Véges test fölötti szeparáló invariánsok vizsgálata (2)

Szerző: Miklósi Roland Botond
Témavezető: Domokos Mátyás

Az *Egyéni kutatómunka 1* tárgyhoz tartozó kutatás során a Gregor Kemper, Artem Lopatin és Fabian Reimers szerzők *Separating Invariants Over Finite Fields* című cikkét dolgoztam fel, és a benne megjelenő eredményekhez hasonló sejtést sikerült megfogalmaznunk a három elemű véges test fölött. Az *Egyéni kutatómunka 2* tárgy keretén belül a megfogalmazott sejtést sikerült belátnunk, és részeredményt értünk el egyéb prímelemű testek esetében. A továbbiakban a sejtés részletes bizonyítása, illetve a részeredmények ismertetése következik.

1. Egy kis emlékeztető

Az újabb eredmények ismertetése előtt elevenítsünk fel néhány dolgot.

Legyen V egy n-dimenziós vektortér az $\mathbb{F}$ test fölött, melynek koordinátagyűrűje az n-változós polinomgyűrű. Adott $G \leq GL(V)$ véges részcsoport invariánsgyűrűjét $\mathbb{F}[V]^G$-vel jelöljük. Ekkor egy $S \subset \mathbb{F}[V]^G$ részhalmazt szeparálórendszernek nevezünk, ha azon $u, v \in V$ vektorok, amelyek szeparálhatóak a teljes invariánsgyűrű által, szeparálhatóak az S által is, vagyis létezik $f \in S$ polinom úgy, hogy $f(u) \neq f(v)$.

Láttuk, hogy egy invariánsgyűrű szeparálórendszere több szempontból is jobb, mint egy generátorrendszer. Pl. mindig létezik véges szeparálórendszer; az ún. Noether korlát szeparáló invariánsokra mindig teljesül; Weyl polarizációs tétele bármilyen karakterisztikában működik, míg generátorrendszerre ez csak 0 karakterisztika esetén igaz.

A véges testek fölötti szeparáló invariánsok vizsgálata az algebrai invariánselmélet egy nagyon fiatal kutatási területe. Az első cikket a témában Gregor Kemper, Artem Lopatin és Fabian Reimers írták, Separating Invariants Over Finite Fields címmel (2020). A cikkben bebizonyítanak egy fontos képletet, miszerint egy elemszámra nézve minimális szeparálórendszer mérete pontosan

$$\gamma = \gamma(q, k) := \left\lceil \log_q(k) \right\rceil,$$

ahol q a test elemszáma, k pedig a $G \times V \to V$ hatás orbitjainak a száma. A szerzők egy explicit konstrukciót is adnak egy γ elemszámú szeparálórendszerre, amelyben a

polinomok fokszámainak a maximuma $|G|\, n\,(q-1)$.

Az $\mathbb{F}=\mathbb{F}_2$ és $G=S_n$ esetben bebizonyítják, hogy az

$$S_{n,1}\left(\mathbb{F}_2\right)=\{s_{2^r}\mid 0\leq r\leq \lfloor \log_2(n)\rfloor\}$$

egy elemszámra nézve minimális szeparálórendszer. Egy általánosabb eredményt is közölnek, miszerint az

$$S_{n,m}\left(\mathbb{F}_2\right)=\{\sigma_{2^r}\left(\underline{\alpha}\right)\mid r\geq 0,|\underline{\alpha}|\geq 1, r+|\underline{\alpha}|-1\leq \lfloor \log_2(n)\rfloor,\ \text{minden } 1\leq j\leq m\}$$

halmaz $\mathbb{F}^2$ fölött $\mathbb{F}\left[V^m\right]^{S_n}$-ben egy elemszámra nézve minimális szeparálórendszer. Itt $\sigma_t\left(\underline{\alpha}\right)$ az $\underline{\alpha}$ vektor által meghatározott t-edik elemi multiszimmetrikus polinom. Természetesen az $m=1$ eset visszaadja az $S_{n,1}$ rendszert.

