Gröbner theory of zero dimensional ideals
with a view toward combinatorics
(Nulla dimenziós ideálok Gröbner-elmélete és kombinatorikai alkalmazásai)

A doktori értekezés tézisei

FELSZEGHY BÁLINT

Budapesti Műszaki és Gazdaságtudományi Egyetem,
Matematika intézet

Témavezető:
Rónyai Lajos

2007

1. Bevezetés

A Gröbner-bázisok polinomideálok bizonyos speciális tulajdonságokkal bíró generátorrendszerei. Az elmélet alapjait – kommutatív algebrai kérdéseket kutatva – B. Buchberger dolgozta ki. Azóta a Gröbner-bázisok a matematika számtalan területén leltek alkalmazásra, mint például algebrai geometriában, szimbolikus számítások elméletében, kódelméletben, automatikus bizonyítások elméletében, egész programozásban, parciális differenciálegyenletek elméletében és numerikus módszerekben. Egy aránylag új alkalmazási területe a Gröbner-elméletnek az (algebrai) kombinatorika.

Kombinatorikus szempontból leginkább nulla dimenziós ideálok Gröbner-elmélete érdekes. Jelen disszertációban ezzel foglalkozunk; az elmélet megalapozása után rátérünk annak kombinatorikai alkalmazásaira.

Az elméletről szóló részekben az $\mathbb{F}$ test feletti $\mathbb{F}[\mathbf{x}]$ többváltozós polinomgyűrű I ideáljaival fogunk dolgozni. Az I egy Gröbner-bázisának ismeretében megkapható a véges dimenziós $\mathbb{F}[\mathbf{x}]/I$ vektortér egy speciális bázisa, a standard monomok halmaza. Néha azonban könnyebben is meghatározhatóak a standard monomok, mint egy Gröbner-bázis kiszámolásával. A dolgozatban bemutatjuk a Lex játékot, mint egy igen hatékony módszert standard monomok meghatározására. Ezzel párhuzamosan nulla dimenziós ideálok Gröbner-bázisainak szerkezetét is alaposan feltérképezzük.

A kombinatorika pontrendszerek eltűnő ideáljain keresztül kerül be a képbe. Legyen V az $\mathbb{F}^n$ véges részhalmaza, amely valami módon leírja a vizsgálandó kombinatorikai objektumot. (Gondolhatunk itt például egy halmazrendszer karakterisztikus vektoraiból álló halmazra, vagy n különböző szám összes permutációi által alkotott halmazra.) A V-n eltűnő n-változós polinomok egy $I(V)$ nulla dimenziós ideált alkotnak. A legegyszerűbb, mégis roppant hasznos észrevétel, hogy V számossága éppen $\dim(\mathbb{F}[\mathbf{x}]/I(V))$, tehát megegyezik a standard monomok számával. A V pontrendszer sok más tulajdonsága is leírható $V \to \mathbb{F}$ függvényekre megfogalmazott állításként. Miután ezen függvénytér izomorf az $\mathbb{F}[\mathbf{x}]/I(V)$ vektortérrel, ezeket a kérdéseket lehetséges Gröbner-elmélettel vizsgálni.

A disszertációban a Gröbner-elmélet segítségével egyszerűbb bizonyításokat adunk ismert tételekre, mint például Harima dualitástétele, Alon kombinatorikus nullhelytétele, a szimmetrikus polinomok alaptételének Garsia-féle általánosítása és Wilson tartalmazási mátrixokra vonatkozó rangformulája. Ugyanakkor ismertetünk két alkalmazást extremális halmazrendszerek elméletében is. Utóbbiak közös alapját az $I(V_{\mathcal{F}})$ ideál algebrai tulajdonságainak

alapos feltérképezése adja, ahol $\mathcal{F}$ modulo q teljes ℓ-széles halmazcsalád. Igen sok számolás árán megadjuk ennek Gröbner-bázisát és Hilbert-függvényét, amik után viszont már nem lesz túl nehéz igazolni két állítást bizonyos tulajdonságoknak eleget tevő halmazrendszerek maximális elemszámáról.

A dolgozat öt cikkünk eredményei alapján íródott, ugyanakkor bizonyos részeit – legalábbis az itt tárgyalt általánosságban – még nem publikáltuk.

2. Alapfogalmak

A következőkben röviden összefoglaljuk a tézisben tárgyaltak megértéséhez szükséges jelöléseket, alapvető definíciókat és tényeket. A disszertáció megfelelő fejezete részletesebb bevezetést ad a Gröbner-bázisok elméletébe.

A dolgozatban n pozitív egész számot jelöl, és $[n] = \{1, 2, \ldots, n\}$. Az $\mathbb{F}$ test, $\mathbb{F}[x_1, \ldots, x_n] = \mathbb{F}[\mathbf{x}]$ pedig n változós polinomgyűrű. Vastagon szedett betűkkel jelöljük az n hosszú vektorokat, például $\mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{F}^n$. Ha $\mathbf{w} \in \mathbb{N}^n$, akkor $\mathbf{x}^\mathbf{w}$ az $x_1^{w_1} \ldots x_n^{w_n} \in \mathbb{F}[\mathbf{x}]$ monom rövidebb leírására szolgál. Néha megjelennek majd $n-1$ dimenziós $\overline{\mathbf{y}} = (y_1, \ldots, y_{n-1})$ vektorok és ennek megfelelő $\overline{\mathbf{x}}^{\overline{\mathbf{w}}} = x_1^{w_1} \ldots x_{n-1}^{w_{n-1}}$ monomok.

2.1. A Gröbner-elmélet alapjai

Monomok egy $\prec$ teljes rendezése *tagsorrend*, ha 1 a legkisebb elem és $\prec$ kompatibilis a monomokkal való szorzással.

A két legtöbbet használt tagsorrend a *lexikografikus* (röviden *lex*) és a *fokkompatibilis lexikografikus* (*deglex*) rendezés. Előbbi szerint $\mathbf{x}^\mathbf{w} \prec_{\text{lex}} \mathbf{x}^\mathbf{u}$ akkor és csak akkor, ha $w_i < u_i$ teljesül a legkisebb olyan i indexre, amelyre $w_i \neq u_i$. Kisebb fokú monomok a deglex rendezésben kisebbek, azonos fokúak között pedig a monomok lexikografikus sorrendje határozza meg a rendezést.

Egy nemnulla $f \in \mathbb{F}[\mathbf{x}]$ polinom $\operatorname{lm}(f)$ *főtagja* az f-ben előforduló legnagyobb monom. Egy I *ideál főtagjai*nak halmaza $\operatorname{Lm}(I) = \{\operatorname{lm}(f) : f \in I\}$. Végül egy monomot az I ideál standard monomjának nevezünk, ha nincs $\operatorname{Lm}(I)$-ben. Jelölje $\operatorname{Sm}(I)$ a standard monomok halmazát.

Az I ideál egy véges G részhalmazát I *Gröbner-bázisá*nak nevezzük, ha minden nemnulla $f \in I$-hez van olyan $g \in G$, amelyre $\operatorname{lm}(g)$ osztja $\operatorname{lm}(f)$-et. Ismert tény, hogy minden ideálnak létezik Gröbner-bázisa.

A legfeljebb m fokú többváltozós polinomok vektorterét jelölje $\mathbb{F}[\mathbf{x}]_{\leq m}$. Ha $I \trianglelefteq \mathbb{F}[\mathbf{x}]$ ideál, akkor $I_{\leq m} = I \cap \mathbb{F}[\mathbf{x}]_{\leq m}$ és $\operatorname{Sm}(I)_{\leq m} = \operatorname{Sm}(I) \cap \mathbb{F}[\mathbf{x}]_{\leq m}$. Az $\mathbb{F}[\mathbf{x}]/I$ $\mathbb{F}$-algebra Hilbert-függvénye $H_I : \mathbb{N} \to \mathbb{N}$, amelyre

$$H_I(m) = \dim_\mathbb{F}\left(\mathbb{F}[\mathbf{x}]_{\leq m} \big/ I_{\leq m}\right).$$

A következő állítás igen fontos lesz számunkra.

2.1.21. Állítás. *Ha $\prec$ fok-kompatibilis rendezés, akkor $\mathrm{Sm}\,(I)_{\leq m}$ lineáris bázisa $\mathbb{F}\,[\mathbf{x}]_{\leq m}\,/I_{\leq m}$-nek. Speciálisan $H_I(m) = \left|\mathrm{Sm}\,(I)_{\leq m}\right|$.*

2.2. Nulla dimenziós ideálok

Egy $V \subseteq \mathbb{F}^n$ véges pontrendszer esetén V *eltűnő ideálja*

$$I(V) = \{f \in \mathbb{F}\,[\mathbf{x}] \,:\, f(\mathbf{y}) = 0 \text{ minden } \mathbf{y} \in \mathbb{F}^n\text{-re}\}\,.$$

Legyen $M_{\mathbf{y}} = \langle x_1 - y_1, \ldots, x_n - y_n\rangle$. Könnyű látni, hogy $I(V)$ primér felbontása $I(V) = \prod_{\mathbf{y}\in V} M_{\mathbf{y}}$.

