Véges test fölötti szeparáló invariánsok vizsgálata

Szerző: Miklósi Roland Botond

Témavezető: Domokos Mátyás

Az egyéni kutatómunka tárgy keretén belül Gregor Kemper, Artem Lopatin és Fabian Reimers szerzők *Separating Invariants Over Finite Fields* (lásd az [1]-es cikket) című cikkét dolgoztuk fel, és a benne megjelenő - szeparáló invariánsokkal kapcsolatos - eredmények általánosításán kezdtünk el gondolkodni tetszőleges véges test fölött. Mindezt komputeralgebrai kísérletekkel könnyítettük meg.

1. Bevezető

Az algebrai invariánselmélet az absztrakt algebra lényeges kutatási területe. Sok matematikai és fizikai probléma szimmetriák és invariánsok számolására redukálódik. Minden geometriai tulajdonság invariáns a megfelelő transzformációs csoport hatására. Például az Euklideszi geometriában ismert tulajdonságok invariánsak a forgatásra, tükrözésre és transzlációra nézve, amelyek az úgynevezett Euklideszi csoportot alkotják.

Matematikailag röviden a következőről van szó. Adott egy n-dimenziós $\mathbb{F}$ test fölötti V vektortér, melynek koordinátagyűrűje az $\mathbb{F}[V] = \mathbb{F}[x_1, ..., x_n]$ n-változós polinomgyűrű. Továbbá legyen G a $GL(V)$ általános lineáris csoport egy részcsoportja. A G csoport a V vektortéren természetes módon hat, amely az $\mathbb{F}[V]$ koordinátagyűrűn indukál egy hatást úgy, hogy bármely $g \in G$ elemhez

$$(g \cdot f)(v) = f\left(g^{-1} \cdot v\right), \forall v \in V.$$

Ekkor az

$$\mathbb{F}[V]^G = \{f \in \mathbb{F}[V] \mid g \cdot f = f, \text{ minden } g \in G\}$$

részgyűrűt alkot $\mathbb{F}[V]$-ben, amit a G csoport invariánsgyűrűjének nevezünk.

Az invariánselmélet a 19. századi matematika központi elemévé vált. A kor neves matematikusait[1] foglalkoztatta az elmélet, és kezdetben a legnagyobb kérdés az volt, hogy tetszőleges G csoport invariánsgyűrűje végesen generált algebra-e. Ezt Gordan 1868-ban az SL_2 speciális lineáris csoportra belátta, majd 1890-ben Hilbert jelentős eredményt

[1] Mint pl. Cayley, Sylvester, Aronhold, Gordan, Hilbert stb.

közölt, miszerint a csoportok elég széles körének (lineáris reduktív csoportok) végesen generált invariánsgyűrűje van.

Jelenleg az invariánselmélet fő feladatai közé tartozik egy olyan $\{I_1, ..., I_m\}$ polinomrendszer meghatározása adott G csoport esetén, amely generálja az invaránsgyűrűt, mint részalgebrát. Továbbá egy igencsak érdekes és hasznos probléma az, hogy adott geometriai tulajdonság hogyan fordítható le az invariáns polinomok nyelvezetére, illetve fordítva. Létezik-e általános eljárás a geometria és algebra közötti út megteremtésére?[2]