Kutatásunkban az $m=1$ és $\mathbb{F}=\mathbb{F}_3$ esetre fókuszálva, számítógépes kísérletekkel a következő állítást sikerült igazolnunk (az Egyéni kutatómunka 1 keretén belül):

1. Állítás. *Ha $\mathbb{F}=\mathbb{F}_3$ és $m=1$, akkor a következő elemi szimmetrikus polinomok benne kell legyenek egy tartalmazásra nézve minimális szeparálórendszerben:*

$$\{s_{3^k}, s_{2\cdot 3^k}\mid 0\leq k\leq \lfloor \log_3(n)-\log_3(2)\rfloor\}.$$

Természetesen itt olyan szeparálórendszerről van szó, amit az összes elemi szimmetrikus polinomból kapunk úgy, hogy néhányat belőlük elhagyunk. Tartalmazásra nézve minimális szeparálórendszerről akkor beszélünk, ha bármelyik polinomot elhagyva a fennmaradó polinomok nem alkotnak szeparálórendszert. Egy elemszámra nézve minimális szeparálórendszer tartalmazásra nézve is minimális, fordítva ez nem igaz.

Az előző beszámolót azzal a sejtéssel zártuk, hogy ezek a polinomok szeparálórendszert alkotnak. A sejtést végül sikerült bizonyítanunk, ennek az ismertetése a következő szakaszban olvasható.

2. A sejtés bizonyítása

Ebben a szakaszban a következő állítást fogjuk belátni.

2. Állítás. *Ha $\mathbb{F}=\mathbb{F}_3$ és $m=1$, akkor a következő halmaz egy tartalmazásra nézve minimális szeparálórendszert alkot $\mathbb{F}\left[V\right]^{S_n}$-ben:*

$$S_{n,1}\left(\mathbb{F}_3\right)=\{s_{3^k}, s_{2\cdot 3^k}\mid 0\leq k\leq \lfloor \log_3(n)-\log_3(2)\rfloor\}.$$

Azt, hogy ez nem mindig lesz elemszámra nézve minimális szeparálórendszer a következő táblázattal szemléltetjük. Például ha $n=9$, akkor a 1-es táblázat alapján $\gamma=4$, de $|S_{n,1}\left(\mathbb{F}_3\right)|=5$.

$n=4$	5	6	7	8	9
$\gamma=3$	3	4	4	4	4

1. táblázat. Minimális méretek néhány speciális esetben

Az $\mathbb{F}=\mathbb{F}_2$ esetén az $S_{n,1}(\mathbb{F}_2)$ rendszer szeparáló tulajdonságát a következő két lemma segítségével láthattuk be.

3. Segédtétel. *Az $\mathbb{F}_2$ test fölött teljesül az*

$$s_{2^r}(e_i)=\xi_r(i),\ \forall r,i\geq 0$$

egyenlőség, ahol $\xi_r(i)$ az i kettes számrendszerbeli felírásának r-edik számjegye, illetve $e_i=\left(\underbrace{1,...,1}_{i\text{-szer}},0,...,0\right)$, $0\leq i\leq n$ a megfelelő orbitreprezentánst jelöli.

4. Segédtétel. *Ha az $s_{2^k}(e_i)$ (minden $0\leq k\leq\lfloor\log_2(n)\rfloor$) értékekből meg tudjuk mondani azt, hogy mennyi az i értéke, akkor az $S_{n,1}(\mathbb{F}_2)$ egy szeparálórendszer.*

Ezek alapján evidens, hogy az $S_{n,1}$ szeparálórendszer, hiszen a $s_{2^k}(e_i)$ ismeretében a 3-as Segédtétel alapján az i kettes számrendszerbeli felírásában minden számjegyet vissza tudunk nyerni.

Hasonló stratégia alapján fogjuk kezelni az $\mathbb{F}=\mathbb{F}_3$ esetet is. Az orbitreprezentánsokat az

$$e_{i,j}=\left(\underbrace{1,...,1}_{i\text{-szer}},\underbrace{-1,...,-1}_{j\text{-szer}},0,...,0\right),\ i+j\leq n$$

módon fogjuk jelölni. A továbbiakban néhány segédtételt fogunk belátni.