Azt mondjuk, hogy az I nulla dimenziós ideál *felbomló*, ha minden primér komponense $M_{\mathbf{y}}$-primér, valamely $\mathbf{y} \in \mathbb{F}^n$ esetén. A továbbiakban csak felbomló ideálokkal foglalkozunk és ennek megfelelően feltesszük, hogy a primér felbontás

$$I = \prod_{\mathbf{y}\in\mathbb{F}^n} Q_{\mathbf{y}} \tag{1}$$

alakú, ahol $Q_{\mathbf{y}}$ $M_{\mathbf{y}}$-primér.

Egy $M \subseteq \mathbb{N}^n$ halmaz *leszálló*, ha $\mathbf{m} \in M$, $\mathbf{r} \in \mathbb{N}^n$ és $\forall\, i\ r_i \leq m_i$-ből következik $\mathbf{r} \in M$. Legyen $\mathbf{y} \in \mathbb{F}^n$ egy pont, $M \subseteq \mathbb{N}^n$ leszálló halmaz és $f \in \mathbb{F}\,[\mathbf{x}]$ polinom. Írjuk fel f-et $\mathbf{x}-\mathbf{y}$ változók polinomjaként, és jelölje $c_{\mathbf{w}}$ az $(\mathbf{x}-\mathbf{y})^{\mathbf{w}}$ $\mathbf{y}$-*monom* együtthatóját. Azt mondjuk, hogy f *multiplicitása* $\mathbf{y}$-*ban* M, ha minden $\mathbf{w} \in M$ esetén $c_{\mathbf{w}} = 0$. (Véges) algebrai multihalmazon olyan $\mathcal{V}\colon \mathbb{F}^n \to 2^{\mathbb{N}^n}$ függvényt értünk, amely értékkészlete véges leszálló halmazokból áll és véges kivételtől eltekintve $\mathcal{V}(\mathbf{y}) = \emptyset$. Legyen $|\mathcal{V}| = \sum_{\mathbf{y}\in\mathbb{F}^n} |\mathcal{V}(\mathbf{y})|$. A $\mathcal{V}$ *eltűnő ideál*ja $I(\mathcal{V})$ az összes olyan f polinomot tartalmazza, amely multiplicitása minden $\mathbf{y} \in \mathbb{F}^n$ esetén $\mathbf{y}$-ban $\mathcal{V}(\mathbf{y})$.

2.2.8. Tétel (Felszeghy, Rónyai). *Egy I felbomló ideál pontosan akkor valamely véges $\mathcal{V}$ algebrai multihalmaz eltűnő ideálja, ha minden $Q_{\mathbf{y}}$ primér komponense generálható $\mathbf{x}-\mathbf{y}$ változókból felépített $\mathbf{y}$-monomokkal.*

3. Dobozok Gröbner-bázisai

A Gröbner-elmélet alapjainak elsajátítása után máris rátérhetünk az első kombinatorikai és algebrai alkalmazásainkra, amelyek közös vonása, hogy az $I(B)$ ideál Gröbner-bázisának meghatározásán alapulnak, ahol B az $\mathbb{F}$ test

n véges részhalmazának direkt szorzata. Az első itt tárgyalt eredmény Harima [30] egy tételének egyszerű bizonyítása. A B dobozban vett V és V^c komplementer-pontrendszereket vizsgálunk; igazolunk egy összefüggést $I(V)$ és $I(V^c)$ Hilbert-függvényei között, illetve megmutatjuk ennek egy alkalmazását bool függvények bonyolultságelméletében. A $B = \{0,1\}^n$ speciális esetre vonatkozó formulát egyébként Pintér és Rónyai [35] más módon igazolták. A 3.1 fejezet eredményeit – kevésbé általánosan tárgyalva – [22] összefoglaló cikkünkben publikáltuk.

A másik alkalmazás többváltozós polinomegyenletek véges testek feletti megoldhatóságával foglalkozik. Rédei egy sejtése [37] elégséges feltételt mond arra, hogy egy polinomnak mikor van gyöke egy véges prímtest felett. Nemrég megjelent [38] munkájában Rónyai adott ellenpéldát a sejtés általános esetére, ugyanakkor speciális alakú polinomokra a sejtés továbbra is nyitott. Egy Rédeiénél némileg erősebb feltevéssel élve igazoljuk a sejtést általánosított diagonális polinomokra. Ehhez Alon kombinatorikus nullhelytételét [3] használjuk fel, amelyet Gröbner-bázisos terminológiával kimondunk és be is bizonyítunk. Ezen tételek [18] cikkünkben jelentek meg.

3.1. Harima tétele véges pontrendszerekre

3.1.1. Definíció. Legyen $V \subseteq \mathbb{F}^n$, és tegyük fel, hogy $V \subseteq B_1 \times B_2 \times \cdots \times B_n = B$ néhány $B_1, \ldots, B_n \subseteq \mathbb{F}$ véges nemüres halmazra. Ekkor B halmazt *doboz*nak nevezzük. A V *(B-beli) komplementere* $V^c = B \setminus V$. Legyen $k_i = |B_i|$, $\mathbf{k} = (k_1, \ldots, k_n)$ és $k = \sum_{i \in [n]} k_i$.

3.1.2. Tétel (Harima; Felszeghy, Pintér, Rónyai). *Ha $m = 0, 1, \ldots, k-n$, akkor $I(V)$ és $I(V^c)$ Hilbert-függvényeire a következő összefüggés teljesül:*

$$H_{I(B)}(m) - |V| = H_{I(V^c)}(m) - H_{I(V)}(k-n-m-1).$$

Harima eredeti tétele a fentinél általánosabb pontrendszerekre vonatkozik. A mi bizonyításunk egyszerű polinom-számításokon alapul, amelynek gerincét az alábbi két állítás képezi.

3.1.3. Lemma. *Az $I(B)$ ideál redukált Gröbner-bázisa tetszőleges tagsorrendre*

$$G = \left\{ \prod_{b \in B_i} (x_i - b) \ : \ i \in [n] \right\}.$$

3.1.4. Állítás. *Legyen $\mathbf{x}^{\mathbf{w}}$ olyan monom, amelyre $w_i < k_i$ minden $i \in [n]$ esetén. Ekkor*

$$\mathbf{x}^{\mathbf{w}} \in \mathrm{Sm}\,(I(V)) \iff \mathbf{x}^{\mathbf{k-w-1}} \in \mathrm{Lm}\,(I(V^c)).$$

A 3.1.2 tétel segítségével egy érdekes minimax állítást fogalmazhatunk meg bool függvények bonyolultságelméletéből ismert mennyiségek között. Ha $V \subsetneq B$, legyen $a(V)$ a V-n eltűnő $\mathrm{Sm}\,(I(B))$-beli monomokat tartalmazó polinomok közül a minimális fokszámú foka. Ha $\emptyset \neq V \subseteq B$, akkor $b(V)$ a legkisebb d egész, amelyre $H_{I(V)}(d) = |V|$.

3.1.5. Következmény. *Tegyük fel, hogy $\emptyset \neq V \subseteq B$. Ekkor teljesül, hogy*

$$a(V^c) + b(V) = k - n.$$

3.2. Alon kombinatorikus nullhelytétele és Rédei sejtése

A 3.1.3 lemma tekinthető Alon kombinatorikus nullhelytételének egy átfogalmazásának. Ezt a tételt rengeteg cikkben a „nemeltűnési tételen" keresztül alkalmazzák.

3.2.1. Tétel (Alon nemeltűnési tétele). *Legyenek $\emptyset \neq B_i \subseteq \mathbb{F}$ halmazok, $|B_i| = k_i$ $(i \in [n])$, és legyen $f \in \mathbb{F}[\mathbf{x}]$ olyan polinom, amelyre $\deg(f) = \sum_{i=1}^{n}(k_i - 1)$ és amelyben $\mathbf{x^{k-1}} = \prod_{i=1}^{n} x_i^{k_i-1}$ együtthatója nem 0. Ekkor f nem tűnik el a $B = B_1 \times \cdots \times B_n$ dobozon, azaz $f \notin I(B)$.*

Rédei László 1946-ban megfogalmazott egy sejtést véges testek feletti polinomegyenletek megoldhatóságáról. Bár Rónyai mutatott ellenpéldát az általános esetre, bizonyos polinomosztályokra a sejtés igaz.

Legyen p prím, $f \in \mathbb{F}_p[\mathbf{x}]$ polinom, és tegyük fel, hogy f x_i-ben vett foka (röviden $\deg_{x_i}(f)$) legfeljebb $p-1$ minden $i \in [n]$ esetén. Más szóval f redukált $I(\mathbb{F}_p^n)$ Gröbner-bázisára nézve.

Az f polinom *rang*ja a legkisebb r pozitív egész, amelyre f homogén lineáris változócserével r változóssá tehető. Ezt $\mathrm{rang}(f) = r$ jelöli.

