Tehát léteznek olyan a_i és b_i polinomok, hogy $a_i f_i + b_i F_i = 1$ teljesül. Vagyis $b_i F_i \equiv 1 \ (mod\ f_i)$, valamint $b_i F_i \equiv 0 \ (mod\ f_j)$, ahol $j \neq i$. Válasszuk h-t a következő képpen: $h = \sum b_i g_i F_i$. Ekkor, ha modulo f_i nézzük, akkor a szummában csak az i. tag nem 0, vagyis igaz a következő:

$$h \equiv g_i b_i F_i \equiv g_i \ (mod\ f_i).$$

Ezzel a létezést bebizonyítottuk.

Az egyértelműség pedig abból következik, hogy ha $\exists\ h_1, h_2$, hogy $h_1 - g_i$ és $h_2 - g_i$ is osztható f_i-vel, akkor a különbségüknek is, azaz $h_1 - h_2$-nek is oszthatónak kell lennie f_i-vel vagyis $f_1 \cdots f_k = f$ osztja $h_1 - h_2$-t, azaz $h_1 \equiv h_2 \ (mod\ f)$. $\square\ \square$

3.3. Az algoritmus

Most megadjuk az algoritmust egy olyan F polinomra, melynek az irreducibilis faktorai páronként különbözők. Először is keresni fogunk egy alkalmas $h \in \mathbb{F}_p[x]$ polinomot, melyre $h(x)^p \equiv h(x)\ (mod\ F)$, továbbá deg $h <$ deg F. Az első lépés azon alapul, hogy a feni $h(x)^p \equiv h(x)\ (mod\ F)$ kongruencia ekvivalens egy $\mathbb{F}_p$ feletti lineáris egyenletrendszerrel, mégpedig a következő módon. Mivel deg $h <$ deg $F = m$, legyen h a kövekező alakú:

$$h(x) = t_0 + t_1 x + \cdots + t_{m-1} x^{m-1}. \tag{3.1}$$

Nyilván ennek vehetjük $\mathbb{F}_p$ felett a p-edik hatványát, amely:

$$h(x)^p = h(x^p) = t_0 + t_1 x^p + \cdots + t_{m-1} x^{p(m-1)}. \tag{3.2}$$

Ekkor minden x^{pj}-t $(j = 0, 1, \ldots, m-1)$ osszunk el maradékosan F-fel:

$$x^{pj} \equiv \sum_{i=0}^{m-1} q_{i,j} x^i\ (mod\ F).$$

Az így kapott maradékokat helyettesítsük (3.2)-be.

$$h(x)^p \equiv t_0 + t_1 \cdot \sum_{i=0}^{m-1} q_{i,1} x^i + \cdots + t_{m-1} \cdot \sum_{i=0}^{m-1} q_{i,(m-1)} x^i\ (\text{mod } F). \tag{3.3}$$

Vegyük észre, hogy (3.3) jobb oldalán egy legfeljebb $(m-1)$-ed fokú polinom áll, ami kongruens $h(x)^p$-nel, így $h(x)$-szel is. Ez csak úgy lehetséges, hogy ha $h(x)$ megegyezik ezzel a polinommal. Ez azt jelenti, hogy h megtalálásához a következő egyenletrendszert kell megoldanunk:

$$\sum_{j=0}^{m-1} t_j q_{i,j} = t_i,\ (i = 1, \ldots, m-1) \tag{3.4}$$

vagyis a (3.3) egyenlet kibontása után kapott együtthatók, azaz $\sum_{j=0}^{m-1} t_j q_{i,j}$-k és a (3.1)-ben szereplő t_i-k egyenlőségét kell megvizsgálnunk.

A 2.3.3. állításából könnyen látszik, hogy a keresett h-k egy k dimenziós alteret alkotnak, ahol k az F irreducibilis faktorainak a száma. Így (3.4) megoldásterének dimenziója egyenlő lesz k-val. Nyilván $q_{0,0} = 1$ és $q_{i,0} = 0$ $(i > 0)$. Ekkor (3.4)-nek triviálisan megoldása: $t_0 = c, t_1 = \cdots = t_{m-1} = 0$, de ez egy konstans h polinomot eredményez, tehát ez nem lehet jó megoldás.

Miután megtaláltuk (3.4) nem triviális megoldását, vegyünk egy bázist a megoldástérből. A bázis első elemének válasszuk a konstans 1 polinomot, és jelöljük $h_1 = 1, h_2, \ldots, h_k$-val. Ha $k = 1$, akkor F irreducibilis. Ha $k > 1$, akkor sorra határozzuk meg $F(x)$ és $h_2(x) - a$ legnagyobb közös osztóját minden $a \in \mathbb{F}_p$-re. Így megkapunk F osztói közül s darabot, legyenek ezek: $g_1, \ldots, g_s$. Ha $s < k$, akkor ezt megismételjük $h_3(x), h_4(x) \ldots$-re egészen addig, amíg meg nem találjuk a k darab különböző irreducibilis faktort.