Az $\{I_1, ..., I_m\}$ generátorrendszer meghatározása szinte mindig Gröbner-bázis számolásba torkollik, ennélfogva egy nagyon összetett komputeralgebrai feladat. Hilbert azt sejtette, hogy bármely csoport invariánsgyűrűje végesen generálható[3], azonban a sejtést Nagata ellenpéldával cáfolta 1959-ben. Egy viszonylag frissnek mondható invariánselméleti problémakör az ún. szeparáló invariánsrendszerek (a szeparáló invariáns fogalmát a későbbiekben definiáljuk) számolása, amelyek könnyebben kezelhetőek és számolhatóak, mint maga az $\{I_1, ..., I_m\}$ generátorrendszer. Például minden invariánsgyűrűnek van véges szeparálórendszere, de nem minden invariánsgyűrű generálható végesen (lásd Nagata). Véges csoport véges dimenziós vektortéren vett lineáris hatása esetén a Noether korlát szeparáló invariánsokra mindig teljesül (vagyis léteznek maximum $|G|$-ed fokú homogén szeparáló invariánsok), azonban az invariánsgyűrű generátorrendszerére a moduláris (vagyis, amikor az $\mathbb{F}$ test karakterisztikája osztja a csoport rendjét) esetben ez nem mindig áll fent. Egy további lényeges erőssége a szeparáló invariánsoknak a generáló invariánsokkal szemben Weyl polarizációs tételében mutatkozik meg: legyen G egy csoport, amely lineárisan hat az n-dimenziós V vektortéren, és legyen S egy generátorrendszere az $\mathbb{F}[V^n]^G$ invariánsgyűrűnek, ahol V^n n db. V direktösszege, amelyre a hatás diagonálisan terjed ki (vagyis minden komponensben G-t hattatjuk a V-n). Ekkor az S elemeiből kapható az $\mathbb{F}[V^m]^G$ invariánsgyűrű egy generátorrendszere bármely m-re, ha a test karakterisztikája 0. Viszont ha generátorrendszer helyett szeparálórendszert tekintünk, akkor a tétel igaz bármilyen karakterisztika esetén.

A továbbiakban az [1]-es cikket foglaljuk röviden össze.

2. A cikk összefoglalása

A bevezető jelöléseit használva legyen V egy n-dimenziós vektortér az $\mathbb{F}$ test fölött, melynek koordinátagyűrűje az n-változós polinomgyűrű, valamint tételezzük fel, hogy G véges részcsoport $GL(V)$-ben. Legyen $S \subset \mathbb{F}[V]^G$ részhalmaz. Azt mondjuk, hogy az $u, v \in V$ *szeparálható* az S által, ha létezik $f \in S$ invariáns úgy, hogy $f(u) \neq f(v)$. Az S-et *szeparálórendszer*nek nevezzük, ha bármely $u, v \in V$ szeparálható az S által. Mivel minden invariáns konstans a G hatás pályáin, ezért elegendő a pályák valamilyen

[2] Felix Klein, Erlangeni program, *„Geometry is Invariant Theory.”*.
[3] Hilbert tizennegyedik problémájaként ismert.

reprezentánsain vizsgálni a szeparálhatóságot.

A Noether szám szeparáló változata is definiálható: legyen $\beta_{sep}\left(\mathbb{F}[V]^G\right)$ az a legkisebb pozitív egész szám (jelöljük ezt β_{sep}-el), amelyre a legfennebb β_{sep}-ed fokú homogén invariánsok halmaza szeparálórendszert alkot.

A cikk sajátossága, hogy véges testek fölötti vektorterek felé tereli a vizsgálódást, ennélfogva a szakirodalom első olyan cikke, ami véges testek fölötti szeparáló invariánsokkal foglalkozik. A továbbiakban az $\mathbb{F} = \mathbb{F}_q$ jelölést használjuk és feltesszük, hogy $G \leq GL(V)$ véges részcsoport. Az első szakasz végeredménye egy nagyon fontos formula a szeparáló invariánsrendszerek méretére vonatkozóan, miszerint

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

a minimális szeparálórendszer mérete, ahol k a G hatás orbitjainak száma. A szerzők egy explicit konstrukciót is adnak egy γ elemszámú szeparálórendszerre, amelyben a polinomok fokszámainak maximuma $|G|\, n(q-1)$ (lásd az [1] cikket).

A második szakaszban az előző eredmény feljavítása történik egy olyan konstrukció által, ami egy γ elemszámú (tehát minimális) szeparálórendszert ad, amelyben a polinomok maximális fokszáma $n(q-1)$ abban az esetben, amikor $|G|$ invertálható $\mathbb{F}_q$-ban.

A harmadik szakaszban a gráf izomorfizmus problémával, mint alkalmazási lehetőséggel motiválja azt, hogy fontos a véges testek fölötti szeparáló invariánsok vizsgálata.