3.2.2. Sejtés (Rédei). *Ha $f \in \mathbb{F}_p[\mathbf{x}]$ nem konstans, $\deg_{x_i}(f) \leq p-1$ $(i \in [n])$, és $\deg(f) \leq \mathrm{rang}(f)$, akkor f-nek van gyöke $\mathbb{F}_p^n$-ben.*

3.2.3. Definíció. Egy p prímre, az $f(\mathbf{x}) = \sum_{i=1}^{n} a_i x_i^d + g(\mathbf{x}) \in \mathbb{F}_p[\mathbf{x}]$ *általánosított diagonális polinom*, amennyiben $1 \leq d \leq p-1$, $a_1 \ldots a_n \neq 0$ és $\deg g < d$.

3.2.4. Tétel (Felszeghy). *Tegyük fel, hogy $\left\lceil \frac{p-1}{\left\lfloor \frac{p-1}{d} \right\rfloor} \right\rceil \leq n$. Ekkor az $f = \sum_{i=1}^{n} a_i x_i^d + g$ általánosított diagonális polinomnak van gyöke $\mathbb{F}_p^n$-ben.*

A bizonyításhoz azt kell megmutatni, hogy $f^{p-1}-1 \notin I(B)$, ahol $B = \mathbb{F}_p^n$.

Vessük össze a 3.2.4 tétel állítását a Rédei-sejtéssel. Ha f általánosított diagonális polinom, akkor $d = 1$ esetén $\operatorname{rang}(f) = 1$, különben $\operatorname{rang}(f) = n$. Ezek szerint Rédei sejtése azt állítja, hogy f-nek van gyöke, ha $d \leq n$. Ez valamivel gyengébb feltétel (hacsak nem $d|p-1$), mint $\left\lceil \frac{p-1}{\left\lfloor \frac{p-1}{d} \right\rfloor} \right\rceil \leq n$, amire szükségünk volt a 3.2.4 tétel bizonyításához.

4. A Lex játék

Ebben a részben bemutatjuk a Lex játékot, amely a tézis hátralevő részében központi szerepet fog kapni. A Lex játékot Lea és Stan játssza. Egy nulla dimenziós ideál és egy monom a játék paraméterei, amelyek meghatározzák, hogy melyik játékosnak van nyerő stratégiája. Egy rögzített I ideál esetén azon monomok halmaza, amelyre Stan tud nyerni $\operatorname{Stan}(I)$. Ideálok egy igen széles családjára ez a halmaz megegyezik a lexikografikus rendezés szerint vett $\operatorname{Sm}(I)$ halmazzal, így tehát a játék ezen ideálokra a lex standard monomok egy kombinatorikus jellemzését adja.

A 4.2 fejezetben igazoljuk, hogy egy multihalmaz I eltűnő ideáljára fennáll, hogy $\operatorname{Stan}(I) = \operatorname{Sm}(I)$.

A rákövetkező fejezetet két alfejezetre osztottuk. Az elsőben bebizonyítunk egy tételt a (redukált) Gröbner-bázisok „alakjáról" kétváltozós polinomgyűrűk esetén. Ezen eredményt – amelyet egyébként önmagában is érdekesnek gondolunk – a fejezet második részében felhasználjuk annak belátására, hogy $\operatorname{Stan}(I) = \operatorname{Sm}(I)$ teljesül olyan I ideálokra is, amelyek pontjai megkülönböztethetőek az utolsó két koordinátájuk alapján.

A lényegesen rövidebb 4.3 fejezetben kiderül, hogy általában $\operatorname{Stan}(I) \neq \operatorname{Sm}(I)$. Megfogalmazunk egy sejtést, amely szerint $\operatorname{Stan}(I)$ (csakúgy, mint $\operatorname{Sm}(I)$) az $\mathbb{F}[\mathbf{x}]/I$ vektortérnek lineáris bázisa.

Ezen rész utolsó fejezete egy $\operatorname{Stan}(I)$ meghatározására szolgáló algoritmust tárgyal, amely tehát az előbbiek szerint sok esetben $\operatorname{Sm}(I)$ kiszámítására is jó. A leggyorsabb ismert algoritmus eltűnő ideálok lex standard monomjainak megadására Cerlienco és Mureddu eljárása [15]. A mi algoritmusunk ugyanezt a feladatot hatékonyabban végzi el. Az általánosabb ideálokra is működő ismert módszerek lényegében mind a Buchberger–Möller algoritmus variánsai, amelyeknél viszont az általánosságért cserébe futásidővel kell fizetni. Amennyiben $\operatorname{Stan}(I) = \operatorname{Sm}(I)$ teljesül, akkor az alábbiakban tárgyalt algoritmus tudomásunk szerint a leghatékonyabb módszer lex standard monomok kiszámítására. A módszert véges pontrendszerek eltűnő ideáljaira Singular programban leprogramoztuk, a kód a tézis függelékében

megtalálható.

A játékot először [20] cikkünkben publikáltuk, az (itt tárgyalt) általános forma pedig [21] cikkben szerepel, együtt a multihalmazos esetre vonatkozó bizonyítással. A 4.3 fejezet eredményei eddig nem jelentek meg. Az algoritmus $I = I(V)$ esetről szóló változatát a [20] cikk tartalmazza; az általános eset ennek csupán egyszerű módosítása.

4.1. A Lex játék szabályai

Legyen I nulla dimenziós felbomló ideál, amelynek primér felbontása (1) alakú és legyen $\mathbf{w} \in \mathbb{N}^n$. Ezen paraméterek rögzítése mellett a Stan és Lea által játszott $\mathrm{Lex}\,(I; \mathbf{w})$ játék a következő.

Lea és Stan is ismeri az I ideált és a $\mathbf{w}$ vektort.

1 Lea választ w_n (nem feltétlen különböző) elemet $\mathbb{F}$-ből.

Stan (Lea tippjeinek ismeretében) választ egy $y_n \in \mathbb{F}$-et.

Legyen r_n az y_n multiplicitása Lea tippjei között.

2 Lea most w_{n-1} (nem feltétlen különböző) elemet választ a testből.

Stan (Lea tippjeinek ismeretében) választ egy $y_{n-1} \in \mathbb{F}$ elemet.

Az r_{n-1} eredményt (y_{n-1}-ek számát Lea tippjei között) rögzítik.

... (A játék ugyanígy folytatódik tovább.)

n Lea választ w_1 (nem feltétlen különböző) elemet $\mathbb{F}$-ből.

Stan végül (Lea tippjeinek ismeretében) választ egy $y_1 \in \mathbb{F}$-et.

A helyes tippek száma legyen r_1.

Tegyük fel, hogy az *eredmény vektor* $\mathbf{r} = (r_1, \ldots, r_n) \in \mathbb{N}^n$. Lea pontosan akkor nyertese a játéknak, ha $\mathbf{x}^{\mathbf{r}} \in \mathrm{Lm}_{\mathrm{lex}}\,(Q_{\mathbf{y}})$. Azt mondjuk, hogy Lea (illetve Stan) nyeri a játékot, ha van nyerő stratégiája.

4.1.2. Definíció. Egy rögzített I felbomló ideálhoz legyen

$$\mathrm{Stan}\,(I) = \{\mathbf{x}^{\mathbf{w}} \ : \ \text{Stan nyeri a } \mathrm{Lex}\,(I; \mathbf{w}) \text{ játékot}\}$$

a *Stan monomok* halmaza.

4.2. Multihalmazok Stan monomjai

E fejezet fő tétele szerint a Lex játék kombinatorikus leírását adja az $I(\mathcal{V})$ alakú ideálok lex standard monomjainak.

4.2.1. Tétel (Felszeghy, Rónyai). *Legyen $\mathcal{V}$ véges algebrai multihalmaz. Ekkor*

$$\mathrm{Sm}_{\mathrm{lex}}\left(I(\mathcal{V})\right) = \mathrm{Stan}\left(I(\mathcal{V})\right).$$

Megfogalmazhatjuk a lex standard monomok e kombinatorikus leírását a játék nélkül is a következők szerint. Ha $y \in \mathbb{F}$ és $m \geq 0$ egész, akkor legyen $\mathcal{V}_{y,m}$ az a véges multihalmaz $\mathbb{F}^{n-1}$-re, amelyre tetszőleges $\overline{\mathbf{y}} \in \mathbb{F}^{n-1}$ esetén

$$\mathcal{V}_{y,m}(\overline{\mathbf{y}}) = \left\{\overline{\mathbf{m}} \in \mathbb{N}^{n-1} \,:\, (\overline{\mathbf{m}}, m) \in \mathcal{V}(\overline{\mathbf{y}}, y)\right\}.$$

4.2.3. Tétel (Felszeghy, Rónyai). *Ha $\mathcal{V}$ véges algebrai multihalmaz, $n \geq 2$ és $\mathbf{w} \in \mathbb{N}^n$, akkor*

$$\mathbf{x}^{\mathbf{w}} \in \mathrm{Sm}_{\mathrm{lex}}\left(I(\mathcal{V})\right) \iff w_n < \left|\left\{(y,m) \in \mathbb{F} \times \mathbb{N} \,:\, \overline{\mathbf{x}}^{\overline{\mathbf{w}}} \in \mathrm{Sm}_{\mathrm{lex}}\left(I(\mathcal{V}_{y,m})\right)\right\}\right|.$$

4.3. Majdnem általános helyzetű pontok

A sík eltűnő ideáljai

A következő tétel olyan $I \trianglelefteq \mathbb{F}[s,t]$ ideálok redukált lex Gröner-bázisait jellemzi, amelyekre $t \in \sqrt{I}$ és $t \prec s$. Eredményünk szinte szó szerint átvihető arra az esetre, amikor $t - y \in \sqrt{I}$ teljesül ($t \in \sqrt{I}$ helyett), ahol $y \in \mathbb{F}$.

