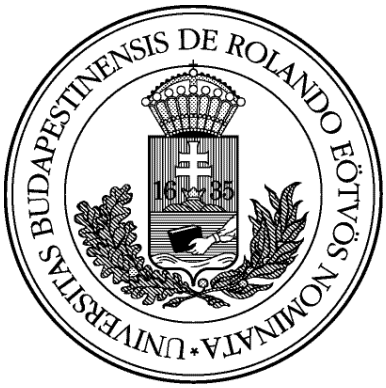
Eötvös Loránd Tudományegyetem
Természettudományi kar

Gábor Hanna
Matematika BSc
Matematikus szakirány

Permutáció-polinomok

Szakdolgozat

Témavezető: Sziklai Péter
Számítógéptudományi tanszék



Budapest, 2015

Köszönetnyilvánítás

Ezúton is szeretném megköszönni Sziklai Péternek a téma ajánlását és segítségét a szakdolgozat létrejöttéhez.

Tartalomjegyzék

1. Bevezetés

A szakdolgozat alapvetően Gerhard Turnwald A new criterion for permutation polynomials című cikkét ([1]) dolgozza fel, ám annál sokkal részletesebben. Először definiáljuk egy véges test feletti polinom különböző jellemzőit, majd az ezek közötti összefüggéseket vizsgáljuk, különös tekintettel arra a kérdésre, hogy mikor lesz egy polinom permutáció-polinom, azaz bijektív. Ezen kívül szó lesz a permutáció-polinomok és bizonyos speciális alakú (ciklikus) mátrixok kapcsolatáról. Végül véges geometriákkal összefüggésben tárgyaljuk, hogy egy f polinomra $f(x)+cx$ hány c-re permutáció-polinom.

1.1. Néhány fogalom és jelölés

Az egész dolgozat során p egy tetszőleges prím, $q = p^m$ prímhatvány és $\mathbb{F}_q$ a q elemű véges testet jelöli. A dolgozatban az $\mathbb{F}_q$ feletti polinomokkal foglalkozunk. f egy tetszőleges ilyen polinomot jelöl, most erre definiáljuk a vizsgálandó értékeket.

Egy kézenfekvő jellemző a polinom foka, jelölje ezt n. A többi jellemző invariáns abban az értelemben, hogy csak attól függ, hogy f mely értékeket milyen multiplicitással veszi fel. Az egyik ilyen invariáns az, hogy mekkora az f értékkészlete, ezt v-vel jelöljük.

A következő invariáns definiálásához szükségünk lesz az elemi szimmetrikus polinomokra. Az n változós elemi szimmetrikus polinomok $1 \leq k \leq n$-re a következők: $s_k(x_1, ..., x_n) = \sum_{1 \leq i_1 < ... < i_k \leq n} x_{i_1} x_{i_2} ... x_{i_k}$. Jelölje s_k az f multiplicitással vett értékeinek k-adik elemi szimmetrikus polinomját, tehát $s_k = s_k(f(a_1), ..., f(a_q))$, ahol $\mathbb{F}_q = \{a_1, ..., a_q\}$. Legyen u az a legkisebb k egész szám, amelyre az f multiplicitással vett értékeinek k-adik elemi szimmetrikus polinomja nem 0, azaz
$u = \min\{k \in \mathbb{Z}^+ : s_k \neq 0\}$. Ha nem létezik ilyen k, akkor $u = \infty$.

Legyen w az a legkisebb k egész szám, amelyre f multiplicitással vett értékeinek k-adik hatványösszege nem 0. A $p_k = \sum_{a \in \mathbb{F}_q} f(a)^k$ jelöléssel
$w = \min\{k \in \mathbb{Z}^+ : p_k \neq 0\}$. Ha nem létezik ilyen k, akkor $w = \infty$.

Többször szükségünk lesz még a Newton-Waring formulára, amely $x_1, \ldots, x_n$ elemi szimmetrikus polinomjai és hatványösszegei közti összefüggést írja le.

1.1.1. Tétel (Newton-Waring formula)**.** *Legyen* $p_k(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i^k$.
Ekkor $1 \leq k \leq n$ *egész számra*

$$(-1)^m \cdot m \cdot s_m(x_1, \ldots, x_n) + \sum_{k=1}^{m} (-1)^{k+m} p_k(x_1 \ldots, x_n) \cdot s_{m-k}(x_1, \ldots, x_n) = 0.$$

2. Permutáció-polinomok és összefüggések az invariánsok között

2.1. u, v, w és n közötti összefüggések

Az s_k értékek felírhatók a $\prod_{a\in\mathbb{F}_q}(x-f(a))$ polinom együtthatóiként. Ennek segítségével kiszámolhatjuk u-t az alábbi állítás alapján.

2.1.1. Állítás.

1. *Ha* $x^q - \prod_{a\in\mathbb{F}_q}(x-f(a))$ *nem konstans, akkor* $\deg\left(x^q - \prod_{a\in\mathbb{F}_q}(x-f(a))\right) = q-u.$
2. $x^q - \prod_{a\in\mathbb{F}_q}(x-f(a)) \equiv c \iff f(a) = c\ (\forall a \in \mathbb{F}_q)$
3. *Ha* $v \geq 2$, *akkor* $1 \leq u < q$.
   Ha $\forall a \in \mathbb{F}_q$*-ra* $f(a) = 0$, *akkor* $u = \infty$.
   Ha $\forall a \in \mathbb{F}_q$*-ra* $f(a) = b \neq 0$, *akkor* $u = q$.

Bizonyítás.

1. $\prod_{a\in\mathbb{F}_q}(x-f(a)) = x^q - s_1x^{q-1} + s_2x^{q-2} - \cdots + (-1)^q s_q.$
2. Tegyük fel, hogy $f(a) = c\ (\forall a \in \mathbb{F}_q)$. Ekkor
$$x^q - \prod_{a\in\mathbb{F}_q}(x-f(a)) = x^q - (x-c)^q = c.$$
Most tegyük fel, hogy $x^q - \prod_{a\in\mathbb{F}_q}(x-f(a)) = c$. Legyen $b \in \mathbb{F}_q$ olyan, hogy $\exists a \in \mathbb{F}_q$, hogy $f(a) = b$. Ekkor $c = b^q - \prod_{a\in\mathbb{F}_q}(b-f(a)) = b^q - 0 = b$.
3. Tegyük fel, hogy $v = 2$. Ekkor (2) miatt $g(x) = x^q - \prod_{a\in\mathbb{F}_q}(x-f(a))$ nem konstans. (1) szerint $q - u = \deg g \geq 1$. Tehát $u \leq q-1$.
Tegyük fel most, hogy $v = 1$. Ekkor $\exists c$, hogy $\forall a \in \mathbb{F}_q\ g(a) = c$. Ha $c = 0$, akkor $s_k = 0\ \forall k$, így $u = \infty$. Ha $c \neq 0$, akkor $s_q = c^q = c$ és $k < q$-ra $s_k = \binom{q}{k}\cdot c^k = 0$, mert $p|\binom{q}{k}$.

□

2.1.2. Példa. *Ha* f *permutáció-polinom, akkor* $v = q$. *Az előző állítás szerint*

$$q - u = deg\Big(x^q - \prod_{a\in\mathbb{F}_q}(x-f(a))\Big) = deg(x^q - x^q + x) = 1,$$

vagyis $u = q - 1$.
w *meghatározásához számoljuk ki a* p_k *értékeket. A Newton-Waring formulák segítségével* p_k *kifejezhető az* s_i *értékekkel:* $p_k = \sum_{i=1}^{k-1}(-1)^{i+k+1}p_i s_{k-i} + (-1)^{k+1}ks_k$

Mivel $i < u = q - 1$ *-re* $s_i = 0$, *ezért* $p_k = \begin{cases} 0 & ha\ 0 < k < q-1 \\ q-1 & ha\ k = q-1 \end{cases}$

Tehát $w = q - 1$.

A későbbiekben is szerepelnek konkrét példák, ahol kiszámoljuk egy adott polinom u, v, w értékeit. A következő állítás alapján ezeket mind meg lehetne fogalmazni általánosabban is.

2.1.3. Állítás.

1. *Ha* $g(x)$ *permutáció-polinom, akkor* $f(x)$ *és* $f \circ g(x)$ u, v, w *értékei megegyeznek.*

2. *Ha* $a, b \in \mathbb{F}_q$, $a \neq 0$ *és* $v = 1$ *esetén* $b = 0$, *akkor* $af(x) + b$ u, v, w *értékei megegyeznek* $f(x)$ u, v, w *értékeivel.*

Bizonyítás.

1. Triviális.

2. Először lássuk be, hogy $f(x)$ és $a \cdot f(x)$ u, v, w értékei megegyeznek:
   v megegyezik, mert $ac = ad \iff c = d$. $(a \neq 0)$
   u megegyezik, mert $s_k(\{a \cdot f(c) : c \in \mathbb{F}_q\}) = a^k \cdot s_k$ és mivel $a \neq 0$, ezért $a^k \cdot s_k = 0 \iff s_k = 0$.
   w megegyezik, mert $\sum_{c\in\mathbb{F}_q}(a \cdot f(c))^k = a^k \sum_{c\in\mathbb{F}_q} f(c)^k$ és mivel $a \neq 0$, ezért $a^k \sum_{c\in\mathbb{F}_q} f(c)^k = 0 \iff \sum_{c\in\mathbb{F}_q} f(c)^k = 0$.
   Most lássuk be, hogy $f(x)$ és $g(x) = f(x) + b$ u, v, w értékei megegyeznek:
   v megegyezik, mert $c + b = d + b \iff c = d$.
   u megegyezése: ha $v = 1$, akkor a feltétel szerint $b = 0$. Ha $v \geq 2$, akkor 2.1.1 szerint

$$q - u_g = \deg\left(x^q - \prod_{c\in\mathbb{F}_q}(x - (f(c) + b))\right) = \deg\left(x^q - \prod_{c\in\mathbb{F}_q}(x - b + f(c))\right) =$$

$$= \deg\left((x-b)^q - \prod_{c\in\mathbb{F}_q}((x-b) + f(c)) + b^q\right) =$$

$$= \deg(\pm s_u(x-b)^{q-u} \mp s_{u+1}(x-b)^{q-u-1} \pm \dots) = q - u.$$

w megegyezik, mert

$$\sum_{c\in\mathbb{F}_q}(f(c)+b)^k=\sum_{c\in\mathbb{F}_q}f(c)^k+\sum_{i=1}^{k-1}d_i\sum_{c\in\mathbb{F}_q}f(c)^i=\begin{cases}0 & \text{ha } k<w\\ \sum\limits_{c\in\mathbb{F}_q}f(c)^w\neq 0 & \text{ha } k=w.\end{cases}$$

□

Most vizsgáljuk meg w-t kicsit közelebbről.

2.1.4. Állítás. *Ha $w<\infty$, akkor $w<q$ és $p\nmid w$.*

Bizonyítás. Ha $\sum\limits_{a\in\mathbb{F}_q}f(a)^k\neq 0$ és $k\geq q$, akkor $\sum\limits_{a\in\mathbb{F}_q}f(a)^{k-q}\neq 0$. Így ha $w<\infty$, akkor $w<q$.
Tegyük fel, hogy $k=pl$ és $\sum\limits_{a\in\mathbb{F}_q}f(a)^k\neq 0$. Mivel $f(a)^k=(f(a)^l)^p=f(a)^l$, ezért ekkor $\sum\limits_{a\in\mathbb{F}_q}f(a)^l\neq 0$. Így ha $w<\infty$, akkor $p\nmid w$. □

Ha $n\geq 1$, akkor w -re tudunk alsó becslést adni q és n segítségével:

2.1.5. Állítás. *Legyen $n\geq 1$. Ekkor $w\geq\frac{q-1}{n}$ és $w=\frac{q-1}{n}\iff n|q-1$.*

Bizonyítás. Legyen $f=\sum\limits_{i=0}^{n}c_ix^i$. Ekkor

$$p_k=\sum_{a\in\mathbb{F}_q}(c_na^n+...+c_1a+c_0)^k=\sum_{a\in\mathbb{F}_q}\Big(c_n^ka^{nk}+\sum_{i=0}^{nk-1}d_ia^i\Big)=c_n^k\sum_{a\in\mathbb{F}_q}a^{nk}+\sum_{i=0}^{nk-1}\Big(\sum_{a\in\mathbb{F}_q}a^i\Big)d_i.$$

Ha $kn<q-1$, akkor $0\leq i\leq kn$ -re $\sum\limits_{a\in\mathbb{F}_q}a^i=0$, ezért $p_k=0$. Tehát $k<\frac{q-1}{n}$-re $p_k=0$, és így $w\geq\frac{q-1}{n}$.
Ha $kn=q-1$, akkor $p_k=-c_n^k\neq 0$. Tehát ha $n|q-1$, akkor $k=\frac{q-1}{n}$-re $p_k\neq 0$, és így $w=\frac{q-1}{n}$. □

2.1.6. Következmény. *Ha f permutáció-polinom (ekkor $w=q-1$) és $n|q-1$, akkor $n=1$.*

Korábban kifejeztük u -t $x^q-\prod\limits_{a\in\mathbb{F}_q}(x-f(a))$ alapján. w is kifejezhető egy alkalmas polinom segítségével az alábbi állítás szerint.

2.1.7. Állítás.

1. *Legyen $g(x)=\sum\limits_{a\in\mathbb{F}_q}(x-f(a))^{q-1}$. Ekkor ha $w<\infty$, akkor $q-w-1=\deg g$. Ha $w=\infty$, akkor $g\equiv 0$.*

2. *$a \in \mathbb{F}_q$-ra jelölje n_a az a f általi őseinek számát. Ekkor $w = \infty \iff \forall a \in \mathbb{F}_q$ - ra $p | n_a$.*

Bizonyítás.