Megfigyelhetjük, hogy ily módon végül tényleg megkapjuk az összes k darab osztót. Ehhez azt kell megmutatnunk, hogy ha f_1 és f_2 két különböző irreducibilis faktora F-nek, akkor van olyan h a fönti polinomok közül, melyre $f_1|(h(x) - a)$ és $f_2|(h(x) - b)$ valamely $a \neq b$-re. Ekkor ugyanis, valamely h_i bázispolinom szét fogja választani f_1 és f_2 faktorokat, azaz megkapjuk őket mint két különböző faktor. Legyen f_1 és f_2 F két különböző irreducibilis faktora. Vegyünk olyan $(a_1 \ldots a_k)$ sorozatot $\mathbb{F}_p$-ből, melyre $a_1 \neq a_2$. Ekkor tudjuk, hogy van olyan h, melyre teljesül:

$$h(x) \equiv a_1 \ (mod\ f_1) \text{ és } h(x) \equiv a_2 \ (mod\ f_2).$$

Ekkor azonban már valamelyik h_i bázispolinomra is teljesülnie kell, hogy $h_i(x) \equiv b_1 \ (mod\ f_1)$ és $h_i(x) \equiv b_2 \ (mod\ f_2)$, ahol tudjuk, hogy $b_1 \neq b_2$.

Megjegyzés. Az algoritmus hatékonyságát növelhetjük, ha $h_i(x) - a = h_i(x) - ah_1(x)$ helyett a következő polinomot vizsgáljuk:

$$H(x) = a_1 h_1(x) + \cdots + a_k h_k(x)$$

ahol $a_1, \ldots, a_k$ tetszőleges véletlen elemek $\mathbb{F}_p$-ből, majd vesszük a legnagyobb közös osztóját F-nek és $H(x)^{\frac{p-1}{2}} - 1$-nek. Ha F reducibilis és $p \geq 3$, akkor $\geq \frac{4}{9}$ valószínűséggel rögtön megkapjuk F nem triviális faktorizációját.

3.4. Példák

Nézzük végig az algoritmust néhány példán keresztül is.

1.) Példa

Konstruáljunk először egy $\mathbb{F}_3$ feletti reducibilis polinomot úgy, hogy a 2.2. táblázat alapján vegyünk néhány irreducibilis polinomot és szorozzuk őket össze, így a végén ellenőrizhetjük, hogy minden faktort helyesen kaptunk-e meg.

$$f = (x^2 + 1)^2(x + 2) = x^5 + 2x^4 + 2x^3 + x^2 + x + 2, \quad f \in \mathbb{F}_3[x]$$

Deriváljuk, hogy csak egyszeres faktorok maradjanak.

$$f' = 5x^4 + 8x^3 + 6x^2 + 2x + 1 = 2x^4 + 2x^3 + 2x + 1$$

Hazározzuk meg f és f' legnagyobb közös osztóját az Euklideszi algoritmus segítségével, egyszerű maradékos osztásokat végezve:

$$\begin{array}{l} (x^5+2x^4+2x^3+x^2+x+2) : (2x^4+2x^3+2x+1) = 2x+2 \\ \underline{-(x^5 + x^4 + x^2 + 2x)} \\ \qquad (x^4 + 2x^3 + 2x + 2) \\ \quad \underline{-(x^4 + x^3 + x + 2)} \\ \qquad\quad x^3 + x \end{array}$$

Az így kapott maradék $x^3 + x = r_1$, tehát f a következő alakú:

$$f = (2x + 2)f' + (x^3 + x).$$

Folytatjuk az algoritmust a tanultak szerint, azaz osszuk el f'-t az r_1 maradékkal:

$$\begin{array}{l} (2x^4 + 2x^3 + 2x + 1) : (x^3 + x) = 2x + 2 \\ \underline{-(2x^4 + 2x^2)} \\ \qquad (2x^3 + x^2 + 2x + 1) \\ \quad \underline{-(2x^3 + 2x)} \\ \qquad\quad x^2 + 1 \end{array}$$

Ebből $x^2 + 1 = r_2$, és $f' = (2x + 2)r_1 + (x^2 + 1)$.
Folytatva, ha r_1-et osztjuk r_2-vel, akkor $r_1 = x \cdot r_2 + 0$-t kapunk. Ekkor a legnagyobb közös osztó az utolsó nem 0 maradék, azaz $x^2 + 1 = (f, f')$.
Majd ha ezzel leosztjuk f-fet, megfelelő alakúvá válik a polinom, és alkalmazhatjuk rá az algoritmust:

$$F = \frac{f}{(f, f')} = \boxed{x^3 + 2x^2 + x + 2}.$$

Megjegyzés. Vegyük észre, hogy itt most (f, f') irreducibilis, így rögtön megkaptuk f egy faktorát. f-et leosztva $x^2 + 1$ egy maximális hatványával, könnyen megkapjuk az f helyes

faktorizációját a Berlekamp algoritmus alkalmazása nélkül is. Ettől függetlenül folytassuk az algoritmust.