4.3.2. Tétel (Felszeghy, Rónyai). *Legyen $I \trianglelefteq \mathbb{F}[s,t]$ ideál, amelyre $t \in \sqrt{I}$. Jelölje ℓ_w a $\min\{\ell \,:\, s^w t^\ell \in \mathrm{Lm}(I)\}$ egész számot ($w = 0, 1, \ldots$), ahol $\mathrm{Lm}(I)$ a $t \prec s$ indukálta lex rendezés szerint értendő. Ha $g(s,t) \in I$ és $\mathrm{lm}(g) = s^w t^{\ell_w}$, akkor $g(s,t) = c \cdot s^w t^{\ell_w} + h(s,t)$ valamely $c \in \mathbb{F}$ konstansra és $h(s,t) \in \mathbb{F}[s,t]$ polinomra, amelyre teljesül $\deg_s(h) < w$, továbbá t^{ℓ_w} osztja $h(s,t)$ polinomot.*

A játék majdnem általános helyzetű pontokra

Először szorzat ideálok lex főtagjairól mutatunk be két állítást, amelyek a fejezet fő tételének bizonyításában kulcsszerepet játszanak.

4.3.4. Állítás. *Tegyük fel, hogy I_1 és I_2 nulla dimenziós felbomló ideálok, amelyekre teljesül, hogy ha $\mathbf{y}$ az I_1, $\mathbf{z}$ az I_2 egy pontja, akkor $y_n \neq z_n$. Ha $\overline{\mathbf{x}}^{\overline{\mathbf{w}}} x_n^{m_1} \in \mathrm{Lm}_{\mathrm{lex}}(I_1)$ és $\overline{\mathbf{x}}^{\overline{\mathbf{w}}} x_n^{m_2} \in \mathrm{Lm}_{\mathrm{lex}}(I_2)$, akkor $\overline{\mathbf{x}}^{\overline{\mathbf{w}}} x_n^{m_1+m_2} \in \mathrm{Lm}_{\mathrm{lex}}(I_1 I_2)$.*

A következő állítás hasonló szerepet játszik fő tételünk igazolásában, mint az előbbi, de lényegesen nehezebb bebizonyítani. Az $\widetilde{\mathbf{x}}^{\widetilde{\mathbf{w}}}$ itt $\prod_{i=1}^{n-2} x_i^{w_i}$ monom rövidítése.

4.3.5. Állítás. *Legyen I_1 és I_2 nulla dimenziós felbomló ideálok, amelyekre ha $\mathbf{y}$ az I_1 és $\mathbf{z}$ az I_2 egy pontja, akkor $y_n = z_n$ és $y_{n-1} \neq z_{n-1}$. Ha $\widetilde{\mathbf{x}}^{\widetilde{\mathbf{w}}} x_{n-1}^{m_1} x_n^{w_n} \in \mathrm{Lm}_{\mathrm{lex}}(I_1)$ és $\widetilde{\mathbf{x}}^{\widetilde{\mathbf{w}}} x_{n-1}^{m_2} x_n^{w_n} \in \mathrm{Lm}_{\mathrm{lex}}(I_2)$, akkor $\widetilde{\mathbf{x}}^{\widetilde{\mathbf{w}}} x_{n-1}^{m_1+m_2} x_n^{w_n} \in \mathrm{Lm}_{\mathrm{lex}}(I_1 I_2)$.*

4.3.6. Tétel (Felszeghy, Rónyai). *Ha I nulla dimenziós felbomló ideál, és I tetszőleges különböző $\mathbf{y}, \mathbf{z}$ pontjaira $y_n \neq z_n$ vagy $y_{n-1} \neq z_{n-1}$, akkor*

$$\mathrm{Stan}(I) = \mathrm{Sm}_{\mathrm{lex}}(I).$$

Speciálisan ha $n = 2$, akkor tetszőleges nulla dimenziós felbomló ideál Stan és lex standard monomjai megegyeznek.

4.4. Az általános eset

Általában a standard és a Stan monomok különbözőek.

4.4.1. *Példa.* Legyen $I \trianglelefteq \mathbb{F}[x_1, x_2, x_3]$ a $Q_{(0,0,0)} = (x_1^3, x_2^2, x_3^3, x_1x_2 + x_3^2)$ és $Q_{(1,0,0)} = ((x_1-1)^3, x_2^2, x_3^3, (x_1-1)x_2 + x_3^2)$ primér ideálok szorzata. Kiszámolható, hogy $x_1^2 x_2 \in \mathrm{Sm}_{\mathrm{lex}}(I) \setminus \mathrm{Stan}(I)$, míg $x_1^4 x_3^2 \in \mathrm{Stan}(I) \setminus \mathrm{Sm}_{\mathrm{lex}}(I)$.

Habár $\mathrm{Sm}_{\mathrm{lex}}(I)$ és $\mathrm{Stan}(I)$ nem egyenlők, hasonló tulajdonságok teljesülnek rájuk. Azt sejtjük, hogy $\mathrm{Stan}(I)$ a standard monomok halmazához hasonlóan lineáris bázisa az $\mathbb{F}[\mathbf{x}]/I$ vektortérnek. Mindenesetre az elemszám megfelelő ehhez.

4.4.2. Állítás. *Legyen I tetszőleges nulla dimenziós felbomló ideál. Ekkor*

$$|\mathrm{Stan}(I)| = \dim_{\mathbb{F}}(\mathbb{F}[\mathbf{x}]/I).$$

4.5. Stan monomok kiszámítása

A következőkben bemutatunk egy gyors kombinatorikus algoritmust, amely nulla dimenziós felbomló ideálok Stan monomjait határozza meg, feltéve, hogy ismert az (1) alakú primér felbontás és $\mathrm{Sm}_{\mathrm{lex}}(Q_{\mathbf{y}})$ halmazok minden $\mathbf{y} \in \mathbb{F}^n$ esetén.

Szófa standard monomjai

Először némi előfeldolgozást végzünk $\mathcal{V}$ multihalmazon: definiáljuk a $T(\mathcal{V})$ szófát (gyökeres fát, amelynek csúcsai címkézettek). Ha $n = 1$, akkor $T(\mathcal{V})$ gyökerének $|\mathcal{V}|$ gyermeke van, amelyek mind a fa levelei. Ha $n > 1$, akkor $T(\mathcal{V})$ gyökerének gyermekei a rekurzíve már értelmezett $T(\mathcal{V}_{y,m})$ szófák gyökerei minden egyes olyan $(y, m) \in \mathbb{F} \times \mathbb{N}$ párra, amelyre $\mathcal{V}_{y,m}$ nem üres. A $T(\mathcal{V})$ fa algoritmikus kiszámítása egy egyelemű multihalmaz fájából kiindulva történhet, egyesével hozzávéve pont-multiplicitás párokat.

Legyen T gyökeres fa, amelynek a levelei mind az n-edik szinten találhatóak. Ha T egyetlen pontból áll ($n = 0$), akkor legyen $\mathrm{Sm}\,(T) = \{1\}$. Egyébként akkor mondjuk, hogy $\mathbf{x}^{\mathbf{w}} \in \mathrm{Sm}\,(T)$, ha a gyökérnek létezik legalább w_n gyermeke, amelyre $\overline{\mathbf{x}^{\mathbf{w}}}$ standard monomja az adott gyermekhez tartozó részfának.

4.5.2. Következmény. *Tetszőleges nemüres algebrai multihalmazra*

$$\mathrm{Sm}\,(I(\mathcal{V})) = \mathrm{Sm}\,(T(\mathcal{V}))\,.$$

Ezentúl tehát gyökeres fák standard monomjainak kiszámítására fogunk koncentrálni.

Egy újabb szófa

Felépítjük az $\mathrm{Sm}\,(T)$ elemeinek szófáját a következő értelemben. Tetszőleges csúcs gyermekei rendre a $0, 1, \ldots$ számokkal lesznek indexelve. Így U egy l leveléhez tartozik egy $\mathbf{w} \in \mathbb{N}^n$ vektor, ahol w_i az i-edik címke a gyökérből l-be vezető úton. Célunk, hogy megkonstruáljuk U szófát, amelyre az U-hoz tartozó vektorok pontosan $\mathrm{Sm}\,(T)$ elemeinek kitevővektorai lesznek.