1. $\sum\limits_{a \in \mathbb{F}_q} (x - f(a))^{q-1} = \sum\limits_{a \in \mathbb{F}_q} \frac{(x-f(a))^q}{x-f(a)} = \sum\limits_{a \in \mathbb{F}_q} \sum\limits_{i=0}^{q-1} f(a)^i \cdot x^{q-1-i} = \sum\limits_{i=0}^{q-1} (\sum\limits_{a \in \mathbb{F}_q} f(a)^i) \cdot x^{q-1-i}$

2. $w = \infty \iff g \equiv 0$
   $g(a) = -n_a \ (\forall a \in \mathbb{F}_q)$
   Ezért ha $g \equiv 0$, akkor $\forall a \in \mathbb{F}_q$ - ra $p | n_a$. Ha pedig $\forall a \in \mathbb{F}_q$ - ra $p | n_a$, akkor g-nek van q gyöke, és $\deg g < q$, ezért $g \equiv 0$.

□

Az első résznek fontos következménye, hogy ha $w < \infty$, akkor felülről becsülhető $v - 1$ -gyel:

2.1.8. Következmény. *Ha $w < \infty$, akkor $w \leq v - 1$.*

Bizonyítás. Legyen $b \in \mathbb{F}_q$ tetszőleges, g mint előbb. Ha $\nexists a \in \mathbb{F}_q$, amire $f(a) = b$, akkor $g(b) = 0$. Tehát g-nek legalább $q - v$ gyöke van. Mivel $w < \infty \iff g \not\equiv 0$, ezért $q - v \leq \deg g = q - w - 1$. □

Az alábbi két példa olyan, ahol w eléri $v - 1$ -et.

2.1.9. Példa. *Ha $f(x)$ permutáció-polinom, akkor $v = q$, $w = q - 1 = v - 1$.*

2.1.10. Példa. *Ha $f(x) = x^n$, akkor $v = \frac{q-1}{(q-1,n)} + 1$, $w = v - 1$.*

Bizonyítás. $\mathbb{F}_q$ multiplikatív csoportja, $\mathbb{F}_q^*$, ciklikus. Legyen ω a generátoreleme,
$d = (q - 1, n)$, $k = \min\{j \in \mathbb{Z}^+ : \omega^{jn} = 1\} = \frac{[n,q-1]}{n}$.
Ha $0 \leq i, j \leq k - 1$ és $i \neq j$, akkor $\omega^{in} \neq \omega^{jn}$. Továbbá $\omega^{in} = \omega^{(i+k)n}$. Ezek alapján ha $\exists a \in \mathbb{F}_q^*$, amire $a^n = b$, akkor b f szerinti őseinek száma $\frac{q-1}{k} = (n, q - 1) = d$.
Tehát $v = \frac{q-1}{d} + 1$.
w meghatározásához először lássuk be, hogy u, v, w nem változik, ha $f(x) = x^n$ helyett $g(x) = x^d$ -t tekintjük. Azt láttuk az előbb, hogy ha $\exists a \in \mathbb{F}_q^*$, amire $a^n = b$, akkor $|f^{-1}(b)| = d$. Ezt g-re alkalmazva azt kapjuk, hogy ha $\exists a \in \mathbb{F}_q^*$, amire $a^d = b$, akkor $|g^{-1}(b)| = d$. Ha $\exists a \in \mathbb{F}_q$, amire $a^n = b$, akkor $c = a^{n/d}$ -re $c^d = b$. Ezek szerint $\forall a \in \mathbb{F}_q$ -ra $|f^{-1}(a)| = |g^{-1}(a)|$, ezért f és g u, v, w értékei megegyeznek.
Innen 2.1.5 szerint $w = \frac{q-1}{(n,q-1)}$.

□

2.1.11. Megjegyzés. *Az eddigiekből több dolog következik v-vel kapcsolatban is:*

1. *A 2.1.5 és a 2.1.8 állítást összevetve $w < \infty$ esetén $v \geq w + 1 \geq \frac{q-1}{n} + 1$.*

2. *Ha $w < \infty$ helyett csak azt tesszük fel, hogy f nem konstans, akkor is tudunk hasonló, bár kicsit gyengébb becslést adni v -re:*
   mivel f nem konstans, ezért a 0 őseinek száma legfeljebb f foka, vagyis n. Tetszőleges $a \in \mathbb{F}_q$-ra ez $(f-a)$-ra is igaz, így $|f^{-1}(a)| = |(f-a)^{-1}(0)| \leq n$. Tehát minden elemnek legfeljebb n őse van, így $v \geq \frac{q}{n}$. Ebből $v \geq [\frac{q-1}{n}] + 1$.

3. *A 2.1.7 állítás második részéből következik, hogy ha $w = \infty$, akkor $\forall a \in \mathbb{F}_q$ -ra $p|n_a$, tehát minden értéknek legalább p őse van. Ebből $v \leq \frac{q}{p}$. Ha azt is feltesszük, hogy $n \geq 1$, akkor mivel a 0-nak is legalább p őse van, ezért $n \geq p$.*

A következő példa 2 dolgot is mutat. Egyrészt azt, hogy ha $q > p$, akkor a megjegyzés első részében nem hagyható el a $w < \infty$ feltétel.
Másrészt azt, hogy a harmadik részben lévő egyenlőtlenségek teljesülhetnek egyenlőséggel is.

2.1.12. Példa. *Ha $f(x) = x^p - x$, akkor $w = \infty$, $n = p$, és $v = \frac{q}{p}$.*

Bizonyítás. f -nek p gyöke van, ez a p gyök éppen $\mathbb{F}_p \leq \mathbb{F}_q$. Ha $\exists a \in \mathbb{F}_q$, amire $f(a) = b$, akkor $\forall c \in \mathbb{F}_p$ -re $f(a+c) = b$. Ez p különböző őse b-nek. Több nem lehet, mert $x^p - x - b$-nek p gyöke lehet. Tehát $v = \frac{q}{p}$. $w = \infty$, mert $\forall a \in \mathbb{F}_q$ - ra $p|n_a$. □

Az alábbi példa alapján a megjegyzés első részében is teljesülhet egyenlőség:

2.1.13. Példa. *Ha $f(x) = x^n$, akkor láttuk, hogy $v = \frac{q-1}{(q-1,n)} + 1$ és $w < \infty$. (2.1.10 példa). Ha $n|q-1$, akkor $(q-1, n) = n$, így $v = \frac{q-1}{n} + 1$.*

Ha a megjegyzés második részében áll egyenlőség, az elárul valamit w-ről és n-ről is:

2.1.14. Állítás.

1. *Ha $v = \frac{q}{n}$, akkor $w = \infty$ vagy $n = 1$.*

2. *Ha $v = [\frac{q-1}{n}] + 1$, akkor $n|q-1$ vagy $w = \infty$.*

Bizonyítás.

1. Tegyük fel, hogy $w < \infty$. Ekkor az előző megjegyzés első állítása szerint $\frac{q}{n} = = v \geq \frac{q-1}{n} + 1 = \frac{q}{n} + \frac{n-1}{n}$, vagyis $0 = \frac{n-1}{n}$. Azaz $n = 1$.

2. Ha $w < \infty$ és $n \not| q-1$, akkor szintén az előző megjegyzés első állítása szerint $v \geq \frac{q-1}{n} + 1 > [\frac{q-1}{n}] + 1$.

□

Ha $f : \mathbb{F}_q \to \mathbb{F}_q$ függvény, akkor Lagrange-interpolációval megadható egy polinom, ami ugyanazt rendeli minden $a \in \mathbb{F}_q$-hoz, mint az eredeti. Tehát feltehető, hogy f polinom. Az $x^q = x$ egyszerűsítés (esetleg többszöri) alkalmazásával el tudunk jutni egy $\hat{f}$-hoz, amelyre $\deg \hat{f} \leq q-1$ és $\forall a \in \mathbb{F}_q$ -ra $f(a) = \hat{f}(a)$. Ezért ha valahol ki van kötve, hogy $\deg f \leq q-1$, akkor arra úgy is lehet gondolni, hogy $\hat{f}$-et kell venni. $\hat{f}$ együtthatói kiszámíthatóak az interpolációs polinom nélkül is a következő állítás szerint.

2.1.15. Állítás. *Ha* $\deg f \leq q-1$ *és* $f(x) = \sum_{1=1}^{q-1} c_i x^i$, *akkor*

$$\sum_{a \in \mathbb{F}_q} a^k f(a) = \begin{cases} -c_{q-k-1} & \text{ha } 0 \leq k < q-1 \\ -c_0 - c_{q-1} & \text{ha } k = q-1 \end{cases}$$

Bizonyítás. $\sum_{a \in \mathbb{F}_q} a^k f(a) = \sum_{a \in \mathbb{F}_q} \Big(a^k \cdot \sum_{i=1}^{q-1} c_i a^i \Big) = \sum_{i=0}^{q-1} \Big(\sum_{a \in \mathbb{F}_q} a^{i+k} \Big) c_i$

Továbbá

$$\sum_{a \in \mathbb{F}_q} a^{i+k} = \begin{cases} 0 & \text{ha } 0 < i+k < q-1 \text{ vagy } q-1 < i+k < 2(q-1) \\ -1 & \text{ha } i+k = q-1 \text{ vagy } i+k = 2(q-1) \end{cases}$$

Innen $\sum_{i=0}^{q-1} \Big(\sum_{a \in \mathbb{F}_q} a^{i+k} \Big) c_i = \begin{cases} -c_{q-k-1} & \text{ha } 0 \leq k < q-1 \\ -c_0 - c_{q-1} & \text{ha } k = q-1 \end{cases}$ □

Mivel $\hat{f}$ együtthatói kiszámolhatóak $\sum_{a \in \mathbb{F}_q} a^k f(a)$-k segítségével, ezért $\hat{f}$ foka is. Illetve kapunk w-re egy új, az eredetivel ekvivalens definíciót:

2.1.16. Következmény.

1. *Ha* $\deg f \leq q-1$, *akkor* $n = q-1 \iff u = 1 (\iff w = 1)$
2. *Ha* $\deg f \leq q-1$, *akkor* $\deg f \leq q-l-2 \iff 0 \leq k \leq l$ *- re* $\sum_{a \in \mathbb{F}_q} a^k f(a) = 0$.
3. $w = \min\{k \in \mathbb{Z}^+ : \deg \widehat{f(x)^k} = q-1\}$ *(Ha nincs ilyen* k, *akkor* $w = \infty$.*)*

Bizonyítás. Legyen $f(x) = \sum_{1=1}^{q-1} c_i x^i$.

1. $-c_0 - c_{q-1} = \sum_{a \in \mathbb{F}_q} a^{q-1} f(a) = \sum_{a \in \mathbb{F}_q} f(a) - f(0) = \sum_{a \in \mathbb{F}_q} f(a) - c_0$.
   Vagyis $\sum_{a \in \mathbb{F}_q} f(a) = -c_{q-1}$. Így $n = q-1 \iff c_{q-1} \neq 0 \iff \sum_{a \in \mathbb{F}_q} f(a) \neq$
   $= 0 \iff u = 1$.

2. $\deg f \leq q-l-2 \iff 0 \leq k \leq l$ -re $c_{q-1-k} = 0 \iff 0 \leq k \leq l$ - re $\sum\limits_{a \in \mathbb{F}_q} a^k f(a) = 0$.

3. Legyen $\widehat{f(x)^k} = \sum\limits_{1=1}^{q-1} d_i x^i$. Ekkor $-d_0 - d_{q-1} = \sum\limits_{a \in \mathbb{F}_q} a^{q-1} f(a)^k = \sum\limits_{a \in \mathbb{F}_q} f(a)^k - f(0)^k = \sum\limits_{a \in \mathbb{F}_q} f(a)^k - d_0$. Vagyis $\sum\limits_{a \in \mathbb{F}_q} f(a)^k = -d_{q-1}$.

□

Ha meg van adva az, hogy f mely értékeket veszi fel és milyen multiplicitással, de az nem, hogy hol kell felvennie ezeket az értékeket, akkor u alapján eldönthető, hogy $\deg \hat{f}$ egyenlő-e $q-1$-gyel. (2.1.16. következmény, 1. pont.) Ha $\deg \hat{f} \neq q-1$,akkor nem dönthető el ilyen könnyen, hogy mennyi $\hat{f}$ foka. Sőt:

2.1.17. Állítás. *Ha $v \geq 2$, akkor felcserélhetjük úgy az értékeket, hogy egy $q-1$ vagy $q-2$ fokú polinomot kapjunk és u, v, w értéke ne változzon.*

Bizonyítás. Feltehető, hogy $\deg f \leq q-1$. Ha $\sum\limits_{a \in \mathbb{F}_q} f(a) \neq 0$, akkor $\deg f = q-1$. Tegyük fel, hogy $\sum\limits_{a \in \mathbb{F}_q} f(a) = 0$. Ekkor nem tudunk belőle az értékek felcserélésével $q-1$ fokút csinálni. Ha $\sum\limits_{a \in \mathbb{F}_q} a \cdot f(a) \neq 0$, akkor 2.1.15 szerint $\deg f = q-2$. Most tegyük fel azt is, hogy $\sum\limits_{a \in \mathbb{F}_q} f(a) = 0$. Mivel $v \geq 2$, ezért $\exists b \in \mathbb{F}_q$, hogy $f(b) \neq$ $= f(0)$. Legyen

$$g(x) = \begin{cases} f(b) & \text{ha } x = 0 \\ f(0) & \text{ha } x = b \\ f(x) & \text{egyébként} \end{cases}$$

Ekkor $\sum\limits_{a \in \mathbb{F}_q} a \cdot g(a) = \sum\limits_{a \in \mathbb{F}_q} a \cdot f(a) - 0 \cdot f(0) - b \cdot f(b) + 0 \cdot g(0) + b \cdot g(b) = \underbrace{\sum\limits_{a \in \mathbb{F}_q} a \cdot f(a)}_{0} +$

$+ \underbrace{b}_{\neq 0} \underbrace{(f(0) - f(b))}_{\neq 0} \neq 0$. Tehát $\deg g = q-2$. □

2.2. Permutáció-polinomok

A fejezet végén megadjuk a permutáció-polinomok sok ekvivalens jellemzését u, v és w segítségével. Például láttuk korábban, hogy ha f permutáció-polinom, akkor $w = q-1$. Ki fog derülni, hogy ennek a megfordítása is igaz. Sőt, többek között az is elég, ha $w > \frac{2}{3}q - 1$.