Ezután találnunk kell egy megfelelő h polinomot, amelynek a foka kisebb, mint F foka, azaz $0 < \deg h < \deg F = 3$, tehát $h = ax^2 + bx + c$ alakú és teljesül, hogy:

$$F|h(x)^3 - h(x) \Rightarrow F|(ax^2 + bx + c)^3 - (ax^2 + bx + c) = ax^6 + bx^3 + c - ax^2 - x - c$$

Osszunk el minden x^{3j} $(j = 1, 2)$ tagot maradékosan F-fel és helyettesítsük be a kapott maradékokat.
x^3-t osztva F-fel:

$$x^3 = 1 \cdot (x^3 + 2x^2 + x + 2) + (x^2 + 2x + 1), \text{ azaz } x^3 \equiv \boxed{x^2 + 2x + 1} \pmod{F}$$

x^6-t osztva F-fel:

$$x^6 = (x^3 + x^2) \cdot (x^3 + 2x^2 + x + 2) + x^2, \text{ azaz } x^6 \equiv \boxed{x^2} \pmod{F}$$

A behelyettesítés után kapott kongruencia:

$$ax^2 + b(x^2 + 2x + 1) + c - ax^2 - bx - c \equiv 0 \ (mod\ F) \Rightarrow bx^2 + bx + b \equiv 0 \ (mod\ F),$$

akkor és csak akkor teljesülhet, ha az a és c szabad változók mellett b mindig 0, azaz $h = ax^2 + c$ alakú. Ekkor a megoldástér pontosan 2 dimenziós. Legyenek a bázis elemei a következők: $h_1 = 1$ szokás szerint, valamint $h_2 = x^3$. Ekkor már csak néhány maradékos osztást kell elvégeznünk, hogy megkapjuk a faktorokat.

Határozzuk meg F és $(h_2(x) - a)$ legnagyobb közös osztóját, ha $a = 0, 1 \in \mathbb{F}_2$.
F osztva x^2-tel:

$$F = (x + 2) \cdot x^2 + \underbrace{(x + 2)}_{r_1},$$

majd x^2 osztva r_1-el:

$$x^2 = (x + 1)(x + 2) + 2.$$

Azaz F és x^2 legnagyobb közös osztója: $(F, x^2) = 2 = g_1$.
F-fet $x^2 + 1$-gyel osztva kapjuk, hogy:

$$F = (x + 2)(x^2 + 1) + 0$$

Tehát $(F, x^2+1) = x^2+1 = g_2$, vagyis $\boxed{x^2+1}$ az F polinom egy irreducibilis faktora. Osszuk le F-et x^2+1-el, akkor $\frac{F}{x^2+1} = \boxed{x+2}$. Ezzel megtaláltuk a keresett faktorokat.

Ekkor ha az eredeti polinomnak (f-nek) vannak többszörös gyökei, mint ebben az esetben is, miután megtaláltuk F faktorait egyszerűen osszuk le velük f-fet és a kapott polinomra ismételjük az eljárást, ha szükséges.

2.) Példa

Most egy $\mathbb{F}_2$ feletti polinomot faktorizáljunk. A 2.1. táblázatból választottam irreducibiliseket és vettem azok szorzatát. Tekintsük a következő polinomot:

$$f = (x+1)^2(x^3+x^2+1)^2 = x^8+x^4+x^2+1.$$

Ennek a deriváltja 0, így a következő helyettesítést kell elvégeznünk:

$$f = g^2 \;\Rightarrow\; g = x^4+x^2+x+1.$$

Ekkor g deriváltja $g' = 1$, ezért alkalmazhatjuk az algoritmust a fenti g polinomra.

Keressünk olyan $h(x)$ polinomot, melynek foka $\deg h < \deg g = 4$, azaz $h(x) = ax^3+bx^2+cx+d$ alakú. Így a következő kongruenciát kell megvizsgálnunk:

$$(ax^6+bx^4+cx^2+d) - (ax^3+bx^2+cx+d) \equiv 0 \pmod{g}.$$

A következő lépésben számoljuk ki az x^{2j} $(j = 2, 3)$ tagok g-vel vett osztási maradékait.

x^6-t osztva g-vel:

$$x^6 = (x^2+1)\cdot(x^4+x^2+x+1) + (x^3+x+1), \text{ azaz } x^6 \equiv \boxed{x^3+x+1} \pmod{g}$$

x^4-t osztva g-vel:

$$x^4 = 1\cdot(x^4+x^2+x+1) + (x^2+x+1), \text{ azaz } x^4 \equiv \boxed{x^2+x+1} \pmod{g}$$