Az algoritmus a következőképpen foglalható össze. A T fa minden levelét először letesszük U gyökerébe. Ezután a levelek lesétálnak U fában, mind egy-egy különböző levélbe. Igazából ők fogják építeni maguk előtt a fát: megmondják, hogy milyen sorszámú csúcsba szeretnének továbblépni. Az alábbi szabályt követik a lefele vándorláskor: ha a T két l_1 and l_2 leveléhez tartozó, T gyökerébe vezető út a T fa $(n - i)$-edik szintjén metszi egymást, akkor U-ban e levelek az i-edik szinten már nem lehetnek együtt. Minden levél az aktuális csúcsának legkisebb sorszámú gyermekébe lép át, amelyikkel nem sérti meg az előző szabályt.

A módszer formális leírását most mellőzzük. (Természetesen a disszertációban ez is szerepel.)

4.5.6. Tétel (Felszeghy, Rónyai). *A fenti algoritmus által adott U szófa szavainak halmaza éppen* $\mathrm{Sm}\,(T)$ *kitevővektorainak halmazával egyezik meg.*

Futásidő

4.5.8. Tétel (Felszeghy, Rónyai). *Legyen r a $T(\mathcal{V})$-beli maximális gyermekszám. Ekkor a fentiekben bemutatott algoritmus* $\mathrm{Sm}\,(I(\mathcal{V}))$ *kiszámolását* $O\left(|\mathcal{V}|\, nr\right)$ *elemi művelettel végzi el. A futásidő (általában durva) felső becslése* $O\left(|\mathcal{V}|^2\, n\right)$.

Vegyük észre, hogy sem $T(\mathcal{V})$, sem U konstrukciója nem használ testbeli műveleteket, csupán egyenlőségtesztre van szükség $\mathbb{F}$-ben.

5. A Lex játék alkalmazásai – bemelegítés

A Lex játék igen hatékony eszköz nulla dimenziós ideálok Gröbner-elméletében. A tézis hátralevő részében számos példával igyekszünk ezen állításunkat alátámasztani. Az 5.1 fejezet eredményeit kivéve az ebben a részben tárgyalt tételek korábban is ismertek voltak. A Lex játék segítségével új, egyszerűbb és talán elegánsabb bizonyításokat adunk ezekre.

Az 5.1 fejezetben bebizonyítjuk azt az elsőre meglepő állítást, hogy $\{0,1\}^n$ halmazbeli pontokat tartalmazó véges multihalmazok ideáljainak redukált lex Gröbner bázisa független az alaptesttől. Az 5.1.1 következmény (egy speciális esetben) a Lex játékról szóló [20] cikkben jelent meg, míg az 5.1.2 következményt eddig nem publikáltuk.

Az második fejezet a szimmetrikus polinomok alaptételének Garsia-féle általánosításával [27] foglalkozik. A bizonyításunk [22] Hegedűs és Rónyai [31] módszerének egyszerűsítése.

A tézis ezután következő részeiben véges $V_{\mathcal{F}}$ halmazok eltűnő ideáljait fogjuk vizsgálni, ahol $V_{\mathcal{F}}$ egy $\mathcal{F}$ halmazrendszer elemeinek karakterisztikus vektoraiból áll. Az 5.3 fejezetben felidézünk egy neves állítást, amely $I(V_{\mathcal{F}})$ standard monomjait, illetve Hilbert-függvényét kapcsolja össze tartalmazási mátrixok rangjával. Ennek mintájára bemutatunk egy másik tételt is, amely az ezután következő fejezetben kerül alkalmazásra: kiszámoljuk egy bizonyos tartalmazási mátrix rangját. Ez utóbbi eredmény Wilson [39] nevéhez fűződik. A mi bizonyításunk Friedl és Rónyai [26] munkáján alapszik, amelyen a Lex játék segítségével tudunk egyszerűsíteni. Ez az eredmény szintén [22] dolgozatunkban jelent meg először.

5.1. Lex Gröbner-bázisok tulajdonságai

Miután most egynél több testet fogunk tekinteni egyszerre, átmenetileg bevezetjük az $I_{\mathbb{F}}(\mathcal{V})$ jelölést az $\mathbb{F}[\mathbf{x}]$-beli $I(\mathcal{V})$ ideálra.

5.1.1. Következmény. *Legyen $\mathcal{V}$ véges multihalmaz $\mathbb{F}^n$-ben és tegyük fel, hogy a $B = B_1 \times \cdots \times B_n \subseteq \mathbb{F}^n$ véges doboz $\mathcal{V}$ minden pontját tartalmazza. Legyen $\hat{\mathbb{F}}$ egy másik test, $\varphi_i \colon B_i \to \hat{\mathbb{F}}$ pedig injektív függvény ($i \in [n]$). Minden $\mathbf{y} \in B$ esetén $\boldsymbol{\varphi}(\mathbf{y}) = (\varphi_1(y_1), \ldots, \varphi_n(y_n))$, és a $\mathcal{V}$ multihalmaz képe $\hat{\mathcal{V}}$, ahol $\hat{\mathcal{V}}(\boldsymbol{\varphi}(\mathbf{y})) = \mathcal{V}(\mathbf{y})$. Ekkor teljesül, hogy*

$$\mathrm{Sm}_{\mathrm{lex}}\left(I_{\mathbb{F}}(\mathcal{V})\right) = \mathrm{Sm}_{\mathrm{lex}}\left(I_{\hat{\mathbb{F}}}\left(\hat{\mathcal{V}}\right)\right).$$

Speciálisan, ha $\mathcal{V}$ minden pontja a $\{0,1\}^n$ dobozban van, akkor $\mathrm{Sm}_{\mathrm{lex}}\left(I_{\mathbb{F}}(\mathcal{V})\right)$ független az $\mathbb{F}$ testtől.

Ha $f \in \mathbb{Z}[\mathbf{x}]$, akkor tetszőleges $\mathbb{F}$ test esetén tekinthetjük f polinomot $\mathbb{F}[\mathbf{x}]$ elemeként (redukálva az együtthatókat modulo p, ha szükséges).

5.1.2. Következmény. *Ha $\mathcal{V}$ minden pontja a $\{0,1\}^n$ dobozban van, akkor $I_{\mathbb{Q}}(\mathcal{V})$ redukált G Gröbner-bázisa egész együtthatós. Tetszőleges $\mathbb{F}$ testre a G-nek megfelelő $\mathbb{F}[\mathbf{x}]$-beli polinomhalmaz a redukált Gröbner-bázisa az $I_{\mathbb{F}}(\mathcal{V})$ ideálnak.*

5.2. A szimmetrikus polinomok alaptételének általánosítása

A szimmetrikus polinomok alaptételének az alábbiakban tárgyalt általánosítását Garsia [27] adta. Itt egy egyszerű bizonyítást közlünk.

Az *i-edik elemi szimmetrikus polinom* $\sigma_i(\mathbf{x}) = \sum_{\mathbf{w}\in\{0,1\}^n,\ \deg(\mathbf{x}^{\mathbf{w}})=i} \mathbf{x}^{\mathbf{w}}$, feltéve, hogy $0 \le i \le n$. Az alábbi tétel igaz.

5.2.1. Tétel (Garsia; Hegedűs, Nagy, Rónyai). *Tetszőleges $f(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$ polinom egyértelműen írható (valamely $\alpha_{\mathbf{w},\mathbf{u}} \in \mathbb{F}$ számokra) az alábbi véges összeg alakban:*

$$f(\mathbf{x}) = \sum_{\substack{\mathbf{w}\in\mathbb{N}^n \\ \mathbf{w}\le\mathbf{v}}} \sum_{\mathbf{u}\in\mathbb{N}^n} \alpha_{\mathbf{w},\mathbf{u}} \mathbf{x}^{\mathbf{w}} \boldsymbol{\sigma}(\mathbf{x})^{\mathbf{u}},$$

ahol $\mathbf{v} = (0, 1, \ldots, n-1)$ és $\mathbf{w} \le \mathbf{v}$ koordinátánként értendő.

A bizonyítás egy véges pontrendszer eltűnő ideálját használja. Legyenek $z_1, \ldots, z_n$ különböző testelemek és definiáljuk a

$$V = \{(z_{\pi(1)}, \ldots, z_{\pi(n)}) \,:\, \pi \in S_n\}$$

halmazt, amely tehát $z_1, \ldots, z_n$ összes permutációiból áll.

Hegedűs, Nagy és Rónyai eredeti cikkükben leírják az $I(V)$ lex standard monomjait és Gröbner bázisát. A Lex játék a lex standard monomok könnyebb meghatározásával egyszerűsíti a bizonyítást.

5.3. Hilbert-függvények és tartalmazási mátrixok

E fejezetben a Gröbner-elmélet kombinatorikai alkalmazásait készítjük elő. Megemlítünk egy ismert tételt, amely Hilbert-függvények és tartalmazási mátrixok között teremt kapcsolatot.