Ehhez először szükségünk van egy lemmára, ami ad egy új definíciót w-re. Ebből belátunk újabb összefüggéseket u, v és w között, majd ezek segítségével bebizonyítjuk a tételt.

2.2.1. Lemma.

1. *Ha* $1 \leq k \leq q$ *és* $k < u + w$, *akkor* $p_k = (-1)^{k-1} k s_k$.
2. $w = \min\{k \in \mathbb{Z}^+ : k s_k \neq 0\}$ *(És ha nincs ilyen* k, *akkor* $w = \infty$.*)*

Bizonyítás.

1. A Newton-Girard formula szerint
$$p_k = \sum_{i=1}^{k-1} (-1)^{i-1} s_i p_{k-i} + (-1)^{k-1} k s_k$$
Ha valamely $1 \leq i \leq k-1$ -re $s_i p_{k-i} \neq 0$, akkor $i \geq u$ és $k - i \geq w$. Ez nem lehet a $k < u + w$ feltétel miatt. Tehát $p_k = (-1)^{k-1} k s_k$.
2. Definíció szerint $w = \min\{k \in \mathbb{Z}^+ : p_k \neq 0\}$. Továbbá az első rész miatt $k \leq w$ -re $p_k = (-1)^{k-1} k s_k$. Így $w = \min\{k \in \mathbb{Z}^+ : k s_k \neq 0\}$.

□

Ebből következik az alábbi összefüggés u és w között.

2.2.2. Állítás.

1. *Ha* $w < \infty$, *akkor* $u \leq w$ *és* $u = w \iff p \nmid u$.
2. *Ha* $w = \infty$, *akkor* $p | u$ *vagy* $u = \infty$.

Bizonyítás.

1. A lemma szerint $w s_w = p_w \neq 0$, ezért $u \leq w$.
Ha $p | u$, akkor $p_u = u s_u = 0$, ezért ekkor $w > u$.
Ha $p \nmid u$, akkor $p_u = u s_u \neq 0$, ezért ekkor $w = u$.
2. A lemma szerint $w = \infty$ esetén $\forall k \in \mathbb{Z}^+$-ra $k s_k = 0$. Ha $u < \infty$, akkor $s_u \neq 0$ és $u s_u = 0$ Ez csak úgy lehetséges, ha $p | u$. Tehát $p | u$ vagy $u = \infty$.

□

2.2.3. Következmény. *Ha $v \geq 2$ és $q = p$, akkor $u = w < \infty$. Ugyanis ha $v \geq 2$, akkor 2.1.1 szerint $1 \leq u < q < \infty$. Ha $q = p$ is igaz, akkor $p \nmid u$, így az előző állítás szerint $w = u < \infty$.*

Az állítás további következményeként adhatunk u-ra egy ugyanolyan becslést, mint a 2.1.5. állításban w-re.

2.2.4. Állítás. *Ha $n \geq 1$, akkor $u \geq \frac{q-1}{n}$ és $u = \frac{q-1}{n} \iff n|q-1$.*

Bizonyítás. Tegyük fel, hogy $0 < kn < q-1$.
Ekkor $\deg(s_k(f(x_1), f(x_2), \ldots, f(x_q))) \leq kn < q-1$.
A szimmetrikus polinomok alaptétele szerint létezik $p \in \mathbb{R}[y_1, \ldots, y_q]$, amelyre
$s_k(f(x_1), \ldots, f(x_q)) = p(s_1(x_1, \ldots, x_q), \ldots, s_q(x_1, \ldots, x_q))$.
Mivel $\deg(s_k(f(x_1), \ldots, f(x_q))) < q-1$, ezért p-ben azon tagok együtthatója, amelyekben szerepel y_{q-1} vagy y_q, az 0. Tehát p tekinthető úgy, mint egy $(q-2)$-változós polinom. $s_k(f(x_1), \ldots, f(x_q))$ konstans tagja (és így p konstans tagja is) $s_k(f(0), \ldots, f(0)) = (f(0))^k \binom{q}{k} = 0$.
Jelölje $\mathbb{F}_q$ elemeit $a_1, \ldots, a_q$. Ekkor $1 \leq j \leq q-2$-re $s_j(a_1, \ldots, a_q) = 0$.
Az eddigiekből $s_k(f(a_1), \ldots, f(a_q)) = p(s_1(a_1, \ldots a_q), \ldots, s_{q-2}(a_1, \ldots, a_q)) =$
$= p(0, \ldots, 0) = 0$. Tehát ha $0 < kn < q-1$, akkor $k < u$.
Másrészt $kn < q-1 \iff k < \frac{q-1}{n}$, ezért $u \geq \frac{q-1}{n}$.
Ha $u = \frac{q-1}{n}$, akkor nyilván $n|q-1$, mert u egész. Tegyük fel most, hogy $n|q-1$. Ekkor 2.1.5 szerint $w = \frac{q-1}{n}$. Mivel $w < \infty$, ezért 2.2.2 első része szerint $u \leq w$. Vagyis $u \leq \frac{q-1}{n}$. Az előbb láttuk, hogy $u \geq \frac{q-1}{n}$, tehát $u = \frac{q-1}{n}$. □

2.2.5. Példa. *Korábban láttuk, hogy $f(x) = x^n$-re $v = \frac{q-1}{d} + 1$ és $w = \frac{q-1}{d}$, ahol $d = (q-1, n)$. Most a fenti állítás segítségével kiszámoljuk u-t is.*
Beláttuk korábban azt is, hogy x^n és x^d u, v, w értékei megegyeznek. Mivel $\deg x^d =$ $= d|q-1$, ezért az előző állítás alapján $u = \frac{q-1}{d}$.
Ha $d = 2$, akkor $u+v = q$. A következő állítás szerint ha $f(x) \not\equiv c$, akkor $u+v$ csak akkor lehet ennél nagyobb, ha f permutáció-polinom. (Ha $f(x) \equiv c$, akkor ez nem igaz, mert $u = \infty$. Ha f permutáció-polinom, akkor meg tudjuk, hogy $u+v = 2q-1$.)

2.2.6. Állítás. *Ha $2 \leq v < q$, akkor $u + v \leq q$.*

Bizonyítás. Legyen $g(x) = x^q - x - \prod_{a \in \mathbb{F}_q} (x - f(a))$.
Mivel $v < q$, ezért $g \not\equiv 0$. $v \neq 1$ és 2.1.1 miatt $q - u \geq \deg g$. Így $\forall a \in \mathbb{F}_q$ - ra $g(f(a)) = 0$, ezért $\deg g \geq v$. □

Korábban kifejeztük u-t $\prod_{a \in \mathbb{F}_q} (x - f(a))$ segítségével. A lemma alapján ennek a deriváltjának a fokával kifejezhetjük w-t:

2.2.7. Állítás. *Legyen* $h(x) = \prod_{a\in\mathbb{F}_q}(x - f(a))$. *Ekkor* $\deg(h') = q - w - 1$.
Továbbá $w = \infty \iff h' \equiv 0$.

Bizonyítás. $h(x) = x^q + \sum_{i=1}^{q}(-1)^i s_i x^{q-i}$

$$h'(x) = qx^{q-1} + \sum_{i=1}^{q-1}(-1)^i(q-i)s_i x^{q-i-1} = \sum_{i=1}^{q-1}(-1)^{i-1} i s_i x^{q-i-1}$$

$\deg(h') = q - \min\{k \in \mathbb{Z}^+ : ks_k \neq 0\} - 1$, ami a lemma második része szerint pont $q - w - 1$.
Szintén a lemma második része szerint
$w = \infty \iff (\nexists k \in \mathbb{Z}^+$, hogy $ks_k \neq 0) \iff h'(x) \equiv 0$. □

2.1.8-ben láttuk, hogy ha $w < \infty$, akkor $w < v$. Nem precízen megfogalmazva ez azt jelenti, hogy w nem lehet nagy, ha v kicsi. A következő állítás szerint w akkor sem lehet nagy, ha v nagy. (Kivéve, ha $v = q$. Ebben az esetben tudjuk, hogy $w = q-1$.)

2.2.8. Állítás. *Ha* $w < \infty$, *akkor* $w < 2(q - v)$ *vagy* $v = q$.

Bizonyítás. Tegyük fel, hogy $w < \infty$ és $v \neq q$. Ekkor $v < q$, és 2.1.8 szerint $w < v$. Legyen h mint előbb,

$$g_1 = \frac{\prod_{a\in\mathbb{F}_q}(x - f(a))}{\prod_{b:\exists a\in\mathbb{F}_q f(a)=b}(x-b)} \text{ és } g_2 = \prod_{c\in\mathbb{F}_q:\nexists a f(a)=c}(x-c).$$

Ekkor

$$\deg g_1 = \deg g_2 = q - v, h(x) = \frac{(x^q - x)g_1(x)}{g_2(x)},$$

$$h'(x) = \frac{((qx^{q-1}-1)g_1(x) + g_1'(x)(x^q - x))g_2(x) - (x^q - x)g_1(x)g_2'(x)}{(g_2(x))^2} =$$

$$= \frac{-g_1(x)g_2(x) + (x^q - x)(g_1'(x)g_2(x) - g_1(x)g_2'(x))}{(g_2(x))^2}$$

g_2 gyökei mind egyszeresek, így nem gyökei g_2' - nak. g_1 - nek sem gyökei a definíciókból adódóan. Ezért $g_1'(x)g_2(x) - g_1(x)g_2'(x) \not\equiv 0$.
Tegyük fel, hogy $2(q - v) < q$. (Különben $2(q - v) \geq q > v > w$.)
Ekkor $\deg(g_1 g_2) = 2(q - v) < q$, ezért $\deg(h'$ számlálója$) \geq q$.
Továbbá $\deg(g_2^2) = 2(q - v)$, ezért $\deg(h') \geq q - 2(q - v)$. Az előző állítás szerint $q - w - 1 = \deg(h')$. Vagyis $q - w - 1 = \deg(h') \geq q - 2(q - v)$.
Azaz $w + 1 \leq 2(q - v)$. □

2.2.9. Következmény. *Ha $w < \infty$ és $v = q-1$, akkor a fenti becslés szerint $w < 2$, azaz $w = 1$.*

2.2.10. Állítás. *Ha f nem permutáció-polinom, akkor a következők teljesülnek:*

1. *ha $n \geq 1$, akkor $v \leq q - \frac{q-1}{n}$.*
2. *ha $w < \infty$, akkor $w \leq \frac{2}{3}q - 1$.*
3. *ha $w < \infty$, akkor $v + w \leq \frac{4}{3}q - 1$.*
4. *ha $v > q - p$ és $v > 1$, akkor $v + w \leq q$.*

Bizonyítás.

1. Ha $n \geq q$, akkor készen vagyunk, mert $v \leq q - 1 < q - \frac{q-1}{q} \leq q - \frac{q-1}{n}$.
   Tegyük fel, hogy $n < q$. Ekkor $n \geq 1$ pontosan akkor, ha $v \geq 2$. A 2.2.6. állítás alapján ekkor $u + v \leq q$. A 2.2.4-beliek szerint $u \geq \frac{q-1}{n}$. Ezeket összetéve $\frac{q-1}{n} + v \leq u + v \leq q$.

2. A 2.1.8 állítás szerint ha $w < \infty$, akkor $w < v$.
   Ha $v \leq \frac{2}{3}q$, akkor készen vagyunk, mivel $w \leq v - 1 \leq \frac{2}{3}q - 1$.
   Tegyük fel, hogy $v > \frac{2}{3}q$. 2.2.8 szerint ha $w < \infty$, akkor $w < 2(q - v)$ vagy $v = q$. Feltettük, hogy f nem permutáció-polinom, ezért $w \leq 2(q - v) - 1 < < 2(q - \frac{2}{3}q) - 1 = \frac{2}{3}q - 1$.

3. Ha $v \leq \frac{2}{3}q$, akkor a 2. rész bizonyítása alapján $v + w \leq \frac{2}{3}q + (\frac{2}{3}q - 1) = \frac{4}{3}q - 1$.
   Tegyük fel, hogy $v > \frac{2}{3}q$. Ekkor szintén a 2. rész alapján $v + w \leq \frac{2}{3}q + \frac{2}{3}q - - 1 = \frac{4}{3}q - 1$.

4. $v > 1$ és a 2.2.6 állítás miatt $u + v \leq q$. Ebből $u \leq q - v < q - (q - p) = p$. Eszerint $p \nmid u$. Ekkor 2.2.2 szerint $u = w$. Ezek alapján $v + w = v + u \leq q$.