Behelyettesítjük:

$$ax^3+ax+a+bx^2+bx+b+cx^2+d+ax^3+bx^2+cx+d \equiv 0 \pmod{g} \Leftrightarrow$$

$$cx^2+(a+b+c)x+(a+b+c) = 0$$

Ez csak akkor teljesülhet, ha $c = 0$ és $a = b$, tehát $h(x) = ax^3+ax^2+d$ alakú. Válasszuk a bázispolinomoknak a következőket: $h_1 = 1,\ h_2 = x^2+x^3$ A faktorok megtalálásához

határozzuk meg g és $h_2 - b$, $b \in \mathbb{F}_2$ polinomok legnagyobb közös osztóit:
g osztva $x^3 + x^2$-tel:

$$x^4 + x^2 + x + 1 = (x + 1) \cdot (x^3 + x^2) + \underbrace{(x + 1)}_{r_1}$$

majd $x^3 + x^2$ osztva r_1-el:

$$x^3 + x^2 = (x^2)(x + 1) + 0$$

Azaz $(g, x^3 + x^2) = \boxed{x + 1} = l_1$, és ez egy irreducibilis faktora g-nek.
g osztva $x^3 + x^2 + 1$-el:

$$x^4 + x^2 + x + 1 = (x + 1) \cdot (x^3 + x^2 + 1) + 0$$

Így $(g, x^3 + x^2 + 1) = \boxed{x^3 + x^2 + 1} = l_2$, egy másik faktora g-nek.

Ha elosztjuk g-t l_1-el, amit kapunk $\frac{x^4+x^2+x+1}{x+1} = (x^3 + x^2 + 1)$, ami éppen l_2. Tehát megtaláltuk g összes irreducibilis faktorát.

Ekkor még csak g faktorizációját határoztuk meg, a keresett f polinom faktorizációja helyett. Ezt a következő módon kaphatjuk, meg g felbontásából. Osszuk le f-et g fent kapott faktoraival, annyiszor ahányszor csak lehet. Így azt kapjuk, hogy f az $x+1$ négyzetével még osztható, de a köbével már nem. Ekkor $\frac{x^8+x^4+x^2+1}{(x+1)^2} = x^6+x^4+1 = (x^3+x^2+1)^2$. Tehát megkaptuk f faktorizációját, pontosan úgy, ahogy azt megadtuk a példa elején.

4. fejezet

Kódelméleti alkalmazás

Maga a kódolás nem összetévesztendő a titkosítással. Mi most nem olyan szöveget szeretnénk kódolni, amit csak mi és a címzett érthet. A kódolás az a folyamat, amikor a küldendő üzenetet egy olyan jelsorozattá (kóddá) alakítunk, hogy a használt eszköz tárolni illetve továbbítani tudja ezeket. Majd a dekódolás ezeknek a jeleknek az eredetivé alakítását jelenit. A továbbítás során számolnunk kell annak a kockázatával, hogy hiba vagy zaj keletkezhet a jelekben és így az információ torzulhat. Az ilyen hibák kiküszöbölésével foglalkozik az algebrai kódelmélet.

Az információ küldés lépései a következők:
A küldő/forrás küldi az üzenetet, amelyet egy kódoló (lehet eszköz, szoftver stb.) megfelelően továbbítható kódolt üzenetté alakítja. A kódunk egy csatornán keresztül (pl: rádióhullám, kábel, CD stb.) érkezik a dekódolóhoz, amely a kódból előállítja az eredeti üzenetet és végül ez jut el a címzetthez/felhasználóhoz. Mivel a csatorna sokszor nem megbízható (pl: megsérül egy helyen a CD), ezért olyan kódolást kell alkalmaznunk, hogy a dekódolásnál a hibák minél nagyobb részét képesek legyünk kiszűrni. Az ilyen kódokat nevezzük hibajavító kódoknak.

4.1. Alapfogalmak, jelölések

A kódoláshoz használt ún. kódábécét, azaz a kódok előállításához használható szimbólumok, számok, betűk stb. halmazát jelöljük Q-val. Ennek elemszáma legyen q. Q elemeiből készített k hosszú sorozatok a *szavak*, ezek halmaza Q^k. A kódolás során definiálunk egy injektív $\varphi : Q^k \mapsto Q^n$ függvényt, ami alapján Q^k elemeit megfeleltetjük Q^n elemeinek. Az így képzett $\varphi(Q^k)=C \subseteq Q^n$ halmaz elemei a *kódszavak*. Ekkor C egy (n,k) *paraméterű*

kód, ahol n a létrehozott kód hossza.

4.1.1. Definíció. *Legyen $t \geq 1$ egész szám. Ekkor a $C \subseteq Q^n$ kód t-hibajelző, ha egy kódszót legfeljebb t helyen megváltoztatunk, akkor az eredmény nem lehet kódszó.*
A C kód t-hibajavító, ha veszünk két különböző kódszót v, w és ezeket bármely legfeljebb t helyen megváltoztatjuk, akkor az így kapott v' és w' nem lehet egyenlő.

Ez azt jeleni, hogy ha a kódunk 3 hibajelező, és egy olyan üzenetet kapunk, amely kevesebb, mint 3 helyen van meghibásodva, akkor könnyen észlelhetjük a hibát. Ezzel szemben, ha szinte minden jel meghibásodott, akkor előfordulhat, hogy az eredetitől különböző értelmes üzenetet kapunk, ekkor már nem valószínű, hogy észrevesszük, hogy meghibásodás történt.

