DIPLOMAMUNKA

Véges pontrendszerek standard monomjai és Gröbner-bázisai

Felszeghy Bálint

Témavezető: Rónyai Lajos
egyetemi tanár

Matematika Intézet,
Algebra Tanszék

BME
2004.

Tartalomjegyzék

1. Bevezetés **3**

2. Standard monomok és Gröbner-bázis **6**
2.1. Tagsorrend 6
2.2. Standard monomok és főtagok 8
2.3. Gröbner-bázis 9
2.4. Adott halmazon eltűnő polinomok ideálja 13

3. A lexikografikus eset kombinatorikus jellemzése **15**
3.1. A lex játék 15
3.2. Ki nyeri a lex játékot? 17
3.3. Lex standard monomok kombinatorikus tulajdonságai 22
3.4. Általánosítás eliminációs rendezésre 24

4. Algoritmusok **26**
4.1. Buchberger algoritmusa 26
4.2. Farr és Gao algoritmusa véges pontrendszerre 30
4.3. A Buchberger–Möller-algoritmus véges pontrendszerre 32
4.4. Véges pontrendszer lex standard monomjai 36

5. Számolások konkrét pontrendszerekre **43**
5.1. Szimmetrikus pontrendszerekről általában 43
5.2. Egy szimmetrikus eset: modulo r ℓ-széles pontrendszer 44
5.3. Partíciók és egy elem generálta szimmetrikus pontrendszerek . 55
5.4. Irányított fák 60

6. Alkalmazások **63**
6.1. Alkalmazás halmazrendszerekre 63
6.2. Egy változat a szimmetrikus polinomok alaptételére 71

7. Összefoglalás **73**

1. Bevezetés

Dolgozatom témája test feletti többváltozós polinomgyűrűk bizonyos tulajdonságainak vizsgálata. Később természetesen a pontos definíciók is szerepelnek, egyelőre annyit mondunk, hogy egy polinomideál Gröbner-bázisa egy jó fajta generátorrendszere, az ideálhoz tartozó standard monomok pedig az ideál szerinti faktorstruktúra – szintén kellemes egyéb tulajdonságokkal is rendelkező – lineáris bázisa. Munkámban olyan ideálok standard monomjaival és Gröbner-bázisaival foglalkozom, amelyek egy véges halmazon (pontrendszeren) eltűnő összes polinomból állnak.

A Gröbner-bázis fogalma Bruno Buchberger osztrák matematikustól származik, aki mintegy 40 éve [5] Ph. D. tézisében és valamivel később megjelent [6] cikkében dolgozta ki az elmélet alapjait. Buchbergert elsősorban kommutatív algebrai és algebrai geometriai kérdések motiválták, de a témavezetője tiszteletére elnevezett Gröbner-bázis – miközben a hetvenes években egyre ismertebbé vált – a matematika legkülönbözőbb területein lelt alkalmazásokra. A *33 Years of Gröbner Bases* címmel tartott konferencia kiadványa [7] ezeknek egy jó összefoglalóját adja: Buchberger eredeti [6] cikkének angol fordítása mellett ismertet alkalmazásokat kódelméletben, egész programozásban, automatikus tételbizonyításokban, szimbolikus számítások elméletében, statisztikában, parciális differenciálegyenletek elméletében és numerikus módszerekben. A legtöbb matematikai program – így a Maple és a Mathematica is – tartalmaz Gröbner-bázist számoló algoritmust és használ Gröbner-bázisokat más jellegű kérdések eldöntésére.

A technika ereje abban rejlik, hogy eszközöket szolgáltat többismeretlenes polinomiális egyenletrendszerek megoldásainak vizsgálatára. A Gröbner-bázisokkal egyszerűen végezhető *redukció*nak nevezett művelet közös általánosítása a lineáris egyenletrendszerek megoldására ismert Gauss eliminációnak és az egyismeretlenes polinomiális egyenletrendszer megoldhatóságának eldöntéséhez szükséges euklideszi algoritmusnak.

Véges pontrendszerekhez tartozó Gröbner-bázisokat dolgozatomban elsősorban kombinatorikus alkalmazásokra tekintve tárgyalom. Lineáris algebrai összefüggések ilyen jellegű használata széles körben ismert; bizonyára az Olvasó is fel tud idézni például olyan bizonyítást, ahol valamilyen objektumok számát felülről becsüljük a hozzájuk tartozó lineárisan független vektorokat tartalmazó tér dimenziójával. Lineáris helyett magasabb fokú polinomok segítségével számos további kombinatorikus kérdés vizsgálható, van tehát helyük a Gröbner-bázisoknak. A módszer alkalmazásában Rónyai Lajos és egy doktorandusz hallgatója, Hegedűs Gábor, szerzett elévülhetetlen érdemeket.

A már említetteken túl a Gröbner-bázisok nagy előnye, hogy mindenféle

kommutatív algebrai előismeret nélkül is könnyen érthetőek. A 2. fejezetben ennek megfelelően bemutatom az elmélet alapjait. A felépítésben nem törekszem a lehető legáltalánosabb formára, de így is, a fejezet nagyjából tartalmazza a témakör definícióit és legfontosabb tételeit, bizonyításokkal együtt. Részletesebb tárgyalás található például [1] és [4] könyvekben.

Egy ideál Gröbner-bázisa és standard monomjai függenek egy – a monomokon értelmezett – rendezéstől. Az egyik lehetséges választást *lexikografikus rendezés*nek (vagy röviden *lex*nek) nevezik. A 3. fejezetben egy kétszemélyes játék segítségével ekvivalens jellemzését adom a lexikografikus rendezésre vett standard monomoknak. Ez új eredmény, amelyet Rónyai Lajossal és Ráth Balázzsal közös [14] cikkünkben is publikálunk. Ezen kombinatorikus jellemzés, a belőle közvetlenül adódó *lex standard monomok rekurzív szerkezet*éről szóló következménnyel együtt, tekinthető a dolgozat központi tételének. A 4. és 5. fejezetekben bemutatott önálló eredmények nagy részét a játék folyományaként sikerült belátni. A már ismert tételek leírásakor is törekedtem arra, hogy a lex standard monomok fenti karakterizációjával adjak egyszerűbb, a dolgozat szerkezetébe jobban illeszkedő bizonyításokat.

A 4. fejezet algoritmusokról szól. Buchberger eredeti módszere, amely általános polinomideál Gröbner-bázisát ki tudja számítani, szerepel minden a témába bevezető könyvben. Itt Adams és Loustaunau [1] munkáját választottam a leírás alapjául. Tárgyalok két további algoritmust, amely véges pontrendszerhez tartozó Gröbner-bázist számol; az általánosság megszorításáért kárpótlásul jóval hatékonyabban. Ezek közül Farr és Gao [12] eredménye aránylag új, de csak speciális esetekben ad jobbat a sokak által alaposan vizsgált Buchberger–Möller-algoritmusnál, amely bemutatásában főként Teo Mora és Lorenzo Robbiano [28] összefoglaló cikkére hagyatkoztam. Annak ellenére, hogy a módszerrel többen foglalkoztak, a futásidőnek nem találtam olyan elemzését, amely nem csak a testben szükséges aritmetikai műveletek összeszámolására korlátozódna. A költségbecslésnél így azt is figyelembe veszem, hogy két monom a választott rendezés szerinti összehasonlítása nem végezhető el konstans időben. Végül ismertetek egy kombinatorikus algoritmust lex standard monomok számítására, amely gyorsabban végez mint az eddig ismert módszer.

Három speciálisan választott típusú pontrendszer standard monomjait és bizonyos esetekben Gröbner-bázisát határozom meg az 5. fejezetben. A *modulo r ℓ-széles pontrendszer* standard monomjait a 3. fejezetben ismertetett játék segítségével tudjuk kiszámolni, csakúgy mint az oszthatóságra nézve minimiális nem standard monomokat, amelyeknek általában a Gröbner-bázis meghatározásakor kulcsszerepük van. Magát a Gröbner-bázist ennek ellenére nem adom meg, helyette egy speciális esetben, az ℓ-széles (tehát nem modulárisan tekintett) pontrendszerét számolom csak ki, amely már ismert eredmény

[20]. A második speciális eset az *egy elem által generált szimmetrikus pontrendszer*, amelynek lex standard monomjait határozzuk meg, szintén a játék következményeként. Ez – bár alapjai ugyanazok a kombinatorikus tények – valamelyest egyszerűsíti Hegedűs és Rónyai [23] korábbi bizonyítását. A Gröbner-bázist itt is csak egy speciális esetre tudom megadni, Hegedűs, Nagy és Rónyai [21] munkája nyomán. Végül ugyanezen cikk alapján ismertetem a harmadik tekintett pontrendszer – amely irányított fák karakterisztikus vektoraiból áll – lex standard monomjait és lex Gröbner-bázisát.

A lehetséges kombinatorikus alkalmazások közül néhányat bemutatok a 6. fejezetben. Jórészt Hegedűs, Friedl és Rónyai [20], illetve Hegedűs és Rónyai [24] munkáiból válogatva, foglalkozom az $\{1, 2, \ldots, n\}$ halmaz bizonyos tulajdonságoknak eleget tevő részhalmazainak családjával. Halmazrendszerek *tartalmazási mátrix*a általánosítása a gráfelméletből ismert illeszkedési mátrixnak. Néhány ilyen rangját kiszámolom és segítségükkel bizonyítok a halmazcsalád elemszámára vonatkozó becslést, többek között igazolva Babai és Frankl egy sejtését. Egy más jellegű alkalmazásként bemutatom Hegedűs, Nagy és Rónyai [21] bizonyítását a szimmetrikus polinomok alaptételének általánosított alakjára.

2. Standard monomok és Gröbner-bázis

Mielőtt rátérnénk a dolgozat központi fogalmainak definiálására, bevezetünk néhány jelölést, amelyeket végig használni fogunk.

A nemnegatív egészek, az egészek és a racionális számok halmazát rendre $\mathbb{N}$, $\mathbb{Z}$ és $\mathbb{Q}$ rövidíti, $\mathbb{F}_p$ pedig a p elemű véges testet jelöli. Mindvégig $\mathbb{F}$ egy tetszőleges test lesz, n pedig pozitív egész. Az $\{1, 2, \ldots, n\}$ halmazra röviden $[n]$ halmazként hivatkozunk, az $\mathbb{F}$ feletti n változós polinomgyűrűre pedig a szokásos $\mathbb{F}[x_1, \ldots, x_n]$ jelölést használjuk.

*Monom*ok alatt $x_1^{w_1} x_2^{w_2} \ldots x_n^{w_n} \in \mathbb{F}[x_1, \ldots, x_n]$ alakú polinomokat értünk. Az $\mathbb{F}[x_1, \ldots, x_n]$ polinomgyűrű tekinthető $\mathbb{F}$ feletti vektortérnek (sőt akár algebrának), ennek a monomok lineáris bázisát alkotják. Azt mondjuk, hogy egy $x_1^{w_1} x_2^{w_2} \ldots x_n^{w_n}$ monom *szerepel* f-ben, ha f-et monomok lineáris kombinációjaként előállítva $x_1^{w_1} x_2^{w_2} \ldots x_n^{w_n}$ együtthatója nem nulla.

Ha $f_1, \ldots, f_m \in \mathbb{F}[x_1, \ldots, x_n]$, akkor az általuk $\mathbb{F}[x_1, \ldots, x_n]$ gyűrűben generált ideált $\langle f_1, \ldots, f_m \rangle$ jelöli.

Vektorok megkülönböztetésére félkövér betűket használunk, koordinátáikra pedig ugyanazon betű megfelelően számozott nem vastag változatával hivatkozunk, például $\mathbf{w} = (w_1, \ldots, w_n)$. Hasonlóan, $f(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$ rövidíti $f(x_1, \ldots, x_n) \in \mathbb{F}[x_1, \ldots, x_n]$-et, $\mathbf{x}^\mathbf{w}$ pedig az $x_1^{w_1} x_2^{w_2} \ldots x_n^{w_n}$ monomot.

2.1. Tagsorrend

Egy $\mathbb{F}[\mathbf{x}]$ monomjain értelmezett $\prec$ teljes rendezést *tagsorrend*nek nevezzük, amennyiben minden $\mathbf{x}^\mathbf{w} \in \mathbb{F}[\mathbf{x}]$ monomra $1 \preceq \mathbf{x}^\mathbf{w}$, és minden $\mathbf{x}^\mathbf{w}, \mathbf{x}^\mathbf{u}, \mathbf{x}^\mathbf{v} \in \mathbb{F}[\mathbf{x}]$ monomra, amelyre $\mathbf{x}^\mathbf{u} \prec \mathbf{x}^\mathbf{v}$, teljesül $\mathbf{x}^\mathbf{u} \cdot \mathbf{x}^\mathbf{w} \prec \mathbf{x}^\mathbf{v} \cdot \mathbf{x}^\mathbf{w}$ is.

Standard monomokról és Gröbner-bázisról mindig egy rögzített tagsorrendet feltételezve beszélünk, más rendezéshez általában mások a standard monomok. Bizonyos alkalmazásokban elegendő egy tetszőleges Gröbner-bázis meghatározása, míg egyes esetekben egyéb tulajdonságoknak is eleget tevő tagsorrendek szükségesek. A következőkben mutatunk néhány példát, és egyben definiáljuk a számunkra legfontosabb két tagsorrendet.

Azt mondjuk, hogy $\mathbf{x}^\mathbf{w}$ a *lexikografikus rendezés* szerint kisebb vagy egyenlő, mint $\mathbf{x}^\mathbf{u}$, ha a legkisebb i-re, amelyre $w_i \neq u_i$, teljesül $w_i < u_i$. Nyilvánvaló, hogy a lexikografikus rendezés tagsorrend. Ezt a rendezést ezentúl röviden *lex*nek fogjuk nevezni.

A másik gyakran használt tagsorrend a *fok-kompatibilis lexikografikus rendezés*, röviden *deglex*. Egy $\mathbf{x}^\mathbf{w}$ a deglex szerint kisebb mint $\mathbf{x}^\mathbf{u}$, amennyiben $\mathbf{x}^\mathbf{w}$ foka kisebb, mint $\mathbf{x}^\mathbf{u}$ foka (azaz $\sum_{i=1}^{n} w_i < \sum_{i=1}^{n} u_i$) vagy pedig azonos fokúak, és $\mathbf{x}^\mathbf{w}$ megelőzi $\mathbf{x}^\mathbf{u}$-t a lexikografikus rendezés szerint. A tagsorrendtől

megkívánt tulajdonságok a deglex rendezésre is triviálisan teljesülnek.

Például $n = 2$ esetén az első néhány monom lex rendezése

$$1 \prec x_2 \prec x_2^2 \prec x_2^3 \prec \cdots \prec x_1 \prec x_1x_2 \prec x_1x_2^2 \prec \cdots \prec x_1^2 \prec x_1^2x_2 \prec x_1^2x_2^2 \prec \ldots$$

deglex rendezése pedig

$$1 \prec x_2 \prec x_1 \prec x_2^2 \prec x_1x_2 \prec x_1^2 \prec x_2^3 \prec x_1x_2^2 \prec x_1^2x_2 \prec x_1^3 \prec \ldots$$

Általában is *fok-kompatibilis*nek hívunk egy tagsorrendet, ha teljesül, hogy kisebb fokú monomok a rendezésben kisebbek.

Mielőtt rátérnénk a tagsorrendek legfontosabb tulajdonságainak igazolására, bizonyítás nélkül közöljük ezen rendezések egy szép jellemzését.

Legyen $\mathbf{a}$ pozitív valós számokból álló n hosszú vektor. Egy $\mathbf{x}^{\mathbf{w}}$ monom $\mathbf{a}$-val súlyozott fokszáma $\mathbf{a}$ és $\mathbf{w}$ skaláris szorzata, azaz $a_1w_1+a_2w_2+\cdots+a_nw_n$. Legyen A egy $n \times n$-es pozitív valós elemekből álló nemszinguláris mátrix, és definiáljunk a segítségével tagsorrendet a következő módon. Egy $\mathbf{x}^{\mathbf{w}}$ monom legyen kisebb, mint $\mathbf{x}^{\mathbf{u}}$, ha A első sora, mint súlyvektor szerinti súlyozott fokszáma $\mathbf{x}^{\mathbf{w}}$-nek kisebb. Amennyiben ezek egyenlőek, hasonlítsuk össze az A második sora szerinti súlyozott fokszámokat. Az eljárást folytatva teljes rendezést kapunk, hiszen amennyiben $\mathbf{x}^{\mathbf{w}}$ és $\mathbf{x}^{\mathbf{u}}$ összes A szerinti súlyozott fokszáma egyenlő, akkor $\mathbf{w}$-t és $\mathbf{u}$-t oszlopvektorként tekintve $A\mathbf{w} = A\mathbf{u}$, így $\mathbf{w} = \mathbf{u}$, hiszen A reguláris. Teljesül $1 \preceq \mathbf{x}^{\mathbf{w}}$, mivel $\mathbf{x}^{\mathbf{w}}$ tetszőleges súlyozott fokszáma nemnegatív. Végül a tagsorrendtől megkívánt harmadik tulajdonság abból következik egyszerűen, hogy $\mathbf{x}^{\mathbf{u}} \cdot \mathbf{x}^{\mathbf{w}}$ súlyozott fokszáma éppen $\mathbf{x}^{\mathbf{u}}$ és $\mathbf{x}^{\mathbf{w}}$ súlyozott fokszámainak összege.