□

2.2.11. Megjegyzés.

1. *Érdekes megfigyelés, hogy az* 1. *pont szerint v nem vehet fel akármilyen értéket: ha $v \neq q$, akkor $v \leq q - \frac{q-1}{n}$. Ez azt jelenti, hogy f nem lehet majdnem permutáció-polinom. A* 2. *pont szerint hasonló igaz w-re és a következő tételben is további hasonló megfigyelések szerepelnek.*
2. *Az* 1. *pontban adott határ elérhető. Ezt most nem számoljuk ki, de ha $q > 3$, $3|q + 1$ és $c \neq 0$, akkor $f(x) = x^3 + cx$-re $v = q - \frac{q-1}{3}$.*
3. *A* 2. *és a* 3. *részben valószínűleg nem éles ez a becslés.*

4. *A 4. részből $q \neq p$ esetén elhagyható a $v > 1$ feltétel, de egyébként nem. Lehet olyan, hogy az állítás feltételei mellett $v + w = q$. Például legyen $f(x) = x^n$, ahol n olyan, hogy $(q-1, n) = 2$. Láttuk, hogy ekkor $u + v = q$.(2.2.5 példa.) Ha $q = p$, akkor $p \nmid u$, így 2.2.2 szerint $u = w$.*

2.2.12. Tétel. *Ha $1 \leq n < q$, akkor a következők ekvivalensek:*

1. *$f(x)$ permutáció-polinom*
2. *$u = q - 1$*
3. *$u > q - \frac{q}{n}$*
4. *$u > q - v$*
5. *$v > q - \frac{q-1}{n}$*
6. *$w = q - 1$*
7. *$\frac{2}{3}q - 1 < w < \infty$*
8. *$q - \frac{q+1}{n} < w < \infty$*
9. *$q - u \leq w < \infty$*
10. *$u > \frac{q-1}{2}$ és $w < \infty$*

Bizonyítás. (1)-ből következik a többi, mert láttuk (a 2.1.2 példában), hogy ha f permutáció-polinom, akkor $v = q$ és $u = w = q - 1$ és ezeket behelyettesítve a többi feltétel nyilvánvalóan teljesül.
(2) $\Rightarrow$ (3): $u = q - 1 > q - \frac{q}{n}$
(3) $\Rightarrow$ (4): Mivel $n \geq 1$, ezért $v \geq \left[\frac{q}{n}\right]$. (a 2.1.11. megjegyzés alapján) Így $u > q - \frac{q}{n} \geq q - v$.
(4) $\Rightarrow$ (1): Indirekt: tegyük fel, hogy a (4)-es feltétel teljesül, de az (1)-es nem: $u > q - v$ és $v < q$. Mivel $n \geq 1$, ezért $2 \leq v < q$. Így alkalmazható a 2.2.6 állítás, ami szerint $u + v \leq q$. Másrészt a (4)-es feltételből $u + v > q$. Ez ellentmondás.
(5) $\Rightarrow$ (1): Indirekt: tegyük fel, hogy $v > q - \frac{q-1}{n}$ és f nem permutáció-polinom. Ekkor a 2.2.10. állítás első pontja szerint $v \leq q - \frac{q-1}{n}$. Ez ellentmondás.
Eddig beláttuk, hogy az első 5 pont ekvivalens.
(6) $\Rightarrow$ (7): Ha $w = q - 1$, akkor $\frac{2}{3}q - 1 < q - 1 = w < \infty$.
(7) $\Rightarrow$ (1): Indirekt: tegyük fel, hogy $v < q$ és $\frac{2}{3}q - 1 < w < \infty$. A 2.2.10. állítás második része szerint ekkor $w \leq \frac{2}{3}q - 1$, ami ellentmond a feltételnek.
(8) $\Rightarrow$ (9): Először belátjuk, hogy ha $q - \frac{q+1}{n} < w$, akkor $q - \frac{q}{n} \leq w$. Majd azt is, hogy ha $q - \frac{q}{n} \leq w$, akkor $q - \frac{q-1}{n} \leq w$. Ezekből következik $q - u \leq w$, mert

a 2.2.4-beliek szerint $u \geq \frac{q-1}{n}$, így $q - u \leq q - \frac{q-1}{n} \leq w$.
$q - \frac{q+1}{n} < w \Rightarrow q - \frac{q}{n} \leq w$ bizonyításhoz tegyük fel, hogy $q - \frac{q+1}{n} < w < q - \frac{q}{n}$.

Ezt átrendezve $q + 1 > (q - w)n > q$.

Ami ellentmondás, mert $(q - w)n \in \mathbb{Z}$.
$q - \frac{q}{n} \leq w \Rightarrow q - \frac{q-1}{n} \leq w$ bizonyításához tegyük fel, hogy $q - \frac{q}{n} \leq w < q - \frac{q-1}{n}$.

Ezt átrendezve $q \geq (q - w)n > q - 1$.

Tehát $n(q-w) = q$. Mivel feltettük, hogy $n < q$, ezért $p|q-w$. Ebből $p|w$. Ami 2.1.4 szerint ellentmondás.
(9) $\Rightarrow$ (1): Ha $w < \infty$, akkor $w < v$. (2.1.8) Így ha $q - u \leq w < \infty$, akkor $q - u < v$, azaz $u + v > q$. 2.2.6 szerint ha $2 \leq v < q$, akkor $u + v \leq q$. Tehát ha f nem permutáció-polinom, akkor $u + v \leq q$. De előbb láttuk be, hogy (9)-ből következik ennek az ellenkezője, tehát ekkor $v = q$.
(10) $\Rightarrow$ (9): 2.2.2 szerint ha $w < \infty$, akkor $u \leq w$. Ezért ha $u > \frac{q-1}{2}$ és $w < \infty$, akkor $u + w \geq 2u > q - 1$. Tehát $u + w \geq q$. □

2.3. Ciklikus mátrixok kapcsolata a permutáció-polinomokkal

2.3.1. Definíció. *Egy mátrixot ciklikusnak hívunk, ha négyzetes és az i-edik sorában ugyanazok az elemek vannak, mint az elsőben, csak $(i-1)$-gyel eltolva. Tehát ha az első sor $(c_0, \ldots, c_{m-1})$, akkor az i-edik sor j-edik eleme c_{j-i}, ahol $(j-i)$-t modulo m értjük.*

A következő állítás szerint egy $m \times m$-es ciklikus mátrix determinánsa kiszámolható az m-edik egységgyökök segítségével.

2.3.2. Állítás. *Legyen m tetszőleges pozitív egész, K tetszőleges test, $c_0, \ldots, c_{m-1}$ tetszőleges K-beli elemek. Jelölje C azt a ciklikus mátrixot, amelynek az első sora $c_0, \ldots, c_{m-1}$. Jelölje továbbá az m. egységgyököket $\zeta_1, \ldots, \zeta_m$ és legyen $g(x) = \sum_{i=0}^{m} c_i x^i$. Ekkor* $\det C = \prod_{k=1}^{m} g(\zeta_k)$.

Bizonyítás. Ha $\zeta^m = 1$, akkor $s_\zeta = (1, \zeta, \zeta^2, \ldots, \zeta^{m-1})^T$ sajátvektora C-nek $g(\zeta)$ sajátértékkel:

$$(Cs_\zeta)_1 = c_0 + c_1\zeta + \cdots + c_{m-1}\zeta^{m-1} = g(\zeta)$$

$$(Cs_\zeta)_2 = c_{m-1} + c_0\zeta + \cdots + c_{m-2}\zeta^{m-1} = \zeta g(\zeta)$$

$$\vdots$$

$$(Cs_\zeta)_m = c_1 + c_2\zeta + \cdots + c_0\zeta^{m-1} = \zeta^{m-1}g(\zeta)$$

Tehát $1 \le i \le m$-re $g(\zeta_i)$ sajátérték. Ha mindegyiket annyiszor kapjuk meg, amennyi a multiplicitása, akkor kész, mert a determináns a sajátértékek szorzata.
$c_0, \ldots, c_{m-1}$-re tekinthetünk úgy, mint $m-1$ független változóra. Ekkor
$1 \le i, j \le m, i \ne j$-re $g(\zeta_i) \ne g(\zeta_j)$. □

2.3.3. Következmény. *Ha* $m = q-1$, *akkor* $\det C = \prod_{a \in \mathbb{F}_q^*} g(a)$.

Az alábbi állítás mutatja az összefüggést a permutáció-polinomok és a ciklikus mátrixok között.

2.3.4. Állítás. *Legyen* $f(x) = \sum_{i=0}^{q-1} c_i x^i \in \mathbb{F}_q[x]$. *Jelölje* C *azt a ciklikus mátrixot, amelynek első sora* $(c_0 + c_{q-1}, c_1, \ldots, c_{q-2})$. *Legyen továbbá* I *a* $(q-1) \times (q-1)$*-es egységmátrix. Ekkor*

1. $\prod_{a \in \mathbb{F}_q} (x - f(a)) = (x - c_0)\det(xI - C)$
2. $f(x)$ *pontosan akkor permutáció-polinom, ha* $\det(xI - C) = (x - c_0)^{q-1} - 1$.

Bizonyítás.

1. Mivel $f(0) = c_0$, ezért a bizonyítandó állítást $(x - c_0)$-lal egyszerűsítve a következőt kapjuk:
$$\prod_{a \in \mathbb{F}_q^*} (x - f(a)) = \det(xI - C).$$
$xI - C$ ciklikus mátrix. (Az első sora $(x - c_0 - c_{q-1}, -c_1, \ldots, -c_{q-2})$.) Ezért az előző állítás szerint
$$\det(xI - C) = \prod_{a \in \mathbb{F}_q^*} (x - c_0 - c_{q-1} - c_1 a - c_2 a^2 - \ldots - c_{q-2}a^{q-2}) = \prod_{a \in \mathbb{F}_q^*} (x - f(a)).$$

2. Az első pont szerint $\frac{\prod_{a \in \mathbb{F}_q} (x - f(a))}{x - c_0} = \det(xI - C)$. Tehát elég lenne azt belátni, hogy $f(x)$ pontosan akkor permutáció-polinom, ha
$$\prod_{a \in \mathbb{F}_q^*} (x - f(a)) = (x - c_0)^{q-1} - 1.$$
f értékkészlete az egész $\mathbb{F}_q$ akkor és csak akkor, ha
$$\prod_{a \in \mathbb{F}_q^*} (x - f(a)) = \prod_{a \in \mathbb{F}_q, a \ne c_0} (x - a).$$

Most állapítsuk meg, hogy mik $(x-c_0)^{q-1}-1$ gyökei.

$$(x-c_0)^{q-1}=\begin{cases}0 & \text{ha } x=c_0\\ 1 & \text{ha } x\in\mathbb{F}_q, x\neq c_0\end{cases}$$

Tehát $(x-c_0)^{q-1}-1$ gyökei $\mathbb{F}_q$ c_0-tól különböző elemei, vagyis

$$(x-c_0)^{q-1}-1=\prod_{a\in\mathbb{F}_q, a\neq c_0}(x-a).$$

□

2.4. Egy másik megközelítés

Legyen $f(x)=\sum_{i=0}^{n}c_ix^i$ és $g(y)=f(y)-x$. Tekintsünk g-re úgy, mint egy $\mathbb{F}_q(x)$ feletti polinomra és jelölje $\eta_1,\ldots,\eta_n$ g gyökeit. Ezeket a következő 3 állításban jobban megvizsgáljuk, aztán ezen állítások segítségével kifejezzük s_k-t, amivel újabb információkhoz jutunk u-val és w-vel kapcsolatban. Ehhez a 3 állításhoz tegyük fel azt is, hogy $c_0=0$ és $c_n=1$.

2.4.1. Állítás. $\prod_{a\in\mathbb{F}_q}\big(x-f(a)\big)=(-1)^{n+1}\prod_{i=1}^{n}(\eta_i^q-\eta_i)=x\prod_{i=1}^{n}(\eta_i^{q-1}-1).$

Bizonyítás. Mivel g gyökei $\eta_1,\ldots,\eta_n$ és $c_n=1$, ezért $\prod_{i=1}^{n}(y-\eta_i)=g(y)=f(y)-x$. Ebből

$$\prod_{a\in\mathbb{F}_q}\big(x-f(a)\big)=\prod_{a\in\mathbb{F}_q}\Big(-\prod_{i=1}^{n}(a-\eta_i)\Big)=(-1)^{q+n}\prod_{i=1}^{n}\Big(\prod_{a\in\mathbb{F}_q}(\eta_i-a)\Big)=(-1)^{n+1}\prod_{i=1}^{n}(\eta_i^q-\eta_i)$$

Ezzel beláttuk az első egyenlőséget. Most lássuk be a másodikat!

$$(-1)^{n+1}\prod_{i=1}^{n}(\eta_i^q-\eta_i)=(-1)^{n+1}\prod_{i=1}^{n}\eta_i(\eta_i^{q-1}-1)=(-1)^{n+1}\prod_{i=1}^{n}\eta_i\cdot\prod_{i=1}^{n}(\eta_i^{q-1}-1)$$

Mivel $\prod_{i=1}^{n}(y-\eta_i)=f(y)-x$ és $c_0=0$, ezért $\prod_{i=1}^{n}\eta_i=(-1)^{n+1}x$. Tehát folytatva az egyenlőséget:

$$(-1)^{n+1}\prod_{i=1}^{n}\eta_i\cdot\prod_{i=1}^{n}(\eta_i^{q-1}-1)=x\prod_{i=1}^{n}(\eta_i^{q-1}-1).$$

□

2.4.2. Állítás. *Jelölje ξ_j az $\eta_1^{q-1}, \dots, \eta_n^{q-1}$ j-edik szimmetrikus polinomját. Ez felírható x $\mathbb{F}_q$-feletti polinomjaként és* $\deg \xi_j(x) \le j\frac{q-1}{n}$.
Továbbá $\prod\limits_{a\in\mathbb{F}_q} \Big(x - f(a)\Big) = x^q + x\sum\limits_{j=0}^{n-1}(-1)^{n-j}\xi_j$.

Bizonyítás. A szimmetrikus polinomok alaptétele szerint $s_j(x_1^{q-1}, \dots, x_n^{q-1})$ előáll $s_1(x_1, \dots, x_n), \dots, s_n(x_1, \dots, x_n)$ polinomjaként. Ebben az előállításban $s_n(x_1, \dots, x_n)$ kitevője legfeljebb $\frac{\deg s_j(x_1^{q-1},\dots,x_n^{q-1})}{n} = \frac{j(q-1)}{n}$.
$s_j(\eta_1, \dots, \eta_n)$-et könnyen ki tudjuk számolni:

$$\prod_{i=1}^{n}(y - \eta_i) = f(y) - x = \sum_{i=1}^{n} c_i y^i - x,$$

ebből $1 \le j < n$-re $s_j(\eta_1, \dots, \eta_n) = (-1)^j c_{n-j}$ és $s_n(\eta_1, \dots, \eta_n) = (-1)^n x$.