4.1.2. Definíció. *v, $u \in Q^n$ kódszó Hamming-távolságán azt értjük, hogy a két szó hány helyen tér el egymástól. Jele: $d(v, u)$.*
A v kódszó Hamming-súlya a nem nulla elemeinek száma. Jelölés: $w(v)$.
A $C \subseteq Q^n$ kód minimális vagy Hamming-távolságán a különböző kódszavak Hamming-távolságainak minimumát értjük. Jele: d.

Kódok létrehozásánál arra kell törekednünk, hogy minél több hibát képesek legyünk javítani, eközben pedig a kód hossza és a kód távolsága minimális legyen. A következő korlátok adhatók ezekre.
Az alábbi állítás nyilvánvaló:

4.1.3. Állítás. *Ha a C kód Hamming-távolsága d, akkor a C kód t-hibajavító minden olyan t-re, melyre $d \geq 2t + 1$. Speciálisan: minden kód $\left[\frac{d-1}{2}\right]$-hibajavító.*

4.1.4. Állítás. *Egy (n, k, d) paraméterű kódban a következő felső becslés adható a d minimális távolságra:*

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

ezt Singleton-korlátnak nevezzük. Ha ez egyenlőséggel teljesül, akkor az ilyen minimális súlyú kódokat MDS kódoknak nevezzük.

Bizonyítás. Legyenek a kódszavaink n hosszúak és a kódszavak távolsága legalább d. Nézzük különböző kódszavak első $n - (d - 1)$ koordinátáit, ezek nem lehetnek teljesen különbözőek, mert akkor csak az utolsó $d-1$ helyen térnének el. Ezért a kódszavak száma q^k legfeljebb q^{n-d+1} (ennyi $n - d + 1$ hosszú szó létezik). □

4.2. Lineáris kódok, Reed-Solomon kódok

Tegyük fel, hogy az üzenet most egy q elemű véges test elemeiből áll ($\mathbb{F}_q$). Ekkor a létrehozható k hosszú üzenetek száma q^k. Ez megfelel az $\mathbb{F}_q$ feletti k dimenziós vektortérnek. Ezt szeretnénk kódolni, vagyis valamilyen függvénnyel $n > k$ hosszú kódszavakat szeretnénk létrehozni, úgy hogy az $\mathbb{F}_q$ feletti k dimenziós vektortér altér legyen az ugyan ezen test felett vett n dimenziós altérnek. Ez a helyzet áll elő, ha a kódoló $\varphi : \mathbb{F}_q^k \mapsto \mathbb{F}_q^n$ függvény lineáris. Az így létrejött (n, k) paraméterű kódokat *lineáris kódoknak* nevezzük és a továbbiakban ilyenekkel foglalkozunk.

4.2.1. Állítás. *Legyen C egy (n, k) paraméterű lineáris kód az $\mathbb{F}_q$ test mint kódábécé fölött, és legyen $\varphi : \mathbb{F}_q^k \mapsto \mathbb{F}_q^n$ a lineáris kódoló függvény. Jelölje $\underline{b}_i = \varphi(\underline{e}_i)$, ahol $\underline{e}_i = (0, \ldots, 0, 1, 0, \ldots, 0)$. Ekkor tehát $C = \varphi(\mathbb{F}_q^k)$, és C-nek a $\underline{b}_1, \ldots, \underline{b}_n$ vektorok egy bázisát alkotják. φ linearitása miatt világos, hogy tetszőleges $\underline{x} = (x_1, \ldots, x_k) \in \mathbb{F}_q^k$ szónak a $\varphi(\underline{x}) = x_1\underline{b}_1 + \cdots + x_k\underline{b}_k$ kódszó fog megfelelni. Ha tehát $B \in \mathbb{F}_q^{k\times n}$ az a mátrix, melynek i-edik eleme $\underline{b}_i$ (mint sorvektor), ekkor $\varphi(\underline{x}) = \underline{x} \cdot B$. Ezt a B mátrixot nevezzük a C kód generátormátrixának.*

Megjegyzés. Ha C lineáris kód, akkor $d = min\{w(v)|v \in C\}$, vagyis a kód Hamming-távolsága megegyezik a különböző kódszavak súlyainak minimimával. Mivel lineáris kódok esetén egy kódszó súlya egyenlő a kód 0 elemétől vett távolságával.

4.2.2. Definíció. *Legyen C egy (n, k) paraméterű kód. Ekkor egy $(n-k)\times n$-es P mátrixot ellenőrző vagy paritásellenőrző mátrixnak nevezzük, amennyiben*

$$P \cdot c^T = 0$$

akkor és csak akkor teljesül, ha $c \in C$.

4.2.3. Definíció. *Legyen c a küldendő kódszó és c' pedig a meghibásodott kódszó, P pedig az ellenőrző mátrix. Ekkor szindrómának nevezzük a következő vektort:*

$$s = P \cdot (c')^T.$$

Megjegyzés. Ez az ellenőrző mátrix definíciója miatt akkor nem 0, ha egy meghibásodott kóddal szorozzuk. Tehát a szindróma csak a hibavektortól függ, így jelzi a hibát.