Robbiano [29] (vagy vázlatosan [30]) igazolta, hogy tetszőleges tagsorrend előáll ilyen alakban valamilyen alkalmasan választott A mátrixszal. A lex rendezést például megadja az $n \times n$-es identitás, a deglexet pedig az

$$\begin{bmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & 0 & 0 & \ldots & 0 \\ 0 & 1 & 0 & \ldots & 0 \\ & & \ddots & & \\ 0 & \ldots & 0 & 1 & 0 \end{bmatrix}$$

mátrix.

2.1. Tétel. *Tetszőleges $\prec$ tagsorrend a monomok közötti oszthatóság finomítása (azaz ha $\mathbf{x}^{\mathbf{w}} \mid \mathbf{x}^{\mathbf{u}}$, akkor $\mathbf{x}^{\mathbf{w}} \preceq \mathbf{x}^{\mathbf{u}}$) és jólrendezés.*

Bizonyítás: Az első állítás igazolásához tegyük fel, hogy $\mathbf{x}^{\mathbf{w}} \mid \mathbf{x}^{\mathbf{u}}$. Ekkor $\frac{\mathbf{x}^{\mathbf{u}}}{\mathbf{x}^{\mathbf{w}}}$ is monom, tehát teljesül $1 \preceq \frac{\mathbf{x}^{\mathbf{u}}}{\mathbf{x}^{\mathbf{w}}}$. Ha beszorzunk $\mathbf{x}^{\mathbf{w}}$-vel, éppen a kívánt egyenlőtlenséget kapjuk.

Tegyük fel indirekte, hogy $\prec$ nem jólrendezés, azaz létezik végtelen hosszú leszálló lánc

$$\mathbf{x}^{\mathbf{w_1}} \succ \mathbf{x}^{\mathbf{w_2}} \succ \mathbf{x}^{\mathbf{w_3}} \succ \cdots \succ \mathbf{x}^{\mathbf{w_i}} \succ \mathbf{x}^{\mathbf{w_{i+1}}} \succ \dots$$

Tekintsük az

$$\langle \mathbf{x}^{\mathbf{w_1}} \rangle \subseteq \langle \mathbf{x}^{\mathbf{w_1}}, \mathbf{x}^{\mathbf{w_2}} \rangle \subseteq \langle \mathbf{x}^{\mathbf{w_1}}, \mathbf{x}^{\mathbf{w_2}}, \mathbf{x}^{\mathbf{w_3}} \rangle \subseteq \dots$$

felszálló ideálláncot. Mivel $\mathbb{F}[\mathbf{x}]$ Noether gyűrű, ez nem lehet végtelen, tehát speciálisan van olyan i, amelyre $\mathbf{x}^{\mathbf{w_{i+1}}} \in \langle \mathbf{x}^{\mathbf{w_1}}, \dots, \mathbf{x}^{\mathbf{w_i}} \rangle$. Ha $h \in \mathbb{F}[\mathbf{x}]$ tetszőleges polinom, akkor minden $\mathbf{x}^{\mathbf{w}} h(\mathbf{x})$-ben szereplő monom nagyobb vagy egyenlő, mint $\mathbf{x}^{\mathbf{w}}$. Emiatt igaz az is, hogy tetszőleges $h_1, \dots, h_i \in \mathbb{F}[\mathbf{x}]$-re minden a $\sum_{j=1}^{i} h_j(\mathbf{x}) \mathbf{x}^{\mathbf{w_j}}$ polinomban szereplő monom nagyobb vagy egyenlő, mint az $\mathbf{x}^{\mathbf{w_1}}, \dots, \mathbf{x}^{\mathbf{w_i}}$ monomok közül a legkisebb. Más szóval, az $\langle \mathbf{x}^{\mathbf{w_1}}, \dots, \mathbf{x}^{\mathbf{w_i}} \rangle$ ideál tetszőleges elemének legkisebb monomja is nagyobb vagy egyenlő, mint $\mathbf{x}^{\mathbf{w_i}}$. Arra jutottunk tehát, hogy $\mathbf{x}^{\mathbf{w_i}} \preceq \mathbf{x}^{\mathbf{w_{i+1}}}$, ami ellentmond indirekt feltevésünknek. □

2.2. Standard monomok és főtagok

Rögzítsünk egy $\prec$ tagsorrendet. Egy $f(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$, $f \neq 0$ *polinom főtagja* avagy *vezető tagja* (a $\prec$ tagsorrendre nézve) a benne szereplő monomok közül a legnagyobb. Az angol *leading monomial* elnevezés rövidítéseként f főtagját $\operatorname{lm}(f)$-fel jelöljük. *Főegyüttható*nak $\operatorname{lm}(f)$ együtthatóját hívjuk.

Legyen $I \trianglelefteq \mathbb{F}[\mathbf{x}]$ egy ideál. Ekkor I *főtagjai*nak $\operatorname{Lm}(I)$ halmaza az I-ben szereplő nemnulla polinomok főtagjaiból áll, azaz

$$\operatorname{Lm}(I) = \{\operatorname{lm}(f) \ : \ f \in I, f \neq 0\}.$$

Látható, hogy $\operatorname{Lm}(I)$ az oszthatóságra nézve felszálló halmaz, azaz $\mathbf{x}^{\mathbf{w}} \in \operatorname{Lm}(I)$ és $\mathbf{x}^{\mathbf{w}} \mid \mathbf{x}^{\mathbf{u}}$ esetén $\mathbf{x}^{\mathbf{u}} \in \operatorname{Lm}(I)$, hiszen amennyiben $\mathbf{x}^{\mathbf{w}} = \operatorname{lm}(f(\mathbf{x}))$, úgy $\mathbf{x}^{\mathbf{u}} = \operatorname{lm}\left(\frac{\mathbf{x}^{\mathbf{u}}}{\mathbf{x}^{\mathbf{w}}} f(\mathbf{x})\right)$.

Az I *ideál standard monomjai* azon monomok, amelyek semelyik $f \in I$ polinomnak sem vezető tagjai, azaz

$$\operatorname{Sm}(I) = \{\mathbf{x}^{\mathbf{w}} \in \mathbb{F}[\mathbf{x}]\} \setminus \operatorname{Lm}(I) = \{\mathbf{x}^{\mathbf{w}} \ : \ \nexists f \in I, \text{amelyre } \operatorname{lm}(f) = \mathbf{x}^{\mathbf{w}}\}.$$

Miután felszálló halmaz komplementere, ezért $\operatorname{Sm}(I)$ leszálló az oszthatóságra nézve.

Néha fogjuk használni ideálok helyett tetszőleges $F \subseteq \mathbb{F}[\mathbf{x}]$ polinomhalmazra is a magától értetődő $\operatorname{Sm}(F)$ és $\operatorname{Lm}(F)$ jelöléseket.

2.3. Gröbner-bázis

Gröbner-bázis létezése

Mielőtt definiálnánk egy ideál Gröbner-bázisát, bebizonyítjuk a 2.3. állítást, ami – mint a definíció fényében rögtön látni fogjuk – azt mondja ki, hogy tetszőleges ideálnak létezik Gröbner-bázisa.

Egy I ideált *monomiális ideál*nak nevezünk, ha van monomokból álló generátorrendszere.

2.2. Lemma. *Ha I monomiális ideál, H monomokból álló generátorrendszere, és $f \in I$, akkor f minden monomja osztható valamely H-beli monommal, tehát f minden monomja is I-ben van. Minden monomiális ideálnak van monomokból álló véges generátorrendszere.*

Bizonyítás: Legyen I monomiális és $f \in I$. Ekkor a feltétel szerint léteznek $\mathbf{x}^{\mathbf{w_1}}, \ldots, \mathbf{x}^{\mathbf{w_m}} \in H$ monomok és $h_1, \ldots h_m \in \mathbb{F}[\mathbf{x}]$ polinomok, amelyekre

$$f(\mathbf{x}) = \sum_{i=1}^{m} h_i(\mathbf{x})\mathbf{x}^{\mathbf{w_i}}.$$

A jobb oldal minden monomja osztható valamely $\mathbf{x}^{\mathbf{w_i}}$-vel, azaz f minden monomjára ugyanez igaz.

Tekintsük I-nek egy véges $f_1, \ldots, f_m$ generátorrendszerét. A lemma első része szerint az ezekben szereplő véges sok monom mind I-ben van. Nyilvánvalóan ezek generálják is I-t, tehát a második állítás is igaz. □

2.3. Állítás. *Tetszőleges I ideál esetén $\mathrm{Lm}(I)$-nek van olyan véges H részhalmaza, amelyre igaz, hogy tetszőleges $\mathbf{x}^{\mathbf{w}} \in \mathrm{Lm}(I)$-t osztja valamely H-beli monom.*

Bizonyítás: Tekintsük az $\mathrm{In}(I) := \langle \mathrm{Lm}(I) \rangle$ monomiális ideál egy monomokból álló véges H generátorrendszerét, amely a 2.2. lemma szerint létezik. Minden $\mathrm{In}(I)$-ben levő monom szerepel $\mathrm{Lm}(I)$-ben is, ugyanis ha $\mathbf{x}^{\mathbf{w}} \in \mathrm{In}(I)$, akkor a 2.2. lemma szerint valamely $\mathrm{Lm}(I)$-beli monom osztja $\mathbf{x}^{\mathbf{w}}$-t, így – kihasználva, hogy $\mathrm{Lm}(I)$ az oszthatóságra nézve felszálló – $\mathbf{x}^{\mathbf{w}} \in \mathrm{Lm}(I)$ is teljesül. Speciálisan tehát $H \subseteq \mathrm{Lm}(I)$. Másrészt, ha $\mathbf{x}^{\mathbf{w}} \in \mathrm{Lm}(I)$, akkor $\mathbf{x}^{\mathbf{w}} \in \mathrm{In}(I)$, így megint csak a 2.2. lemma alapján valamely H-beli monom osztja őt. Ezek szerint H megfelel a követelményeknek. □

Az I ideál *Gröbner-bázis*ának nevezünk egy olyan véges $G \subseteq I$ halmazt, amelyre teljesül, hogy minden $f \in I$, $f \neq 0$ polinomhoz létezik $g \in G$, amelyre $\mathrm{lm}(g)$ osztója $\mathrm{lm}(f)$-nek. Vegyük észre, hogy a 2.3. állítás éppen

azt mondja ki, hogy minden ideálnak létezik Gröbner-bázisa, hiszen az ott szereplő H halmaz minden $\mathbf{x}^{\mathbf{w}}$ eleméhez van $g \in I$, amelyre $\mathrm{lm}(g) = \mathbf{x}^{\mathbf{w}}$, és ezen g polinomok halmaza I egy Gröbner-bázisa. Fontos megjegyezni, hogy miután egy polinom vezető tagja függ a választott tagsorrendtől, ezért általában a Gröbner-bázis sem független tőle.

Redukció

A definícióból nem látszik közvetlenül a Gröbner-bázisok legfontosabb tulajdonsága, amelyet az alábbiakban fogunk vizsgálni, és amely szerint a Gröbner-bázis egy nagyon jó adottságokkal rendelkező generátorrendszere az ideálnak.

Legyen $f, g \in \mathbb{F}[\mathbf{x}]$, tegyük fel, hogy f egy $\mathbf{x}^{\mathbf{w}}$ monomja osztható $\mathrm{lm}(g)$-vel, $\mathbf{x}^{\mathbf{w}}$ együtthatója f-ben c_f, g főegyütthatója pedig c_g. Legyen

$$\hat{f}(\mathbf{x}) = f(\mathbf{x}) - \frac{c_f \cdot \mathbf{x}^{\mathbf{w}}}{c_g \cdot \mathrm{lm}(g)} g(\mathbf{x}). \tag{1}$$

Vegyük észre, hogy $\hat{f}$-ban $\mathbf{x}^{\mathbf{w}}$ helyébe nála szigorúan kisebb monomok kerültek, hiszen $\frac{\mathbf{x}^{\mathbf{w}}}{\mathrm{lm}(g)} g(\mathbf{x})$ főtagja $\mathbf{x}^{\mathbf{w}}$ éppen kiesik. Ezt a műveletet *redukció*nak hívjuk.

Ha G polinomok véges halmaza és $f(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$, akkor azt mondjuk, hogy f *redukált G-re nézve*, amennyiben f semelyik monomját sem osztja semelyik $g \in G$ vezető tagja. Legyen most f tetszőleges, és redukáljuk (1) szerint G elemeivel, amíg G-re nézve redukált polinomot nem kapunk, úgy hogy mindig a szereplő legnagyobb monomot helyettesítjük kisebbekkel. Ez az eljárás véges sok lépésben véget ér, hiszen minden egyes redukcióval kisebb lesz a legnagyobb G-vel redukálható monom. Az is világos, hogy az eljárás során megkapjuk f-nek egy

$$f(\mathbf{x}) = \sum_{i=1}^{m} g_i(\mathbf{x}) h_i(\mathbf{x}) + \hat{f}(\mathbf{x})$$

előállítását, ahol $G = \{g_1, \ldots, g_m\}$, $h_1, \ldots, h_m \in \mathbb{F}[\mathbf{x}]$, $\hat{f}$ redukált polinom G-re nézve, és teljesül $\mathrm{lm}(g_i h_i) \preceq \mathrm{lm}(f)$. Azt mondjuk, hogy *$\hat{f}$ az f (egy) redukáltja G-re nézve*, amennyiben léteznek ilyen tulajdonságú $h_1, \ldots, h_m$ polinomok.

Példa. Legyen $g_1(x_1, x_2) = x_1x_2 + x_1$, $g_2(x_1, x_2) = x_1x_2 + x_2$, $G = \{g_1, g_2\}$ és $f(x_1, x_2) = 2x_1x_2 + x_1 + x_2$. Ha f-et először g_1-gyel redukáljuk, akkor $x_2 - x_1$-et kapunk, ha g_2-vel, akkor $x_1 - x_2$-t. Világos, hogy mindkettő f redukáltja G-re nézve. Ráadásul $f = g_1 + g_2$, ezért a redukált definíciója alapján a 0

polinom is f redukáltja, annak ellenére, hogy (1) szerinti redukciós lépésekkel nem kapható meg.

Látni fogjuk azonban, hogy ennek az az oka, hogy G nem Gröbner-bázisa a $\langle G \rangle$ ideálnak. Hamarosan igazoljuk, hogy Gröbner-bázis szerint minden polinom redukáltja egyértelmű, és így meg is kapható a fenti redukciós lépésekkel.

Az alábbi tétel az első fontos állításunk, amit a Gröbner-bázis fogalma segítségével tudunk bizonyítani.

2.4. Tétel. *Ha I ideál $\mathbb{F}[\mathbf{x}]$-ben, akkor az $\mathbb{F}$ feletti $\mathbb{F}[\mathbf{x}]/I$ vektortérnek lineáris bázisát adják* $\mathrm{Sm}(I)$ *elemeinek I szerinti ekvivalenciaosztályai.*

Bizonyítás: $\mathrm{Sm}(I)$ ekvivalenciaosztályai lineárisan függetlenek $\mathbb{F}[\mathbf{x}]/I$-ben, ugyanis amennyiben

$$\sum_{i=1}^{m} a_i \left(\mathbf{x}^{\mathbf{w_i}} + I\right) = 0$$

egy nemtriviális lineáris összefüggés, akkor

$$f(\mathbf{x}) := \sum_{i=1}^{m} a_i \mathbf{x}^{\mathbf{w_i}} \in I,$$

amiből $\mathrm{lm}(f) \in \mathrm{Lm}(I)$ következik, ellentmondva annak, hogy csupa standard monomot tekintettünk.

Legyen G az I tetszőleges Gröbner-bázisa, $f \in \mathbb{F}[\mathbf{x}]$ és $\hat{f}$ az f egy G szerinti redukáltja. Ekkor $\hat{f}$ és f azonos I szerinti mellékosztályban van, hiszen $\sum_{i=1}^{m} g_i(\mathbf{x}) h_i(\mathbf{x}) \in I$. Másrészt $\hat{f}$ redukált G-re nézve, ezért monomjai nem lehetnek $\mathrm{Lm}(I)$-ben, tehát $\hat{f}$ standard monomok lineáris kombinációja. Ezek szerint f is előáll modulo I, mint $\mathrm{Sm}(I)$ elemeinek lineáris kombinációja. □

2.5. Következmény. *Ha G az I ideál Gröbner-bázisa, akkor $f \in \mathbb{F}[\mathbf{x}]$ polinom G szerinti redukáltja egyértelmű, és $f \in I$ pontosan akkor, ha a redukált 0. Speciálisan $\langle G \rangle = I$ teljesül.*

Bizonyítás: Amint az előző bizonyításban láttuk, $f \in \mathbb{F}[\mathbf{x}]$ polinom G szerinti redukáltja standard monomok lineáris kombinációja, ami $\mathrm{Sm}(I)$ bázis tulajdonsága miatt egyértelműen meghatározott az $f + I$ mellékosztály által. A második állítás következik, hiszen $f \in I$ esetén f és 0 modulo I azonos, redukáltjuk ezért megegyezik. Ugyanakkor a 0 polinom már redukált, tehát f redukáltja 0. □

A 2.5. következmény megfordításai is igazak.

2.6. Állítás. *Ha $G \subseteq I$ véges, és minden $f \in I$ polinom G-vel redukálható 0-ra, akkor G Gröbner-bázis.*
Ha $G \subseteq I$ véges, és minden $f \in \mathbb{F}[\mathbf{x}]$ polinom G szerinti redukáltja egyértelmű, akkor G Gröbner-bázis.