Az utolsó szakaszban a multiszimmetrikus polinomokkal kapcsolatos eredményeket mutatnak be. Itt $G = S_n$, amely hat a $V = \mathbb{F}^n$ vektortéren a koordináták permutációjával. Legyen V^m m db. V direktösszege, amelyen az S_n diagonálisan hat. Ekkor az

$$\mathbb{F}[V^m] = \mathbb{F}\left[x(j)_i \,|\, 1 \leq i \leq n, 1 \leq j \leq m\right]$$

koordinátagyűrűn a hatás a $\sigma \cdot x(j)_i = x(j)_{\sigma(i)}$ összefüggéssel adott. Ismert, hogy S_n invariánsgyűrűjének algebra generátorai éppen az elemi szimmetrikus polinomok, amelyeknek V^m-re való kiterjesztésük az ún. *elemi multiszimmetrikus polinomok*. Adott $\underline{\alpha} = (\alpha_1, ..., \alpha_m) \in \mathbb{N}^m$ vektorra bevezetjük az $x_i^{\underline{\alpha}} = x(1)_i^{\alpha_1} \cdots x(m)_i^{\alpha_m}$ jelölést minden $1 \leq i \leq n$. Ekkor a

$$\sigma_t(\underline{\alpha}) = \sum_{1 \leq i_1 < \cdots < i_t \leq n} x_{i_1}^{\underline{\alpha}} \cdots x_{i_t}^{\underline{\alpha}} \in \mathbb{F}[V^m]^{S_n}\ ,\ \text{,minden } 1 \leq t \leq n$$

az $\underline{\alpha}$ vektor által meghatározott *t-edik elemi multiszimmetrikus polinom.* Például ha $m = n = 2$ és $\underline{\alpha} = (1, 2)$, akkor

$$\sigma_1(\underline{\alpha}) = x(1)_1\, x(2)_1^2 + x(1)_2\, x(2)_2^2$$
$$\sigma_2(\underline{\alpha}) = x(1)_1\, x(2)_1^2\, x(1)_2\, x(2)_2^2\,.$$

Értelemszerűen ha $m = 1$ és $\underline{\alpha} = 1$, akkor $\sigma_t(1) = s_t$ elemi szimmetrikus polinomokat kapjuk vissza.

Az $\mathbb{F}_2$ test fölötti esetben minimális szeparálórendszert adnak tetszőleges $m \geq 1$-re az elemi multiszimmetrikus polinomok segítségével.

1. Tétel. *$\mathbb{F} = \mathbb{F}_2$ fölött $m \geq 1$ és $n \geq 2$ esetén a következő rendszer szeparáló és minimális elemszámú $\mathbb{F}[V^m]^{S_n}$-ben:*

$$S_{n,m} = \{\sigma_{2^r}(\underline{\alpha}) \,|\, r \geq 0, |\underline{\alpha}| \geq 1, r + |\underline{\alpha}| - 1 \leq \lfloor log_2(n) \rfloor \ \ minden\ 1 \leq j \leq m\}.$$

A cikk végén a Noether korlátra vonatkozó tételt bizonyítanak be.

2. Tétel. *Az $\mathbb{F} = \mathbb{F}_2$ esetben igazak a következő egyenlőségek*

1. $\beta_{sep}\left(\mathbb{F}[V^m]^{S_n}\right) = 2^{\lfloor \log_2(n) \rfloor}$;
2. *$\sigma(n) = \lfloor \log_2(n) \rfloor + 1$, ahol $\sigma(n)$ az a legkisebb m_0, amire egy adott $S \subset \mathbb{F}[V^{m_0}]^{S_n}$ szeparálórendszer kibővíthető $\mathbb{F}[V^m]^{S_n}$-beli szeparálórendszerré minden $m \geq m_0$.*

A továbbiakban a témához való eddigi hozzájárulásunkat mutatjuk be

3. Eredményeink

Az eddigiek alapján természetes kérdésként vetődik fel, hogy hogyan általánosíthatóak az eredmények tetszőleges $\mathbb{F}_q$ testre. Van-e általános formula az 2-es tételre vonatkozóan?