A 4-es Segédtétel átfogalmazása a következőképpen történik.

5. Segédtétel. *Ha az $s_{3^k}(e_{i,j})$ és $s_{2\cdot 3^k}(e_{i,j})$ értékek meghatározzák az i,j értékeket, akkor az $S_{n,1}(\mathbb{F}_3)$ egy szeparálórendszer.*

6. Segédtétel. *Az $s_k(e_{i,j})$ értéke nem más, mint az $(1+x)^i(1-x)^j\in\mathbb{F}_3[x]$ szorzatban a k-adfokú tag együtthatója.*

Bizonyítás. Vegyük észre, hogy az

$$(1+\lambda_1x)(1+\lambda_2x)\cdots(1+\lambda_nx)$$

szorzatban a k-adfokú együttható pontosan az $s_k(\lambda_1,...,\lambda_n)$ elemi szimmetrikus polinom. □

7. Segédtétel. *Legyen i és j hármas számrendszerbeli felírása*

$$i = i_0 + i_1 \cdot 3 + ... + i_t \cdot 3^t =: (i_t i_{t-1} ... i_0)_3 ,$$
$$j = j_0 + j_1 \cdot 3 + ... + j_v \cdot 3^v =: (j_v j_{v-1} ... j_0)_3 ,$$

ahol $i_0, ..., i_t \in \{0,1,2\}$, $j_0, ..., j_v \in \{0,1,2\}$. Ekkor

$$(1+x)^i = \sum_{l_t, l_{t-1}, ..., l_0 \in \{0,1,2\}} (-1)^{\sharp\{u \in \{0,1,...,t\} |\, l_u = 1,\, i_u = 2\}} x^{(l_t l_{t-1} ... l_0)_3},\ l_t \le i_t, ..., l_0 \le i_0,$$
$$(1-x)^j = \sum_{m_v, m_{v-1}, ..., m_0 \in \{0,1,2\}} (-1)^{\sharp\{w \in \{0,1,...,v\} |\, m_w = 1,\, j_w = 2\}} (-x)^{(m_v m_{v-1} ... m_0)_3},\ m_v \le j_v, ..., m_0 \le j_0.$$

Bizonyítás. A bizonyítás az

$$(1+x)^i = \left(1+x^{3^t}\right)^{i_t} \left(1+x^{3^{t-1}}\right)^{i_{t-1}} \cdots \left(1+x^3\right)^{i_1} (1+x)^{i_0} ,$$
$$(1-x)^j = \left(1-x^{3^v}\right)^{j_v} \left(1-x^{3^{v-1}}\right)^{j_{v-1}} \cdots \left(1-x^3\right)^{j_1} (1-x)^{j_0}$$

összefüggések alapján azonnal adódik. □

8. Segédtétel. *Az i_0 és j_0 értékeket egyértelműen meghatározzák az s_1, illetve s_2 polinomok orbitreprezentánsokon vett kiértékeléseik.*

Bizonyítás. Vegyük észre, hogy az

$$(1+x)^i = \left(1+x^{3^t}\right)^{i_t} \left(1+x^{3^{t-1}}\right)^{i_{t-1}} \cdots \left(1+x^3\right)^{i_1} (1+x)^{i_0} ,$$
$$(1-x)^j = \left(1-x^{3^v}\right)^{j_v} \left(1-x^{3^{v-1}}\right)^{j_{v-1}} \cdots \left(1-x^3\right)^{j_1} (1-x)^{j_0}$$

egyenlőségek miatt az első, illetve másodfokú tagokat csak az $(1+x)^{i_0}$ és $(1-x)^{j_0}$ befolyásolja. Ez azt jelenti, hogy az s_1 és s_2 kiértékeléseihez az $i_t, ..., i_1$ és $j_v, ..., j_1$ értékeket figyelmen kívül hagyhatjuk, vagyis ha két különböző orbitreprezentáns esetén a nekik megfelelő i_0 és j_0 megegyezik, akkor az ők kiértékeléseik is meg fognak egyezni az s_1 és s_2 polinomokon.