5.3.1. Definíció. *Halmazcsalád*on vagy *halmazrendszer*en $2^{[n]}$ egy részhalmazát értjük. Jelölje $\binom{[n]}{m}$ az $[n]$ összes m elemű részhalmazából álló családot, és legyen $\binom{[n]}{\leq m} = \bigcup_{i=0}^{m} \binom{[n]}{i}$.

A $\mathbf{v}_F$ vektor az F halmaz karakterisztikus vektorát jelöli, $V_{\mathcal{F}}$ pedig az $\mathcal{F}$ halmazrendszer elemeihez tartozó karakterisztikus vektorok halmazát. Egy halmazcsalád eltűnő ideálja

$$I(\mathcal{F}) = I(V_{\mathcal{F}}) = \{f \in \mathbb{F}[\mathbf{x}] \,:\, f(\mathbf{v}_F) = 0 \text{ minden } F \in \mathcal{F} \text{ esetén}\},$$

a $\mathcal{F}$ *Hilbert-függvény*e pedig $H_{\mathcal{F}}(m) = H_{I(\mathcal{F})}(m)$. A kombinatorikában $H_{\mathcal{F}}$ függvényt gyakran tartalmazási mátrixszal definiálják: az 5.3.4 állításban rögvest meglátjuk, hogy hogyan.

5.3.2. Definíció. Két $\mathcal{F}, \mathcal{G} \subseteq 2^{[n]}$ halmazrendszer *tartalmazási mátrix*a egy $|\mathcal{F}| \times |\mathcal{G}|$-es $I(\mathcal{F}, \mathcal{G})$ mátrix, amely sorai és oszlopai $\mathcal{F}$ és $\mathcal{G}$ elemeivel indexeltek. Az (F, G)-hez tartozó elem pontosan akkor 1, ha $G \subseteq F$ és 0 különben $(F \in \mathcal{F}, G \in \mathcal{G})$.

5.3.3. Definíció. Egy $M \subseteq [n]$ halmazra x_M a $\prod_{i \in M} x_i$ monomot jelöli.

5.3.4. Állítás.

$$H_{\mathcal{F}}(m) = \dim_{\mathbb{F}} \left(\mathbb{F}[\mathbf{x}]_{\leq m} \,/\, I(\mathcal{F})_{\leq m} \right) = \operatorname{rang}_{\mathbb{F}} I\left(\mathcal{F}, \binom{[n]}{\leq m}\right).$$

Egy hasonló állítást fogunk használni az 5.4 fejezetben:

5.3.5. Állítás. *Legyen $\mathcal{P}_{\mathcal{F},m}$ a multilineáris m-edfokú homogén polinomokkal reprezentálható $V_{\mathcal{F}} \to \mathbb{F}$ függvények tere. Ekkor*

$$\dim_{\mathbb{F}} (\mathcal{P}_{\mathcal{F},m}) = \operatorname{rang}_{\mathbb{F}} I\left(\mathcal{F}, \binom{[n]}{m}\right).$$

5.4. Wilson rangformulája

Tekintsük az $A = I\left(\binom{[n]}{d}, \binom{[n]}{m}\right)$ tartalmazási mátrixot, ahol $m \leq d \leq n-m$. Richard M. Wilson [39] egy híres tétele leírja A diagonális alakját az egész számok felett. Ennek következményeképpen Wilson megadja A mátrix $\mathbb{F}_p$ feletti rangját.

Vegyük észre, hogy $\operatorname{rang}_{\mathbb{F}_p} A$ éppen $\mathcal{P}_{\binom{[n]}{d},m} = \mathcal{P}_{d,m}$ vektortér $\mathbb{F}_p$ feletti rangja (ld 5.3.5 állítás). Tegyük fel, hogy $m \leq \frac{n}{2}$. Egy $M \subseteq [n]$, $|M| \leq m$ halmazra a legyen y_M a következő négyzetmentes polinom:

$$y_M = \sum_{\substack{M' \supseteq M \\ |M'|=m}} x_{M'}.$$

Ennek segítségével Wilson rangformuláját a következőképpen mondhatjuk ki.

5.4.3. Tétel (Wilson; Friedl, Rónyai). *Ha $m \leq d \leq n-m$, akkor a $\mathcal{P}_{d,m}$ tér egy lineáris bázisa*

$$B = \left\{ y_M \,:\, x_M \in \operatorname{Sm}\left(I\left(\binom{[n]}{m}\right)\right), p \nmid \binom{d-|M|}{m-|M|} \right\}.$$

Ebből következik, hogy

$$\dim_{\mathbb{F}_p}(\mathcal{P}_{d,m}) = |B| = \sum_{\substack{0 \leq i \leq m \\ p \nmid \binom{d-i}{m-i}}} \binom{n}{i} - \binom{n}{i-1}.$$

A Lex játék a következő, döntő fontosságú lemma bizonyításával járul hozzá a tétel igazolásához.

5.4.4. Lemma. *Tetszőleges tagsorrend és $0 \leq i \leq m \leq \frac{n}{2}$ egészek esetén $\operatorname{Sm}\left(I\left(\binom{[n]}{m}\right)\right)$ halmazban pontosan $\binom{n}{i} - \binom{n}{i-1}$ az i fokú monomok száma.*

6. Extremális kombinatorikai alkalmazások

Az utolsó rész célja, hogy két extremális halmazrendszerek elméletébe tartozó kérdésre választ adjon. A Gröbner-elmélet ezen alkalmazásainak közös alapja az $I(V_{\mathcal{F}})$ ideál algebrai tulajdonságainak alapos megismerése, ahol $\mathcal{F}$ egy modulo q teljes ℓ-széles halmazcsalád. Az első – meglehetősen hosszú – fejezet $I(V_{\mathcal{F}})$ standard monomjait, egy Gröbner-bázisát és Hilbert-függvényét számolja ki. Ha mindezeket meghatároztuk, akkor már aránylag könnyen be

fogjuk tudni bizonyítani a következő fejezetek fő tételeit, amelyek egy-egy halmazrendszer maximális elemszámára adnak becslést.

Elsőként modulo q L-kerülő L-metsző $\mathcal{G}$ családokkal fogunk foglalkozni. Némi betekintést adunk a téma ismert eredményeibe, majd igazoljuk, hogy amennyiben q prímhatvány, L egy modulo q intervallum, és $|L| \leq n-q+2$, akkor $|\mathcal{G}| \leq \sum_{k=|L|}^{q-1} \binom{n}{k}$. Ez az eredmény az $|L| = q-1$ esetben a Babai–Frankl Sejtés néven ismert, amelyet egyébként nemrég Hegedűs és Rónyai [32] igazolt.

A dolgozat utolsó fejezete éles felső korlátot ad az olyan $\mathcal{G}$ modulo q ℓ-széles családok elemszámára, amelyek nem zúznak szét $m+1$ elemű halmazt, nevezetesen $|\mathcal{G}| \leq \sum_{i=0}^{\infty} \sum_{k=0}^{\ell-1} \binom{n}{m-iq-k}$, ahol q prímhatvány és teljesül $0 \leq m \leq \frac{n+\ell}{2}$. Ezen eredményünket Frankl egy máig nyitott sejtésének tükrében értékeljük.

A 6.1 fejezet lex standard monomokról szóló része a Lex játék első változatával együtt [20] cikkünkben jelent meg először. A további itt tárgyalt eredményeket, köztük a Hilbert-függvény meghatározását, és a két alkalmazást [19] munkánkban publikáltuk.

6.1. Számolások modulo q teljes ℓ-széles családokkal

6.1.1. Definíció. Legyen q, d, ℓ egész számok, amelyekre $1 \leq \ell < q$. Ekkor a *modulo q teljes ℓ-széles család*

$$\mathcal{F} = \{F \subseteq [n] \,:\, \exists\, f \in \mathbb{Z} \text{ amelyre } d \leq f < d+\ell \text{ és } |F| \equiv f \pmod{q}\}\,.$$

Ezen halmazrendszer részhalmazait *modulo q ℓ-széles család*nak nevezzük.

Ha d helyére olyan d' számot helyettesítünk, amelyre $d \equiv d' \pmod{q}$, akkor az így definiált $\mathcal{F}$ nem változik. Ezért a továbbiakban azt is feltehetjük, hogy $\frac{n-q-\ell}{2} < d \leq \frac{n+q-\ell}{2}$ fennáll.

A $\mathcal{F}$ család $H_{\mathcal{F}}(m)$ Hilbert-függvényének kiszámítása három nagyobb lépésben történik. Meghatározzuk $I(\mathcal{F})$ lexikografikus standard monomjait, majd ennek segítségével megadjuk egy lex Gröbner-bázisát, amelyről rögtön látszani fog, hogy a deglex rendezésre nézve is Gröbner-bázis. A harmadik lépés tehát $H_{\mathcal{F}}(m)$ meghatározásához a legfeljebb m-edfokú (lex) standard monomok összeszámolása lesz.