Az $u = u_1u_2 \ldots u_k$ szó helyett tekinthetjük az $u(x) = u_1x^{k-1} + \cdots + u_{k-1}x + u_k$ polinomot.

4.2.4. Definíció. *Legyen $g \in Q[x]$ egy $(n-k)$ fokú polinom. Ekkor a g generátorpolinomú C polinomkódot a következőképpen definiálhatjuk*

$$C = \{g(x)u(x) \ : \ deg\ u \leq k\}.$$

Ekkor a kódolás nem más, mint a generátor polinommal való szorzás.

4.2.5. Állítás. *Legyen C egy g generátorpolinomú polinomkód, ahol g egy $(n-k)$-ad fokú $\mathbb{F}_q$ feletti polinom. Tegyük fel, hogy $\alpha \neq 0$ az $\mathbb{F}_q$ test egy bővítésének olyan eleme, amelynek multiplikatív rendje legalább n. Ha a g polinomot, úgy választjuk, hogy $\alpha, \alpha^2, \ldots, \alpha^{d-1}$ gyöke legyen valamely $d \leq n$ egészre, akkor a kód minimális távolsága legalább d.*

Bizonyítás. Be kell látnunk, hogy minden $v = ug \neq 0$ alakú polinomnak, azaz minden nem nulla kódszónak, legalább d darab nem nulla együtthatója van. Legyen $v(x) = v_1x^{n_1} + v_2x^{n_2} + \cdots + v_kx^{n_k}$, ahol $k < d$. Ennek gyöke $\alpha, \alpha^2, \ldots, \alpha^{d-1}$, ezért:

$$\begin{pmatrix} \alpha^{n_1} & \ldots & \alpha^{n_k} \\ \alpha^{2n_1} & \ldots & \alpha^{2n_k} \\ \vdots & & \vdots \\ \alpha^{kn_1} & \ldots & \alpha^{kn_k} \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_k \end{pmatrix} = \begin{pmatrix} v(\alpha) \\ v(\alpha^2) \\ \vdots \\ v(\alpha^k) \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Ez egy homogén lineáris egyenletszendszernek is felfogható, ahol az ismeretlenek $v_1, v_2 \ldots, v_k$. Determinánsa a következő:

$$\alpha^{n_1+\cdots+n_k} \cdot \prod_{i>j}(\alpha^{n_i} - \alpha^{n_j}),$$

hiszen az i-edik oszlopból α^{n_i}-t kiemelve ($\forall$ i-re) egy Vandermonde-determináns marad.

Mivel a v polinom megfelel egy kódszónak, a foka kisebb, mint n és így mindegyik n_i kitevő is kisebb n-nél. Ezzel szemben α rendje legalább n, és így az α^{n_i} elemek páronként különbözők. Mivel $\alpha \neq 0$, a fenti determináns sem 0. Ekkor a fenti homogén lineáris egyenletrendszernek csak triviális megoldása van, vagyis mindegyik $v_i = 0$, azaz $v = 0$. □

4.2.6. Definíció. *Legyen α az $\mathbb{F}_q$ test egy nem nulla eleme, melynek a multiplikatív rendje legalább n, továbbá, hogy:*

$$g(x) = (x - \alpha) \cdot (x - \alpha^2) \cdots (x - \alpha^{d-1}).$$

Ekkor a g generátorpolinomú n hosszú kódot Reed-Solomon kódnak nevezzük.

Megjegyzés. Tehát a Reed-Solomon kódok olyan kódok, amelyeket a generáló polinomjuk gyökeivel meg lehet határozni. Gyakran választjuk α-nak az $\mathbb{F}_q$ primitív elemét.

Ezt a kódot előszeretettel alkalmazzák különböző optikai adattárolóknál, adathordozóknál, többek között CD-k adatainak kódolásához. A Reed-Solomon kód közel optimális, mivel a Singleton-féle korlátban egyenlőség áll fenn, azaz a kód minimális távolsága: $d = n - k + 1$.

4.2.7. Definíció. *Legyen $\alpha \neq 0$ az $\mathbb{F}_q$ test egy bővítésének legalább n rendű eleme, és g az $\alpha, \alpha^2, \ldots, \alpha^{d-1}$ elemek $\mathbb{F}_q$ feletti minimálpolinomjainak legkisebb közös többszöröse. A g generálta n hosszú kódot BCH-kódnak nevezzük, és $d \leq n$ szám a kód tervezett távolsága.*

Megjegyzés. Tehát a Reed-Solomon kódok speciális BCH-kódok.

4.3. Reed-Solomon kódok generálása

Nézzük meg, hogyan is tudunk ilyen kódokat léterhozni. Az alábbi példák megtalálhatók [2]-ben. Két egyszerű, szemléletes feladatot dolgoztam fel, amely arra szolgál, hogy a kódelmélet és a véges testek feletti polinomok kapcsolatát megmutassam.