A 2-es Táblázat alapján készen vagyunk, hiszen a táblázat oszlopai páronként különböznek, ami pontosan azt jelenti, hogy az i_0 és j_0 értékek egyértelműen meghatározottak. □

	$i_0 = 0,\ j_0 = 0$	$1,0$	$0,1$	$2,0$	$0,2$	$1,1$	$2,1$	$1,2$	$2,2$
$s_1(e_{i,j})$	0	1	−1	−1	1	0	1	−1	0
$s_2(e_{i,j})$	0	0	0	1	1	−1	−1	−1	1

2. táblázat. i_0 és j_0 egyértelműen meghatározottak az s_1 és s_2 segítségével

Fontos megjegyezni, hogy ez a bizonyítás esetünkben elégséges, azonban az eredmények tetszőleges $\mathbb{F}_p$ testre való általánosításához egy olyan bizonyításra lesz szükségünk, ami független a p-től.

A következő lemma tetszőleges p prímre bizonyítható, most a $p=3$ esetre látjuk be. A továbbiakban feltesszük, hogy az i és j hármas számrendszerbeli felírásában ugyanannyi tag szerepel, különben valamelyik kipótolható kellő számú 0-val.

9. Segédtétel. *Ha* $3 \mid i$ *és* $3 \mid j$, *akkor*

$$s_{3d}\left(e_{i,j}\right) = s_d\left(e_{i/3,j/3}\right).$$

Lemma

Bizonyítás. Legyen $i = (i_t i_{t-1} ... i_0)_3$ és $j = (j_t j_{t-1} ... j_0)_3$. Az oszthatóságból következik, hogy $i_0 = j_0 = 0$. Ekkor az

$$\begin{aligned}(1+x)^i (1+2x)^j = &\left(1+x^{3^t}\right)^{i_t}\left(1+x^{3^{t-1}}\right)^{i_{t-1}} \cdots \left(1+x^3\right)^{i_1} \cdot \\ &\cdot \left(1+(2x)^{3^t}\right)^{j_t}\left(1+(2x)^{3^{t-1}}\right)^{j_{t-1}} \cdots \left(1+(2x)^3\right)^{j_1} \\ &\overset{x^3 \leftrightarrow y}{=} (1+y)^{i/3}(1+2y)^{j/3}\end{aligned}$$

egyenlőség bal oldalán szereplő szorzatban az x^{3d} tag együtthatója megegyezik a jobb oldalon álló szorzatban az y^d tag együtthatójával, (a 6-os Segédtétel értelmében) vagyis

$$s_{3d}\left(e_{i,j}\right) = s_d\left(e_{i/3,j/3}\right).$$

□

Még egy lemma bizonyítása maradt hátra.

10. Segédtétel. *Az* $i_0, j_0, i_1, j_1, ..., i_k, j_k$ *és* $s_{3^{k+1}}\left(e_{i,j}\right), s_{2\cdot 3^{k+1}}\left(e_{i,j}\right)$ *értékek meghatározzák az* $s_{3^{k+1}}\left(e_{i-(i_k i_{k-1}...i_0)_3, j-(j_k j_{k-1}...j_0)_3}\right)$, *illetve* $s_{2\cdot 3^{k+1}}\left(e_{i-(i_k i_{k-1}...i_0)_3, j-(j_k j_{k-1}...j_0)_3}\right)$ *értékeket.*

Bizonyítás. Vezessük be az

$$\begin{aligned}f &:= (1+x)^{i_0}\left(1+x^3\right)^{i_1} \cdots \left(1+x^{3^k}\right)^{i_k} \cdot (1+2x)^{j_0}\left(1+(2x)^3\right)^{j_1} \cdots \left(1+(2x)^{3^k}\right)^{j_k}, \\ g &:= \left(1+x^{3^{k+1}}\right)^{i_{k+1}} \cdots \left(1+x^{3^t}\right)^{i_t} \cdot \left(1+(2x)^{3^{k+1}}\right)^{j_{k+1}} \cdots \left(1+(2x)^{3^t}\right)^{j_t}\end{aligned}$$

polinomokat.