Az eddigiekből $\xi_j = s_j(\eta_1^{q-1}, \dots, \eta_n^{q-1}) \in \mathbb{F}_q[x]$ és $\deg \xi_j \le \frac{j(q-1)}{n}$.
Az 2.4.1. állítást felhasználva

$$\prod_{a\in\mathbb{F}_q} \big(x - f(a)\big) = x\prod_{i=1}^{n}(\eta_i^{q-1} - 1) = x\sum_{j=0}^{n}(-1)^{n-j}\xi_j = x\xi_n + x\sum_{j=0}^{n-1}(-1)^{n-j}\xi_j.$$

Az állítás bizonyításához tehát azt kéne belátni, hogy $x\xi_n = x^q$.

$$x\xi_n = x\prod_{i=1}^{n}\eta_i^{q-1} = x\Big(\prod_{i=1}^{n}\eta_i\Big)^{q-1} = x\big((-1)^{n+1}x\big)^{q-1} = x^q.$$

□

2.4.3. Jelölés. *Annak érdekében, hogy a következő két állítást egyszerűbben meg lehessen fogalmazni vezessünk be 2 új jelölést. Legyen*

$$I = \left\{ i = (i_1, \dots, i_n) \in \mathbb{N}_0^n : \sum_{j=1}^{n} j i_j = q - 1 \right\}$$

$$\text{és } c_q(i) = c_q(i_1, \dots, i_n) = (q-1)\frac{(i_1 + \ldots + i_n - 1)!}{i_1! \cdot \ldots \cdot i_n!}$$

2.4.4. Állítás.

1. *Bármely $i \in I$-re $c_q(i) \in \mathbb{Z}^+$.*
2. $\xi_{n-1} = \sum\limits_{i\in I} c_q(i)\Big(\prod\limits_{j=1}^{n} c_j^{i_j}\Big)x^{q-1-\sum\limits_{j=1}^{n} i_j}$

Bizonyítás.

1. $i \in I$-re $c_q(i) = \frac{(q-1)!}{i_1!\ldots i_n!}$ multinomiális együttható.

2. Először alakítsuk át ξ_{n-1}-et:

$$\xi_{n-1} = s_{n-1}(\eta_1^{q-1}, \ldots, \eta_n^{q-1}) = \Big(\prod_{k=1}^{n} \eta_k^{q-1}\Big) \cdot \Big(\sum_{k=1}^{n} \frac{1}{\eta_k^{q-1}}\Big) = x^{q-1} \sum_{k=1}^{n} \frac{1}{\eta_k^{q-1}} = \sum_{k=1}^{n} \Big(\frac{x}{\eta_k}\Big)^{q-1}$$

A folytatáshoz szükségünk lesz a Waring-formulára. A rövidség kedvéért legyen $\sigma_j = s_j(x_1, \ldots, x_n)$. Ezzel a jelöléssel a Waring-formula a következő:

$$\sum_{l=1}^{n} x_l^k = \sum_{\substack{i_1,\ldots,i_n \in \mathbb{N}_0, \\ \sum_{j=1}^{n} j i_j = k}} (-1)^{(i_2+i_4+i_6+\ldots)} k \frac{(i_1 + i_2 + \ldots + i_n - 1)!}{i_1!\, i_2! \ldots i_n!} \sigma_1^{i_1} \sigma_2^{i_2} \ldots \sigma_n^{i_n}$$

Ez $k = q - 1$-re:

$$\sum_{l=1}^{n} x_l^{q-1} = \sum_{i \in I} (-1)^{(i_2+i_4+i_6+\ldots)} c_q(i) \sigma_1^{i_1} \sigma_2^{i_2} \ldots \sigma_n^{i_n}$$

Ez utóbbit szeretnénk $(x_1, \ldots, x_n) = \left(\frac{x}{\eta_1}, \ldots, \frac{x}{\eta_n}\right)$-re alkalmazni. Ehhez jó lenne többet tudni az $s_j\left(\frac{x}{\eta_1}, \ldots, \frac{x}{\eta_n}\right)$ értékekről.

$$s_j\left(\frac{x}{\eta_1}, \ldots, \frac{x}{\eta_n}\right) = x^j \frac{s_{n-j}(\eta_1, \ldots, \eta_n)}{\eta_1 \ldots \eta_n} = x^j \frac{s_{n-j}(\eta_1, \ldots, \eta_n)}{(-1)^{n+1} x} =$$

$$= (-1)^{n+1} x^{j-1} s_{n-j}(\eta_1, \ldots, \eta_n) = (-1)^{n+1} x^{j-1} (-1)^{n-j} c_j = (-1)^{j-1} x^{j-1} c_j$$

Ezeket beírva a Waring-formulába

$$\sum_{k=1}^{n} \left(\frac{x}{\eta_k}\right)^{q-1} = \sum_{i \in I} (-1)^{(i_2+i_4+i_6+\ldots)} c_q(i) \prod_{j=1}^{n} \left((-1)^{j-1} x^{j-1} c_j\right)^{i_j}$$

Mivel $i_2 + i_4 + i_6 + \ldots + i_{2n} \equiv \sum_{j=1}^{n} (j-1) i_j \mod 2$, ezért

$$\sum_{k=1}^{n} \left(\frac{x}{\eta_k}\right)^{q-1} = \sum_{i \in I} c_q(i) \prod_{j=1}^{n} (x^{j-1} c_j)^{i_j} = \sum_{i \in I} c_q(i) \prod_{j=1}^{n} x^{(j-1) i_j} \prod_{j-1}^{n} c_j^{i_j} =$$

$$= \sum_{i \in I} c_q(i) x^{\left(\sum_{j=1}^{n} (j-1) i_j\right)} \prod_{j=1}^{n} c_j^{i_j} = \sum_{i \in I} c_q(i) x^{\left(\sum_{j=1}^{n} j i_j - \sum_{j=1}^{n} i_j\right)} \prod_{j=1}^{n} c_j^{i_j} =$$

$$= \sum_{i\in I} c_q(i) x^{\left(q-1-\sum_{j=1}^n i_j\right)} \prod_{j=1}^n c_j^{i_j}$$

□

2.4.5. Állítás. *Legyen* $f(x) = \sum_{j=1}^n c_j x^j, n > 1$. $c_n \neq 0$ *és* $1 \leq k < 2\frac{q-1}{n}$. *Ekkor*

1. $s_k = (-1)^{k-1} \sum_{\substack{i\in I,\\ \sum_{j=1}^n i_j = k}} c_q(i) \prod_{j=1}^n c_j^{i_j}$

2. $\big(-f(x)\big)^k$*-ban* x^{q-1} *együtthatója* ks_k.

Bizonyítás.

1. Először foglalkozzunk csak a $c_n = 1$ esettel. Ekkor a 2.4.2-beliek szerint $\prod_{a\in\mathbb{F}_q} \big(x - f(a)\big) = x^q + x\sum_{j=0}^{n-1}(-1)^{n-j}\xi_j$.
   Vagyis $x^q - s_1x^{q-1} + s_2x^{q-2} - \cdots + (-1)^q s_q = x^q + x\sum_{j=0}^{n-1}(-1)^{n-j}\xi_j$.
   Tehát $(-1)^k s_k = \left(x^{q-k-1} \text{ együtthatója } \sum_{j=0}^{n-1}(-1)^{n-j}\xi_j\text{-ben}\right)$.
   Megmutatjuk, hogy ha k a megadott tartományba esik, akkor a jobboldali szummában $(q-k-1)$-fokú tag csak ξ_{n-1}-ben lehet. 2.4.2 szerint $\deg \xi_j(x) \leq \leq j\frac{q-1}{n}$, ezért

$$\deg\left(\sum_{j=0}^{n-2}(-1)^{n-j}\xi_j\right) \leq (n-2)\frac{q-1}{n} = q - 1 - 2\frac{q-1}{n} < q-k-1.$$

   Tehát ha $1 \leq k < 2\frac{q-1}{n}$, akkor $(-1)^k s_k = \big(x^{q-k-1} \text{ együtthatója } -\xi_{n-1}\text{-ben}\big)$.
   A 2.4.4. állítás szerint $\xi_{n-1} = \sum_{i\in I} c_q(i)\Big(\prod_{j=1}^n c_j^{i_j}\Big) x^{q-1-\sum_{j=1}^n i_j}$, azaz ξ_{n-1}-ben x^{q-1-k} együtthatója $\sum_{\substack{i\in I,\\ \sum_{j=1}^n i_j = k}} c_q(i)\prod_{j=1}^n c_j^{i_j}$.
   Most tegyük fel, hogy $c_n \neq 1$. Ekkor $\frac{f(x)}{c_n}$-re tudjuk, hogy igaz az állítás:

$$\frac{s_k}{c_n^k} = (-1)^{k-1} \sum_{\substack{i\in I,\\ \sum_{j=1}^n i_j = k}} c_q(i) \prod_{j=1}^n \left(\frac{c_j}{c_n}\right)^{i_j} = (-1)^{k-1} \sum_{\substack{i\in I,\\ \sum_{j=1}^n i_j = k}} \left(c_q(i)\prod_{j=1}^n c_j^{i_j}\right)\frac{1}{c_n^k}$$

   Innen c_n^k-nal szorozva az egyenlőséget megkapjuk a bizonyítandó állítást.

2. $(-1)^k f(x)^k = (-1)^k \left(\sum_{j=1}^{n} c_j x^j \right)^k$

Mi x^{q-1} együtthatója? Válasszunk a szorzat minden tagjából egy elemet. Jelölje i_j azt, hogy a szorzat hány tagjából választjuk a $c_j x^j$ tagot. Egy $(i_1, \ldots, i_n)$ szám-n-es akkor 'érvényes', ha $\sum_{j=1}^{n} i_j = k$, vagyis a szorzat mindegyik tagjából választottunk. A kiválasztott tagok szorzatában x kitevője pontosan akkor $q-1$, ha $\sum_{j=1}^{n} j i_j = q-1$. Ebben az esetben az elemek szorzata így néz ki: $\left(\prod_{j=1}^{n} c_j^{i_j} \right) x^{q-1}$. Egy $(i_1, \ldots, i_n)$ szám-n-eshez $\frac{(i_1+\ldots+i_n)!}{i_1!\ldots i_n!} = \frac{k!}{i_1!\ldots i_n!}$-féle kiválasztás tartozik. Így x^{q-1} együtthatója a következő:

$$(-1)^k \sum_{\substack{i \in I \\ \sum_{j=1}^{n} i_j = k}} \prod_{j=1}^{n} c_j^{i_j} \frac{k!}{i_1! \ldots i_n!}$$

Ezt tovább alakítva

$$(-1)^k \sum_{\substack{i \in I \\ \sum_{j=1}^{n} i_j = k}} \prod_{j=1}^{n} c_j^{i_j} \frac{k!}{i_1! \ldots i_n!} = (-1)^k \sum_{\substack{i \in I \\ \sum_{j=1}^{n} i_j = k}} \prod_{j=1}^{n} c_j^{i_j} c_q(i) \frac{k}{q-1} =$$

$$= (-1)^{k-1} k \sum_{\substack{i \in I \\ \sum_{j=1}^{n} i_j = k}} \prod_{j=1}^{n} c_j^{i_j} c_q(i)$$

Ez az első pont szerint éppen $k s_k$.

□

2.4.6. Megjegyzés.

1. *A 2.2.4. állítás azt mondta ki, hogy ha $n \geq 1$, akkor $u \geq \frac{q-1}{n}$, és $u = \frac{q-1}{n} \iff n | q-1$. Ezt be tudjuk bizonyítani az előző állítás első részének segítségével is, a következőképpen.*
Ha $(i_1, \ldots, i_n) \in I$ és $\sum_{j=1}^{n} i_j = k$, akkor $q - 1 = \sum_{j=1}^{n} j i_j \leq n \sum_{j=1}^{n} i_j = nk$. Ezt átrendezve $\frac{q-1}{n} \leq k$.
Tehát ha $k < \frac{q-1}{n}$, akkor nem létezik ilyen $(i_1, \ldots, i_n)$, így

$$s_k = (-1)^{k-1} \sum_{\substack{i \in I, \\ \sum_{j=1}^{n} i_j = k}} c_q(i) \prod_{j=1}^{n} c_j^{i_j} = 0.$$

Ebből $u \geq \frac{q-1}{n}$.
Tegyük fel most, hogy $n|q-1$ *és legyen* $k = \frac{q-1}{n}$. *Ekkor* $\sum_{j=1}^{n} i_j = k$ *és* $\sum_{j=1}^{n} j i_j = q-1$ *pontosan akkor igaz, ha* $i_n = k$ *és* $1 \leq j < k$*-ra* $i_j = 0$. *Tehát*

$$s_k = (-1)^{k-1} \sum_{\substack{i \in I, \\ \sum_{j=1}^{n} i_j = k}} c_q(i) \prod_{j=1}^{n} c_j^{i_j} = (-1)^{k-1} \frac{(k-1)!}{k!}(q-1)c_n^k = (-1)^k \frac{1}{k} c_n^k \neq 0$$

Így ha $n|q-1$, *akkor* $u = \frac{q-1}{n}$. *Ennek a megfordítása nyilván igaz.*

2. *2.4.5 második részét bizonyíthattuk volna a 2.1. fejezetben is. A következő három állításra van hozzá szülségünk:*
A 2.1.5. állítás szerint ha $n \geq 1$, *akkor* $w \geq \frac{q-1}{n}$.
A 2.2.4. állítás szerint ha $n \geq 1$, *akkor* $u \geq \frac{q-1}{n}$.
A 2.2.1. lemma szerint ha $1 \leq k \leq q$ *és* $k < u + w$, *akkor* $p_k = (-1)^{k-1} k s_k$.
Ezek alapján ha $n > 1$ *és* $1 \leq k < 2\frac{q-1}{n}$, *akkor* $k < 2\frac{q-1}{n} \leq u + w$ *és így* $p_k = (-1)^{k-1} k s_k$.
Legyen $h(x) = f(x)^k$ *és* $\mathbb{F}_q$ *elemeit jelölje* $a_1, \ldots, a_q$. *Ekkor* h*-ban* x^{q-1} *együtthatója* $-s_1\left(h\left(a_1\right), \ldots, h(a_q)\right) = -\sum_{a \in \mathbb{F}_q} \left(f(a)\right)^k = -p_k$.
Tehát $(-1)^k f(x)^k$*-ban* x^{q-1} *együtthatója:*

$$(-1)^{k+1} p_k = (-1)^{k+1}(-1)^{k-1} k s_k = k s_k.$$

Ha $n|q+1$, akkor a 2.2.4. állításhoz nagyon hasonlót állíthatunk. Most több feltételre lesz szükségünk, de $\frac{q-1}{n}$ helyett $\frac{q+1}{n}$-nel becsüljük alulról u-t és w-t.

