Véges test fölötti szeparáló invariánsok vizsgálata

Szerző: Miklósi Roland Botond
Témavezető: Domokos Mátyás

Eötvös Loránd Tudományegyetem, Budapest

Áttekintés

Matektörténeti vonatkozás

- 19. századi matematika egyik központi eleme;
- Cayley, Sylvester, Aronhold, Gordan, Hilbert stb.;
- probléma:
  - legyen V egy n-dimenziós $\mathbb{F}$ fölötti vektortér, és $G \leq GL(V)$ részcsoport, amely természetes módon hat a V-n;
  - indukált hatás a V koordinátagyűrűjén, vagyis az $\mathbb{F}[V] = \mathbb{F}[x_1, \ldots, x_n]$ n-változós polinomgyűrűn:

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

  - 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, amelyet a G csoport *invariánsgyűrűjének* nevezünk;

Matektörténeti vonatkozás

- 19. századi matematika egyik központi eleme;
- Cayley, Sylvester, Aronhold, Gordan, Hilbert stb.;
- probléma:
  - legyen V egy n-dimenziós $\mathbb{F}$ fölötti vektortér, és $G \leq GL(V)$ részcsoport, amely természetes módon hat a V-n;
  - indukált hatás a V koordinátagyűrűjén, vagyis az $\mathbb{F}[V] = \mathbb{F}[x_1, \ldots, x_n]$ n-változós polinomgyűrűn:

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

  - 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, amelyet a G csoport *invariánsgyűrűjének* nevezünk;

Matektörténeti vonatkozás

- 19. századi matematika egyik központi eleme;
- Cayley, Sylvester, Aronhold, Gordan, Hilbert stb.;
- probléma:
  - legyen V egy n-dimenziós $\mathbb{F}$ fölötti vektortér, és $G \leq GL(V)$ részcsoport, amely természetes módon hat a V-n;
  - indukált hatás a V koordinátagyűrűjén, vagyis az $\mathbb{F}[V] = \mathbb{F}[x_1, ..., x_n]$ n-változós polinomgyűrűn:

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

  - az $\mathbb{F}[V]^G = \{f \in \mathbb{F}[V] \,|\, g \cdot f = f, \text{ minden } g \in G\}$ részgyűrűt alkot $\mathbb{F}[V]$-ben, amelyet a G csoport *invariánsgyűrűjének* nevezünk;

Matektörténeti vonatkozás

- 19. századi matematika egyik központi eleme;
- Cayley, Sylvester, Aronhold, Gordan, Hilbert stb.;
- probléma:
  - legyen V egy n-dimenziós $\mathbb{F}$ fölötti vektortér, és $G \leq GL(V)$ részcsoport, amely természetes módon hat a V-n;
  - indukált hatás a V koordinátagyűrűjén, vagyis az $\mathbb{F}[V] = \mathbb{F}[x_1, ..., x_n]$ n-változós polinomgyűrűn:

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

  - az $\mathbb{F}[V]^G = \{f \in \mathbb{F}[V] \,|\, g \cdot f = f, \text{ minden } g \in G\}$ részgyűrűt alkot $\mathbb{F}[V]$-ben, amelyet a G csoport *invariánsgyűrűjének* nevezünk;

Matektörténeti vonatkozás

- 19. századi matematika egyik központi eleme;
- Cayley, Sylvester, Aronhold, Gordan, Hilbert stb.;
- probléma:
  - legyen V egy n-dimenziós $\mathbb{F}$ fölötti vektortér, és $G \leq GL(V)$ részcsoport, amely természetes módon hat a V-n;
  - indukált hatás a V koordinátagyűrűjén, vagyis az $\mathbb{F}[V] = \mathbb{F}[x_1, ..., x_n]$ n-változós polinomgyűrűn:

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

  - az $\mathbb{F}[V]^G = \{f \in \mathbb{F}[V] \,|\, g \cdot f = f, \text{ minden } g \in G\}$ részgyűrűt alkot $\mathbb{F}[V]$-ben, amelyet a G csoport *invariánsgyűrűjének* nevezünk;

Az invariánselmélet kérdései

- végesen generált algebra-e az invariánsgyűrű, azaz létezik-e olyan $\{I_1, ..., I_m\}$ véges polinomrendszer, hogy minden invariáns felírható az $I_1, ..., I_m$ polinomok polinomjaként?
- Gordan: 1868, SL_2-re belátta; Hilbert: 1890, lineárisan reduktív csoportokra bizonyította;
- Hilbert tizennegyedik problémája, Nagata 1959-ben ellenpéldával cáfolta;
- adott geometriai tulajdonság hogyan fordítható le az invariáns polinomok nyelvezetére, illetve fordítva?
- Felix Klein, Erlangeni program, „*Geometry is Invariant Theory*”;