Az 6-os Segédtétel alapján tudjuk, hogy

$$\begin{aligned}s_{3^{k+1}}\left(e_{i,j}\right) &= \text{"az } f \cdot g \text{ szorzatban az } x^{3^{k+1}} \text{ tag együtthatója"}, \\ s_{2\cdot 3^{k+1}}\left(e_{i,j}\right) &= \text{"az } f \cdot g \text{ szorzatban az } x^{2\cdot 3^{k+1}} \text{ tag együtthatója"}.\end{aligned}$$

Könnyen ellenőrizhető, hogy az f polinom fokszáma maximum

$$4 \cdot \left(1 + 3 + ... + 3^k\right) = 2 \cdot 3^{k+1} - 2$$

lehet.

Írjuk fel az f, g és $f \cdot g$ polinomokat az

$$f = \sum_n f_n x^n,$$
$$g = \sum_n g_n x^n,$$
$$f \cdot g = \sum_n c_n x^n$$

alakban. Feladatunk tulajdonképpen a $g_{3^{k+1}}$ és $g_{2 \cdot 3^{k+1}}$ együtthatók meghatározása. Feltétel szerint az $f \cdot g$ szorzatban ismertek a $c_{3^{k+1}}$, illetve $c_{2 \cdot 3^{k+1}}$ együtthatók, valamint az $i_0, j_0, ..., i_k, j_k$ ismerete miatt az $f_{3^{k+1}}$ és $f_{2 \cdot 3^{k+1}}$ együtthatókat is ismerjük.

A $c_{3^{k+1}}$ a következőképpen keverhető ki:

$$c_{3^{k+1}} = g_{3^{k+1}} + f_{3^{k+1}},$$

ahol a $c_{3^{k+1}}$ és $f_{3^{k+1}}$ ismertek, tehát a $g_{3^{k+1}}$ meghatározható.

A $c_{2 \cdot 3^{k+1}}$ együttható a

$$c_{2 \cdot 3^{k+1}} = g_{2 \cdot 3^{k+1}} + f_{3^{k+1}} \cdot g_{3^{k+1}}$$

összefüggésből adódik, hiszen $\deg(f) \leq 2 \cdot 3^{k+1} - 2$. Ebben $c_{2 \cdot 3^{k+1}}, f_{3^{k+1}}$ ismertek, és az előző lépésből a $g_{3^{k+1}}$ is meghatározott, tehát a $g_{2 \cdot 3^{k+1}}$ kiszámolható.

Ezzel a bizonyítás teljes. □

Most már rátérhetünk a 2-es Állítás bizonyítására.

Bizonyítás. (2-es Állítás) Az állítást induktív módon bizonyítjuk. Tételezzük fel, hogy ismertek az $s_{3^k}(e_{i,j}), s_{2 \cdot 3^k}(e_{i,j})$ értékek. A 8-as Segédtétel alapján az $s_1(e_{i,j}), s_2(e_{i,j})$ értékek meghatározzák az i_0, j_0 jegyeket. Ekkor a 10-es Segédtétel szerint az i_0, j_0 és $s_3(e_{i,j}), s_6(e_{i,j})$ már elegendő információt tartalmaz ahhoz, hogy az $s_3(e_{i-i_0,j-j_0}), s_6(e_{i-i_0,j-j_0})$ értékek meg legyenek határozva. Most a 9-es Segédtétel révén tudjuk, hogy

$$s_3(e_{i-i_0,j-j_0}) = s_1\left(e_{(i-i_0)/3,(j-j_0)/3}\right),$$
$$s_6(e_{i-i_0,j-j_0}) = s_2\left(e_{(i-i_0)/3,(j-j_0)/3}\right).$$

Innen a 8-as Segédtételt használva adódik az i_1, j_1 ismerete.