Az első állítás világos, hiszen ha 0-ra redukálható egy $f \in I$, akkor $f = \sum_{i=1}^{m} g_i h_i$, ahol $G = \{g_1, \ldots, g_m\}$, $h_i \in \mathbb{F}[\mathbf{x}]$ és minden i-re $\mathrm{lm}(g_i h_i) \preceq \mathrm{lm}(f)$. Ráadásul valamely i-re biztosan $\mathrm{lm}(g_i h_i) = \mathrm{lm}(f)$, így erre $\mathrm{lm}(g_i)$ osztja $\mathrm{lm}(f)$-et. A második állítás bizonyítása valamivel több számolást igényel, de egyáltalán nem nehéz.

Redukált Gröbner-bázis

Egy I ideál Gröbner-bázisa természetesen nem egyértelmű, például egy G Gröbner-bázishoz hozzávéve I véges sok elemét, a kapott halmaz is Gröbner-bázisa I-nek. Bizonyos kézenfekvő további tulajdonságot is megkövetelve viszont már egyértelmű lesz. Ha G Gröbner-bázisra teljesül, hogy minden $g \in G$ redukált $G \setminus \{g\}$-re nézve és főegyütthatója 1, akkor G *redukált Gröbner-bázis*. Más szóval G Gröbner-bázis pontosan akkor redukált, ha minden $g \in G$-ben $\mathrm{lm}(g)$-től eltekintve csupa standard monom szerepel és g főegyütthatója 1.

2.7. Tétel. *Tetszőleges I ideálhoz egy rögzített tagsorrend mellett létezik redukált Gröbner-bázis és az egyértelmű.*

Bizonyítás: A létezés igazolásához legyen G tetszőleges Gröbner-bázisa I-nek, amelyben minden főegyüttható 1, és módosítsuk az alábbiak szerint. Dobjuk el (valamilyen sorrendben haladva) azokat a $g \in G$ polinomokat, amelyek vezető tagjait osztja valamely másik még el nem dobott G-beli polinom főtagja. Az így kapott G_1 polinomhalmaz nyilván továbbra is Gröbner-bázis, hiszen $\mathrm{Lm}(I)$ minden – az oszthatóságra nézve – minimális $\mathbf{x}^{\mathbf{w}}$ eleméhez pontosan egy $g \in G$-t tartottunk meg, aminek főtagja $\mathbf{x}^{\mathbf{w}}$.

Ha $g \in G_1$, akkor legyen $\hat{g}$ a $g - \mathrm{lm}(g)$ polinom G_1 szerinti redukáltja és

$$G_2 := \{\mathrm{lm}(g) + \hat{g} \,:\, g \in G_1\}\,.$$

Ekkor G_2 szintén Gröbner-bázis, hiszen pontosan ugyanazok G_1 és G_2 elemeinek főtagjai. Az is világos, hogy G_2 redukált.

Az egyértelműség bizonyításához tegyük fel, hogy G és H is redukált Gröbner-bázis. Mivel a főtagok speciálisan egymást sem oszthatják redukált Gröbner-bázisban, ezért G és H vezető tagjai is éppen $\mathrm{Lm}(I)$ minimális elemei, így $|G| = |H|$. Legyen $g \in G$ és $h \in H$, amelyre $\mathrm{lm}(g) = \mathrm{lm}(h)$.

Ekkor $g - h$ standard monomokból áll, ugyanakkor $g - h \in I$, ezért csak $g - h = 0$, lehet. Ezek szerint $G = H$. □

A redukált Gröbner-bázis elemeinek főtagjait $\mathrm{Lm}\,(I)$ *minimális generátorai*nak hívjuk, hiszen – amint az előbbi bizonyításban is láttuk – ezek éppen az oszthatóságra nézve minimális I-beli vezető tagok.

2.4. Adott halmazon eltűnő polinomok ideálja

A dolgozat nagy részében bizonyos speciális tulajdonságú ideálokkal fogunk dolgozni. Ebben az alfejezetben bevezetjük ezeket az ideálokat, és igazolunk egy alapvető tényt standard monomjaik számáról.

Ha $f(x_1, \ldots, x_n) \in \mathbb{F}[\mathbf{x}]$ polinom, és $\mathbf{y} \in \mathbb{F}^n$ az $\mathbb{F}$ feletti n dimenziós affin tér egy pontja, akkor behelyettesíthetjük f változói helyére $\mathbf{y}$-t, azaz f tekinthető $\mathbb{F}^n \to \mathbb{F}$ függvénynek. Legyen $V \subseteq \mathbb{F}^n$ és jelölje $I(V)$ a V-n eltűnő polinomok halmazát, azaz

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

Világos, hogy $I(V)$ ideál $\mathbb{F}[\mathbf{x}]$-ben. Az $\mathbb{F}$ feletti $\mathbb{F}[\mathbf{x}]/I(V)$ vektortér a V-*n értelmezett polinomfüggvények* tere. Az elnevezés jogos, hiszen f_1 és f_2 polinomok pontosan akkor egyeznek meg függvényként a V halmazon, ha $f_1 - f_2$ a teljes V-n eltűnik, azaz ha f_1 és f_2 modulo $I(V)$ azonos.

Tegyük fel, hogy V véges. Ekkor egyszerű interpolációval látható, hogy tetszőleges $V \to \mathbb{F}$ függvény reprezentálható polinommal. Ebben az esetben tehát $\mathbb{F}[\mathbf{x}]/I(V)$ megegyezik a $V \to \mathbb{F}$ függvények vektorterével. Miután egyrészt az utóbbi $\mathbb{F}$ feletti dimenziója $|V|$, másrészt a 2.4. tétel szerint $\mathbb{F}[\mathbf{x}]/I(V)$ éppen $|\mathrm{Sm}\,(I(V))|$ dimenziós, ezért igazoltuk, hogy

$$|\mathrm{Sm}\,(I(V))| = |V|\,,$$

amely alapvető összefüggést a továbbiakban gyakran fogjuk használni.

A fentiek egyszerű következménye, hogy amennyiben G az $I(V)$ véges pontrendszerhez tartozó ideál Gröbner-bázisa, akkor $i = 1, \ldots, n$-re létezik $g \in G$, amely vezető tagja x_i hatványa. Ehhez ráadásul csak annyit kell felhasználni, hogy $\mathrm{Sm}\,(I(V))$ véges. Ez esetben ugyanis az $1, x_i, x_i^2, \ldots$ monomok lineárisan összefüggőek, azaz van olyan $f(x_i) \in \mathbb{F}[x_i]$, amely $I(V)$-ben van. Ennek főtagja x_i^w valamely w kitevőre, ezért $x_i^w \in \mathrm{Lm}\,(I(V))$, következésképpen G-ben kell legyen egy kívánt tulajdonságú polinom.

Valójában ez a feltétel ekvivalens $\mathrm{Sm}\,(I)$ végességével, azaz igaz az is, hogy ha egy tetszőleges I ideál Gröbner-bázisára teljesül, hogy minden x_i változóra van a Gröbner-bázisnak $x_i^{w_i}$ főtagú eleme, akkor $\mathrm{Sm}\,(I)$ véges. Ezt

könnyű látni, ugyanis egy $\mathbf{x^u}$ monom legfeljebb akkor lehet $\mathrm{Sm}\,(I)$-ben, ha minden i-re $u_i < w_i$ (hiszen $x_i^{w_i} \in \mathrm{Lm}\,(I)$), ilyenből viszont csak véges sok $(w_1 \cdot w_2 \ldots w_n)$ van.

Ezeket az ideálokat 0 *dimenziós*aknak hívjuk. Általában nem teljesül, hogy egy 0 dimenziós ideál valamely véges pontrendszerhez tartozna.

Végül bebizonyítunk egy lemmát, amit később többször is felhasználunk annak bizonyítására, hogy egy $F = \{f_1, \ldots, f_m\}$ polinomhalmaz Gröbner-bázis.

2.8. Lemma. *Legyen I tetszőleges 0 dimenziós ideál és $F = \{f_1, \ldots, f_m\} \subseteq I$. Pontosan akkor Gröbner-bázisa I-nek F, ha $|\mathrm{Sm}\,(F)| = |\mathrm{Sm}\,(I)|$.*

Bizonyítás: A definícióból nyilvánvaló, hogy $\mathrm{Sm}\,(F) \supseteq \mathrm{Sm}\,(I)$ mindig teljesül. Az elemszámok egyenlősége tehát ekvivalens a halmazok egyenlőségével. Viszont $\mathrm{Sm}\,(F) = \mathrm{Sm}\,(I)$ azt jelenti, hogy minden $\mathbf{x^w} \in \mathrm{Lm}\,(I)$ monom F-re nézve nem redukált, azaz valamelyik $f_i \in F$ főtagja osztja, tehát F Gröbner-bázis. □

Vegyük észre, hogy amennyiben $I = I(V)$ valamely véges V pontrendszerre, akkor $|\mathrm{Sm}\,(I)| = |V|$, ezért a feltétel a számunkra érdekes esetekben könnyen ellenőrizhető lesz.

3. A lexikografikus eset kombinatorikus jellemzése

Ebben a fejezetben $\prec$ végig a lexikografikus rendezést fogja jelenteni, tehát speciálisan $x_1 \succ x_2 \succ \cdots \succ x_n$. Ismertetünk egy kétszemélyes játékot, amely felhasználható lesz véges $V \subseteq \mathbb{F}^n$ pontrendszerekhez tartozó $\mathrm{Sm}\,(I(V))$ lexikografikus standard monomok leírására. A karakterizációnak tárgyaljuk néhány egyszerű következményét, más fontos alkalmazásokat pedig a következő két fejezetre hagyunk. A játék természetéből következni fog, hogy a lex rendezéssel tekintett $\mathrm{Sm}\,(I(V))$ halmaz független V koordinátáinak konkrét értékétől és a V-t tartalmazó testtől; V kombinatorikus szerkezete önmagában meghatározza a lex standard monomokat.

3.1. A lex játék

Szabályok és jelölések

Legyen $V \subseteq \mathbb{F}^n$ nemüres véges pontrendszer és $\mathbf{w} = (w_1, \ldots, w_n) \in \mathbb{N}^n$. Ezen rögzített paraméterek mellett a $\mathrm{Lex}(V; \mathbf{w})$ játék a következő.

Az egyik játékos, Stan, gondol egy $\mathbf{y} = (y_1, \ldots, y_n) \in V$ pontra. A másik játékos, Lea feladata, hogy kitalálja $\mathbf{y}$ egy koordinátáját a következő szabályok szerint. Először y_n értékére tippelhet, legfeljebb w_n-szer. Amennyiben eltalálja, a játéknak vége, Lea nyert. Egyébként Stan elárulja y_n értékét. A következő körben Lea w_{n-1} alkalommal tippelhet y_{n-1}-re, és így tovább. A játéknak akkor van vége, ha Lea valamely y_i-re helyesen tippelt (ekkor Lea nyer), vagy ha végül y_1-et sem találta el Lea. Utóbbi esetben Stan a győztes. Fontos megjegyezni, hogy természetesen mindketten ismerik a szabályokat, azaz a V és $\mathbf{w}$ paramétereket.

Példa. Legyen $\alpha, \beta \in \mathbb{F}$, $n = 5$, és álljon V azon 5 hosszú α-β sorozatokból, amelyekben 1, 2, vagy 3 koordináta értéke α. A $\mathbf{w} = (1, 1, 1, 0, 0)$ kérdésvektorra van Leának nyerő stratégiája. Mivel $w_5 = w_4 = 0$, ezért a játék első két körében Stan egyszerűen elárulja y_5, majd y_4 értékét. Ezek után Lea egyszer tippelhet y_3-ra. A következő módon tud nyerni. Amennyiben $y_5 = y_4 = \beta$, akkor Lea tippeljen y_3, y_2 és y_1 értékére is α-t. Így biztosan nyer, hiszen $\mathbf{y}$ valamelyik eleme biztosan α. Amennyiben viszont y_5 és y_4 valamelyike α volt, akkor tippeljen mindháromszor β-ra. Megint csak nyerni fog, hiszen nem lehet, hogy $y_1 = y_2 = y_3 = \alpha$ legyen, mert akkor $\mathbf{y}$-nak már négy α koordinátája lenne.

Hasonlóan végiggondolható, hogy a $\mathbf{w} = (0, 1, 1, 1, 0)$ sorozatra viszont nincs Leának nyerő stratégiája, azaz bárhogyan is játszik, előfordulhat olyan $\mathbf{y}$, amire az adott stratégiával nem nyer.

Érdemes kiterjeszteni a játékot a $V = \emptyset$ esetre is, máskülönben bizonyos érveléseknél ezzel külön kellene foglalkozni. Később látni fogjuk, hogy az értelmes definíció az, hogy tetszőleges $\mathbf{w} \in \mathbb{N}^n$ kérdésvektor mellett a $\mathrm{Lex}(\emptyset; \mathbf{w})$ játék győztese Lea.

A játék rekurzív szerkezete miatt leginkább teljes indukcióval fogjuk tudni állításainkat bizonyítani. Emiatt célszerű bevezetni az alábbi jelöléseket. Ha $\beta \in \mathbb{F}$, akkor V-nek a β-ra végződő $n-1$ hosszú kezdőszeletei halmaza

$$V_\beta := \left\{(v_1, \ldots, v_{n-1}) \in \mathbb{F}^{n-1} \ : \ (v_1, \ldots, v_{n-1}, \beta) \in V\right\}.$$

Világos, hogy amennyiben Stan és Lea egy $\mathrm{Lex}(V; (w_1, \ldots, w_n))$ játékot kezdenek játszani és Leának nem sikerül kitalálnia y_n-et, akkor a játék úgy folytatódik, mintha éppen akkor kezdenének bele egy $\mathrm{Lex}(V_{y_n}; (w_1, \ldots, w_{n-1}))$ játékba. Általánosabban, $i > 1$ esetén $\beta_i, \beta_{i+1}, \ldots, \beta_n$ testelemekre legyen

$$V_{\beta_n \beta_{n-1} \ldots \beta_i} = \left\{(v_1, \ldots, v_{i-1}) \in \mathbb{F}^{i-1} \ : \ (v_1, \ldots, v_{i-1}, \beta_i, \ldots \beta_n) \in V\right\},$$

és így amennyiben Lea nem találta el y_n, y_{n-1}, $\ldots$, y_i egyikét sem, akkor valójában egy $\mathrm{Lex}(V_{y_n y_{n-1} \ldots y_i}; (w_1, \ldots, w_{i-1}))$ játékot játszanak tovább.

Legyen $\{\alpha_1, \ldots, \alpha_k\} \subseteq \mathbb{F}$ a V elemeinek koordinátáiban előforduló értékek halmaza. Ekkor természetesen

$$V \subseteq \{\alpha_1, \ldots, \alpha_k\}^n.$$

Nyugodtan feltehetjük, hogy Lea tippjei $\mathbf{y}$ koordinátáira az $\{\alpha_1, \ldots, \alpha_k\}$ halmazból kerülnek ki, hiszen értelmetlen volna mást választania, ha nyerni szeretne. Jelölje V^c a V pontrendszer $\{\alpha_1, \ldots, \alpha_k\}$-ban vett komplementerét, azaz legyen

$$V^c = \{\alpha_1, \ldots, \alpha_k\}^n \setminus V.$$

Nyerő stratégiák

A játékkal kapcsolatos fő kérdés, hogy mely rögzített paraméterek mellett van Leának nyerő stratégiája. A fejezet legfontosabb és egyben erre választ adó tételét a következő alfejezetben igazoljuk, előtte azonban a játékosok stratégiáira vonatkozó néhány egyszerűbb állítást tárgyalunk.

A játék elemzését megkönnyíti, ha használjuk a számítástudományból jól ismert *ellenség módszer*t (ld például [26] 5.3.2. fejezetét) Stan stratégiájának meghatározásához. A mi esetünkben ez azt jelenti, hogy megengedjük Stannek, hogy csaljon a játékban, mindaddig, amíg ezt Lea nem tudja meg. Pontosabban, feltesszük, hogy Stan valójában nem is rögzít egy $\mathbf{y} \in V$ elemet, hanem egyszerűen egészen addig állítja Leának, hogy rosszul tippelt, amíg van olyan $\mathbf{y} \in V$, amivel az addigi válaszai mind konzisztensek. Van tehát értelme arról beszélni, hogy a játékban Stannek van nyerő stratégiája.

3.1. Lemma. *Ha $n > 1$, akkor Stannek pontosan akkor van nyerő stratégiája a* $\mathrm{Lex}(V; (w_1, \ldots, w_{n-1}, w_n))$ *játékban, ha van legalább* $w_n + 1$ *olyan* $\beta \in \{\alpha_1, \ldots, \alpha_k\}$, *amelyre van nyerő stratégiája* $\mathrm{Lex}(V_\beta; (w_1, \ldots, w_{n-1}))$*-ben. Hasonlóan, $n > 1$ esetén Leának pontosan akkor nincs nyerő stratégiája a* $\mathrm{Lex}(V; (w_1, \ldots, w_{n-1}, w_n))$ *játékban, ha létezik legalább* $w_n + 1$ *olyan* $\beta \in \{\alpha_1, \ldots, \alpha_k\}$, *amelyre nincs nyerő stratégiája* $\mathrm{Lex}(V_\beta; (w_1, \ldots, w_{n-1}))$*-ben.*

Bizonyítás: Tegyük fel, hogy van w_n+1 olyan $\beta \in \{\alpha_1, \ldots, \alpha_k\}$, amelyre Stannek van nyerő stratégiája a $\mathrm{Lex}(V_\beta; (w_1, \ldots, w_{n-1}))$ játékban. Ekkor $\mathrm{Lex}(V; (w_1, \ldots, w_{n-1}, w_n))$-ben nyerő stratégia számára, ha Lea minden tippjére nemmel válaszol, majd azt állítja, hogy $y_n = \beta$ egy olyan β-ra, amelyre Lea nem kérdezett, de Stannek van nyerő stratégiája $\mathrm{Lex}(V_\beta; (w_1, \ldots, w_{n-1}))$-ben. Mivel Lea w_n-szer tippelhetett, ilyen β a feltétel szerint létezik.