Az invariánselmélet kérdései

- végesen generált algebra-e az invariánsgyűrű, azaz létezik-e olyan $\{I_1, ..., I_m\}$ véges polinomrendszer, hogy minden invariáns felírható az $I_1, ..., I_m$ polinomok polinomjaként?
- Gordan: 1868, SL_2-re belátta; Hilbert: 1890, lineárisan reduktív csoportokra bizonyította;
- Hilbert tizennegyedik problémája, Nagata 1959-ben ellenpéldával cáfolta;
- adott geometriai tulajdonság hogyan fordítható le az invariáns polinomok nyelvezetére, illetve fordítva?
- Felix Klein, Erlangeni program, „*Geometry is Invariant Theory*”;

Az invariánselmélet kérdései

- végesen generált algebra-e az invariánsgyűrű, azaz létezik-e olyan $\{I_1, ..., I_m\}$ véges polinomrendszer, hogy minden invariáns felírható az $I_1, ..., I_m$ polinomok polinomjaként?
- Gordan: 1868, SL_2-re belátta; Hilbert: 1890, lineárisan reduktív csoportokra bizonyította;
- Hilbert tizennegyedik problémája, Nagata 1959-ben ellenpéldával cáfolta;
- adott geometriai tulajdonság hogyan fordítható le az invariáns polinomok nyelvezetére, illetve fordítva?
- Felix Klein, Erlangeni program, „*Geometry is Invariant Theory*”;

Az invariánselmélet kérdései

- végesen generált algebra-e az invariánsgyűrű, azaz létezik-e olyan $\{I_1, ..., I_m\}$ véges polinomrendszer, hogy minden invariáns felírható az $I_1, ..., I_m$ polinomok polinomjaként?
- Gordan: 1868, SL_2-re belátta; Hilbert: 1890, lineárisan reduktív csoportokra bizonyította;
- Hilbert tizennegyedik problémája, Nagata 1959-ben ellenpéldával cáfolta;
- adott geometriai tulajdonság hogyan fordítható le az invariáns polinomok nyelvezetére, illetve fordítva?
- Felix Klein, Erlangeni program, „*Geometry is Invariant Theory*”;

Az invariánselmélet kérdései

- végesen generált algebra-e az invariánsgyűrű, azaz létezik-e olyan $\{I_1, ..., I_m\}$ véges polinomrendszer, hogy minden invariáns felírható az $I_1, ..., I_m$ polinomok polinomjaként?
- Gordan: 1868, SL_2-re belátta; Hilbert: 1890, lineárisan reduktív csoportokra bizonyította;
- Hilbert tizennegyedik problémája, Nagata 1959-ben ellenpéldával cáfolta;
- adott geometriai tulajdonság hogyan fordítható le az invariáns polinomok nyelvezetére, illetve fordítva?
- Felix Klein, Erlangeni program, „*Geometry is Invariant Theory*”;

Szeparáló invariánsok

- egy szeparálórendszer „jobban viselkedik”, mint egy generátorrendszer:
  - minden invariánsgyűrűnek van véges szeparálórendszere, véges generátorrendszer nem mindig adható (lásd Nagata);
  - a Noether korlát szeparáló invariánsokra mindig teljesül, generátorrendszerre ez nem mindig igaz moduláris esetben;
  - Weyl polarizációs tétele;

Szeparáló invariánsok

- egy szeparálórendszer „jobban viselkedik”, mint egy generátorrendszer:
  - minden invariánsgyűrűnek van véges szeparálórendszere, véges generátorrendszer nem mindig adható (lásd Nagata);
  - a Noether korlát szeparáló invariánsokra mindig teljesül, generátorrendszerre ez nem mindig igaz moduláris esetben;
  - Weyl polarizációs tétele;

Szeparáló invariánsok

- egy szeparálórendszer „jobban viselkedik”, mint egy generátorrendszer:
  - minden invariánsgyűrűnek van véges szeparálórendszere, véges generátorrendszer nem mindig adható (lásd Nagata);
  - a Noether korlát szeparáló invariánsokra mindig teljesül, generátorrendszerre ez nem mindig igaz moduláris esetben;
  - Weyl polarizációs tétele;

Szeparáló invariánsok

- egy szeparálórendszer „jobban viselkedik”, mint egy generátorrendszer:
  - minden invariánsgyűrűnek van véges szeparálórendszere, véges generátorrendszer nem mindig adható (lásd Nagata);
  - a Noether korlát szeparáló invariánsokra mindig teljesül, generátorrendszerre ez nem mindig igaz moduláris esetben;
  - Weyl polarizációs tétele;