A fenti eljárást folytatva az i és j hármas számrendszerbeli felírásában minden jegyet megkapunk, ami pontosan azt mutatja, hogy az $s_{3^k}(e_{i,j})$ és $s_{2\cdot 3^k}(e_{i,j})$ értékekek meghatározzák az i,j számokat, vagyis a 6-os Segédtétel alapján készen vagyunk. □

3. Részeredmények az $\mathbb{F}_p$ véges testre

A előzőekben látott eredmény fényében az $\mathbb{F}_p$ véges test esetével kezdtünk el foglalkozni, és itt részeredményeket sikerült elérni. Ezek többek között az előző szakaszban látott lemmák általánosításai. A sejtésünk a következőképpen fogalmazható meg $\mathbb{F}_p$-re:

11. Feltevés. *Ha $\mathbb{F}=\mathbb{F}_p$ és $m=1$, akkor a következő halmaz egy tartalmazásra nézve minimális szeparálórendszert alkot $\mathbb{F}[V]^{S_n}$-ben:*

$$S_{n,1}(\mathbb{F}_p)=\left\{s_{p^k},s_{2\cdot p^k},...,s_{(p-1)\cdot p^k}\;\middle|\;0\le k\le\left\lfloor\log_p(n)-\log_p(p-1)\right\rfloor\right\}.$$

Az orbitreprezentánsok jelölése a következőképpen fog történni:

$$e_{k_1,...,k_{p-1}}=\left(\underbrace{1,...,1}_{k_1\text{-szer}},\underbrace{2,...,2}_{k_2\text{-szer}},...,\underbrace{p-1,...,p-1}_{k_{p-1}\text{-szer}},0,...,0\right),\ \sum_{i=1}^{p-1}k_i\le n.$$

Továbbá legyen k_i p alapú számrendszerbeli felírása

$$k_i=\left(k_{i_t}k_{i_{t-1}}...k_{i_0}\right)_p.$$

A 6-os lemmához hasonló módon tudjuk kiszámolni az $s_l\left(e_{k_1,...,k_{p-1}}\right)$ értékét.

12. Segédtétel. *Az $s_l\left(e_{k_1,...,k_{p-1}}\right)$ értéke nem más, mint a $\prod_{i=1}^{p-1}(1+i\cdot x)^{k_i}\in\mathbb{F}_p[x]$ szorzatban a l-edfokú tag együtthatója.*

A következő lemma a 9-es Segédtétel általánosítása.

13. Segédtétel. *Ha $p\,|k_i$ minden $i=\overline{1,p-1}$, akkor*

$$s_{p\cdot d}\left(e_{k_1,...,k_{p-1}}\right)=s_d\left(e_{k_1/p,...,k_{p-1}/p}\right).$$

Bizonyítás. A $p\,|k_i$ feltétel alapján $k_{i_0}=0$ minden $i=\overline{1,p-1}$. Ekkor az

$$(1+x)^{k_1}(1+2x)^{k_2}\cdots(1+(p-1)x)^{k_{p-1}}=\prod_{i=1}^{p-1}\prod_{s=0}^{t}\left(1+(i\cdot x)^{p^s}\right)^{k_{j_s}}$$

egyenlőségben elvégezve az $x^p\leftrightarrow y$ változócserét, és kihasználva a Kis Fermat-tételt az

$$(1+x)^{k_1}(1+2x)^{k_2}\cdots(1+(p-1)x)^{k_{p-1}}=(1+y)^{k_1/p}(1+2y)^{k_2/p}\cdots(1+(p-1)y)^{k_{p-1}/p}$$

azonosság adódik, ahonnan azonnal következik az

$$s_{p\cdot d}\left(e_{k_1,\ldots,k_{p-1}}\right) = s_d\left(e_{k_1/p,\ldots,k_{p-1}/p}\right)$$

egyenlőség. □

A 10-es Segédtétel az alábbi módon általánosítható.

14. Segédtétel. *A* $k_{i_0}, k_{i_1}, ..., k_{i_l}$, $i = \overline{1, p-1}$ *és*

$$s_{i\cdot p^{l+1}}\left(e_{k_1,\ldots,k_{p-1}}\right),\ \textit{minden}\ i = \overline{1, p-1}$$

értékek meghatározzák az

$$s_{i\cdot p^{l+1}}\left(e_{k_1-\left(k_{1_l}k_{1_{l-1}}\ldots k_{1_0}\right)_p,\ldots,k_{p-1}-\left(k_{p-1_l}k_{p-1_{l-1}}\ldots k_{p-1_0}\right)_p}\right),$$