Megfordítva, tegyük fel, hogy legfeljebb w_n olyan $\beta \in \{\alpha_1, \ldots, \alpha_k\}$ létezik, amelyre $\mathrm{Lex}(V_\beta; (w_1, \ldots, w_{n-1}))$-ben Stannek van nyerő stratégiája. Amennyiben Lea az összes ilyen β-ra tippel egyet, akkor Stannek vagy igennel kell felelnie, vagy $y_n = \beta$-t kell válaszolnia egy olyan másik $\beta \in \{\alpha_1, \ldots, \alpha_k\}$-ra, amelyre nincs nyerő stratégiája a maradék $\mathrm{Lex}(V_\beta; (w_1, \ldots, w_{n-1}))$ játékban. Ez viszont azt jelenti, hogy $\mathrm{Lex}(V; (w_1, \ldots, w_{n-1}, w_n))$-ben sem biztos, hogy tud nyerni.

A második állítás teljesen hasonlóan igazolható. □

Az alábbi következményben igazoljuk, hogy a két játékos valamelyikének mindenképpen van nyerő stratégiája. Más szóval, a játék paraméterei előre meghatározzák, hogy ki nyeri meg a játékot, feltéve, hogy mindkét játékos a lehető legjobban játszik. Mi élni fogunk ezzel a feltevéssel, és ezért a következő alfejezettől kezdve ahelyett, hogy nyerő stratégiáról beszélnénk, egyszerűen azt mondjuk, hogy a $\mathrm{Lex}(V; \mathbf{w})$ játékban Lea illetve Stan nyer.

3.2. Következmény. *Stannek pontosan akkor van nyerő stratégiája, ha Leának nincs.*

Bizonyítás: Az állítást n-re vonatkozó teljes indukcióval igazoljuk. Az indukciós lépést megadja a 3.1. lemma, míg az $n = 1$ eset a játék definíciója alapján triviális. □

3.2. Ki nyeri a lex játékot?

A következő két tétel teremt kapcsolatot a lex játék és a valójában vizsgálni kívánt lexikografikus vezető tagok és standard monomok között.

3.3. Tétel. *Legyen $V \subseteq \mathbb{F}^n$ véges pontrendszer és $\mathbf{w} \in \mathbb{N}^n$. Ekkor Lea pontosan akkor nyeri meg a* $\mathrm{Lex}(V; \mathbf{w})$ *játékot, ha $\mathbf{x}^{\mathbf{w}} \in \mathrm{Lm}\,(I(V))$.*

A 3.2. következmény alapján a 3.3. tétel ekvivalens az alábbival

3.4. Tétel. *Stan akkor és csak akkor nyer a* $\mathrm{Lex}(V;\mathbf{w})$ *játékban, ha* $\mathbf{x}^{\mathbf{w}} \in \mathrm{Sm}\,(I(V))$.

Példa. Az előző alfejezet példájában láttuk, hogy amennyiben V az 5 hosszú α-β sorozatok közül azokat tartalmazza, amelyekben 1, 2, vagy 3 koordináta α, úgy a $\mathrm{Lex}(V;(1,1,1,0,0))$ játékot Lea nyeri, míg $\mathrm{Lex}(V;(0,1,1,1,0))$-ban Stan a győztes. Ez a 3.3. illetve 3.4. tételek fényében azt jelenti, hogy $x_1x_2x_3$ vezető tag, míg $x_2x_3x_4$ standard monomja az $I(V)$ ideálnak.

3.3. tétel bizonyítása, első rész: Ha Lea megnyeri a $\mathrm{Lex}(V;\mathbf{w})$ játékot, akkor $\mathbf{x}^{\mathbf{w}} \in \mathrm{Lm}\,(I(V))$.

Miután $x_1,\ldots,x_n$ minden monomja benne van $\mathrm{Lm}\,(I(\emptyset))$-ban, ezért az állítás ezen esetre triviális. Tegyük fel a továbbiakban, hogy $V \neq \emptyset$.

Legyen $f_{j,1}$, $f_{j,2}$, …, f_{j,w_j} Lea nyerő stratégiája szerinti tippjei y_j értékére $(j = 1,2,\ldots,n)$. Amikor Lea megpróbálja kitalálni y_j-t, akkor már ismeri az $y_{j+1}, y_{j+2}, \ldots, y_n$ értékeket, így $f_{j,i}$ valójában $n-j$ változós függvény, amelynek változói $x_{j+1}, x_{j+2}, \ldots, x_n$. Világos, hogy $f_{j,i}$ értelmezési tartománya véges, hiszen $(y_{j+1}, y_{j+2}, \ldots, y_n)$ a zárószelete valamely $\mathbf{y} \in V$-nek és V a feltétel szerint véges. Emiatt az $f_{j,i}$ függvény reprezentálható polinommal. Az egyszerűség kedvéért tegyük fel, hogy maga $f_{j,i}(x_{j+1}, x_{j+2}, \ldots, x_n)$ is $\mathbb{F}$ feletti polinom. Tekintsük az alábbi $l(\mathbf{x}) \in \mathbb{F}\,[\mathbf{x}]$-et.

$$l(\mathbf{x}) = l(x_1,\ldots,x_n) := \left(\prod_{i=1}^{w_n}(x_n - f_{n,i})\right)\cdot\left(\prod_{i=1}^{w_{n-1}}(x_{n-1} - f_{n-1,i}(x_n))\right)\ldots$$
$$\left(\prod_{i=1}^{w_j}(x_j - f_{j,i}(x_{j+1}, x_{j+2}, \ldots, x_n))\right)\ldots\left(\prod_{i=1}^{w_1}(x_1 - f_{1,i}(x_2,\ldots,x_n))\right) \quad (2)$$

Először is, $l(\mathbf{x})$ eltűnik V-n, hiszen minden $\mathbf{y} \in V$-re Lea eltalálja az egyik y_j koordinátát, tehát a megfelelő $x_j - f_{j,i}(x_{j+1}, x_{j+2}, \ldots, x_n)$ tényező eltűnik $\mathbf{y}$-on. Ezek szerint $l(\mathbf{x}) \in I(V)$.

Másrészt $f_{j,i}$ nem függ $x_1,\ldots,x_j$-től, emiatt – kihasználva a lexikografikus rendezés tulajdonságait – $x_j - f_{j,i}(x_{j+1}, x_{j+2}, \ldots, x_n)$ főtagja x_j, tehát

$$\mathrm{lm}\left(\prod_{i=1}^{w_j}(x_j - f_{j,i}(x_{j+1}, x_{j+2}, \ldots, x_n))\right) = x_j^{w_j},$$

és így $\mathrm{lm}\,(l(\mathbf{x})) = \mathbf{x}^{\mathbf{w}}$. Ezt összevetve $l(\mathbf{x}) \in I(V)$-vel, kapjuk, hogy $\mathbf{x}^{\mathbf{w}} \in \mathrm{Lm}\,(I(V))$, amint állítottuk.

A fordított irány igazolásához szükségünk van egy egyszerű lemmára.

3.5. Lemma. *Legyen $n > 1$, $l(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$, amely vezető tagja $\mathbf{x}^{\mathbf{w}}$. Ekkor léteznek olyan $g \in \mathbb{F}[x_n]$ és $h \in \mathbb{F}[\mathbf{x}]$ polinomok, amelyekre teljesül, hogy* $\deg g = w_n$, *h minden monomja kisebb, mint $x_1^{w_1} \dots x_{n-1}^{w_{n-1}}$ és*

$$l(x_1, \dots, x_n) = x_1^{w_1} \dots x_{n-1}^{w_{n-1}} g(x_n) + h(x_1, \dots, x_n).$$

Bizonyítás: Gyűjtsük össze $l(\mathbf{x})$ minden olyan monomját, amelyben $j = 1, \dots, n-1$-re x_j kitevője w_j. Ezzel megkapjuk a felbontás $x_1^{w_1} \dots x_{n-1}^{w_{n-1}} g(x_n)$ tagját. Nyilván $\deg g = w_n$, miután az ebben a részben szereplő monomok között a rendezést éppen x_n kitevője határozza meg, és tudjuk, hogy a legnagyobb monom (ezek között is) $\mathbf{x}^{\mathbf{w}} = x_1^{w_1} \dots x_{n-1}^{w_{n-1}} x_n^{w_n}$.

Legyen $h(\mathbf{x}) = l(\mathbf{x}) - x_1^{w_1} \dots x_{n-1}^{w_{n-1}} g(x_n)$ és h kívánt tulajdonságának igazolása érdekében tegyük fel, hogy $\mathbf{x}^{\mathbf{u}}$ egy $l(\mathbf{x})$-ben szereplő monom.

Amennyiben $\mathbf{x}^{\mathbf{u}} \succeq x_1^{w_1} \dots x_{n-1}^{w_{n-1}}$, akkor $u_j = w_j$ minden $j = 1, \dots, n-1$-re, mert máskülönben $\mathbf{x}^{\mathbf{u}} \succ \mathbf{x}^{\mathbf{w}}$ lenne, a lexikografikus rendezés definíciója alapján. De ez azt jelenti, hogy $\mathbf{x}^{\mathbf{u}}$ az $x_1^{w_1} \dots x_{n-1}^{w_{n-1}} g(x_n)$ részhez tartozik. Ezzel állításunkat bebizonyítottuk. □

3.3. tétel bizonyítása, második rész: Ha $\mathbf{x}^{\mathbf{w}} \in \mathrm{Lm}\,(I(V))$, akkor Lea nyeri a $\mathrm{Lex}(V; \mathbf{w})$ játékot.

A $V = \emptyset$ eset megint triviális, feltehetjük tehát az ellenkezőjét.

Az állítást n-re vonatkozó indukcióval fogjuk belátni.

Ha $n = 1$, akkor $x^w \in \mathrm{Sm}\,(I(V)) \iff w < |V|$, felhasználva, hogy $\mathrm{Sm}\,(I(V))$ az oszthatóságra nézve leszálló és hogy $|V| = |\mathrm{Sm}\,(I(V))|$. Ezek szerint tehát Lea legalább $|V|$-szor tippelhet y értékére, ami nyilván elég ahhoz, hogy nyerjen.

Tegyük fel, hogy az állítás igaz $n-1$-re. Legyen $V \subseteq \mathbb{F}^n$ és $l(\mathbf{x}) \in I(V)$ polinom, amely vezető tagja $\mathbf{x}^{\mathbf{w}}$. Legyen továbbá g és h a 3.5. lemma szerint létező polinom és

$$\hat{l}(x_1, \dots, x_{n-1}) := l(x_1, \dots, x_{n-1}, \beta),$$

ahol $\beta \in \mathbb{F}$ tetszőleges. Ha $g(\beta) \neq 0$, akkor a 3.5. lemma szerinti h-ra tett feltevésből következik, hogy $\hat{l}$ főtagja $x_1^{w_1} \dots x_{n-1}^{w_{n-1}}$. Miután l eltűnik V-n, nyilvánvaló, hogy $\hat{l}$ eltűnik V_β-n. Ez azt jelenti, hogy $x_1^{w_1} \dots x_{n-1}^{w_{n-1}} \in \mathrm{Lm}\,(I\,(V_\beta))$, ezért az indukciós feltevés szerint Lea nyer a $\mathrm{Lex}(V_\beta; (w_1, \dots, w_{n-1}))$ játékban.

Ezek után Lea a következő stratégiával nyerheti meg $\mathrm{Lex}(V, \mathbf{w})$-t. Mivel $\deg g = w_n$, így g-nek legfeljebb w_n gyöke van $\mathbb{F}$-ben. Ha Lea először ezekre tippel, akkor – amennyiben nem találta el az utolsó koordináta értékét – Stan csak olyan β értéket mondhat y_n-re, amire $g(\beta) \neq 0$. Az előző bekezdés szerinti érveléssel viszont a maradék $\mathrm{Lex}(V_\beta; (w_1, \dots, w_{n-1}))$ játékban ilyenkor Lea lesz a győztes. Vegyük észre, hogy az érvelés érvényes akkor is, ha

$w_n = 0$. A 3.3. tétel – és így az ekvivalens 3.4. tétel – bizonyítása készen van. □

A bizonyításban szereplő (2) polinom bizonyos értelemben kódolja Lea stratégiáját. Következő állításunk ezzel analóg, konstruálunk benne egy polinomot, ami Stan stratégiáját írja le. A polinom bizonyítékul fog szolgálni arra, hogy ha Stan nyeri a $\mathrm{Lex}(V;\mathbf{w})$ játékot, akkor $x_1^{k-1-w_1}\dots x_n^{k-1-w_n} \in \mathrm{Lm}\,(I(V^c))$. A következő alfejezetben egyébként igazoljuk, hogy utóbbi ekvivalens $x_1^{w_1}\dots x_n^{w_n} \in \mathrm{Sm}\,(I(V))$-vel.

3.6. Állítás. *Ha Stan nyeri a* $\mathrm{Lex}(V;\mathbf{w})$ *játékot, akkor* $x_1^{k-1-w_1}\dots x_n^{k-1-w_n} \in \mathrm{Lm}\,(I(V^c))$

Bizonyítás: Legyen $f_{j,1},\ f_{j,2},\ \dots,\ f_{j,w_j+1}$ Stan lehetséges válaszai közül néhány, amikor el kell árulja Leának y_j értékét. Világos, hogy ilyenből legalább w_j+1 különböző van, hiszen egyébként Lea tudna nyerni a játék j. körében, úgy, hogy rákérdez az összes lehetőségre. Amikor Lea y_j értékére tippel, akkor $y_{j+1}, y_{j+2}, \dots, y_n$ már mindkét játékos számára ismert, tehát $f_{j,i} = f_{j,i}(x_{j+1}, x_{j+2}, \dots, x_n)$ valójában $n-j$ változótól függő függvény. Rögzített j-re legyen

$$\left\{g_{j,1}, g_{j,2}, \dots, g_{j,k-1-w_j}\right\} = \left\{f_{j,1}, f_{j,2}, \dots, f_{j,w_j+1}\right\}^c.$$

Minden $g_{j,i} = g_{j,i}(x_{j+1}, x_{j+2}, \dots, x_n)$ ismét függvény, amelynek értelmezési tartománya ráadásul véges, mivel V-nek $n-j$ hosszú zárószeletei halmazán értelmezett. Emiatt van olyan polinom, ami függvényként tekintve $g_{j,i}$-vel megegyezik, tegyük tehát fel, hogy $g_{j,i}(x_{j+1}, x_{j+2}\dots x_n)$ eleve polinom.

A Stan stratégiáját kódoló polinom ezek után a következő:

$$s(\mathbf{x}) = s(x_1,\dots,x_n) := \left(\prod_{i=1}^{k-1-w_n}(x_n - g_{n,i})\right)\cdot\left(\prod_{i=1}^{k-1-w_{n-1}}(x_{n-1} - g_{n-1,i}(x_n))\right)\cdots$$
$$\left(\prod_{i=1}^{k-1-w_j}(x_j - g_{j,i}(x_{j+1},\dots,x_n))\right)\cdots\left(\prod_{i=1}^{k-1-w_1}(x_1 - g_{1,i}(x_2,\dots,x_n))\right). \quad (3)$$

Látható, hogy $s(\mathbf{x})$ vezető tagja $x_1^{k-1-w_1}\dots x_n^{k-1-w_n}$. Az $s(\mathbf{x}) \in I(V^c)$ állítás igazolásához tegyük fel, hogy $s(\mathbf{y}) \neq 0$ valamely $\mathbf{y} \in \{\alpha_1,\dots,\alpha_k\}^n$-re. Ekkor $s(\mathbf{x})$ és $g_{j,i}$ definíciója miatt világos, hogy minden j-re létezik i_j, amelyre $y_j = f_{j,i_j}(y_{j+1},\dots,y_n)$. Ez azt jelenti, hogy $\mathbf{y}$ egy Stan számára egy lehetséges választás, tehát $\mathbf{y} \in V$. Beláttuk ezzel, hogy $s(\mathbf{x})$ eltűnik $I(V^c)$-en, amiből következik $\mathrm{lm}\,(s) = x_1^{k-1-w_1}\dots x_n^{k-1-w_n} \in \mathrm{Lm}\,(I(V^c))$. □

A 3.6. állítás fenti bizonyítása a 3.3. tétel bizonyításának első részével teljesen analóg módon ment. Most a 3.3. tétel bizonyításának második részét utánozva mutatunk egy tanulságos közvetlen bizonyítást a 3.4. tétel egyik irányára.

3.7. Állítás. *Ha* $\mathbf{x}^{\mathbf{w}} \in \mathrm{Sm}\,(I(V))$ *akkor Stan nyer a* $\mathrm{Lex}(V;\mathbf{w})$ *játékban.*

Bizonyítás: Teljes indukciót használunk n-re.

Az $n = 1$ eset egyszerű, hiszen $x^w \in \mathrm{Sm}\,(I(V))$-ből következik $|V| > w$, és így Stan nyugodtan felelhet nemmel Lea mind a w tippjére.