Áttekintés

Definíciók

- $\mathbb{F} = \mathbb{F}_q$ véges test, V egy n-dimenziós vektortér $\mathbb{F}$ fölött, $G \leq GL(V)$ véges részcsoport;
- legyen $S \subset \mathbb{F}[V]^G$, az $u, v \in V$ *szeparálható* az S által, ha létezik $f \in S$ úgy, hogy $f(u) \neq f(v)$;
- S *szeparálórendszer* pontosan akkor, ha bármely $u, v \in V$ szeparálható az S által;
- Noether szám: $\beta_{\text{sep}}\left(\mathbb{F}[V]^G\right)$ a legkisebb természetes szám, amelyre a legfennebb β_{sep}-ed fokú homogén invariánsok halmaza szeparálórendszert alkot;

Definíciók

- $\mathbb{F} = \mathbb{F}_q$ véges test, V egy n-dimenziós vektortér $\mathbb{F}$ fölött, $G \leq GL(V)$ véges részcsoport;
- legyen $S \subset \mathbb{F}[V]^G$, az $u, v \in V$ *szeparálható* az S által, ha létezik $f \in S$ úgy, hogy $f(u) \neq f(v)$;
- S *szeparálórendszer* pontosan akkor, ha bármely $u, v \in V$ szeparálható az S által;
- Noether szám: $\beta_{\text{sep}}\left(\mathbb{F}[V]^G\right)$ a legkisebb természetes szám, amelyre a legfennebb β_{sep}-ed fokú homogén invariánsok halmaza szeparálórendszert alkot;

Definíciók

- $\mathbb{F} = \mathbb{F}_q$ véges test, V egy n-dimenziós vektortér $\mathbb{F}$ fölött, $G \leq GL(V)$ véges részcsoport;
- legyen $S \subset \mathbb{F}[V]^G$, az $u, v \in V$ *szeparálható* az S által, ha létezik $f \in S$ úgy, hogy $f(u) \neq f(v)$;
- S *szeparálórendszer* pontosan akkor, ha bármely $u, v \in V$ szeparálható az S által;
- Noether szám: $\beta_{\text{sep}}\left(\mathbb{F}[V]^G\right)$ a legkisebb természetes szám, amelyre a legfennebb β_{sep}-ed fokú homogén invariánsok halmaza szeparálórendszert alkot;

Definíciók

- $\mathbb{F} = \mathbb{F}_q$ véges test, V egy n-dimenziós vektortér $\mathbb{F}$ fölött, $G \leq GL(V)$ véges részcsoport;
- legyen $S \subset \mathbb{F}[V]^G$, az $u, v \in V$ *szeparálható* az S által, ha létezik $f \in S$ úgy, hogy $f(u) \neq f(v)$;
- S *szeparálórendszer* pontosan akkor, ha bármely $u, v \in V$ szeparálható az S által;
- Noether szám: $\beta_{\text{sep}}\left(\mathbb{F}[V]^G\right)$ a legkisebb természetes szám, amelyre a legfennebb β_{sep}-ed fokú homogén invariánsok halmaza szeparálórendszert alkot;

A cikk tartalma

- *első szakasz*: elemszámra nézve minimális szeparálórendszer mérete

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

ahol k a hatás orbitjainak a száma; konstrukció egy γ elemszámú szeparálórendszerre, amelyben a polinomok maximális fokszáma $|G|\, n(q-1)$;

- *második szakasz*: az előző eredmény feljavítása, amikor a csoport rendje invertálható $\mathbb{F}_q$-ban: $|G|\, n(q-1)$ helyett $n(q-1)$;
- *harmadik szakasz*: szeparáló invariánsok alkalmazása a gráf izomorfizmus problémára;
- *negyedik szakasz*: multiszimmetrikus polinomokkal kapcsolatos eredmények;

A cikk tartalma

- *első szakasz*: elemszámra nézve minimális szeparálórendszer mérete

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

ahol k a hatás orbitjainak a száma; konstrukció egy γ elemszámú szeparálórendszerre, amelyben a polinomok maximális fokszáma $|G|\, n(q-1)$;
- *második szakasz*: az előző eredmény feljavítása, amikor a csoport rendje invertálható $\mathbb{F}_q$-ban: $|G|\, n(q-1)$ helyett $n(q-1)$;
- *harmadik szakasz*: szeparáló invariánsok alkalmazása a gráf izomorfizmus problémára;
- *negyedik szakasz*: multiszimmetrikus polinomokkal kapcsolatos eredmények;