Az előző szakasz végén említettük, hogy a cikkben minimális szeparálórendszert adnak $\mathbb{F}_2$ test fölött tetszőleges $m \geq 1$ esetben. A cikk az $m = 1$ esetre külön is kitér, amelyet a továbbiakban röviden ismertetni fogunk. Az $m > 1$ esetet jelen beszámolóban nem célunk részletezni, mivel meglehetősen bonyolult jelölésrendszere van, illetve a mi munkánk egyelőre az $m = 1$ esetre fókuszál.

Kissé nehéz lenne a problémát teljes általánosságban megtámadni, ezért eddigi munkánk során az $m = 1$ esetet vizsgáltuk meg $\mathbb{F}_3$ fölött. Még mielőtt rátérnénk ennek az ismertetésére, bemutatjuk az $m = 1$, $\mathbb{F}_2$ esetet.

Az S_n-et hattatva $V = \mathbb{F}_2^n$-en az orbit reprezentánsok a $e_i = (1, ..., 1, 0, ..., 0)$ vektorok, ahol az 1 pontosan i-szer jelenik meg, ahol $0 \leq i \leq n$. Az i kettes számrendszerbeli felírását $(i_t i_{t-1} ... i_o)_2$ módon jelöljük és $\xi_j(i) \in \mathbb{F}_2$ az i kettes számrendszerbeli felírásának j-edik számjegyét jelöli. A következő lemma kulcsfontosságú a minimális szeparálórendszer szempontjából.

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

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

egyenlőség.

Bizonyítás. A cikktől eltérő bizonyítást adunk. Feltehetjük, hogy $i > 2^r$, különben $s_{2^r}(e_i) = 0 = \xi_r(i)$ vagy egyenlőség esetén $s_{2^r}(e_i) = 1 = \xi_r(i)$. Az $s_{2^r}(e_i)$ érték pontosan az $(1+x)^i$ kifejezés 2^r-edik együtthatója. Ez könnyen látható abból az észrevételből, hogy az

$$(1+\lambda_1 x)(1+\lambda_2 x)\cdots(1+\lambda_n x)$$

k-adik együtthatója éppen az $s_k(\lambda_1, ..., \lambda_n)$ elemi szimmetrikus polinom.

Legyen $(i_t i_{t-1} ... i_o)_2$ az i kettes számrendszerbeli felírása, vagyis $i = i_0 + i_1 \cdot 2 + i_2 \cdot 2^2 + ... + i_r \cdot 2^r + ... + i_t \cdot 2^t$. Ekkor

$$\begin{aligned}(1+x)^i &= (1+x)^{i_0+i_1\cdot 2+i_2\cdot 2^2+...+i_t\cdot 2^t} \\ &= (1+x)^{i_0}\left(1+x^2\right)^{i_1}\cdots\left(1+x^{2^r}\right)^{i_r}\cdots\left(1+x^{2^t}\right)^{i_t},\end{aligned}$$

tehát, ha $i_r = 1$, akkor x^{2^r} együtthatója 1, ha pedig $i_r = 0$, akkor x^{2^r} együtthatója 0. □

A következő tétel tulajdonképpen az 1-es tétel sajátos esete, vagyis minimális szeparálórendszert ad $\mathbb{F}[V]^{S_n}$-ben.

4. Tétel. *Ha $\mathbb{F} = \mathbb{F}_2$ és $m = 1$, akkor a következő halmaz egy minimális szeparálórendszer $\mathbb{F}[V]^{S_n}$-ben:*

$$S_{n,1} = \{s_{2^r} \mid 0 \le r \le \lfloor \log_2(n) \rfloor\}.$$

Vagyis kételemű test fölött a 2 hatványadik elemi szimmetrikus polinomok minimális szeparálórendszert alkotnak.

A bizonyításhoz a következő lemmát fogjuk használni.

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

Bizonyítás. (4. Tétel) Az 3-as lemma alapján az $s_{2^k}(e_i)$ értékekből vissza tudjuk nyerni az i kettes számrendszerbeli alakját, ezért a 5-ös lemma értelmében az $S_{n,1}$ szeparálórendszert alkot.