2.4.7. Állítás. *Tegyük fel, hogy* $3 \leq n < q$, $n|q+1$, $f(x) = \sum_{j=0}^{n} c_j x^j$ *és* $c_{n-1} = 0$. *Ekkor* $u, w \geq \frac{q+1}{n}$ *és* $u = w = \frac{q+1}{n}$ *akkor és csak akkor ha* $c_{n-2} \neq 0$.

Bizonyítás. Először azt bizonyítjuk, hogy u-ra igaz az állítás. 2.2.4 szerint $u \geq \frac{q-1}{n}$. Mivel $n|q+1$ és $n > 2$, ezért $n \not| q-1$, és így $u > \frac{q-1}{n}$. Az $u \geq \frac{q+1}{n}$ állítást indirekten bizonyítjuk. Tegyük fel, hogy $\frac{q-1}{n} < u < \frac{q+1}{n}$. Ezt átrendezve
$n(q-1) < un < q+1$. Tehát $un = q$. Ez ellentmondás, mert $n|q+1$ miatt $n \not| q$.
Az egyenlőség bizonyításához legyen $k = \frac{q+1}{n}$. Ha $1 \leq k < 2\frac{q-1}{n}$, akkor s_k kiszámolásához tudnánk alkalmazni a 2.4.5. állítást.

$$\frac{q+1}{n} < 2\frac{q-1}{n} \iff q+1 < 2(q-1) = 2q-2 \iff 3 < q$$

Tehát $k = \frac{q+1}{n}$-re alkalmazhatjuk a 2.4.5. állítást, ami szerint

$$s_k = (-1)^{k-1} \sum_{\substack{i \in I, \\ \sum_{j=1}^{n} i_j = k}} c_q(i) \prod_{j=1}^{n} c_j^{i_j}.$$

Mivel $c_{n-1} = 0$, ezért a szumma azon tagjai, ahol $i_{n-1} \neq 0$, mind 0-k. Ha $\sum\limits_{j=1}^{n} j i_j =$ $= q - 1$, akkor $n i_n \leq q - 1$, azaz $i_n \leq \frac{q-1}{n} < \frac{q+1}{n} = k$. Tehát létezik $l \geq 1$ egész, amire $i_n = k - l$.
Ezt felhasználva $\sum\limits_{j=1}^{n-1} j i_j = q - 1 - n i_n = nk - 2 - n(k-l) = nl - 2$.
Ha $\sum\limits_{j=1}^{n} i_j = k$, akkor $\sum\limits_{j=1}^{n-1} i_j = k - (k-l) = l$. Mivel $c_{n-1} = 0$, ezért $\sum\limits_{j=1}^{n-1} i_j = \sum\limits_{j=1}^{n-2} i_j$.
Az előző két sor szerint $nl - 2 = \sum\limits_{j=1}^{n-2} j i_j \leq (n-2)l$. Ezt átrendezve $l \leq 1$. Ez csak úgy lehet, ha $l = 1$. Tehát $i_n = k - 1$, $i_{n-1} = 0$ és létezik egyetlen $j \leq n - 2$, amire $i_j = 1$. Melyik lehet ez a j?

$$\sum_{j=1}^{n} j i_j = q - 1 \iff j i_j + n(k-1) = q - 1 \iff j + n\left(\frac{q+1}{n} - 1\right) = q - 1 \iff$$

$$\iff j + q + 1 - n = q - 1 \iff j = n - 2$$

Így a szummából csak egyetlen tag marad:

$$s_k = (-1)^{k-1} c_q(0, \ldots, 0, 1, 0, k-1) c_{n-2}^1 c_n^{k-1} = (-1)^{k-1} \frac{(k-1)!}{(k-1)!} (q-1) c_n^{k-1} c_{n-2} =$$

$$= (-1)^k c_n^{k-1} c_{n-2}.$$

Ebből $s_k = 0$ pontosan akkor, ha $c_{n-2} = 0$. Vagyis $u = \frac{q+1}{n}$ akkor és csak akkor ha $c_{n-2} \neq 0$.
w-re az állítást a 2.2.2 segítségével látjuk be. Eszerint ha $w < \infty$, akkor $u \leq w$ és $u = w \iff p \not| u$. Tehát $w \geq u \geq \frac{q+1}{n}$ és ha $u = \frac{q+1}{n}$, akkor mivel $p \not| u$, ezért $u = w$.
A 2.2.2 állításban az is szerepel, hogy ha $w = \infty$, akkor $p|u$ vagy $u = \infty$. $u = \frac{q+1}{n}$ esetén egyik sem áll fenn, ezért $w < \infty$. □

A fenti állítás a $c_{n-1} = 0$ feltételt elhagyva és a $c_{n-2} = 0$ feltételt megfelelően módosítva igaz marad.

2.4.8. Állítás. *Tegyük fel, hogy* $3 \leq n < q$, $n|q+1$ *és* $f(x) = \sum\limits_{j=0}^{n} c_j x^j$. *Ekkor* $u, w \geq \frac{q+1}{n}$ *és* $u = w = \frac{q+1}{n}$ *akkor és csak akkor ha* $n^2 c_n c_{n-2} \neq \binom{n}{2} c_{n-1}^2$.

Bizonyítás. A bizonyítás nagy része úgy megy, mint az előbb: a w-ről szóló részt visszavezethetjük az u-ról szólóra és az egyenlőtlenség bizonyítása is megegyezik. Tehát elég azt belátnunk, hogy $u = \frac{q+1}{n}$ pontosan akkor ha $n^2 c_n c_{n-2} \neq \binom{n}{2} c_{n-1}^2$.
Legyen $k = \frac{q+1}{n}$. Mint az előbb láttuk, erre alkalmazhatjuk a 2.4.5. állítást, ami szerint

$$s_k = (-1)^{k-1} \sum_{\substack{i \in I, \\ \sum_{j=1}^n i_j = k}} c_q(i) \prod_{j=1}^n c_j^{i_j}.$$

Az is szerepelt, hogy ha $\sum_{j=1}^n j i_j = q-1$, akkor létezik $l \geq 1$ egész, amire $i_n = k - l$ és ekkor $\sum_{j=1}^{n-1} j i_j = nl - 2$ és ha $\sum_{j=1}^n i_j = k$, akkor $\sum_{j=1}^{n-1} i_j = l$.
Ebből $nl - 2 = \sum_{j=1}^{n-1} j i_j \leq l(n-1)$, azaz $2 \geq l$. Az $l = 1$ esetre tudjuk, hogy ekkor egy tag marad a szummából: $-c_n^{k-1} c_{n-2}$.
Legyen $l = 2$. Ekkor $i_n = k - 2$. $\sum_{j=1}^n i_j = k$ miatt létezik $r, s \leq n-1$, hogy $j \neq r, s$-re $i_j = 0$ és $r \neq s$ esetén $i_r = i_s = 1$, $r = s$ esetén $i_r = i_s = 2$. Mindkét esetre igaz a következő:

$$q - 1 = \sum_{j=1}^n j i_j = r + s + n(k-2) = r + s + n\left(\frac{q+1}{n} - 2\right) = r + s + q + 1 - 2n.$$

Vagyis $q - 1 = r + s + q + 1 - 2n$. Ezt átrendezve azt kapjuk, hogy $r + s = 2n - 2 = 2(n-1)$. Mivel $r, s \leq n-1$, ezért ez csak úgy lehet, ha $r = s = n-1$. Tehát a szummában egyetlen tag van, ahol $l = 2$:

$$c_q(0, \ldots, 0, 2, k-2) c_{n-1}^2 c_n^{k-2} = \frac{(k-1!)}{2(k-2)!}(q-1) c_{n-1}^2 c_n^{k-2} = -\frac{k-1}{2} c_{n-1}^2 c_n^{k-2}.$$

Az eddigiekből $s_k = (-1)^k \left(-c_n^{k-1} c_{n-2} - \frac{k-1}{2} c_{n-1}^2 c_n^{k-2}\right)$. Azaz

$$s_k = 0 \iff -c_n^{k-1} c_{n-2} = \frac{k-1}{2} c_{n-1}^2 c_n^{k-2} \iff -c_{n-2} c_n = \frac{k-1}{2} c_{n-1}^2 \iff$$

$$\iff n^2 c_{n-2} c_n = -n^2 \frac{k-1}{2} c_{n-1}^2.$$

Tehát azt kéne belátni, hogy $-n^2 \frac{k-1}{2} = \binom{n}{2}$. Ez igaz, mert

$$-n^2 \frac{k-1}{2} = -n^2 \frac{(n-2)!}{2!\,(n-2)!}(k-1) = -n^2 \frac{n!}{2!\,(n-2)!} \cdot \frac{k-1}{n(n-1)} = -n \binom{n}{2} \frac{\frac{q+1}{n} - 1}{n-1} =$$

$$= -\binom{n}{2} \frac{q+1-n}{n-1} = -\binom{n}{2} \frac{-(n-1)}{n-1} = \binom{n}{2}$$

□

2.4.9. Következmény. *Ha* $3 \leq n < q$, $n|q+1$ *és* $n^2 c_n c_{n-2} \neq \binom{n}{2} c_{n-1}^2$, *akkor* f *nem permutáció-polinom.*

Bizonyítás. A feltételek mellett a fenti állítás szerint $u = \frac{q+1}{n}$.
A 2.2.12. tétel alapján f pontosan akkor permutáció-polinom, ha
$q - \frac{q}{n} < u = \frac{q+1}{n}$.

$$q - \frac{q}{n} < u = \frac{q+1}{n} \iff nq - q < q + 1 \iff (n-2)q < 1$$

Ez $3 \leq n < q$ miatt nem igaz, tehát f nem permutáció-polinom. □

3. Permutáció-polinomok lineáris differenciával

3.1. Permutáció-polinomos megközelítés

Ebben a fejezetben azzal foglalkozunk, hogy $f(x) + cx$ mikor, illetve hány c-re permutáció-polinom. Ehhez $0 \leq k \leq q$-ra legyen $s_k(y)$ az a függvény, amely minden $c \in \mathbb{F}_q$-hoz hozzárendeli az $f(x) + cx$ polinom s_k értékét. Így $\prod_{a \in \mathbb{F}_q} \big(x - ay - f(a)\big) = \sum_{k=0}^{q} (-1)^k s_k(y) x^{q-k}$. Tudjuk, hogy $f(x) + cx$ pontosan akkor permutáció-polinom, ha $\prod_{a \in \mathbb{F}_q} \big(x - ac - f(a)\big) = \prod_{a \in \mathbb{F}_q} (x - a) = x^q - x$. Így $s_k(y)$ segítségével kapunk egy ekvivalens definíciót arra, hogy $f(x)+cx$ permutáció polinom. Nevezetesen azt, hogy

$$s_k(c) = \begin{cases} 0 & \text{ha } 1 \leq k \leq q-2 \text{ vagy } k = q \\ 1 & \text{ha } k = q-1 \end{cases}$$

Ezért érdemes megvizsgálni a $\prod_{a \in \mathbb{F}_q} \big(x - ay - f(a)\big)$ polinom együtthatóit.

3.1.1. Lemma. *Legyen* $f(x) = \sum_{k=0}^{q-1} c_k x^k \in \mathbb{F}_q[x]$. *Ekkor minden* $0 \leq k \leq q-1$*-re* $x^k y^{q-k-1}$ *együtthatója* $\prod_{a \in \mathbb{F}_q} \big(x - ay - f(a)\big) \in \mathbb{F}_q[x, y]$*-ban megegyezeik* c_k*-val.*

Bizonyítás. Jelölje $x^{q-k-1}y^k$ együtthatóját γ_k. Ezzel a jelöléssel a bizonyítandó állítás az, hogy $\gamma_k = c_{q-1-k}$. Jelölje $\mathbb{F}_q$ elemeit $a_1, \ldots, a_q$, és legyen $b_i = f(a_i)$.
k-ra menő indukcióval fogunk bizonyítani. γ_0-ra igaz az állítás, mert x^{q-1} együtthatója $= -\sum_{i=1}^{q} f(a_i) = c_{q-1}$.