Tegyük most fel, hogy $n > 1$. Legyen

$$Y = \left\{\beta \in \{\alpha_1, \ldots, \alpha_k\} \,:\, x_1^{w_1} \ldots x_{n-1}^{w_{n-1}} \in \mathrm{Sm}\,(I(V_\beta))\right\}.$$

Azt állítjuk, hogy $|Y| > w_n$. Ha ez igaz, akkor Stan a következő egyszerű stratégiával tud nyerni. Nemmel felel Lea w_n tippjére, majd választ egy olyan $\beta \in Y$-t, amely nem volt Lea tippjei között és azt mondja, hogy $y_n = \beta$. Miután $|Y| > w_n$, biztosan létezik is ilyen β. Definíció szerint $x_1^{w_1} \ldots x_{n-1}^{w_{n-1}} \in \mathrm{Sm}\,(I(V_\beta))$, ezért az indukciós feltevés alapján Stan nyer a $\mathrm{Lex}(V_\beta; (w_1, \ldots, w_{n-1}))$ játékban.

Igazolnunk kell tehát, hogy $|Y| > w_n$. Elegendő ehhez megmutatni, hogy $x_1^{w_1} \ldots x_{n-1}^{w_{n-1}} x_n^{|Y|} \in \mathrm{Lm}\,(I(V))$, miután $\mathrm{Sm}\,(I(V))$ az oszthatóságra nézve leszálló, és $x_1^{w_1} \ldots x_{n-1}^{w_{n-1}} x_n^{w_n} \in \mathrm{Sm}\,(I(V))$.

Minden $\beta \in \{\alpha_1, \ldots, \alpha_k\} \setminus Y$-ra van olyan $f_\beta(x_1, \ldots, x_{n-1})$ polinom, amelyre $x_1^{w_1} \ldots x_{n-1}^{w_{n-1}} + f_\beta(x_1, \ldots, x_{n-1})$ eltűnik V_β-n és f_β minden monomja kisebb, mint $x_1^{w_1} \ldots x_{n-1}^{w_{n-1}}$. Legyen

$$f(x_1, \ldots, x_n) := \sum_{\beta \in \{\alpha_1, \ldots, \alpha_k\} \setminus Y} \chi_\beta(x_n) f_\beta(x_1, \ldots, x_{n-1}),$$

ahol $\chi_\beta(x_n)$ a β karakterisztikus függvényének egy polinom reprezentációja, azaz $\{\alpha_1, \ldots, \alpha_k\}\setminus\{\beta\}$-n eltűnő polinom, amelyre teljesül még $\chi_\beta(\beta) = 1$. Világos, hogy $f(x_1, \ldots, x_{n-1}, \beta) = f_\beta(x_1, \ldots, x_{n-1})$ minden $\beta \in \{\alpha_1, \ldots, \alpha_k\}\setminus Y$ esetén. A lexikografikus rendezés tulajdonságai miatt f minden monomja kisebb, mint $x_1^{w_1} \ldots x_{n-1}^{w_{n-1}}$.

Ezekből azonnal következik, hogy

$$s(\mathbf{x}) = \left(x_1^{w_1} \ldots x_{n-1}^{w_{n-1}} + f(\mathbf{x})\right) \prod_{\beta \in Y} (x_n - \beta)$$

eltűnik V-n és hogy $\mathrm{lm}\,(s(\mathbf{x})) = x_1^{w_1} \ldots x_{n-1}^{w_{n-1}} x_n^{|Y|} \in \mathrm{Lm}\,(I(V))$. □

3.3. Lex standard monomok kombinatorikus tulajdonságai

A 3.4. tételnek az alábbiakban ismertetjük néhány egyszerű következményét. Az első közülük azt állítja, hogy a $V \subseteq \mathbb{F}^n$ véges pontrendszerhez tartozó lexikografikus standard monomok nagyban függetlenek $\mathbb{F}$-től, illetve V „elhelyezkedésétől" $\mathbb{F}$-en belül.

3.8. Következmény. *Legyen $\hat{\mathbb{F}}$ tetszőleges test és tegyük fel, hogy adottak $\varphi_j : \{\alpha_1, \ldots, \alpha_k\} \to \hat{\mathbb{F}}$ injektív függvények $j = 1, 2, \ldots, n$-re. Legyen $\hat{V} \subseteq \hat{\mathbb{F}}$ a V képe, azaz*

$$\hat{V} = \{(\varphi_1(v_1), \ldots, \varphi_n(v_n)) \ : \ (v_1, \ldots, v_n) \in V\}.$$

Ekkor a V-hez tartozó lex standard monomok $\mathbb{F}[\mathbf{x}]$-ben ugyanazok, mint a $\hat{V}$-hoz tartozóak $\hat{\mathbb{F}}[\mathbf{x}]$-ben. Speciálisan, ha $V \subseteq \{0,1\}^n$, akkor $\mathrm{Sm}\,(I(V))$ minden $\mathbb{F}$ test felett azonos.

Bizonyítás: A $\mathrm{Lex}(V; \mathbf{w})$ játék ugyanaz, mint a $\mathrm{Lex}(\hat{V}; \mathbf{w})$, hiszen csak a koordinátaértékek neveit cseréltük fel (egy-egyértelműen). A második rész pedig tényleg az első speciális esete, hiszen $0, 1 \in \mathbb{F}$ minden $\mathbb{F}$ testre. □

A következmény $V \subseteq \{0,1\}^n$-re vonatkozó részét más módszerrel igazolta Anstee, Sali és Rónyai [2]. Most megmutatjuk, hogy a $V \subseteq \{0,1\}^n$ pontrendszerhez tartozó lexikografikus redukált Gröbner-bázis lényegében ugyanaz minden test felett. Ez szintén ismert eredmény (Friedl és Rónyai [17]), de szorosan kapcsolódik az előbbihez, továbbá használni is fogjuk, ezért itt is közöljük bizonyítását.

Jelöljük ezen következményben az $\mathbb{F}$ test feletti polinomgyűrűben tekintett $I(V)$ ideált $I_{\mathbb{F}}(V)$-vel. Ha $f \in \mathbb{Z}[\mathbf{x}]$, akkor minden 0 karakterisztikájú $\mathbb{F}$ testre természetesen $f \in \mathbb{F}[\mathbf{x}]$, továbbá tetszőleges $p > 0$ karakterisztika esetén is tekinthető f az $\mathbb{F}[\mathbf{x}]$ elemének, amennyiben f egész együtthatóit redukáljuk modulo p.

3.9. Következmény. *Ha $V \subseteq \{0,1\}^n$, akkor az $I_{\mathbb{Q}}(V)$ ideál G redukált lex Gröbner-bázisa egész együtthatós. Tetszőleges $\mathbb{F}$ test esetén a G polinomhalmaz $\mathbb{F}[\mathbf{x}]$-beli megfelelője redukált Gröbner-bázisa $I_{\mathbb{F}}(V)$ ideálnak.*

Bizonyítás: Legyen a $\mathbb{Q}$ feletti G redukált Gröbner-bázis egy eleme $\mathbf{x}^{\mathbf{w}} + g(\mathbf{x})$, ahol $g \in \mathbb{Q}[\mathbf{x}]$ minden monomja kisebb, mint $\mathbf{x}^{\mathbf{w}}$ és tegyük fel indirekte, hogy $g \notin \mathbb{Z}[\mathbf{x}]$.

Legyen $z \in \mathbb{Z}$ olyan, amelyre $zg(\mathbf{x})$ együtthatói egészek, amelyeknek nincs 1-nél nagyobb közös osztójuk. Ha p prím z egy osztója, akkor tekintsük a $zg \in \mathbb{Z}[\mathbf{x}]$ polinomnak az $\mathbb{F}_p$ testbeli redukáltját. Nyilvánvalóan ez olyan nem

azonosan nulla polinom, amely (modulo p) eltűnik V-n, ugyanis $z\mathbf{x}^{\mathbf{w}} + zg(\mathbf{x})$ eltűnik V-n, de $z \equiv 0 \pmod{p}$. Ezek szerint $zg(\mathbf{x})$ főtagja $\mathrm{Lm}\left(I_{\mathbb{F}_p}(V)\right) = \mathrm{Lm}\left(I_{\mathbb{Q}}(V)\right)$-ben van. Utóbbi egyenlőség a 3.8. következmény alapján igaz. Ez viszont azt jelenti, hogy g egy monomja vezető tag $I_{\mathbb{Q}}(V)$-re, ellentmondásban azzal, hogy $\mathbf{x}^{\mathbf{w}} + g(\mathbf{x})$ a redukált Gröbner-bázis eleme. Megmutattuk tehát, hogy $G \subseteq \mathbb{Z}[\mathbf{x}]$.

Legyen $\mathbb{F}$ most tetszőleges test és tekintsük G-t $\mathbb{F}[\mathbf{x}]$ részhalmazaként. Nyilván így is $G \subseteq I_{\mathbb{F}}(V)$ és a főtagok változatlanok. Miután G elemei vezető tagjuktól eltekintve standard monomok $\mathbb{F}$-lineáris kombinációi, ezért G az $I_{\mathbb{F}}(V)$ ideálnak is redukált Gröbner-bázisa. □

Most újrafogalmazzuk a 3.1. lemmát. Ez a következmény a későbbiekben döntő szerepet fog kapni, és úgy is fogunk állítására hivatkozni, mint a lex standard monomok rekurzív tulajdonsága.

3.10. Következmény. ($\mathrm{Sm}\left(I(V)\right)$ és $\mathrm{Lm}\left(I(V)\right)$ rekurzív tulajdonsága)

(i) Ha $n > 1$, akkor $\mathbf{x}^{\mathbf{w}} \in \mathrm{Sm}\left(I(V)\right)$ pontosan akkor teljesül, ha van legalább $w_n + 1$ olyan $\beta \in \{\alpha_1, \ldots, \alpha_k\}$, amelyre $x_1^{w_1} \ldots x_{n-1}^{w_{n-1}} \in \mathrm{Sm}\left(I(V_\beta)\right)$.

(ii) Ha $n > 1$, akkor $\mathbf{x}^{\mathbf{w}} \in \mathrm{Lm}\left(I(V)\right)$ akkor és csak akkor, ha létezik legalább $k - w_n$ olyan $\beta \in \{\alpha_1, \ldots, \alpha_k\}$, amelyre fennáll $x_1^{w_1} \ldots x_{n-1}^{w_{n-1}} \in \mathrm{Lm}\left(I(V_\beta)\right)$.

Bizonyítás: (i) nyilvánvaló a 3.1. lemma és 3.4. tétel miatt.
(ii) bizonyításához tekintsük a következő állításokat.

1. $\mathbf{x}^{\mathbf{w}} \in \mathrm{Lm}\left(I(V)\right)$;
2. $\mathbf{x}^{\mathbf{w}} \notin \mathrm{Sm}\left(I(V)\right)$;
3. Legfeljebb w_n olyan $\beta \in \{\alpha_1, \ldots, \alpha_k\}$ létezik, amelyre $x_1^{w_1} \ldots x_{n-1}^{w_{n-1}} \in \mathrm{Sm}\left(I(V_\beta)\right)$;
4. Létezik legalább $k - w_n$ olyan $\beta \in \{\alpha_1, \ldots, \alpha_k\}$, amelyre $x_1^{w_1} \ldots x_{n-1}^{w_{n-1}} \notin \mathrm{Sm}\left(I(V_\beta)\right)$;
5. Létezik legalább $k - w_n$ olyan $\beta \in \{\alpha_1, \ldots, \alpha_k\}$, amelyre $x_1^{w_1} \ldots x_{n-1}^{w_{n-1}} \in \mathrm{Lm}\left(I(V_\beta)\right)$;

Felhasználva jelen következmény (i) pontját is, könnyű látni, hogy ezek ekvivalensek. □

Az alábbi következmény leírja V^c főtagjait és standard monomjait.

3.11. Következmény. *Tetszőleges $\mathbf{x}^{\mathbf{w}}$-re igaz, hogy $x_1^{w_1} \ldots x_n^{w_n} \in \mathrm{Sm}\left(I(V)\right)$ akkor és csak akkor, ha $x_1^{k-1-w_1} \ldots x_n^{k-1-w_n} \in \mathrm{Lm}\left(I(V^c)\right)$.*

Bizonyítás: n-re vonatkozó indukcióval bizonyítunk.

Az $n = 1$ eset világos, hiszen $x^w \in \mathrm{Sm}\,(I(V)) \iff w < |V| \iff k-1-w > k-1-|V| \iff k-1-w \geq |V^c| \iff x^{k-1-w} \in \mathrm{Lm}\,(I(V^c))$.

Tegyük fel, hogy $n > 1$ és hogy az állítás igaz $n-1$-re. Miután minden $\beta \in \{\alpha_1, \ldots, \alpha_k\}$ esetén

$$(V_\beta)^c = \left\{(v_1, \ldots, v_{n-1}) \in \{\alpha_1, \ldots, \alpha_k\}^{n-1} \,:\, (v_1, \ldots, v_{n-1}, \beta) \notin V\right\} = (V^c)_\beta\,,$$

ezért írhatunk egyszerűen V^c_β-t.

A 3.10. következmény (i) pontja szerint $x_1^{w_1} \ldots x_n^{w_n} \in \mathrm{Sm}\,(I(V))$ azzal ekvivalens, hogy létezik $w_n + 1$ olyan $\beta \in \{\alpha_1, \ldots, \alpha_k\}$, amelyre $x_1^{w_1} \ldots x_{n-1}^{w_{n-1}} \in \mathrm{Sm}\,(I(V_\beta))$. Az indukciós feltétel szerint ez pontosan akkor teljesül, ha van $w_n + 1$ olyan $\beta \in \{\alpha_1, \ldots, \alpha_k\}$, amelyre $x_1^{k-1-w_1} \ldots x_{n-1}^{k-1-w_{n-1}} \in \mathrm{Lm}\left(I(V^c_\beta)\right)$. Végül alkalmazva a 3.10. következmény (ii) részét ($k-1-w_n$-et írva w_n helyébe), azt kapjuk, hogy a fenti akkor és csak akkor áll fent, ha igaz $x_1^{k-1-w_1} \ldots x_n^{k-1-w_n} \in \mathrm{Lm}\,(I(V^c))$. Állításunkat beláttuk. □

Ha $\mathbf{x}^\mathbf{w} \in \mathrm{Lm}\,(I(V))$, akkor ezt tudjuk „bizonyítani" egyetlen polinommal, nevezetesen egy olyan $f(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$-szel, amely eltűnik V-n és vezető tagja éppen $\mathbf{x}^\mathbf{w}$. A 3.11. következmény azt is mutatja, hogy $\mathbf{x}^\mathbf{w} \in \mathrm{Sm}\,(I(V))$-nek is létezik hasonló bizonyítéka, nevezetesen egy olyan $f(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$ polinom, amely V^c-en eltűnik és főtagja $x_1^{k-1-w_1} \ldots x_n^{k-1-w_n}$.

3.4. Általánosítás eliminációs rendezésre

A standard monomok rekurzív szerkezetére vonatkozó állítás igazolható a játék segítsége nélkül is. Ebben a fejezetben mutatunk egy bizonyítást, ami ráadásul a fenti eset általánosítása, lexikografikus rendezés helyett ugyanis más rendezéseket is tekinthetünk. Megmutatjuk, hogy amennyiben a változókat két csoportra osztva a tagsorrend eleget tesz egy bizonyos feltételnek – ez lép a lexikografikus rendezésnél látott tulajdonság helyébe –, akkor a standard monomok meghatározhatók úgy, hogy a két változócsoportra és alkalmasan választott pontrendszerekre külön-külön számoljuk a standard monomokat.

Legyenek $\mathbf{x} = (x_1, \ldots, x_n)$ és $\mathbf{y} = (y_1, \ldots, y_m)$ változók, és tegyük fel, hogy adottak $\prec_x$ és $\prec_y$ – a megfelelő $\mathbb{F}[\mathbf{x}]$ illetve $\mathbb{F}[\mathbf{y}]$ polinomgyűrű monomjain – tetszőleges tagsorrendek. Definiálunk $\mathbb{F}[x_1, \ldots, x_n, y_1, \ldots, y_m] = \mathbb{F}[\mathbf{x}, \mathbf{y}]$ monomjain egy $\prec$ tagsorrendet. Pontosan akkor legyen $\mathbf{x}^{\mathbf{w_1}}\mathbf{y}^{\mathbf{u_1}} \prec \mathbf{x}^{\mathbf{w_2}}\mathbf{y}^{\mathbf{u_2}}$, ha $\mathbf{x}^{\mathbf{w_1}} \prec_x \mathbf{x}^{\mathbf{w_2}}$, vagy $\mathbf{x}^{\mathbf{w_1}} = \mathbf{x}^{\mathbf{w_2}}$ és $\mathbf{y}^{\mathbf{u_1}} \prec_y \mathbf{y}^{\mathbf{u_2}}$. Ekkor $\prec$ az $\mathbf{x}, \mathbf{y}$ *változók egy eliminációs rendezése, amelyben* $\mathbf{x}$*-ek nagyobbak* $\mathbf{y}$*-oknál.*

Nyilvánvaló, hogy az $x_1, \ldots, x_n$ változók lexikografikus rendezése bármely $x_1, \ldots, x_i$ és $x_{i+1}, \ldots, x_n$ csoportba osztással teljesíti a fenti feltételt, úgy, hogy az $x_1, \ldots, x_i$ változók nagyobbak az $x_{i+1}, \ldots, x_n$-eknél.