Lexikografikus standard monomok

A leírást rögtön ideálok egy valamivel általánosabb osztályára vonatkozó tétellel kezdjük. A 6.1.3 állítás érvényes minden olyan $I(\mathcal{F})$ ideálra, amelyre

teljesül, hogy bármely $f \in \mathbb{Z}$ esetén vagy $\binom{[n]}{f} \subseteq \mathcal{F}$ vagy $\binom{[n]}{f} \cap \mathcal{F} = \emptyset$. Az ilyen típusú ideálokra be is vezetünk egy jelölést. Ha $D \subseteq \mathbb{Z}$, akkor

$$\mathcal{F}_{D,n} = \{F \subseteq [n] \,:\, |F| \in D\}\,.$$

Tetszőleges $t \in \mathbb{Z}$ és $A \subseteq \mathbb{Z}$ esetén legyen $A - t = \{a - t : a \in A\}$. Ha $A \subseteq \mathbb{Z}$, akkor definiáljuk az $A^{(0)}$ és $A^{(0)}$ halmazokat a következők szerint: $A^{(0)} = A \cup (A-1)$ és $A^{(1)} = A \cap (A-1)$. Amennyiben $\mathbf{w} \in \{0,1\}^n$, akkor

$$D^{(\mathbf{w})} = \Big(\dots\Big(\big(D^{(w_1)}\big)^{(w_2)}\Big)^{\dots}\Big)^{(w_n)}\,.$$

Végül $M \subseteq [n]$ esetén $D^{(M)}$ ugyanaz, mint $D^{(\mathbf{v}_M)}$.

6.1.3. Állítás. $x_M \in \mathrm{Sm}_{\mathrm{lex}}\left(I(\mathcal{F}_{D,n})\right) \iff 0 \in D^{(M)}$.

Itt most átugorjuk a lex standard monomok konkrét leírásáról szóló tételt, helyette a minimális főtagok jellemzését adjuk csak meg, amely természetesen ekvivalens az előbbivel. Ezentúl $\mathcal{F}$ megint a fent definiált modulo q teljes ℓ-széles családot jelöli.

6.1.7. Definíció. Legyen $M = \{m_1, \dots, m_k\} \subseteq [n]$, ahol $m_1 < \dots < m_k$.

Az $\mathcal{L}_1$ az összes olyan M halmazt tartalmazza, amelyre igazak a következők: $1 \le k \le \min\{d+\ell-1, n-d\}+1$, $2i-\ell < m_i < 2i-\ell+q-1$ minden $1 \le i \le k-1$ esetén és $m_k = 2k-\ell$.

Az M akkor és csak akkor legyen $\mathcal{L}_2$ rendszer eleme, ha $k = \min\{d+\ell-1, n-d\}+1$, $2i-\ell < m_i < 2i-\ell+q-1$ minden $1 \le i \le k$ egész számra.

Végül legyen

$$L_3 = \begin{cases} \emptyset, & \text{ha } \mathcal{F} = \{\emptyset\} \text{ vagy } \mathcal{F} = \{[n]\};\\ \{n\}, & \text{ha } \mathcal{F} = \{\emptyset, [n]\};\\ \{2,\dots,n\}, & \text{máskülönben, ha } \ell = 1;\\ \{1,2,\dots,n\}, & \text{egyébként (amikor } \ell > 1).\end{cases}$$

6.1.8. Tétel (Felszeghy, Hegedűs, Rónyai). *Az $I(\mathcal{F})$ ideál lex rendezésre tekintett kezdeti ideáljának az*

$$\{x_M \,:\, M \in \mathcal{L}_1 \cup \mathcal{L}_2\} \cup \{x_j^2 \,:\, j \in L_3\}$$

halmaz minimális generátorrendszere.

Egy Gröbner-bázis

Tegyük fel mostantól, hogy p prím, q egy p-hatvány és $\mathbb{F}$ pedig p karakterisztikájú test. Az alábbiakban $I(\mathcal{F}) \trianglelefteq \mathbb{F}[\mathbf{x}]$ egy lex Gröbner-bázisát konstruáljuk meg, majd igazoljuk, hogy más tagsorrendekre nézve is Gröbner-bázist kaptunk.

Legyen $M \in \mathcal{L}_1$, $M = \{m_1, \ldots, m_k\}$ és $m_1 < \cdots < m_k$. Minden $0 \leq i \leq n - m_k = n - 2k + \ell$ egészre $m_{k+i} = m_k + i$ és legyen

$$M' = \{m_1, \ldots, m_{n-k+\ell}\} = \{m_1, \ldots, m_k, m_k + 1, m_k + 2, \ldots, n\}.$$

Az M' halmaz $U = [n] \setminus M'$ komplementere ekkor $k - \ell$ elemet tartalmaz, legyenek ezek $u_0 > u_1 > \cdots > u_{k-\ell-1}$. Ha $t = (k - q + 1)^+$, akkor definiáljuk az

$$s_M(\mathbf{x}) = \sum_{i=t+1}^{n-k+\ell} x_{m_i}$$

és a

$$g_M(\mathbf{x}) = \left(\prod_{i=1}^{t} \left(x_{m_i} - x_{u_{t-i}}\right) \binom{s_M(\mathbf{x}) - d - \ell + k}{k - t} \right)$$

redukálva $x_j^2 - x_j$ polinomokkal

polinomokat. Könnyű látni, hogy $g_M \in \mathbb{Z}[\mathbf{x}]$ és így $g_M \in \mathbb{F}[\mathbf{x}]$ szintén igaz.

Tegyük most fel, hogy $\min\{d + \ell - 1, n - d\} = d + \ell - 1$. Legyen továbbá $M = \{m_1, \ldots, m_{d+\ell}\} \in \mathcal{L}_2$, $m_1 < \cdots < m_{d+\ell}$ és $U = [n] \setminus M = \{u_0, u_1, \ldots, u_{n-d-\ell-1}\}$, $u_0 > u_1 > \cdots > u_{n-d-\ell-1}$. Ha most t számot $t = (n - d - q + 1)^+$ szerint definiáljuk, akkor

$$h_M(\mathbf{x}) = \prod_{i=1}^{t} \left(x_{m_i} - x_{u_{t-i}}\right) \prod_{i=t+1}^{d+\ell} x_{m_i}$$

$I(\mathcal{F})$ olyan eleme, amelynek főtagja x_M.

A másik estben, amikor $\min\{d + \ell - 1, n - d\} = n - d$, akkor $M = \{m_1, \ldots, m_{n-d+1}\} \in \mathcal{L}_2$, $m_1 < \cdots < m_{n-d+1}$, és a komplementer $U = [n] \setminus M = \{u_0, u_1, \ldots, u_{d-2}\}$, feltéve természetesen, hogy $u_0 > u_1 > \cdots > u_{d-2}$ is fennáll. A helyes választás ekkor $t = (d + \ell - q)^+$ és

$$h_M(\mathbf{x}) = \prod_{i=1}^{t} \left(x_{m_i} - x_{u_{t-i}}\right) \prod_{i=t+1}^{n-d+1} (x_{m_i} - 1).$$

6.1.15. Tétel (Felszeghy, Hegedűs, Rónyai). *Legyen $\mathcal{L}_1$, $\mathcal{L}_2$ és L_3 a 6.1.7 definíciónak megfelelő halmazok és g_M, h_M pedig az iménti polinomok. Tegyük fel, hogy $\prec$ olyan tagsorrend, amelyre $x_n \prec \cdots \prec x_1$, $\mathbb{F}$ egy p karakterisztikájú test és q pedig p-hatvány. Ekkor*

$$G = \{g_M \,:\, M \in \mathcal{L}_1\} \cup \{h_M \,:\, M \in \mathcal{L}_2\} \cup \{x_j^2 - x_j \,:\, j \in L_3\}$$

Gröbner-bázisa az $I(\mathcal{F}) \trianglelefteq \mathbb{F}[\mathbf{x}]$ ideálnak $\prec$ rendezésre nézve. Speciálisan $\mathrm{Sm}_{\prec}(I(\mathcal{F})) = \mathrm{Sm}_{\mathrm{lex}}(I(\mathcal{F}))$.

Hilbert-függvény

Az $\mathcal{F}$ család Hilbert-függvényének megadásához meg kell számoljuk az adott fokú standard monomokat valamely fok-kompatibilis tagsorrendre. A 6.1.15 tétel szerint használhatjuk a lex standard monomokat is e célra. Néhány technikai részletet (rácspoligonok halmazainak elemszámainak számolgatása tükrözési elv segítségével) itt mellőzünk .

6.1.22. Tétel (Felszeghy, Hegedűs, Rónyai). *Legyen $r = \min\{d + \ell - 1, n - d\}$ és tegyük fel, hogy $\mathbb{F}$ egy p karakterisztikájú test, q pedig p egy hatványa.*
Ha $0 \le m \le r$, akkor

$$H_{\mathcal{F}}(m) = \sum_{i=0}^{\infty} \sum_{k=0}^{\ell-1} \binom{n}{m - iq - k},$$

és ha $m > r$, akkor

$$H_{\mathcal{F}}(m) = \sum_{i=-\infty}^{\infty} \sum_{k=0}^{\ell-1} \binom{n}{r + iq - k} - \sum_{i=1}^{\infty} \sum_{k=0}^{\ell-1} \binom{n}{m + iq - k}.$$

A kombinatorikai alkalmazásokban az alábbi következményt fogjuk használni.