értékeket, minden $i = \overline{1, p-1}$

Bizonyítás. Vegyük az

$$f := \prod_{i=1}^{p-1}\prod_{s=0}^{l}\left(1+(ix)^{p^s}\right)^{k_{i_s}},$$
$$g := \prod_{i=1}^{p-1}\prod_{s=l+1}^{t}\left(1+(ix)^{p^s}\right)^{k_{i_s}}$$

polinomokat. Itt az f polinom maximális fokszáma

$$(p-1)^2\left(1+p+\cdots+p^l\right) = (p-1)\cdot\left(p^{l+1}-1\right)$$

lehet.

Írjuk fel az f, g és $f\cdot g$ polinomokat az

$$f = \sum_n f_n x^n,$$
$$g = \sum_n g_n x^n,$$
$$f\cdot g = \sum_n c_n x^n$$

alakban. Tudjuk, hogy

$$s_{i\cdot p^{l+1}}\left(e_{k_1,\ldots,k_{p-1}}\right) = \text{"az } f\cdot g \text{ szorzatban az } x^{i\cdot p^{l+1}} \text{ tag együtthatója"} = c_{i\cdot p^{l+1}},$$

amelyek feltétel szerint ismertek, minden $i = \overline{1, p-1}$. Továbbá a $k_{i_0}, k_{i_1}, ..., k_{i_l}$ ismerete

miatt az $f_{i\cdot p^{l+1}}$ együtthatók is ismertek. Az $f \cdot g$ szorzatban az együtthatókra a következő egyenletrendszert kapjuk:

$$\begin{aligned}
c_{p^{l+1}} &= f_{p^{l+1}} + g_{p^{l+1}} \\
c_{2\cdot p^{l+1}} &= f_{2\cdot p^{l+1}} + g_{2\cdot p^{l+1}} + f_{p^{l+1}} \cdot g_{p^{l+1}} \\
c_{3\cdot p^{l+1}} &= f_{3\cdot p^{l+1}} + g_{3\cdot p^{l+1}} + f_{2\cdot p^{l+1}} \cdot g_{p^{l+1}} + f_{p^{l+1}} \cdot g_{2\cdot p^{l+1}} \\
c_{4\cdot p^{l+1}} &= g_{4\cdot p^{l+1}} + f_{4\cdot p^{l+1}} + f_{2\cdot p^{l+1}} \cdot g_{2\cdot p^{l+1}} + f_{p^{l+1}} \cdot g_{3\cdot p^{l+1}} + f_{3\cdot p^{l+1}} \cdot g_{p^{l+1}} \\
&\vdots \\
c_{(p-1)\cdot p^{l+1}} &= g_{(p-1)\cdot p^{l+1}} + \sum_{i=1}^{p-1} f_{(p-1-i)p^{l+1}} \cdot g_{i\cdot p^{l+1}}.
\end{aligned}$$

Innen a $g_{i\cdot p^{l+1}}$ együtthatók egyértelműen meghatározhatóak. Ezzel a lemmánkat beláttuk. □

Láthattuk, hogy a 2-es Állítás indukciós bizonyításában az indukció első lépésében kulcsfontosságú szerepet töltött be a 8-as Segédtétel. Az általános sejtés hasonló indukciós bizonyításához már csak az alábbi sejtés bizonyítása hiányzik:

15. Feltevés. *Az* $s_1\left(e_{k_1,\ldots,k_{p-1}}\right), \ldots, s_{p-1}\left(e_{k_1,\ldots,k_{p-1}}\right)$ *értékek meghatározzák az* $k_{i_0}, \ldots, k_{p-1_0}$ *értékeket.*

A fenti sejtést még nem sikerült bizonyítanunk, így ez egy további feladatnak számít, viszont számítógépes program segítségével teszteltük a $p = 5$ esetet, amelyre a sejtés igaznak bizonyult.

Hivatkozások

[1] G. Kemper, A. Lopatin, F. Reimers, Separating Invariants Over Finite Fields, Journal of Pure and Applied Algebra, 226 (2022), 106904.