Az alábbi tétel a standard monomok rekurzív szerkezetére vonatkozó 3.10. következmény általánosítása. Vegyük észre, hogy a bizonyítás a játékról szóló főtétel (3.3. tétel és 3.7. állítások) bizonyításainak általánosítása.

3.12. Tétel. *Rögzítsük az* $x_1, \ldots, x_n, y_1, \ldots, y_m$ *változók egy eliminációs rendezését, amelyben az* $\mathbf{x}$*-ek nagyobbak az* $\mathbf{y}$ *változóknál. Legyen* $\mathbf{w} \in \mathbb{N}^n$ *és* $\mathbf{u} \in \mathbb{N}^m$ *kitevővektorok és* $V \subseteq \{\alpha_1, \ldots, \alpha_k\}^{n+m}$ *véges. Ekkor*

$$\mathbf{x}^{\mathbf{w}}\mathbf{y}^{\mathbf{u}} \in \mathrm{Sm}\,(I(V)) \iff \mathbf{y}^{\mathbf{u}} \in \mathrm{Sm}\,(I(Y))\,,$$

ahol

$$Y := \left\{(\beta_1, \ldots, \beta_m) \in \{\alpha_1, \ldots, \alpha_k\}^m \,:\, \mathbf{x}^{\mathbf{w}} \in \mathrm{Sm}\left(I(V_{\beta_m\beta_{m-1}\ldots\beta_1})\right)\right\},$$

$I(V_{\beta_m\beta_{m-1}\ldots\beta_1}) \subseteq \mathbb{F}[\mathbf{x}]$ *és* $I(Y) \subseteq \mathbb{F}[\mathbf{y}]$.

Bizonyítás:

($\Leftarrow$) Tegyük fel, hogy $\mathbf{x}^{\mathbf{w}}\mathbf{y}^{\mathbf{u}} \in \mathrm{Lm}\,(I(V))$ és legyen $f \in I(V)$, amely főtagja $\mathbf{x}^{\mathbf{w}}\mathbf{y}^{\mathbf{u}}$. Ekkor az eliminációs rendezés megfelelő tulajdonságát használva létezik a 3.5. lemmában szereplőhöz hasonló felbontás, azaz

$$f(\mathbf{x}, \mathbf{y}) = \mathbf{x}^{\mathbf{w}} g(\mathbf{y}) + h(\mathbf{x}, \mathbf{y}),$$

ahol $\mathrm{lm}\,(g) = \mathbf{y}^{\mathbf{u}}$ és h minden monomja kisebb $\mathbf{x}^{\mathbf{w}}$-nél. A feltétel szerint tehát $\mathrm{lm}\,(g)$ az Y standard monomja, ezért g nem tűnhet el a teljes Y-on. Létezik ezek szerint $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_m) \in Y$, amelyre $g(\boldsymbol{\beta}) \neq 0$. Ez a h-ra szabott feltétellel együtt azonban azt adja, hogy $\hat{f}(\mathbf{x}) := f(\mathbf{x}, \boldsymbol{\beta})$ vezető tagja $\mathbf{x}^{\mathbf{w}}$. Mivel $f \in I(V)$, ezért $\hat{f} \in I(V_{\beta_m\beta_{m-1}\ldots\beta_1})$, amiből viszont azt láthatjuk, hogy $\mathbf{x}^{\mathbf{w}} \in \mathrm{Lm}\left(I(V_{\beta_m\beta_{m-1}\ldots\beta_1})\right)$, ellentmondásban $\boldsymbol{\beta} \in Y$-nal.

($\Rightarrow$) Tegyük most fel, hogy az állítással ellentétben $\mathbf{y}^{\mathbf{u}} \in \mathrm{Lm}\,(I(Y))$ és legyen g az ezt tanúsító polinom, azaz $\mathrm{lm}\,(g) = \mathbf{y}^{\mathbf{u}}$ és $g \in I(Y)$.

Ha $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_m) \notin Y$, akkor van olyan $h_{\boldsymbol{\beta}}(\mathbf{x})$ polinom, amely monomjai mind kisebbek $\mathbf{x}^{\mathbf{w}}$-nél és $\mathbf{x}^{\mathbf{w}} + h_{\boldsymbol{\beta}}(\mathbf{x})$ eltűnik $V_{\beta_m\beta_{m-1}\ldots\beta_1}$-en. Legyen $\chi_{\boldsymbol{\beta}}(\mathbf{y})$ olyan polinom, ami eltűnik az $\{\alpha_1, \ldots, \alpha_k\}^m \setminus \{\boldsymbol{\beta}\}$ halmazon, és $\chi_{\boldsymbol{\beta}}(\boldsymbol{\beta}) = 1$. Ekkor

$$h(\mathbf{x}, \mathbf{y}) := \mathbf{x}^{\mathbf{w}} + \sum_{\boldsymbol{\beta} \in \{\alpha_1, \ldots, \alpha_k\}^m \setminus Y} h_{\boldsymbol{\beta}}(\mathbf{x})\chi_{\boldsymbol{\beta}}(\mathbf{y})$$

polinom főtagja az eliminációs rendezés definíciója szerint $\mathbf{x}^{\mathbf{w}}$ és $\boldsymbol{\beta} \notin Y$ esetén $h(\mathbf{x}, \boldsymbol{\beta}) = \mathbf{x}^{\mathbf{w}} + h_{\boldsymbol{\beta}}(\mathbf{x})$. Megmutatjuk, hogy $h(\mathbf{x}, \mathbf{y})g(\mathbf{y})$ eltűnik a teljes V-n. Ha egy $(\boldsymbol{\gamma}, \boldsymbol{\beta}) = (\gamma_1, \ldots, \gamma_n, \beta_1, \ldots, \beta_m) \in V$ pontra $\boldsymbol{\beta} \in Y$, akkor $g(\boldsymbol{\beta}) = 0$. Ha viszont $\boldsymbol{\beta} \notin Y$, akkor $h(\boldsymbol{\gamma}, \boldsymbol{\beta}) = \boldsymbol{\gamma}^{\mathbf{w}} + h_{\boldsymbol{\beta}}(\boldsymbol{\gamma}) = 0$, hiszen $\boldsymbol{\gamma} \in V_{\beta_m\beta_{m-1}\ldots\beta_1}$. Állításunkat ezzel beláttuk. □

4. Algoritmusok

Négy algoritmust mutatunk be ebben a fejezetben. Az első Buchberger 1965-ös [5] dolgozatában már szerepelt, amely azon kívül, hogy általános módszert ad egy ideál egy Gröbner-bázisának meghatározására, a redukcióról is sok mindent elárul.

A második és harmadik a bennünket igazán érdeklő esetekre specializált algoritmus, mindkettő véges V pontrendszerhez tartozó $I(V)$ ideál Gröbner-bázisának meghatározására szolgál. Az irodalomban számtalan egyéb algoritmust lehet találni, közöttük olyanokat, amelyek általánosabban nulla dimenziós ideálokkal is működnek. A Buchberger–Möller-algoritmust egyszerűsége és ugyanakkor gyors futásideje miatt választottuk ki bemutatásra. Farr és Gao algoritmusa merőben más alapötleten nyugszik, és a gyakorlatban nagyjából hasonló idő alatt végez, mint a Buchberger–Möller, bár elméleti futásideje rosszabb. Farr és Gao módszerét inkább elméleti következményei miatt tárgyaljuk, segítségével jobban megérthetjük véges pontrendszerek Gröbner-bázisainak szerkezetét. Ugyanezért viszont mellőzzük a futásidő elemzését, amíg a Buchberger–Möller-algoritmust ebből a szempontból is részletesen vizsgáljuk.

Végül bemutatunk egy módszert, amely $I(V)$ ideál lexikografikus standard monomjait adja meg, természetesen lényegesen gyorsabban, mint az előtte vázolt teljes Gröbner-bázist kiszámoló algoritmusok. A helyesség bizonyításához az előző fejezetben bemutatott lex játék egy következményét fogjuk használni.

4.1. Buchberger algoritmusa

Az algoritmus ismertetéséhez szükségünk lesz néhány új fogalomra, a helyesség bizonyításához pedig a Gröbner-bázisok egy ekvivalens definíciójára.

Legyenek f és g nemnulla polinomok, és legyen f és g főtagjának legkisebb közös többszöröse $\mathbf{x}^{\mathbf{w}}$, azaz

$$w_i = \max\{(\operatorname{lm}(f)\text{-ben } x_i \text{ kitevője}), (\operatorname{lm}(g)\text{-ben } x_i \text{ kitevője})\}.$$

Legyen f főegyütthatója c_f, g polinomé pedig c_g. Ekkor *f és g S-polinomja*

$$S(f,g) = \frac{\mathbf{x}^{\mathbf{w}}}{c_f \operatorname{lm}(f)} f(\mathbf{x}) - \frac{\mathbf{x}^{\mathbf{w}}}{c_g \operatorname{lm}(g)} g(\mathbf{x}).$$

Könnyű látni, hogy $\operatorname{lm}\left(\frac{\mathbf{x}^{\mathbf{w}}}{c_f \operatorname{lm}(f)} f(\mathbf{x})\right) = \mathbf{x}^{\mathbf{w}} = \operatorname{lm}\left(\frac{\mathbf{x}^{\mathbf{w}}}{c_g \operatorname{lm}(g)} g(\mathbf{x})\right)$, ugyanakkor $\mathbf{x}^{\mathbf{w}}$ kiesik $S(f,g)$-ből, így $\operatorname{lm}(S(f,g)) \prec \mathbf{x}^{\mathbf{w}}$. Előfordulhat emiatt, hogy $S(f,g)$ nem redukálható f-fel vagy g-vel.

Az alfejezet fő tételében belátjuk, hogy egy véges G polinomhalmaz pontosan akkor Gröbner-bázis (az általa generált ideálban), ha tetszőleges két eleme S-polinomjának G szerinti redukáltja 0. Szükségünk lesz a következő lemmára.

4.1. Lemma. *Legyenek $f_1, \ldots, f_s$ közös $\mathbf{x}^{\mathbf{w}}$ főtagú és 1 főegyüttható jú polinomok. Tegyük fel továbbá, hogy $f = \sum_{i=1}^{s} c_i f_i$ valamilyen $c_i \in \mathbb{F}$ együtthatókkal. Ha $\operatorname{lm}(f) \prec \mathbf{x}^{\mathbf{w}}$, akkor f előáll, $\sum_{i=1}^{s-1} c_i^* S(f_i, f_{i+1})$ alakban, ahol $c_i^* \in \mathbb{F}$.*

Bizonyítás: Miután $\mathbf{x}^{\mathbf{w}}$ együtthatója 0, ezért $\sum_{i=1}^{s} c_i = 0$. Felhasználva $S(f_i, f_{i+1}) = f_i - f_{i+1}$ egyenlőséget is, látható, hogy

$$f = \sum_{i=1}^{s} c_i f_i = \sum_{i=1}^{s-1} \left(\left(\sum_{j=1}^{i} c_j \right) (f_i - f_{i+1}) \right) = \sum_{i=1}^{s-1} c_i^* S(f_i, f_{i+1}).$$

□

4.2. Tétel. *Legyen $G = \{g_1, \ldots, g_m\}$ nemnulla polinomok halmaza. G pontosan akkor Gröbner-bázisa a $\langle G \rangle$ ideálnak, ha minden $g_i, g_j \in G$ esetén $S(g_i, g_j)$-nek G-vel vett redukáltja 0.*

Bizonyítás: Ha G Gröbner-bázis, akkor a 2.5. következmény szerint minden $f \in \langle G \rangle$ redukáltja 0. Nyilván $S(g_i, g_j) \in \langle G \rangle$, tehát a feltétel szükséges.

Tegyük most fel, hogy minden $g_i, g_j \in G$-re az $S(g_i, g_j)$ polinom 0-ra redukálható G-vel. Az általánosság megszorítása nélkül feltehető, hogy minden g_i főegyüttható ja 1. A 2.6. állítás (bizonyított része) szerint elegendő megmutatni, hogy minden $f \in \langle G \rangle$ redukálható 0-ra. Indirekt tegyük fel, hogy f ellenpélda. Tekintsünk egy olyan

$$f = \sum_{i=1}^{m} g_i h_i \tag{4}$$

előállítást, amelyben $\mathbf{x}^{\mathbf{w}} := \max_{i=1\ldots m} \operatorname{lm}(g_i h_i)$ minimális. Ilyen létezik, hiszen $f \in \langle G \rangle$ miatt van megfelelő előállítás, továbbá minden tagsorrend jólrendezés (így a minimum létezik). Nyilván $\operatorname{lm}(f) \preceq \mathbf{x}^{\mathbf{w}}$, ráadásul egyenlőség sem állhat fenn, különben (4) azt mutatná, hogy f redukálható 0-ra.

Megkonstruáljuk f-nek egy (4)-hez hasonló előállítását, amelyben azonban a szereplő monomok mind $\mathbf{x}^{\mathbf{w}}$-nél kisebbek lesznek, ellenmondva $\mathbf{x}^{\mathbf{w}}$

minimalitásának. Jelölje L azon i indexek nemüres halmazát, amelyre $\mathbf{x}^{\mathbf{w}} = \operatorname{lm}(g_i h_i)$. Leválasztva azokat a tagokat, ahol $\mathbf{x}^{\mathbf{w}}$ szerepel, kapjuk, hogy

$$f(\mathbf{x}) = \sum_{i=1}^{m} g_i(\mathbf{x}) h_i^*(\mathbf{x}) + \sum_{i \in L} c_i g_i(\mathbf{x}) \mathbf{x}^{\mathbf{w_i}},$$

ahol $\operatorname{lm}(g_i h_i^*) \prec \mathbf{x}^{\mathbf{w}}$ és $\operatorname{lm}(g_i(\mathbf{x})\mathbf{x}^{\mathbf{w_i}}) = \mathbf{x}^{\mathbf{w}}$. Teljesül ekkor $\sum_{i \in L} c_i = 0$, hiszen ez $\mathbf{x}^{\mathbf{w}}$ együtthatója. Legyen $g(\mathbf{x}) = \sum_{i \in L} c_i g_i(\mathbf{x}) \mathbf{x}^{\mathbf{w_i}}$. Ha g előállítható g_i-k polinomokkal vett lineáris kombinációjával úgy, hogy minden előforduló monom kisebb $\mathbf{x}^{\mathbf{w}}$-nél, akkor megkapjuk f-nek is egy hasonló tulajdonságú előállítását, ami ellentmondás. Ez lesz tehát mostantól a célunk.

A 4.1. lemma alkalmazható $g(\mathbf{x}) = \sum_{i \in L} c_i g_i(\mathbf{x}) \mathbf{x}^{\mathbf{w_i}}$-re, így kapjuk, hogy

$$g(\mathbf{x}) = \sum_{i,j \in L} c_{i,j}^* S\left(g_i(\mathbf{x})\mathbf{x}^{\mathbf{w_i}}, g_j(\mathbf{x})\mathbf{x}^{\mathbf{w_j}}\right).$$

Számoljuk most ki a szereplő S-polinomokat. Legyen $\operatorname{lm}(g_i)$ és $\operatorname{lm}(g_j)$ legkisebb közös többszöröse $\mathbf{x}^{\mathbf{u_{ij}}}$. Világos, hogy $\mathbf{x}^{\mathbf{u_{ij}}} \mid \mathbf{x}^{\mathbf{w}}$. Ekkor

$$S(g_i(\mathbf{x})\mathbf{x}^{\mathbf{w_i}}, g_j(\mathbf{x})\mathbf{x}^{\mathbf{w_j}}) = \frac{\mathbf{x}^{\mathbf{w}}}{\operatorname{lm}(g_i)} g_i - \frac{\mathbf{x}^{\mathbf{w}}}{\operatorname{lm}(g_j)} g_j = \frac{\mathbf{x}^{\mathbf{w}}}{\mathbf{x}^{\mathbf{u_{ij}}}} S(g_i, g_j)$$

Miután a feltétel szerint $S(g_i, g_j)$ 0-ra redukálódik, ezért létezik

$$S(g_i, g_j) = \sum_{\ell=1}^{m} h_{ij\ell} g_\ell$$

előállítás, ahol minden ℓ-re $\operatorname{lm}(h_{ij\ell} g_\ell) \preceq \operatorname{lm}(S(g_i, g_j))$.

Az előzőekkel összevetve kapjuk, hogy

$$g(\mathbf{x}) = \sum_{i,j \in L} c_{i,j}^* \frac{\mathbf{x}^{\mathbf{w}}}{\mathbf{x}^{\mathbf{u_{ij}}}} \sum_{\ell=1}^{m} h_{ij\ell} g_\ell(\mathbf{x}) = \sum_{\ell=1}^{m} \left(g_\ell(\mathbf{x}) \sum_{i,j \in L} c_{i,j}^* h_{ij\ell} \frac{\mathbf{x}^{\mathbf{w}}}{\mathbf{x}^{\mathbf{u_{ij}}}} \right).$$

Itt $\operatorname{lm}(h_{ij\ell} g_\ell) \preceq \operatorname{lm}(S(g_i, g_j)) \prec \mathbf{x}^{\mathbf{u_{ij}}}$, ezért

$$\operatorname{lm}\left(g_\ell(\mathbf{x}) \sum_{i,j \in L} c_{i,j}^* h_{ij\ell} \frac{\mathbf{x}^{\mathbf{w}}}{\mathbf{x}^{\mathbf{u_{ij}}}} \right) \prec \mathbf{x}^{\mathbf{w}},$$

és éppen ilyen tulajdonságú előállítást kerestünk. □

Buchberger algoritmusa ezek után igen egyszerű. Legyen I ideál $\mathbb{F}[\mathbf{x}]$-ben és $F \subseteq I$ egy tetszőleges véges generátorrendszere, $F = \{f_1, \ldots, f_s\}$.