6.1.23. Következmény. *Ha $0 \le m \le \frac{n+\ell}{2}$, akkor*

$$H_{\mathcal{F}}(m) \le \sum_{i=0}^{\infty} \sum_{k=0}^{\ell-1} \binom{n}{m - iq - k}.$$

6.2. L-kerülő L-metsző családok maximális elemszáma

6.2.1. Definíció. Legyen L egész számok egy halmaza és $\mathcal{G}$ pedig egy halmazrendszer. Ekkor $\mathcal{G}$ *modulo* q *L-kerülő*, amennyiben $G \in \mathcal{G}$ és $f \in L$ esetén $|G| \not\equiv f \pmod{q}$. Azt mondjuk, hogy $\mathcal{G}$ *L-metsző*, ha bármely két különböző $G_1, G_2 \in \mathcal{G}$ elemére $|G_1 \cap G_2| \equiv f \pmod{q}$ teljesül valamely $f \in L$ esetén.

A modulo q L-kerülő halmazrendszerek maximális elemszámát többen is vizsgálták.

Babai és Frankl fogalmazták meg a sejtést [7, p. 115], hogy $|L| = q - 1$ esetben a $\binom{n}{q-1}$ binomiális együttható felső korlátja a modulo q L-metsző L-kerülő halmazrendszerek elemszámának. Nemrég Hegedűs és Rónyai [32] igazolták ezt. A mi eredményünk ennek általánosítása L-ek egy bővebb családjára.

6.2.2. Definíció. Azt mondjuk, hogy $L \subseteq \{0, \ldots, q-1\}$ *modulo q intervallum*, ha L vagy egészek egy intervalluma, vagy két L_1, L_2 intervallum uniója, amelyekre fennáll $0 \in L_1$ és $q - 1 \in L_2$.

6.2.3. Tétel (Felszeghy, Hegedűs, Rónyai). *Legyen q egy p prím hatványa, L egy q intervallum és $\mathcal{G} \subseteq 2^{[n]}$ pedig modulo q L-kerülő L-metsző halmazrendszer. Ha $|L| \leq n - q + 2$, akkor*

$$|\mathcal{G}| \leq \sum_{k=|L|}^{q-1} \binom{n}{k}.$$

A bizonyítás vázlata a következő. Beágyazzuk $\mathcal{G}$ családot egy modulo q teljes ℓ-széles $\mathcal{F}$ halmazrendszerbe. Az $\mathbb{F}_p[\mathbf{x}]/I(\mathcal{G})$ vektortér egy lineáris bázisát megadva kapunk $|\mathcal{G}|$ polinomot, amelyek mint $\mathbb{F}_p[\mathbf{x}]/I(\mathcal{F})$ elemei is lineárisan függetlenek, ráadásul úgy készítjük el őket, hogy fokszámuk legfeljebb $q - 1$ legyen. Ezek miatt polinomjaink $|\mathcal{G}|$ számára felső korlátot jelent $I(\mathcal{F})$ legfeljebb $q - 1$ fokú monomjainak száma, tehát $H_{\mathcal{F}}(q-1)$.

6.3. Kis halmazokat szétzúzó halmazcsaládok

6.3.1. Definíció. Tekintsünk egy $\mathcal{G}$ halmazrendszert az $[n]$ alaphalmazon. Azt mondjuk, hogy $\mathcal{G}$ *szétzúzza* az $M \subseteq [n]$ halmazt, ha

$$\{G \cap M \,:\, G \in \mathcal{G}\} = 2^M.$$

6.3.2. Definíció. A $\mathcal{G}$ család *ℓ-antilánc*, ha nem tartalmaz $\ell + 1$ különböző $G_0, \ldots, G_n$ halmazt, amelyre $G_0 \subsetneq G_1 \subsetneq \cdots \subsetneq G_\ell$.

Frankl [23] azt sejtette, hogy amennyiben a $\mathcal{G}$ ℓ-antilánc nem zúz szét $m+1$ elemű halmazt valamely $0 \leq m \leq \frac{n+\ell}{2} - 1$ egész esetén, akkor $|\mathcal{G}| \leq \sum_{k=0}^{\ell-1} \binom{n}{m-k}$.

Egy ℓ-széles család ℓ-antilánc. Friedl, Hegedűs és Rónyai [25] munkájukban igazolták, hogy a felső korlát ℓ-széles családokra fennáll. Tételünk utóbbi eredmény általánosítása, a speciális eset $q > n$ választással adódik belőle.

6.3.3. Tétel (Felszeghy, Hegedűs, Rónyai). *Legyen $\mathcal{G} \subseteq 2^{[n]}$ modulo q ℓ-széles halmazcsalád, ahol q prímhatvány. Ha $\mathcal{G}$ nem zúz szét $m+1$ elemű halmazt valamely $0 \leq m \leq \frac{n+\ell}{2}$ egészre, akkor*

$$|\mathcal{G}| \leq \sum_{i=0}^{\infty} \sum_{k=0}^{\ell-1} \binom{n}{m-iq-k}.$$

Ismert, hogy amennyiben x_M standard monomja valamely $\mathcal{G}$ halmazrendszernek, akkor $\mathcal{G}$ szétzúzza M halmazt. A 6.3.3 tétel bizonyítása ezt és a modulo q teljes ℓ-széles család Hilbert-függvényére vonatkozó becslést használja.

Az egyenlőtlenség éles: válasszuk a $d = m-\ell+1$ paramétert az $\mathcal{F}$ modulo q teljes ℓ-széles családhoz, és legyen $\mathcal{G} = \mathcal{F} \cap \binom{[n]}{\leq m}$.

Hivatkozások

[3] N. Alon, Combinatorial Nullstellensatz, *Combinatorics, Probability and Computing* **8 (1-2)** (1999), 7–29.

[7] L. Babai, P. Frankl, Linear Algebra Methods in Combinatorics, *Preliminary Version 2*, September 1992.

[15] L. Cerlienco, M. Mureddu, From algebraic sets to monomial linear bases by means of combinatorial algorithms, Formal power series and algebraic combinatorics, (Montreal, PQ, 1992) *Discrete Mathematics* **139** (1995), no. 1–3, 73–87.

[18] B. Felszeghy On the solvability of some special equations over finite fields *Publ. Math. Debrecen* **68** (2006), 15–23.

[19] B. Felszeghy, G. Hegedűs, L. Rónyai, Algebraic properties of modulo q complete ℓ-wide families, *manuscript*, 2006.

[20] B. Felszeghy, B. Ráth, L. Rónyai, The lex game and some applications, *J. Symbolic Computation* **41** (2006), 663–681.

[21] B. Felszeghy, L. Rónyai, On the lexicographic standard monomials of zero dimensional ideals, *Proc. 10th Rhine Workshop on Computer Algebra (RWCA)* (2006), 95–105.

[22] B. Felszeghy, L. Rónyai, Some meeting points of Gröbner bases and combinatorics, *manuscript*, 2007.

[23] P. Frankl, Traces of antichains, *Graphs Comb.* **Vol 5. No 1.** (1989), 295–299.

[25] K. Friedl, G. Hegedűs, L. Rónyai, Gröbner bases for complete ℓ-wide families, *to appear in Publ. Math. Debrecen* (2007).

[26] K. Friedl, L. Rónyai, Order shattering and Wilson's theorem, *Discrete Mathematics* **270** (2003), 127–136.

[27] A. M. Garsia, Pebbles and expansions in the polynomial ring, In: *Polynomial identities and combinatorial methods*, Lecture Notes in Pure and Appl. Math. **235** 2003, 261–285.

[30] T. Harima, Characterization of Hilbert functions of Gorenstein Artin algebras with the weak Stanley property, *Proc. Amer. Math. Soc.* **123** (1995), 3631–3638.

[31] G. Hegedűs, A. Nagy, L. Rónyai, Gröbner bases for permutations and oriented trees, *Annales Univ. Sci. Budapest., Sectio Computatorica* **23** (2004), 137–148.

[32] G. Hegedűs, L. Rónyai, Standard monomials for q-uniform families and a conjecture of Babai and Frankl, *Central European Journal of Mathematics* **1** (2003), 198–207.

[35] D. Pintér, L. Rónyai, On the Hilbert function of complementary set families, *to appear in Annales Univ. Sci. Budapest., Sectio Computatorica.*

[37] L. Rédei, Zur Theorie der Gleichungen in endlichen Körpern, *Acta Univ. Szeged Sect. Sci. Math.* **11** (1946), 63–70.

[38] L. Rónyai, On a conjecture of László Rédei, *Acta Univ. Szeged Sect. Sci. Math.* **69** (2003), 523–531.

[39] R. M. Wilson, A diagonal form for the incidence matrices of t-subsets vs. k-subsets, *Europ. J. Combin.* **11** (1990), 609–615.