1. Példa Legyen α az $\mathbb{F}_4$ test multiplikatív csoportjának egy generátoreleme, ekkor $o(\alpha) = n = 3$ és $d = 3$ a tervezett távolság. Ekkor $Q = \mathbb{F}_4$, azaz 4 jelünk van a kódok létrehozásához. Mint már beláttuk a négyelemű test elemei az $x^4 - x$ polinom gyökei, melyek legyenek: $0 = \alpha^0,\ \alpha^1,\ \alpha^2,\ \alpha^3 = 1$, ekkor

$$g(x) = (x - \alpha)(x - \alpha^2) = \frac{x^4 - x}{x(x-1)} = x^2 + x + 1.$$

Mivel g foka $n - k = 2$, ezért $n = 3$ miatt a kód $k = 1$-dimenziós. Tehát a kód elemei a konstansok $g(x)$-szeresei:

$$\{0,\ \ x^2 + x + 2,\ \ \alpha x^2 + \alpha x + \alpha,\ \ \alpha^2 x^2 + \alpha^2 x + \alpha^2\} \text{ azaz } \{000,\ \ 111,\ \ \alpha\alpha\alpha,\ \ \alpha^2\alpha^2\alpha^2\}$$

Ezek bináris változata az, amit valójában elküldünk, és ezt a következő módon hozzuk létre:

$$0 \leftrightarrow 00, \qquad 1 \leftrightarrow 01, \qquad \alpha \leftrightarrow 10, \qquad \alpha^2 \leftrightarrow 11.$$

Ez a megfeleltetés tehát a következő: $a\alpha + b \leftrightarrow ab$, ahol a, b az $\mathbb{F}_4$ prímtestének elemei.

Tehát az így kapott kód 2 bit hosszúságú darabokra bontja a küldendő jeleket, és minden ilyen darabot megháromszorozva küld tovább. Legyen az üzenet $M = \alpha 01$, ekkor ezt először a fenti megfeleltetés alapján bitpárokká alakítjuk: 10 00 01. Majd megháromszorozzuk, így a következőt kapjuk: 101010 000000 010101. Abban az esetben, ha a kapott kód 111011 000000 010101, akkor az aláhúzott rész miatt egyértelmű, hogy ez nem lehet kódszó, tehát könnyen látható, hogy 2-hibajelző a kód. Ha ki szeretnénk javítani ezt a hibát, akkor, ha a hozzá legközelebbi kódra javítjuk, akkor azt kapnánk, hogy az üzenet: 111111 000000 010101 volt. Így az is látszik, hogy a kód 1-hibajavító.

2. Példa Legyen α az $\mathbb{F}_{16} = L$ test multiplikatív csoportjának egy generátoreleme, ekkor $o(\alpha) = n = 15$, $d = 5$, $m(x) = x^4 + x^3 + 1$ pedig egy L feletti irreducibilis polinom (a 2.1. táblázatban megtalálható).

Adjuk meg az L testet $\mathbb{F}_2/(m)$ alakban. Ekkor ezen test felett α a következő alakú: $\alpha = x+(m)$. Hogy megértsük az így generálható kód jellegét, először vizsgáljuk meg L szerkezetét. Elemeit kétféle alakban írhatjuk, az egyik az $\mathbb{F}_2$ feletti $a_3\alpha^3+a_2\alpha^2+a_1\alpha+a_0$, amit a $a_3a_2a_1a_0 \in \{0,1\}^4$ sorozattal rövidíthetünk. A másik az α elem hatványaikénti felírás. Az α^i-hez tartozó sorozatot megkaphatjuk, ha x^i-t maradékosan elosztjuk x^4+x^3+1-gyel. Meg kell adnunk minden ilyen α hatványt, mivel $\alpha = x$, ami a 0010 sorozatnak felel meg, ezért ez alapján sorra vehetjük a hatványait: $\alpha^2 = x^2 = 0100$, $\alpha^3 = x^3 = 1000$, $\alpha^4 = x^4$, mivel x^4-nek az $x^4 + x^3 + 1$-gyel vett osztási maradéka $x^3 + 1$, ezért $\alpha^4 = x^3 + 1 = 1001$. Ekkor α hatványai a következők:

0	0000	0	α	0010	x	α^2	0100	x^2	α^3	1000	x^3
α^4	1001	x^3+1	α^5	1011	x^3+x+1	α^6	1111	x^3+x^2+x+1	α^7	0111	x^2+x+1
α^8	1110	x^3+x^2+x	α^9	0101	x^2+1	α^{10}	1010	x^3+x	α^{11}	1101	x^3+x^2+1
α^{12}	0011	$x+1$	α^{13}	0110	x^2+x	α^{14}	1100	x^3+x^2	α^{15}	0001	1

4.1. táblázat. Az $\mathbb{F}_2/(x^4 + x^3 + 1)$ feletti α primitív elem hatványai