A cikk tartalma

- *első szakasz*: elemszámra nézve minimális szeparálórendszer mérete

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

ahol k a hatás orbitjainak a száma; konstrukció egy γ elemszámú szeparálórendszerre, amelyben a polinomok maximális fokszáma $|G|\, n(q-1)$;
- *második szakasz*: az előző eredmény feljavítása, amikor a csoport rendje invertálható $\mathbb{F}_q$-ban: $|G|\, n(q-1)$ helyett $n(q-1)$;
- *harmadik szakasz*: szeparáló invariánsok alkalmazása a gráf izomorfizmus problémára;
- *negyedik szakasz*: multiszimmetrikus polinomokkal kapcsolatos eredmények;

A cikk tartalma

- *első szakasz*: elemszámra nézve minimális szeparálórendszer mérete

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

ahol k a hatás orbitjainak a száma; konstrukció egy γ elemszámú szeparálórendszerre, amelyben a polinomok maximális fokszáma $|G|\, n(q-1)$;
- *második szakasz*: az előző eredmény feljavítása, amikor a csoport rendje invertálható $\mathbb{F}_q$-ban: $|G|\, n(q-1)$ helyett $n(q-1)$;
- *harmadik szakasz*: szeparáló invariánsok alkalmazása a gráf izomorfizmus problémára;
- *negyedik szakasz*: multiszimmetrikus polinomokkal kapcsolatos eredmények;

A negyedik szakasz

- itt $G = S_n$ és V^m a $V = \mathbb{F}^n$ m db. direktösszege; koordinátagyűrű:

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

amelyen a hatás: $\sigma \cdot x\left(j\right)_i = x\left(j\right)_{\sigma(i)}$;

- *elemi multiszimmetrikus polinomok*: $\underline{\alpha} = (\alpha_1, ..., \alpha_m) \in \mathbb{N}^m$, $x_i^{\underline{\alpha}} = x\left(1\right)_i^{\alpha_1} \cdots x\left(m\right)_i^{\alpha_m}$ jelölésekkel,

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

A negyedik szakasz

- itt $G = S_n$ és V^m a $V = \mathbb{F}^n$ m db. direktösszege; koordinátagyűrű:

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

  amelyen a hatás: $\sigma \cdot x\left(j\right)_i = x\left(j\right)_{\sigma(i)}$;
- *elemi multiszimmetrikus polinomok*: $\underline{\alpha} = (\alpha_1, ..., \alpha_m) \in \mathbb{N}^m$, $x_i^{\underline{\alpha}} = x\left(1\right)_i^{\alpha_1} \cdots x\left(m\right)_i^{\alpha_m}$ jelölésekkel,

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

A negyedik szakasz - folytatás

- $\mathbb{F}_2$ fölött a következő két tételt bizonyítják be:

Tétel 1

Ha $\mathbb{F} = \mathbb{F}_2$, $m \geq 1$ *és* $n \geq 2$, *akkor a következő rendszer szeparáló és minimális elemszámú* $\mathbb{F}\left[V^m\right]^{S_n}$*-ben:*

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

A negyedik szakasz - folytatás

Tétel 2

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

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

Áttekintés

Eredményeink

- *negyedik szakasz*: $m = 1$ eset:

Tétel 3

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

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

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

Eredményeink

- az $m = 1$, $\mathbb{F} = \mathbb{F}_3$ esettel foglalkoztunk, és számítógépes kísérletekkel (MATLAB) sikerült megsejtenünk, majd bebizonyítanunk a következő állítást:

Tétel 4

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

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

Eredményeink

- sejtjük, hogy az

$$\overline{S}_{n,1} = \{s_1, s_2, s_{3^k}, s_{2.3^k} \mid 1 \leq k \leq \lfloor \log_3(n) \rfloor\}$$

  tartalmazásra nézve minimális szeparálórendszert alkot $\mathbb{F}[V]^{S_n}$-ben;
- ez nem mindig lesz minimális elemszámú, pl. $n = 9$-re a $\gamma = 4$, de $\left|\overline{S}_{n,1}\right| = 5$;

Eredményeink

- sejtjük, hogy az

$$\overline{S}_{n,1} = \{s_1, s_2, s_{3^k}, s_{2.3^k} \mid 1 \leq k \leq \lfloor \log_3(n) \rfloor\}$$

  tartalmazásra nézve minimális szeparálórendszert alkot $\mathbb{F}[V]^{S_n}$-ben;
- ez nem mindig lesz minimális elemszámú, pl. $n = 9$-re a $\gamma = 4$, de $\left|\overline{S}_{n,1}\right| = 5$;

További tervek

- az előző sejtés bizonyítása (vagy esetleges cáfolása);
- további véges testek fölötti vizsgálódás, az eredmények kiterjesztése $m \geq 1$ esetekre;

További tervek

- az előző sejtés bizonyítása (vagy esetleges cáfolása);
- további véges testek fölötti vizsgálódás, az eredmények kiterjesztése $m \geq 1$ esetekre;

Hivatkozás I


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

Köszönöm a figyelmet!