Tegyük fel, hogy $1 \leq k \leq q-1$. Ekkor $\gamma_k = (-1)^{k+1} \sum_{i_1 < \cdots < i_k} \left(a_{i_1} \ldots a_{i_k} \sum_{i \neq i_j} b_i \right)$.
Jelölje $\bar{\gamma}_{k-1}$ azt, hogy γ_{k-1}-be b_i-k helyett $a_i b_i$-t írunk:

$$\bar{\gamma}_{k-1} = (-1)^k \sum_{i_1 < \cdots < i_{k-1}} \left(a_{i_1} \ldots a_{i_{k-1}} \sum_{i \neq i_j} a_i b_i \right).$$

Ezzel

$$\gamma_k = (-1)^{k+1} s_k(a_1, \ldots, a_q) \sum_{i=1}^{q} b_i + \bar{\gamma}_{k-1} = \begin{cases} \bar{\gamma}_{k-1} & \text{ha } 1 \leq k < q-1 \\ -c_{q-1} + \bar{\gamma}_{q-2} & \text{ha } k = q-1 \end{cases}$$

Legyen $\bar{f}(x) = \sum_{k=1}^{q-1} c_{k-1} x^k + c_{q-1} x$. Felhasználva, hogy $\mathbb{F}_q$ elemeire $x^q = x$, ez tulaj-

donképpen $xf(x)$. Tehát $\bar{f}(a_i) = a_i b_i$, így

$$\bar{\gamma}_{k-1} = \Big(x^{q-k} \text{ együtthatója } \prod_{a\in\mathbb{F}_q} \big(x - ay - \bar{f}(a)\big)\text{-ban}\Big).$$

Tegyük fel, hogy $1 \le k \le q-2$ és $k-1$-re teljesül az állítás. Ekkor

$$\gamma_k = \bar{\gamma}_{k-1} = \Big(x^{q-k} \text{ együtthatója } \prod_{a\in\mathbb{F}_q} \big(x - ay - \bar{f}(a)\big) \text{ -ban}\Big).$$

Az indukciós feltevést $\bar{f}$-ra alkalmazva ez pont c_{q-k-1}.
Most legyen $k = q-1$. Ekkor

$$\gamma_k = -c_{q-1} + \bar{\gamma}_{q-2} = -c_{q-1} + \Big(x \text{ együtthatója } \prod_{a\in\mathbb{F}_q} \big(x - ay - \bar{f}(a)\big)\text{-ban}\Big) =$$

$$= -c_{q-1} + c_{q-1} + c_0 = c_0.$$

□

3.1.2. Következmény. *Ha $1 \le k < q-1$, akkor $\deg s_k(y) \le k-1$ és egyenlőség akkor és csak akkor teljesül , ha $c_{q-k} \neq 0$.*

Bizonyítás. $s_k(y)$ megyegyezik x^{q-k} együtthatójával $\prod_{a\in\mathbb{F}_q} \big(x - ay - f(a)\big) \in \mathbb{F}_q(y)$-ban.
A $\prod_{a\in\mathbb{F}_q} \big(x-ay-f(a)\big)$ szorzatban hogy keletkezhet olyan tag, amiben x a $(q-k)$-adik hatványon van? Ehhez a szorzat $q-k$ tagjából x-et kell választani, k-szor $-ay$-t vagy $-f(a)$-t és ezeket összeszorozni. Ha legalább egyszer $-f(a)$-t választjuk, akkor y legfeljebb a $k-1$-edik hatványon szerepel majd. Ha egyszer sem választjuk $-f(a)$-t, akkor olyan, mintha $\prod_{a\in\mathbb{F}_q} (x-ay) = x^q - xy^{q-1}$-ban tekintenénk x^{q-k} együtthatóját. Ez $1 \le k < q-1$ esetén 0. Tehát $\deg s_k(y) \le k-1$.
Az eddigiekből $\deg s_k(y) = k-1$ pontosan akkor, ha $x^{q-k}y^{k-1}$ együtthatója nem 0. A lemma szerint $x^{q-k}y^{k-1}$ együtthatója éppen c_{q-k}. □

Azon c-k száma, melyre $f(x) + cx$ permutáció-polinom kapcsolatban van $f(x)$ hatványainak fokával. Az összefüggést a következő tétel írja le.

3.1.3. Tétel. *Legyen $1 \le r < q-1$. Tegyük fel, hogy legalább r különböző $c \in \mathbb{F}_q$-ra $f(x) + cx$ permutáció-polinom. Jelölje n_t az $f(x)^t$ fokát azután, hogy az $x^q = x$ egyszerűsítést elvégeztük annyiszor, ahányszor lehetett. Ekkor*

1. *$n_1 < q - r$.*
2. *ha $r < p$, akkor minden $t \ge 1$-re $n_t < q - r + t - 1$.*

3. ha $r+1<p$ és $n_1<q-r-1$, akkor $t\geq 1$-re $n_t<q-r+t-2$.

Bizonyítás. Mielőtt rátérnénk az egyes részek bizonyítására, következzék két észrevétel.
Egyrészt feltehető, hogy $n=n_1$, tehát $n<q$.
Másrészt a fejezet elején megállapítottuk, hogy ha $f(x)+cx$ permutáció-polinom, akkor $1\leq k\leq q-2$-re $s_k(c)=0$. Tehát ha $s_k(y)\not\equiv 0$, akkor $r\leq \deg s_k(y)$.

1. Ha $n=1$, akkor $q-r>q-(q-1)=n_1$.
   Tegyük fel, hogy $n>1$. Legyen $k=q-n$. Ekkor $1\leq k<q-1$, ezért ha $s_k(y)\not\equiv 0$, akkor $r\leq \deg s_k(y)$. A 3.1.2. következmény szerint
   $\deg s_k(y)\leq k-1=q-n_1-1$, így $n_1<q-r$. Ha $s_k(y)\equiv 0$, akkor $\prod_{a\in\mathbb{F}_q}(x-ay-f(a))$-ben nincs $x^{q-k}=x^n$-es tag. De a lemma szerint $x^n y^{q-n-1}$ együtthatója itt $c_n\neq 0$. Ez ellentmondás, tehát $s_k(y)\not\equiv 0$.

2. Legyen $1\leq k\leq r<p$. Ekkor $s_k(y)\equiv 0$, mert különben $k-1\geq \deg s_k(y)\geq$ $\geq r$, ami ellentmondás. Jelölje $\mathbb{F}_q$ elemeit $a_1,\dots,a_q$. Ekkor $s_k(y)=s_k(a_1y+$ $+f(a_1),\dots,a_qy+f(a_q))$. A Newton-Girard formulák alapján $\sum_{a\in\mathbb{F}_q}(ay+f(a))^k$ előáll $s_1(y),\dots,s_k(y)$ polinomjaként, és így $1\leq k\leq r$-re $\sum_{a\in\mathbb{F}_q}(ay+f(a))^k=0$.
   Másrészt $\sum_{a\in\mathbb{F}_q}(ay+f(a))^k=\sum_{j=1}^{k}\sum_{a\in\mathbb{F}_q}\binom{k}{j}a^jf(a)^{k-j}y^j$. Mivel $p\not|\binom{k}{j}$, mert $k<p$, ezért ebből következik, hogy ha $j+t\leq r$, akkor $\sum_{a\in\mathbb{F}_q}a^jf(a)^t=0$.
   A 2.1.16. következmény 2. pontja szerint

$$\deg f\leq q-l-2 \iff 0\leq k\leq l\text{-re } \sum_{a\in\mathbb{F}_q}a^kf(a)=0.$$

   Ezt felhasználva $n_t\leq q-(r-t)-2=q-r+t-2$.

3. Tegyük fel, hogy $r+1<p$ és $n_1<q-r-1$. A 2 rész bizonyításánál láttuk, hogy $1\leq k\leq r$ esetén $s_k(y)\equiv 0$. Ha $s_{r+1}(y)\equiv 0$ is teljesülne, akkor ugyanúgy befejezhetnénk a bizonyítást, mint a 2. pontban.
   A feltételek szerint $q-(r+1)>n_1=n$, így $c_{q-(r+1)}=0$. A 3.1.2. következmény szerint ekkor $\deg s_{r+1}(y)<r$. Ha $s_{r+1}(y)\not\equiv 0$, akkor $r\leq \deg s_k(y)<r$, ami ellentmondás, tehát $s_{r+1}(y)\equiv 0$.

□

3.1.4. Állítás. *Jelölje r azon $c\in\mathbb{F}_q$-k számát, amelyre $f(x)+cx$ permutáció-polinom. Tegyük fel, hogy* $\deg f(x)\leq q-1$. *Ekkor*

1. *$r\leq q-1$ és egyenlőség pontosan akkor teljesül, ha $n\leq 1$.*

2. *ha* $1 < n$, *akkor* $r \leq q - \frac{q-1}{n-1}$.

3. $r \leq q - \sqrt{q} - 1$ *vagy* $r = q - 1$.

Bizonyítás. Először a 2. állítást bizonyítjuk, aztán ennek segítségével az 1.-t és végül a 3.-at.

2. Tegyük fel, hogy $1 < n$. Legyen $g(x) = \frac{f(0)-f(x)}{x}$. Mivel $\deg g = n - 1$, ezért minden elem ősképe legfeljebb $n - 1$ elemű. A 0 őse csak a 0. Ebből

$$|\{c : \exists a \neq 0, \text{ hogy } g(a) = c\}| \geq \frac{q-1}{n-1}.$$

Ha valamely $a \neq 0$-ra $c = g(a) = \frac{f(0)-f(a)}{a}$, akkor $f(x) + cx$ nem permutáció-polinom, mert ekkor $ac + f(a) = f(0) = 0 \cdot c + f(0)$. Tehát

$$q - r \geq |\{c : \exists a \neq 0, \text{ hogy } g(a) = c\}| \geq \frac{q-1}{n-1}.$$

Ezt átrendezve $r \leq q - \frac{q-1}{n-1}$.

1. Ha $n \leq 1$, akkor $\exists a, b$, hogy $f(x) = ax + b$. Ekkor $c = -a$ kivételével minden c-re $f(x) + cx$ permutáció-polinom, így $r = q - 1$.
Ha $n > 1$, akkor a 2. rész szerint $r \leq q - \frac{q-1}{n-1} < q - \frac{q-1}{q-1} = q - 1$.

3. Tegyük fel, hogy $r < q - 1$. Ekkor az 1. rész szerint $1 < n$.
Ha $\sqrt{q} \leq n$, akkor a 3.1.3. tétel 1. állítása szerint $\sqrt{q} \leq n < q - r$, azaz $\sqrt{q} \leq q - r - 1$. Ezt átrendezve $r \leq q - \sqrt{q} - 1$.
Ha $n < \sqrt{q}$, akkor a 2. állítást felhasználva

$$r \leq q - \frac{q-1}{n-1} < q - \frac{q-1}{\sqrt{q}-1} = q - (\sqrt{q} + 1).$$

□

3.1.5. Példa. *Ha* $f(x) = x^n$ *és* $n|q$, *akkor* $f(x) + cx$ *pontosan akkor permutáció-polinom, ha* $a \neq 0$ *esetén* $a^n + ca \neq 0$.

Bizonyítás. $f(x) + cx$ pontosan akkor nem permutáció-polinom, ha $\exists b_1 \neq b_2$, hogy $b_1^n + cb_1 = b_2^n + cb_2$. Az $n|q$ feltétel miatt ez ekvivalens azzal, hogy $\exists b_1 \neq b_2$, hogy $(b_1 - b_2)^n + c(b_1 - b_2) = 0$. Ez utóbbi pont azt jelenti, hogy $\exists a \neq 0$, amire $a^n + ca = 0$. □

3.1.6. Megjegyzés.

1. *Ha a példa feltételei mellett azt is feltesszük, hogy $n > 1$, akkor*

$$q - r = |\{a \in \mathbb{F}_q^* : \exists b \in \mathbb{F}_q, \text{ hogy } b^{n-1} = a\}| = \frac{q-1}{(q-1, n-1)}.$$

Ugyanis $b \neq 0$-ra $b^n + cb = 0$ pontosan akkor, ha $b^{n-1} = -c$.

2. *Ha még azt is feltesszük, hogy $n = p$, akkor $(q-1, n-1) = (p^m - 1, p-1) = = p - 1 = n - 1$. Így $r = q - \frac{q-1}{n-1}$, azaz elérhető az előző állítás 2. pontjában szereplő határ.*

3. *Ha $n = \frac{q}{p}$, akkor*

$$(q-1, n-1) = \left(q-1, \frac{q}{p} - 1\right) = \left(q-1, \frac{q-p}{p}\right) = (q-1, q-p) = (q-1-(q-p), q-p) =$$

$$= (p-1, q-p) = (p-1, p(p^{m-1} - 1)) = (p-1, p^{m-1} - 1) = p - 1.$$

Így $r = q - \frac{q-1}{p-1}$.
A 3.1.3. tétel 2. pontja szerint ha $r < p$, akkor minden $t \geq 1$-re $n_t < q-r+t- -1$. Most már tudjuk, hogy nem hagyható el az $r < p$ feltétel, ha $1 < t < p < q$. Ugyanis ekkor $n_t = \frac{q}{p}t$ és

$$q - r + t - 1 = q - \left(q - \frac{q-1}{p-1}\right) + t - 1 = \frac{q-1}{p-1} + t - 1 =$$

$$= \frac{q-1-(p-1)}{p-1} + t = \frac{q-p}{p-1} + t.$$

Tehát

$$n_t < q - r + t - 1 \iff \frac{q}{p}t < \frac{q-p}{p-1} + t \iff \frac{q-p}{p}t < \frac{q-p}{p-1} \iff$$

$$\iff \frac{q-p}{p-1} \cdot \frac{p-1}{p}t < \frac{q-p}{p-1} \iff \frac{p-1}{p}t < 1.$$

Ez utóbbi nem teljesül, így $n_t \geq q - r + t - 1$.

3.1.7. Állítás. *Jelölje r azon $c \in \mathbb{F}_q$-k számát, amelyre $f(x) + cx$ permutációpolinom. Ekkor $p | r + 1$.*

Bizonyítás.