Tudjuk, hogy az orbitok száma $n+1$. Induljunk ki a $\gamma = \lceil \log_2(n+1) \rceil$ egyenlőségből. Innen

$$\begin{gathered}\gamma - 1 < \log_2(n+1) \le \gamma \\ 2^{\gamma-1} < n+1 \le 2^\gamma\end{gathered}$$

egyenlőtlenségeket kapjuk. Másrészt $|S_{n,1}| = \lfloor \log_2(n) \rfloor + 1$, ahonnan

$$\begin{aligned} |S_{n,1}| - 1 \leq \log_2(n) < |S_{n,1}| \\ 2^{|S_{n,1}|-1} \leq n < 2^{|S_{n,1}|} \end{aligned}$$

egyenlőtlenségek adódnak.

A kapott egyenlőtlenségek alapján $|S_{n,1}| = \gamma$. □

Egy hasonló eredmény reményében kezdtünk el az $m = 1$ és $\mathbb{F} = \mathbb{F}_3$ esettel foglalkozni. Ebben az esetben az orbit reprezentánsok az $e_{i,j} = \left(\underbrace{1, ..., 1}_{i}, \underbrace{2, ..., 2}_{j}, 0..., 0 \right)$ vektorok, ahol $0 \leq i, j \leq n$ és $i + j \leq n$. Könnyű látni, hogy ezekből éppen $k = \frac{(n+1)(n+2)}{2}$ db. van. A következő táblázat néhány konkrét n értékre a minimális szeparálórendszer méretét tartalmazza.

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

1. táblázat. Minimális méretek néhány speciális esetben

Tudjuk, hogy az elemi szimmetrikus polinomok együttesen szeparálórendszert alkotnak $\mathbb{F}[V]^{S_n}$-ben. A kérdés az, hogy milyen polinomok hagyhatóak el ebből a rendszerből, úgy hogy a megmaradt polinomok továbbra is szeparáljanak. Ezt a stratégiát tartottuk szem előtt és egy MATLAB programmal könnyítettük meg a kutatásunkat.

Előbb felépítettük az adott n-re az orbit reprezentánsok mátrixát, azaz minden oszlopba egy orbit került, így egy $n \times k$-as mátrixot kaptunk. Ezután egy szintén $n \times k$-as mátrixot építettünk fel, aminek az i-edik sorában és j-edik oszlopában az s_i kiértékelése került a j-edik orbiton. Az utóbbi mátrixot jelöljük A-val. Ekkor a fenti kérdés a következőképpen fogalmazható meg: milyen sorok hagyhatóak el úgy, hogy az így kapott $\overline{A}$ mátrix oszlopai páronként különbözzenek. Algoritmusunk előbb meghatározza az összes olyan sorindexet, amik biztosan nem hagyhatóak el. Az i-edik sor pontosan akkor nem hagyható el, ha létezik két olyan oszlop, amelyek csak az i-edik komponensükben térnek el. Ez pontosan azt jelenti, hogy az s_i elemi szimmetrikus polinom mindenképpen része kell hogy legyen a szeparálórendszernek. Miután ismerjük az összes olyan sort amik nem hagyhatóak el, elkezdjük kitörölni a potenciálisan elhagyható sorokat. Ha a módosított mátrixban találunk nem elhagyható sort, akkor azt megjegyezzük, különben meg töröljük a következő potenciálisan elhagyható sort.

Ezzel az eljárással egy szép mintát véltünk felfedezni, ami egy sejtés megfogalmazásához vezetett. Ezt később matematikailag is bizonyítani tudtuk, így állításként fogalmazzuk meg.

Tartalmazásra nézve minimális szeparálórendszerről akkor beszélünk, ha bármelyik polinomot elhagyva a fennmaradó polinomok nem alkotnak szeparálórendszert. Egy minimális szeparálórendszer tartalmazásra nézve is minimális, fordítva ez nem igaz.

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

$$\{s_1, s_2, s_{3^k}, s_{2\cdot 3^k} \mid 1 \leq k \leq \lfloor \log_3(n) \rfloor\}.$$

Természetesen itt olyan szeparálórendszerről van szó, amit az összes elemi szimmetrikus polinomból kapunk úgy, hogy néhányat belőlük elhagyunk.