Válasszunk két polinomot F-ből, például f_1, f_2-t, számítsuk ki $S(f_1, f_2)$-t és redukáljuk F-fel. Amennyiben a redukált $r \neq 0$, akkor vegyük hozzá $f_{|F|+1} := r$-et F-hez. Ha a redukált 0, akkor nem teszünk semmit. Az algoritmus általános lépése hasonló, válasszunk az aktuális F-ből két polinomot, amelyeket együtt addig még nem vizsgáltunk, számoljuk ki S-polinomjuk redukáltját az aktuális F-re nézve, és azt – amennyiben nem 0 – vegyük hozzá F-hez. Az eljárást egészen addig folytatjuk, amíg el nem fogynak a még nem vizsgált polinompárok.

A helyesség bizonyítása a 4.2. tétel alapján egyszerű. Tudjuk, hogy $\langle F \rangle = I$ az elején, a továbbiakban hozzávett polinomok pedig I-beli polinomok S-polinomjainak néhány I-beli polinommal vett redukáltjai, ezért maguk is I-ben vannak. Tehát a végén kapott F-re is $\langle F \rangle = I$. A konstrukció alapján világos, hogy F bármely két polinomjának S-polinomja F-fel 0-ra redukálható (hiszen ahol ez nem volt igaz, ott hozzávettük a redukáltat, amit felhasználva viszont már nyilván 0-ra redukálódik). A 4.2. tétel szerint tehát I egy Gröbner-bázisát kapjuk így.

Végül megmutatjuk, hogy az eljárás véges sok lépésben véget ér. Ellenkező esetben volna olyan $F_1 \subsetneq F_2 \subsetneq \ldots$ végtelen sorozata I generátorainak, amelyre $F_i \cup \{r_i\} = F_{i+1}$ egy F_i-re nézve redukált r_i polinomra. Teljesül $\mathrm{Lm}(F_i) \subsetneq \mathrm{Lm}(F_{i+1})$ is, hiszen $\mathrm{lm}(r_i) \in \mathrm{Lm}(F_{i+1}) \setminus \mathrm{Lm}(F_i)$. De ekkor $\mathrm{lm}(r_i) \in \langle \mathrm{Lm}(F_{i+1}) \rangle \setminus \langle \mathrm{Lm}(F_i) \rangle$ is igaz, ugyanis $\langle \mathrm{Lm}(F_i) \rangle$ monomiális ideál, tehát a 2.2. lemma miatt ha $\mathrm{lm}(r_i) \in \langle \mathrm{Lm}(F_i) \rangle$ lenne, akkor $\mathrm{lm}(r_i) \in \mathrm{Lm}(F_i)$ is teljesülne. Így viszont

$$\langle \mathrm{Lm}(F_1) \rangle \subsetneq \langle \mathrm{Lm}(F_2) \rangle \subsetneq \ldots$$

ideálok végtelen növő lánca, ami $\mathbb{F}[\mathbf{x}]$-ben nem létezik. □

Látjuk tehát, hogy a Buchberger-algoritmus $\mathbb{F}[\mathbf{x}]$ tetszőleges véges generátorrendszerrel megadott ideáljához véges sok lépésben előállít egy Gröbner-bázist. Természetesen ez általában nem lesz redukált, sőt tipikusan a szükségesnél sokkal több elemet tartalmaz. Emiatt az algoritmus lépésszámára nem igazán mondható használható felső becslés. Ugyanakkor a módszeren lehet gyorsítani néhány egyszerű és néhány bonyolultabb trükkel. Miután bennünket elsősorban véges pontrendszeren eltűnő polinomok ideálja érdekel, ezért nem foglalkozunk ilyenekkel, az érdeklődő Olvasó találhat javításokat [1] 3.3. alfejezetében vagy Giovini, Mora, Niesi, Robbiano és Traverso [19] munkájában.

A következő két alfejezetben egy-egy véges pontrendszerre működő algoritmust tárgyalunk. Emiatt, míg a Buchberger-algoritmus bemeneteként az ideált egy véges generátorrendszerével adtuk meg, a további algoritmusoknál egy véges V pontrendszerből indulunk ki.

4.2. Farr és Gao algoritmusa véges pontrendszerre

Az algoritmust szerzőik [12] cikkben publikálták.

Legyen $V = \{\mathbf{v}_1, \ldots, \mathbf{v}_m\} \subseteq \mathbb{F}^n$ a vizsgált nemüres pontrendszerünk, és jelölje $\mathbf{v}_i$ j. koordinátáját v_{ij}. A bemutatandó algoritmus $i = 1, \ldots, m$-re kiszámolja a $\{\mathbf{v}_1, \ldots, \mathbf{v}_i\}$-hez tartozó redukált Gröbner-bázist, felhasználva $I(\{\mathbf{v}_1, \ldots, \mathbf{v}_{i-1}\})$-ét.

Feltesszük, hogy a tagsorrendünk által a változókon adott rendezés $x_1 \succ x_2 \succ \cdots \succ x_n$. Az algoritmus egyszerűbb leírása érdekében polinomokra is kiterjesztjük a rendezést: $f_1 \prec f_2$ akkor és csak akkor, ha $\operatorname{lm}(f_1) \prec \operatorname{lm}(f_2)$.

Szükségünk lesz egy `Redukált(`f`,`G`)` függvényre, amely tetszőleges f polinom és G Gröbner-bázis esetén megadja f-nek G-re vett redukáltját.

$G := \{1\}$;
`For` $i = 1$ `to` m `do`
  $g := \min\{f \in G : f(\mathbf{v}_i) \neq 0\}$; $G := G \setminus \{g\}$;
  `For` $f \in G$ `do` $f(\mathbf{x}) := f(\mathbf{x}) - \frac{f(\mathbf{v}_i)}{g(\mathbf{v}_i)} g(\mathbf{x})$; `endfor;`
  `For` $j = n$ `downto` 1 `if` $x_j \cdot \operatorname{lm}(g) \notin \operatorname{Lm}(G)$ `then do`
    $G := G \cup$`Redukált(`$(x_j - v_{ij})g$`,`G`);`
  `endfor;`
`endfor;`

Bebizonyítjuk, hogy az algoritmus helyes. Jelöljük a külső `For` ciklus i. lefutása után kapott G polinomhalmazt G_i-vel és a $\{\mathbf{v}_1, \ldots, \mathbf{v}_i\} \subseteq V$ pontrendszert V_i-vel. Teljes indukcióval igazoljuk, hogy G_i redukált Gröbner-bázisa $I(V_i)$ ideálnak, ha $i \leq m$.

Ez $i = 0$-ra, azaz az első lefutás előtt fennáll, hiszen $I(\emptyset) = \mathbb{F}[\mathbf{x}]$ redukált Gröbner-bázisa $G_0 = \{1\}$.

Tegyük fel, hogy G_{i-1} az $I(V_{i-1})$ redukált Gröbner-bázisa. Az

$$f(\mathbf{x}) := f(\mathbf{x}) - \frac{f(\mathbf{v}_i)}{g(\mathbf{v}_i)} g(\mathbf{x})$$

értékadással G_{i-1} elemeit G_i-ben olyan polinomokra cseréljük, amelyek eltűnnek a teljes V_i-n. Ráadásul főtagjaik nem változnak, ugyanis g-t úgy választottuk, hogy ha $\operatorname{lm}(g) \succ \operatorname{lm}(f)$, akkor $f(\mathbf{v}_i) = 0$, tehát akkor f-en nem változtattunk semmit.

Vizsgáljuk most meg a további G_i-hez vett polinomokat. Az algoritmus ezen pontján használt polinomhalmazt G-vel jelöljük, hiszen már $G_{i-1} \neq G$ és általában még $G \subsetneq G_i$. Most a második belső `For` ciklusra végzett egyszerű indukcióval láthatjuk, hogy $G \subseteq I(V_i)$. Legyen ugyanis $h =$ `Redukált(`$(x_j - v_{ij})g$`,`G`)`. Nyilván $(x_j - v_{ij})g \in I(V_i)$, ezért ugyanez igaz $I(V_i)$-ben szereplő

polinomokkal vett h redukáltjára. Az is világos, hogy $\operatorname{lm}(h) = x_j \cdot \operatorname{lm}(g)$, hiszen $x_j \cdot \operatorname{lm}(g) \notin \operatorname{Lm}(G)$ miatt a főtag már redukált. Ezek szerint teljesül

$$\operatorname{Lm}(G_{i-1}) = \operatorname{Lm}(G_i) \cup \{\operatorname{lm}(g)\},$$

így a komplementerek elemszámát nézve

$$i - 1 = |\operatorname{Sm}(G_{i-1})| = |\operatorname{Sm}(G_i) \setminus \{\operatorname{lm}(g)\}| \geq |\operatorname{Sm}(G_i)| - 1, \qquad (5)$$

miután G_{i-1} az $I(V_{i-1})$ ideál Gröbner-bázisa. Másrészt $\operatorname{Sm}(I(V_i)) \subseteq \operatorname{Sm}(G_i)$ miatt $|\operatorname{Sm}(G_i)| \geq i$, tehát (5) egyenlőséggel teljesül. Következésképp igaz $|\operatorname{Sm}(G_i)| = i = |V_i|$, így a 2.8. lemma szerint G_i Gröbner-bázis. Azt is beláttuk ezzel, hogy $\operatorname{Sm}(I(V_{i-1})) \cup \{\operatorname{lm}(g)\} = \operatorname{Sm}(I(V_i))$.

Hátravan még annak igazolása, hogy G_i redukált. G_i azon elemei, amelyeket

$$f(\mathbf{x}) := f(\mathbf{x}) - \frac{f(\mathbf{v}_i)}{g(\mathbf{v}_i)} g(\mathbf{x})$$

alakban kapunk, vezető tagjuktól eltekintve $I(V_i)$-re nézve standard monomok lineáris kombinációi, ugyanis az indukciós feltétel alapján f és g nem főtagjai $\operatorname{Sm}(I(V_{i-1})) \subseteq \operatorname{Sm}(I(V_i))$-ben vannak, továbbá $\operatorname{lm}(g) \in \operatorname{Sm}(I(V_i))$ az előző bekezdés alapján. Különböző ilyenek vezető tagjai nem oszthatják egymást, különben már G_{i-1}-ben is osztották volna.

A $h = \texttt{Redukált}((x_j - v_{ij})g, G)$ alakú polinomok esetén csak azt kell megmutatni, hogy h nem redukálható olyan G_i-ben levő polinommal, amit csak később veszünk be G-be. Ez viszont világos, ugyanis minden később bevett $\hat{h}$ polinomra $\operatorname{lm}\left(\hat{h}\right) = x_\ell \operatorname{lm}(g)$ és $\ell < j$, tehát $x_\ell \succ x_j$ és $\operatorname{lm}\left(\hat{h}\right) \succ \operatorname{lm}(h)$. Ezzel állításunkat igazoltuk. □

Az algoritmus elméleti futásidejének becslését a $\texttt{Redukált}((x_j - v_{ij})g, G)$ időigénye határozza meg, amelyet összesen $O(mn)$-szer hívunk. Az egyéb feladatok összesen csak $O(m^3 n)$ aritmetikai műveletet és – megfelelő adatszerkezet használata esetén – $O(mn \log(mn))$ összehasonlítást ($\prec$ szerint) igényelnek. Később látni fogjuk, hogy ez éppen ugyanannyi, amennyit a Buchberger–Möller-algoritmus is használ. Sajnos azonban a redukált számolására ismert legjobb algoritmus is már ennél időigényesebbé teszi a módszert.

A helyesség bizonyításából és az algoritmus menetéből világos, hogy igaz a következő standard monomokra vonatkozó állítás.

4.3. Következmény. *Ha $V' \subseteq V$ véges pontrendszerek, akkor*

$$\operatorname{Sm}(I(V')) \subseteq \operatorname{Sm}(I(V)),$$

sőt, ha $V \neq V'$, *és* $V = V' \cup \{\mathbf{v}\}$, *akkor*

$$\mathrm{Sm}\,(I(V')) \cup \{\mathbf{x}^{\mathbf{w}}\} = \mathrm{Sm}\,(I(V))\,,$$

ahol $\mathbf{x}^{\mathbf{w}} = \mathrm{lm}\,(g)$ *a* V' *redukált Gröbner-bázisának legkisebb vezető tagú* g *elemére, amelyre* $g(\mathbf{v}) \neq 0$.

4.3. A Buchberger–Möller-algoritmus véges pontrendszerre

Az algoritmus változatai több cikkben megtalálhatóak, az eredeti Buchberger és Möller 1982-ben megjelent [8] munkája. Részletes költségelemzést tartalmaz és elég általános Marinari, Möller és Mora [27] dolgozata, végül jó összefoglalót ad Mora és Robbiano [28]. Ugyanezen az alapötleten múlik Faugère, Gianni, Lazard és Mora [13] algoritmusa, amely a számításhoz felteszi, hogy valamely más tagsorrendre már ismert a redukált Gröbner-bázis.

A Buchberger–Möller-algoritmus véges pontrendszerhez tartozó ideál redukált Gröbner-bázisát számolja ki, aminek elemeit sorra adjuk hozzá a kezdetben üres G halmazhoz. Egyúttal készítünk egy S halmazt, ami az algoritmus végére az összes standard monomból fog állni. Az eljárás minden lépésében megvizsgálunk egy $\mathbf{x}^{\mathbf{w}}$ monomot, amely, ha standard monom S-be kerül, ha $\mathrm{Lm}\,(I(V))$ minimális generátora, akkor a redukált Gröbner-bázis hozzátartozó elemét betesszük G-be, egyébként pedig nem foglalkozunk vele tovább. Az adott tagsorrendre nézve egyre nagyobb monomokat vizsgálunk, amelyeket egy – néha bővülő – M listából választunk.

Az algoritmus folyamán egy $U \subseteq V$ halmazt is folyamatosan bővítünk. Kezdetben $U = \emptyset$, a végén $U = V$ lesz, és végig igaz marad, hogy S pontosan az U-ban levő pontokhoz tartozó ideál standard monomjait tartalmazza, azaz $S = \mathrm{Sm}\,(I(U))$. Végül a szereplő q_i monomokra teljesül, hogy amennyiben U az $\mathbf{u}_1, \ldots, \mathbf{u}_\ell$ pontokból áll (bekerülésük sorrendjében) és $i < \ell$, akkor minden $j < i$-re $q_i(\mathbf{u}_j) = 0$ és $q_i(\mathbf{u}_i) = 1$.

Lássuk tehát az algoritmus pontos működését.

$G := \emptyset$; $S := \emptyset$; $U := \emptyset$; $M := \{1\}$; $i := 0$;
`While` $M \neq \emptyset$ `do`
  $\mathbf{x}^{\mathbf{w}} := \min M$; $M := M \setminus \{\mathbf{x}^{\mathbf{w}}\}$;
  `If` $\mathbf{x}^{\mathbf{w}} \notin \mathrm{Lm}\,(G)$ `then`
    $p(\mathbf{x}) := \mathbf{x}^{\mathbf{w}}$;
    `For` $j = 1$ `to` i `do` $p(\mathbf{x}) := p(\mathbf{x}) - p(\mathbf{u}_j)q_j(\mathbf{x})$; `endfor`;
    `If` $p(\mathbf{x}) \in I(V)$ `then`
      $G := G \cup \{p(\mathbf{x})\}$;

```
      else
         i := i + 1;
         legyen v ∈ V, amire p(v) ≠ 0; u_i := v;
         U := U ∪ {u_i};
         q_i(x) := p(x)/p(u_i);
         S := S ∪ {x^w};
         M := M ∪ {x_j · x^w : j = 1 ... n};
      endif;
   endif;
endwhile;
```

Most bebizonyítjuk, hogy az algoritmus helyes, sőt eleget tesz a fent leírt egyéb követelményeknek is. Nevezzük vizsgáltnak azon monomokat, amelyeket az algoritmus 3. sora szerint valamikor $\mathbf{x}^{\mathbf{w}}$-nek választunk.

Először is vegyük észre, hogy a vizsgált $\mathbf{x}^{\mathbf{w}}$ monomok egyre nagyobbak. Valóban, amikor $\mathbf{x}^{\mathbf{w}}$-t választjuk M-ből, akkor ő a minimális elem, és M-be később már csak olyan monomok kerülhetnek be (tekintsünk az első `endif` előtti sorra), amelyeknek valamelyik már bent levő monom osztója, tehát olyan, ami $\mathbf{x}^{\mathbf{w}}$-nél nagyobb. Világos emiatt az is, hogy amikor $\mathbf{x}^{\mathbf{w}}$-t vizsgáljuk, akkor a már készen levő $q_1, \ldots, q_i$ polinomok csupa kisebb monomból állnak, hiszen csakis vizsgált (ráadásul S-ben levő) monomokat tartalmaznak. Tehát $\mathrm{lm}\,(p) = \mathbf{x}^{\mathbf{w}}$ igaz, így amikor $p \in I(V)$, akkor a vizsgált monom főtag.

Másodszor i-re vonatkozó indukcióval megmutatjuk, hogy q_i eleget tesz a kívánalmaknak, azaz ha az U-ba bekerült pontok rendre $\mathbf{u}_1, \ldots, \mathbf{u}_i$, akkor $j < i$ esetén $q_i(\mathbf{u}_j) = 0$ és $q_i(\mathbf{u}_i) = 1$. Ezt a tulajdonságot természetesen nem változtatja meg, hogy később további pontokat is beveszünk U-ba.