Az $m(x)$ polinom gyökei $\alpha, \alpha^2, \alpha^4, \alpha^8$, hiszen a négyzetre emelés relatív automorfizmus, azaz egy olyan $\varphi : \mathbb{F}_2 \mapsto \mathbb{F}_2$ testizomorfizmus, amely a $\mathbb{F}_2/(m)$ test minden elemét fixen hagyja. Ezért m gyökei a szorzásra nézve mind generátorelemek, hiszen ezek a kitevők a 15-höz relatív prímek, tehát m egy primitív polinom. Mivel a 15-höz relatív prímek száma $\varphi(15) = 8$, ezért van még 4 generátorelem, amelyek pontosan az α-nak a 15-höz relatív prím kitevőjű hatványai, vagyis $\alpha^7, \alpha^{14}, (\alpha^{14})^2 = \alpha^13$ és $(\alpha^{13})^2 = \alpha^{11}$. Mivel ezek pont az

$\alpha, \alpha^2, \alpha^4, \alpha^8$ reciprokai, a közös minimálpolinomjuk x^4+x+1, ami éppen a másik negyedfokú primitív polinom. Az alaptest elemei 0, és $\alpha^{15} = 1$ ezek minimálpolinomja elsőfokú. A másodfokú elemek egy négy elemű testben vannak, és így a multiplikatív rendjük 3. Ezek α^5 és α^{10}, közös minimálpolinomjuk x^2+x+1 (ami szintén primitív). A fennmaradó négy elem: $\alpha^3, \alpha^6, \alpha^{12}, (\alpha^{12})^2 = \alpha^9$, tehát csakis a még nem vizsgált negyedfokú irreducibilis polinomnak, $x^4 + x^3 + x^2 + x + 1$-nek lehetnek gyökei, ezek pont a multiplikatív csoport ötödrendű elemei, és így ez a polinom nem primitív.

A BCH-kódhoz tartozó g generátorpolinom az $\alpha, \alpha^2, \alpha^3, \alpha^4$ minimálpolinomjainak legkisebb közös többszöröse, azaz:

$$g(x) = m(x)m_3(x) = (x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1) = x^8 + x^4 + x^2 + x + 1.$$

Ez nyolcadfokú, azaz a kód dimenziója $k = 15 - 8 = 7$, tehát ez a kód egy N hosszú üzenetet $(\frac{15}{7})N$-szeresére növel. Ez a kódolás pedig már 2-hibajavító, mivel $d = 5$.

Irodalomjegyzék

[1] Victor V. Prasolov: *Polynomials*, Springer, 2004

[2] Kiss Emil: *Bevezetés az algebrába*, Typotex, 2007

[3] Berlekamp E. R. *Factoring polynomials over finite fields*, Bell System Tech j 46, 1967

[4] Freud Róbert és Gyarmati Edit: *Számelmélet*, Nemzeti Tankönyvkiadó, 2006

[5] Lakatos Piroska és Huber Balázs: *Bevezetés a véges testek elméletébe* 2007, elektronikus jegyzet, megtekinthető: http://www.math.klte.hu/~lapi/veges_ testek.pdf

[6] Gonda János: *Véges testek* 2011, elektronikus jegyzet, megtekinthető: http://compalg.inf.elte.hu/material/DOWNLOAD/vt.pdf

[7] Pelikán József és Gröller Ákos *Gyűrűk és testek*, 2000, elektronikus jegyzet, megtekinthető: http://www.cs.elte.hu/~pelikan/07_Gyuruk.pdf

[8] Lakatos Piroska: *Kódelmélet* elektronikus jegyzet 2010, megtekinthető: http://www.math.unideb.hu/~lapi/kodelm.pdf

[9] Maróti Miklós: *Hibajavító kódolás* elektronikus jegyzet 2008, megtekinthető: http://www.math.u-szeged.hu/~mmaroti/okt/2009t/kodolas.pdf

[10] Csercsa Richárd: *Reed-Solomon kódok* elektronikus jegyzet, megtekinthető: http://digitus.itk.ppke.hu/~cseri/edu/i%E9ke/ct/reed_sol.pdf

[11] Visontay Péter *Kódelmélet összefoglaló* elektronikus jegyzet 2002, megtekinthető: http://www.doksi.hu/get.php?lid=7346

[12] Wettl Ferenc: *Kódelmélet és kriptográfia* elektronikus jegyzet 2011, megtekinthető: http://www.math.bme.hu/~wettl/okt/kodkripto/2014/kk.pdf

Köszönetnyilvánítás

Szeretném megköszönni témavezetőmnek, Ágoston Istvánnak, hogy tanácsaival és bátorításával folyamatosan ösztönzött arra, hogy minél jobban elsajátítsam ezen témakört. Valamint köszönettel tartozom családomnak, és barátaimnak, hogy a tanulmányaim során támogattak, és segítettek céljaim elérésében.

Nyilatkozat

Név: Csohány Dóra
ELTE Természettudományi kar, szak: Matematika BSc
Neptun azonosító: ENCT42
Szakdolgozat címe: Polinomok véges testek felett

A **szakdolgozat** szerzőjeként fegyelmi felelősségem tudatában kijelentem, hogy a dolgozatom önálló munkám eredménye, saját szellemi termékem, abban a hivatkozások és idézetek standard szabályait következetesen alkalmaztam, mások által írt részeket a megfelelő idézés nélkül nem használtam fel.

Budapest, 2014

_____
a hallgató aláírása