Bizonyítás. Azt kell megmutatni, hogy az $\{s_1, s_2, s_{3^k}, s_{2\cdot 3^k} \mid 1 \leq k \leq \lfloor \log_3(n) \rfloor\}$ halmazból mindenik s_l polinomhoz tudunk adni két olyan orbit reprezentánst, amit csak az s_l szeparál.

Az $e_{1,0} = (1, 0, 0, ..., 0)$ és $e_{0,1} = (2, 0, 0, ..., 0)$ orbitokat az s_1 polinom szeparálja, hiszen $s_1(e_{1,0}) = 1 \neq 2 = s_1(e_{0,1})$, de minden más s_l-re $s_k(e_{1,0}) = 0 = s_l(e_{0,1})$.

Az $e_{1,1} = (1, 1, 0, ..., 0)$ és $e_{0,1} = (2, 0, 0, ..., 0)$ orbitokat az s_2 polinom szeparálja, mivel $s_2(e_{1,1}) = 1 \neq 0 = s_2(e_{0,1})$, viszont minden más s_l-re $s_k(e_{1,1}) = s_l(e_{0,1})$.

Az $e_{3^k,0} = (1, 1, ..., 1, 0, ..., 0)$ és $e_{0,3^k} = (2, 2, ..., 2, 0, ..., 0)$ orbitokat az s_{3^k} polinom szeparálja, mert $s_{3^k}\left(e_{3^k,0}\right) = 1 \neq 2 = s_{3^k}\left(e_{0,3^k}\right)$. Továbbá minden más s_l-re $s_l\left(e_{3^k,0}\right) = 0 = s_l\left(e_{0,3^k}\right)$.

Az $e_{0,2\cdot 3^k} = (2, 2, ..., 2, 0, ..., 0)$ és $e_{3^k,0} = (1, ..., 1, 0, ..., 0)$ orbitokat az $s_{2\cdot 3^k}$ szeparálja, mivel $s_{2\cdot 3^k}\left(e_{0,2\cdot 3^k}\right) = 1 \neq 0 = s_{2\cdot 3^k}\left(e_{3^k,0}\right)$. Ha $l < 2 \cdot 3^k$ és $l \neq 3^k$, akkor $s_l\left(e_{0,2\cdot 3^k}\right) = 2 \cdot \binom{2\cdot 3^k}{l} = 0 = s_l\left(e_{3^k,0}\right)$. Ha $l = 3^k$, akkor $s_l\left(e_{0,2\cdot 3^k}\right) = 2 \cdot \binom{2\cdot 3^k}{3^k} = 1 = s_l\left(e_{3^k,0}\right)$.

Ezzel a bizonyításunk teljes. □

A kódunk alapján azt is sejtjük, hogy ezek a polinomok szeparálórendszert alkotnak, hiszen az összes többi polinomnak megfelelő sort elhagyva a módosított mátrix oszlopai páronként különböznek, azonban ezt matematikailag még nem sikerült bizonyítanunk, ezért sejtésként fogalmazzuk meg.

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

$$\overline{S}_{n,1} = \{s_1, s_2, s_{3^k}, s_{2\cdot 3^k} \mid 1 \leq k \leq \lfloor \log_3(n) \rfloor\}.$$

Vegyük észre azt, hogy ha igaz az állítás, akkor az így kapott rendszer nem mindig lesz minimális elemszámú, azonban tartalmazásra nézve mindig minimális. Például ha $n = 9$, akkor a 1-es táblázat alapján $\gamma = 4$, de $\left|S_{n,1}^3\right| = 5$.

További céljaink közé tartozik az 7-es sejtés bizonyítása (vagy esetleges cáfolása), majd hasonló eredmények kidolgozása más véges testekre, illetve tetszőleges $m \geq 1$-re. Úgy gondoljuk, hogy az 3-as lemmához hasonlóan az $s_{3^k}(e_{i,j})$ és $s_{2\cdot 3^k}(e_{i,j})$ értékekből az (i,j) meghatározásának az i és j hármas számrendszerbeli felírásához lehet köze.

Hivatkozások

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