Legyen $p_k(y) = \sum_{a \in \mathbb{F}_q} (f(a) + ya)^k$. A 2.2.12. tétel szerint g_c pontosan akkor permutáció-

polinom, ha $w_c = q-1$, azaz $p_k(c) = \begin{cases} 0 & \text{ha } 1 \le k < q-1 \\ -1 & \text{ha } k = q-1 \end{cases}$. Ebből

$$-r = \sum_{c\in\mathbb{F}_q} p_{q-1}(c) = \sum_{c\in\mathbb{F}_q}\sum_{a\in\mathbb{F}_q} (f(a)+ca)^{q-1} =$$

$$= \underbrace{f(0)^{q-1}q}_{0} + \sum_{a\in\mathbb{F}_q^*} \underbrace{\sum_{c\in\mathbb{F}_q} (f(a)+ca)^{q-1}}_{\substack{-1, \text{ mert csak } c=\frac{-f(a)}{a}\text{-ra} \\ \text{lesz 0, egyébként 1}}} = (q-1)(-1)$$

Tehát $r+1 = q$, azaz $p|r+1$. □

3.1.8. Állítás. *Jelölje r azon $c \in \mathbb{F}_q$-k számát, amelyre $f(x)+cx$ permutáció-polinom. Tegyük fel, hogy $r > \frac{q-3}{2}$. Ekkor*

1. *ha $g_c(x) = f(x)+cx$ nem permutáció-polinom, akkor g értékkészletének minden elemére a g szerinti őseinek szám osztható p-vel.*
2. *$r \ge q - \frac{q-1}{p-1}$*
3. *Ha $n < q$, akkor $f'(x) = f'(0)$.*

Bizonyítás. Feltehető, hogy $n < q$.

1. Ha $f(x)+cx$ permutáció-polinom, akkor $1 \le k < q-1$-re $s_k(c) = 0$. Tehát azon c-k száma, amelyre ez teljesül, legalább r, ami a feltevés szerint nagyobb, mint $\frac{q-3}{2}$. Mivel r, q egészek, ezért ekkor $r \ge \frac{q}{2} - 1$. A 3.1.2. következményt is felhasználva $s_k(y) \not\equiv 0$ és $1 \le k < q-1$ esetén $\frac{q}{2} - 1 \le \deg s_k(y) \le k-1$, tehát $\frac{q}{2} \le k$.
   Jelölje u_c, v_c, w_c az $f(x)+cx$ megfelelő értékeit. A fentiek szerint $k < \frac{q}{2}$ esetén $s_k(y) \equiv 0$, így $s_k(c) = 0$ és ezért $u_c \ge \frac{q}{2}$.
   Ha f konstans, $c = 0$, akkor $w_c = \infty$. Egyéb esetekben $\deg(f(x)+cx) \ge 1$ és ekkor a 2.2.12. tétel 1. és 10. pontja szerint

   $$f(x)+cx \text{ nem permutáció-polinom} \iff u_c \le \frac{q-1}{2} \text{ vagy } w = \infty.$$

   Mivel $u_c \ge \frac{q}{2} > \frac{q-1}{3}$, ezért ha $f(x)+cx$ nem permutáció-polinom, akkor $w_c = \infty$.
   A 2.1.7. állítás alapján $w_c = \infty \iff \forall a \in \mathbb{F}_q$ - ra a-nak az $f(x)+cx$ - általi őseinek száma osztható p-vel.
2. Minden c-re $f(0) + c\cdot 0 = f(0)$. Az 1. pont szerint ha $g_c(x)$ nem permutáció-polinom, akkor $f(0)$-nak minimum $p-1$ őse van $\mathbb{F}_q^*$-ban. Másrészt ha $a \in \mathbb{F}_q^*$-ra

létezik $c \in \mathbb{F}_q$, amire $f(a) + ca = f(0)$, akkor ez a c egyértelmű. Ez utóbbi azért van így, mert ha létezik $d \neq c$, amire $f(a)+ca = f(0) = f(a)+da$, akkor $a(c-d) = 0$, ami csak úgy lehet, ha $a = 0$. Tehát azon c-k száma, amelyre f nem permutáció-polinom legalább $\frac{q-1}{p-1}$.

3. Legyen $f(x) = \sum_{k=0}^{q-1} c_k x^k$. Ekkor $f'(x) = \sum_{k=1}^{q-1} k c_k x^{k-1}$.
A 2.1.16. állítás szerint $0 \leq k < q-1$ - re $\sum_{a \in \mathbb{F}_q} a^k f(a) = -c_{q-k-1}$. Ez azt jelenti, hogy $1 \leq k < q$ - ra $\sum_{a \in \mathbb{F}_q} k a^{k-1} f(a) = -k c_{q-k}$.
$p_k(y) = \sum_{a \in \mathbb{F}_q} (f(a) + ya)^k$-ban y^{k-1} együtthatója éppen $\sum_{a \in \mathbb{F}_q} k a^{k-1} f(a)$.
$1 \leq k \leq q-2$ - re $p_k(y) = 0$, mert ha g_c permutáció-polinom, akkor $w_c = q-1$ (2.2.12. tétel), és így $p_k(c) = 0$, ha pedig g_c nem permutáció-polinom, akkor az 1. pont szerint $w = \infty$, és így $p_k(c) = 0$.
Tehát az eddigieket összetéve:

$$1 \leq k \leq q-2\text{-re: } -k c_{q-k} = \sum_{a \in \mathbb{F}_q} k a^{k-1} f(a) = (y^{k-1} \text{ együtthatója } p_k(y)\text{-ban}) = 0$$

Így $f'(x) = \sum_{k=1}^{q-1} k c_k x^{k-1} = c_1 = f'(0)$.

□

3.2. Kapcsolat a véges geometriával

3.2.1. Definíció. *Egy affin sík pontokból és egyenesekből (a pontok bizonyos részhalmazaiból) áll, melyek teljesítik a következő axiómákat:*

1. *Bármely két különböző pontot pontosan egy egyenes tartalmaz.*
2. *Minden l egyenesre és P pontra pontosan egy egyenes létezik, amely tartalmazza P-t és nem metszi l-et.*
3. *Létezik három olyan pont, amelyre nem létezik olyan egyenes, amely mind a hármat tartalmazza.*

3.2.2. Definíció. *Egy projektív sík pontokból és egyenesekből (a pontok bizonyos részhalmazaiból) áll, melyek teljesítik a következő axiómákat:*

1. *Bármely két különböző pontot pontosan egy egyenes tartalmaz.*
2. *Bármely két egyenes pontosan egy pontban metszi egymást.*

3. *Létezik három olyan pont, amelyre nem létezik olyan egyenes, amely mind a hármat tartalmazza.*

Definiálható egy véges affin sík a következő módon. A pontok legyenek $\mathbb{F}_q \times \mathbb{F}_q$ elemei és minden $k, m \in \mathbb{F}_q$-ra $\{(a,b) : b = ma + k\}$ és $\{(a,b) : a = k\}$ alkosson egy-egy egyenest. Az így definiált affin síkot $AG(2,q)$-val jelöljük. Ehhez hozzávéve egy megfelelő egyenest egy projektív síkot kapunk. A hozzávett egyenest ideális egyenesnek hívjuk, l_∞-nel jelöljük, és a pontjai megfeleltethetőek $\mathbb{F}_q \cup \{\infty\}$ elemeinek. Ha $m \in l_\infty$ és m egy $\mathbb{F}_q$-beli elemnek felel meg, akkor az m-et tartalmazó egyenesek azok, melyek előállnak $\{(a,b) : b = ma + k\}$ alakban (és persze l_∞). Ha $m \in l_\infty$ és m éppen a ∞-nek felel meg, akkor az m-et tartalmazó egyenesek pont az $\{(a,b) : a = k\}$ alakúak (és persze l_∞).

Legyen $U \subseteq AG(2,q)$. Azt mondjuk, hogy U meghatároz egy $m \in \mathbb{F}_q \cup \{\infty\}$ irányt vagy pontot az ideális egyenesen, ha létezik (a_1, b_1) és $(a_2, b_2) \in U$, $(a_1, b_1) \neq (a_2, b_2)$, amelyre $m = \frac{b_2 - b_1}{a_2 - a_1}$, úgy értve, hogy ha $a_1 = a_2$, akkor a ∞ irányt határozzák meg. Így az (a_1, b_1) és az (a_2, b_2) pontokon átmenő egyenes l_∞-t az általuk meghatározott irányban metszi. Egy sokat vizsgált kérdés, mekkora lehet a meghatározott irányok halmaza. Az esetek nagy részében az összes irány meghatározott. Pédául ha $|U| > q$, akkor U által minden irány meg van határozva. Ugyanis tetszőleges $m \in l_\infty$-ent q egyenes tartalmaz és ez a q egyenes lefedi $AG(2,q)$-t. Így a skatulya-elv szerint lesz olyan egyenes, amely legalább két U-beli pontot is tartalmaz. De mi a helyzet akkor, ha $|U| \leq q$?

Jelölje D a meghatározott irányok halmazát és N a D elemszámát. Tegyük fel, hogy $|U| = q$ és $N \neq q + 1$. Ekkor egy esetleges affin transzformációval elérhető, hogy a ∞ nem meghatározott irány, azaz $\forall a \in \mathbb{F}_q$-hoz legfeljebb egy $b \in \mathbb{F}_q$ létezik, amelyre $(a,b) \in U$. $|U| = q$ miatt ez pont azt jelenti, hogy U egy $f : \mathbb{F}_q \to \mathbb{F}_q$ függvény grafikonja.
m pontosan akkor meghatározott irány, ha létezik $a_1 \neq a_2 \in U$, amelyre $\frac{f(a_2) - f(a_1)}{a_2 - a_1} = $
$= m$. Ezt átrendezve $f(a_2) - ma_2 = f(a_1) - ma_1$. Tehát m akkor és csak akkor meghatározott irány, ha $f(x) - mx$ nem permutáció-polinom. Eszerint az előző fejezetbeli állítások, amelyekben r azt jelöli, hogy $f(x) + cx$ hány c-re permutáció-polinom, egyben arról is szólnak, hogy hány m van meghatározva f grafikonja által (jelölje ezt N_f). Például a 3.1.4. állítás a $q = r + N_f$ egyenlőséget használva a következőképpen szól:

3.2.3. Állítás. *Tegyük fel, hogy* $\deg f(x) \leq q - 1$. *Ekkor*

1. $1 \leq N_f$ *és egyenlőség pontosan akkor teljesül, ha* $n \leq 1$.
2. *ha* $1 < n$, *akkor* $\frac{q-1}{n-1} \leq N_f$.
3. $N_f \geq \sqrt{q} + 1$ *vagy* $N_f = 1$.

Az első pont ebben a megközelítésben nyilvánvaló: $N_f = 1$ pontosan akkor, ha minden $a, b \in \mathbb{F}_q$-ra $\frac{f(a)-f(b)}{a-b} = m$, azaz $f(a) + ma = f(b) + mb = k$. Ez pont azt jelenti, hogy $f(x) = -mx + k$, azaz $\deg f \leq 1$.
A 2. és a 3. pont egy alsó határt ad N_f-re abban az esetben, ha $N_f \neq 1$.

Rédei bizonyította [2]-ben, hogy ha $q = p$ prím, akkor a 3. pontnál (és általában a 2.-nál is) erősebb is igaz: ha $U \in AG(2, p)$ nem egy egyenes, akkor $N \geq \frac{p+1}{2}$. Később Megyesi bebizonyította, hogy N nem lehet $\frac{p+1}{2}$, tehát $N \geq \frac{p+3}{2}$. Ez a határ már elérhető: a következő példa $d = \frac{p}{2}$-re olyan, hogy $N = \frac{p+3}{2}$. Lovász és Schrijver bizonyította ([3]), hogy affin transzformációktól eltekintve ez az egyetlen p elemű halmaz $AG(2, p)$-ben, amely $\frac{p+3}{2}$ irányt határoz meg.

3.2.4. Példa. *Legyen $1 < d < q-1$ olyan, hogy $d|q-1$ és G egy d elemű részcsoportja $\mathbb{F}_q^*$-nak. Ekkor az $U = \{(a, 0) : a \in G\} \cup \{(0, a) : a \notin G\}$ által meghatározott irányok száma $q + 1 - d$.*

Bizonyítás. G ciklikus csoport. Legyen a generátoreleme b. Ekkor minden $c \notin G$-re a $(0, b)$ és az $(c, 0)$ pontok által meghatározott irány $-\frac{c}{b}$. Mivel $-\frac{c_1}{b} = -\frac{c_2}{b}$ pontosan akkor, ha $c_1 = c_2$, ezért ily módon $q-d$ irányt meghatároztunk. Két $\{(0, a) : a \notin G\}$-beli pont a ∞-t határozza meg, ez eddig nem szerepelt. Két $\{(a, 0) : a \in G\}$-beli pont a 0-t határozza meg, de ezt már számoltuk, mert $0 \notin G$. Legyen $a_1 \in G$,
$a_2 \notin G$. Ekkor $a_1 = b^k$ valamely k-ra. Az $(a_1, 0)$ és a $(0, a_2)$ által meghatározott irány $-\frac{a_2}{a_1} = -\frac{a_2}{b^k} = -\frac{a_2 b^{d-k+1}}{b}$. Mivel $a_2 b^{d-k+1} \notin G$, ezért ezt már számoltuk. □

Hivatkozások

[1] G. Turnwald: A new criterion for permutation polynomials, *Finite Fields and their Applications* 1 (1995), 64-82

[2] L. Rédei: *Lückenhafte Polynome über endlichen Körpern*, Akadémiai Kiadó, Budapest és Birkhäuser Verlag, Basel, 1970 (Angol fordítás: *Lacunary polynomials over finite fields*, Akadémiai Kiadó, Budapest és North Holland, Amsterdam, 1973).

[3] L.Lovász, A.Schrijver: Remarks on a theorem of Rédei, *Studia Scientiarum Mathematicarum Hungarica* 16 (1981) 449-454.