Tekintsük a következő

$$A := \begin{bmatrix} q_1(\mathbf{u}_1) & q_1(\mathbf{u}_2) & \ldots & q_1(\mathbf{u}_{i-1}) \\ q_2(\mathbf{u}_1) & q_2(\mathbf{u}_2) & \ldots & q_2(\mathbf{u}_{i-1}) \\ & \ldots & & \\ q_{i-1}(\mathbf{u}_1) & q_{i-1}(\mathbf{u}_2) & \ldots & q_{i-1}(\mathbf{u}_{i-1}) \\ \mathbf{u_1}^{\mathbf{w}} & \mathbf{u_2}^{\mathbf{w}} & \ldots & \mathbf{u_{i-1}}^{\mathbf{w}} \end{bmatrix}$$

mátrixot. Az indukciós feltevést alkalmazva

$$A = \begin{bmatrix} 1 & q_1(\mathbf{u}_2) & q_1(\mathbf{u}_3) & \ldots & q_1(\mathbf{u}_{i-1}) \\ 0 & 1 & q_2(\mathbf{u}_3) & \ldots & q_2(\mathbf{u}_{i-1}) \\ 0 & 0 & 1 & \ldots & q_3(\mathbf{u}_{i-1}) \\ & & \ldots & & \\ 0 & 0 & 0 & \ldots & 1 \\ \mathbf{u_1}^{\mathbf{w}} & \mathbf{u_2}^{\mathbf{w}} & \mathbf{u_3}^{\mathbf{w}} & \ldots & \mathbf{u_{i-1}}^{\mathbf{w}} \end{bmatrix}.$$

Nullázzuk ki az utolsó sor elemeit rendre az első $i-1$ sor segítségével. Ekkor az utolsó sorban $p(\mathbf{x})$ polinom $\mathbf{u}_1, \ldots, \mathbf{u}_{i-1}$ helyen vett helyettesítési értéke fog szerepelni, hiszen éppen a `For` ciklusban szereplő műveleteket végeztük el. Tehát $p(\mathbf{u}_j) = 0$, ha $j < i$. Ugyanakkor $p(\mathbf{x}) \notin I(V)$ miatt van olyan V-beli pont, ami u_i-nek választható, tehát $p(\mathbf{u}_i) \neq 0$. Ráadásul a fentiek szerint u_i biztosan különbözik a már U-ban levő pontoktól. Ebből q_i definíciójára tekintve az állítás világos.

Most már láthatjuk, hogy az algoritmus véges sok lépésben leáll, ugyanis ha már $i = |V| =: m$, akkor minden újabb p polinom az $U = \{u_1, \ldots, u_m\} = V$ helyeken eltűnik, ezért M-be több elem már nem kerül, tehát előbb-utóbb kiürül.

Ezek után igazoljuk, hogy az algoritmus végére minden monom vagy $\mathrm{Lm}\,(G)$-ben vagy S-ben van. Tegyük fel, hogy $\mathbf{x}^{\mathbf{w}}$ egy minimális ellenpélda. Az 1 monom az első lépésben bekerül S-be, tehát $\mathbf{x}^{\mathbf{w}}$-nek van eggyel kisebb fokú osztója. A minimalitás miatt ez szerepel $\mathrm{Lm}\,(G)$-ben vagy S-ben. $\mathrm{Lm}\,(G)$ felszálló, ezért csak S-ben lehet. Akkor viszont abban a lépésben, amikor bekerült, $\mathbf{x}^{\mathbf{w}}$ monomot felvettük az M listára. Valamikor tehát vizsgáltuk $\mathbf{x}^{\mathbf{w}}$-t, így viszont vagy p polinom főtagjaként bekerül $\mathrm{Lm}\,(G)$-be, vagy S-hez vesszük hozzá.

Láttuk, hogy standard monom nem kerülhet $\mathrm{Lm}\,(G)$-be, tehát biztosan $\mathrm{Sm}\,(I(V)) \subseteq S$, ráadásul az algoritmus folyamán végig igaz $\mathrm{Sm}\,(I(U)) \subseteq S$ is. Miután $|\mathrm{Sm}\,(I(V))| = |V| = m = |S|$ (illetve a közbenső lépések során végig $|\mathrm{Sm}\,(I(U))| = |U| = i = |S|$), ezért igaz, hogy $\mathrm{Sm}\,(I(V)) = S$ (illetve $\mathrm{Sm}\,(I(U)) = S$ az algoritmus közben). Komplementert véve adódik, hogy $\mathrm{Lm}\,(I(V)) = \mathrm{Lm}\,(G)$, tehát G Gröbner-bázis.

Végül azt sem nehéz belátni, hogy G redukált Gröbner-bázis. Mivel a q_i polinomok mind S-beli, tehát standard monomok lineáris kombinációi, ezért ugyanez igaz főtagjától eltekintve az összes szereplő p polinomra is. Így speciálisan G elemei vezető tagjuktól eltekintve standard monomokból állnak. Már csak azt kell igazolni, hogy G különböző elemeinek főtagjai nem oszthatják egymást. Ez viszont abból világos, hogy két vezető tag közül a kisebbet előbb vizsgáltuk, ezért amikor a nagyobb $\mathbf{x}^{\mathbf{w}}$ monomra került a sor, már $\mathbf{x}^{\mathbf{w}} \in \mathrm{Lm}\,(G)$ lett volna, amennyiben a kisebb $\mathbf{x}^{\mathbf{w}}$-nek osztója lenne. □

4.4. Tétel. *Tegyük fel, hogy az aritmetikai műveletek $\mathbb{F}$ testben a, két n változós monom $\prec$ szerinti összehasonlítása pedig nb költségűek. Ekkor a Buchberger–Möller-algoritmus $O\left(am^3n + bmn^2 \log(mn)\right)$ időben megvalósítható. Például egy kis elemszámú véges testben a lex vagy deglex rendezéssel dolgozva, és valamely $\varepsilon > 0$ számra $m^{1-\varepsilon} > n$-et feltéve a futásidő $O(m^3n)$.*

Bizonyítás Először teszünk néhány észrevételt, amelyekre a futásidő csökkentése miatt lesz szükségünk. Először is, M elemeit érdemes valamilyen

bináris keresőfában tárolni. A pontos definíciók megtalálhatóak például [31] 3. fejezetében, vagy [10] 13. fejezetében. Itt csak annyit használunk, hogy $O(\log |M|)$ összehasonlítással meg tudjuk kapni M minimális elemét, illetve ugyanekkora költséggel tudunk törölni és beszúrni elemeket.

Ahelyett, hogy valamiféle kereséssel direkt módon próbálnánk eldönteni, hogy $\mathbf{x}^{\mathbf{w}} \in \mathrm{Lm}\,(G)$ fennáll-e, a következőt tesszük. Feljegyezzük M elemei mellé, hogy hány alkalommal szúrtuk be őket. Bebizonyítjuk, hogy ha $\mathbf{x}^{\mathbf{w}}$ az M minimális eleme egy lépésben, akkor pontosan akkor teljesül $\mathbf{x}^{\mathbf{w}} \notin \mathrm{Lm}\,(G)$, ha az $\mathbf{x}^{\mathbf{w}}$ mellé feljegyzett szám megegyezik az $\mathbf{x}^{\mathbf{w}}$-ben nemnulla kitevővel szereplő változók számával.

Egy $\mathbf{x}^{\mathbf{w}}$ pontosan akkor standard monom, vagy $\mathrm{Lm}\,(I)$ minimális generátora, ha minden eggyel kisebb fokú osztója standard monom. Amikor $\mathbf{x}^{\mathbf{w}}$-vel foglalkozunk, addigra már az összes osztójával végeztünk (tehát vagy vizsgáltuk már, vagy többé nem is fogjuk). Ha minden eggyel kisebb fokú osztója standard monom, akkor $\mathbf{x}^{\mathbf{w}}$-t mindnél beszúrtuk M-be. Tehát a fent javasolt számláló $\mathbf{x}^{\mathbf{w}}$-re pontosan akkor egyenlő az $\mathbf{x}^{\mathbf{w}}$-ben szereplő változók számával, ha $\mathbf{x}^{\mathbf{w}} \in \mathrm{Sm}\,(I(V))$ vagy $\mathbf{x}^{\mathbf{w}}$ monom $\mathrm{Lm}\,(I)$ minimális generátora. Ez viszont ekvivalens azzal, hogy $\mathbf{x}^{\mathbf{w}} \notin \mathrm{Lm}\,(G)$ amikor ezt tesztelnünk kell.

Szükségünk van $\mathbf{u_j}^{\mathbf{w}}$ kiszámolására is. Ehhez M elemei mellé még további értékeket is érdemes felírni. Ha $x_\ell \mathbf{x}^{\mathbf{w}'} = \mathbf{x}^{\mathbf{w}}$ és $\mathbf{x}^{\mathbf{w}}$-t most első ízben szúrjuk be M-be, akkor írjuk fel mellé a már úgyis kiszámolt $\mathbf{u_j}^{\mathbf{w}'}$ értékeket (és persze ℓ-et se feledjük). Így minden egyes $\mathbf{u_i}^{\mathbf{w}}$ kiszámolható egyetlen szorzással, ez összesen tehát $i \leq m$ aritmetikai művelet.

Legyen $V \setminus U = \{\mathbf{v}_1, \ldots, \mathbf{v}_{m-i+1}\}$. Amikor p polinommal dolgozunk, $p \in I(V)$ eldöntéséhez szükségünk lesz rá, hogy minden pontban kiszámoljuk p helyettesítési értékét. Így nem túl nagy többletköltséggel megtudjuk, és eltároljuk q_i-nek V-n felvett értékeit is. Emiatt p számolásakor feltehető, hogy az alábbi

$$\left[\begin{array}{cccc|ccccc} 1 & q_1(\mathbf{u}_2) & \ldots & q_1(\mathbf{u}_{i-1}) & q_1(\mathbf{v}_1) & \ldots & q_1(\mathbf{v}_{m-i+1}) & q_1(\mathbf{x}) \\ 0 & 1 & \ldots & q_2(\mathbf{u}_{i-1}) & q_2(\mathbf{v}_1) & \ldots & q_2(\mathbf{v}_{m-i+1}) & q_2(\mathbf{x}) \\ & \ldots & & & & & \ldots & \\ 0 & 0 & \ldots & 1 & q_{i-1}(\mathbf{v}_1) & \ldots & q_{i-1}(\mathbf{v}_{m-i+1}) & q_{i-1}(\mathbf{x}) \\ \mathbf{u_1}^{\mathbf{w}} & \mathbf{u_2}^{\mathbf{w}} & \ldots & \mathbf{u_{i-1}}^{\mathbf{w}} & \mathbf{v_1}^{\mathbf{w}} & \ldots & \mathbf{v_{i-1}}^{\mathbf{w}} & \mathbf{x}^{\mathbf{w}} \end{array}\right]$$

mátrixot ismerjük. Amint a helyesség bizonyításában is láttuk, ha ezen mátrix utolsó sorának első $i-1$ elemét kinullázzuk az első $i-1$ sor segítségével, akkor éppen az algoritmusban leírt lépéseket végezzük, tehát az alsó sorban a $p(\mathbf{u}_j)$, illetve a $p(\mathbf{v}_j)$ értékek fognak szerepelni, a jobb alsó polinom pedig éppen $p(\mathbf{x})$ lesz. Kihasználva, hogy a $q_j(\mathbf{x})$ polinomok csupa standard monomból állnak, így legfeljebb m nemnulla monomot tartalmaznak (sőt q_j

legfeljebb j-t), látható, hogy $p(\mathbf{u}_j)$ $(j = 1 \ldots m)$ és $p(\mathbf{x})$ polinom számításához $O(m^2)$ aritmetikai operáció elegendő.

Minden standard monomra összesen n elemet szúrunk be M-be, azaz összesen nm-et. Egy beszúrás költsége $\log |M| \leq \log(mn)$-nel arányos, tehát ebből a részből a költség $O(bmn^2 \log(mn))$. Az is következik, hogy összesen legfeljebb mn monomra kellett kiszámolni a megfelelő p polinomot, ennek ára $O(m^3 n)$ aritmetikai művelet.

A további műveletek nagyságrendje láthatóan kisebb, az teljes futásidő ezért valóban $O\left(am^3 n + bmn^2 \log(mn)\right)$.

A tipikus használat esetét mutató példában az $O(m^3 n)$ költség könnyen ellenőrizhető, hiszen ilyenkor a és b konstans, és $O(\log(mn)) = O(\log(m)) < O(m^\varepsilon)$. □

4.4. Véges pontrendszer lex standard monomjai

Ebben az alfejezetben kombinatorikus algoritmust mutatunk véges pontrendszerhez tartozó $I(V)$ ideál lex standard monomjainak kiszámolására. Ez azt jelenti, hogy a módszer aritmetikai operáció nélkül működik, ráadásul nagyvonalúan elemezve is mindössze $O\left(m^2 n\right)$ elemi műveletre lesz szükségünk, amely becslést később még javítjuk. Cerlienco és Mureddu [9] munkájából más kombinatorikus algoritmus már ismert. A futásidőt ők ugyan nem elemezték, de ellenőrizhető, hogy módszerük költsége $m^2 n^2$-tel arányos.

Szükségünk lesz V bizonyos előfeldolgozására: egy V fordított elemeit tartalmazó szófát készítünk. A számunkra lényeges definíciókat felidézzük, részletesebb leírás található például [26] 6.3. fejezetében. A V pontrendszer fordított szófája könnyen feldolgozható struktúrában tárol minden számunkra érdekes információt V-ről.

Szófa

Elsőként idézzük fel a szófa nevű adatstruktúrával kapcsolatos definíciókat.

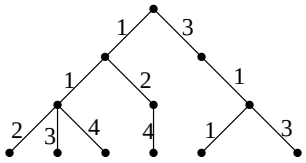
*Gyökeres fá*nak hívunk egy olyan – gráfelméleti értelemben vett – fát, amelynek van egy *gyökér*nek nevezett kitüntetett csúcsa. Azt mondjuk, hogy egy csúcs a fa *i. szintjé*n van, ha a csúcs gyökértől vett távolsága i. Speciálisan tehát a gyökér a 0. szinten található. A *fának n szintje van*, vagy n *mélységű*, ha a gyökértől legtávolabb levő csúcs az n. szinten van. Ha v egy a gyökértől különböző csúcs, akkor v *szülője* a gyökeret v-vel összekötő úton v-t megelőző u csúcs. Ilyenkor v az u egy *gyermeke*. A gyökérnek nincs szülője. Az olyan pontokat, amelyeknek nincs gyermekük, *levél*nek nevezzük. Ha v az $i > 0$ szinten levő csúcs, akkor tetszőleges $0 \leq j < i$ esetén v *csúcs*

*j. szintű felmenőjé*nek hívjuk azt az egy u csúcsot, amely a v-t a gyökérrel összekötő úton a fa j. szintjén van. Ilyenkor v az u *leszármazott*ja.

A *szófa* olyan gyökeres fa, amelynek minden élére egy rögzített ábécé valamely jelét írjuk. Egy csúcsból a gyermekei felé mutató élekre különböző értékek kerülnek. Így a csúcsokat megnevezhetjük az ábécé véges hosszú szavaival: egy csúcs neve a gyökértől hozzá vezető úton a szimbólumok összeolvasásával kapott szó lehet. A mi esetünkben az ábécé egy esetben a természetes számok halmaza, egy esetben pedig az $\{\alpha_1, \ldots, \alpha_k\}$ halmaz lesz, ahol $V \subseteq \{\alpha_1, \ldots, \alpha_k\}^n$.

Az algoritmus naiv változata

Legyen most is $|V| = m$, és a fejezet további részében feltesszük, hogy $m > 0$. Legyen T a V fordított elemeihez épített szófa, azaz T egy n szintű fa, m levele van, amelyek mind az n. szinten találhatóak és a gyökértől egy levélig vezető úton összeolvasva az éleken szereplő értékeket, olyan $\beta_n, \beta_{n-1}, \ldots, \beta_1$ sorozatot kapunk, amelyre $(\beta_1, \ldots, \beta_n) \in V$. Röviden T-t a V *fordított szófájá*nak fogjuk nevezni. Az alábbi ábra egy egyszerű példát mutat: a $V = \{(2,1,1), (3,1,1), (4,1,1), (4,2,1), (1,1,3), (3,1,3)\}$ pontrendszerhez tartozó T fordított szófát adtuk meg.



Emlékeztetjük az Olvasót, hogy $\beta_i, \beta_{i+1}, \ldots, \beta_n$ testelemekre

$$V_{\beta_n\beta_{n-1}\ldots\beta_i} = \left\{(v_1, \ldots, v_{i-1}) \in \mathbb{F}^{i-1} \ : \ (v_1, \ldots, v_{i-1}, \beta_i, \ldots \beta_n) \in V\right\}.$$

Ha $V_{\beta_n\beta_{n-1}\ldots\beta_i} \neq \emptyset$, akkor létezik (és egyértelmű) egy olyan v csúcs T szófa $(n-i+1)$. szintjén, amelyhez a gyökérből a rendre $\beta_n, \beta_{n-1}, \ldots, \beta_i$-vel jelölt élekből álló út vezet. Vegyük észre, hogy a $V_{\beta_n\beta_{n-1}\ldots\beta_i}$ pontrendszer fordított szófája éppen T azon részfája, amely v-ből és v összes T-beli leszármazottjából áll, és gyökere v. Az algoritmus első – naiv – változata nem tesz mást, mint ezt az észrevételt ötvözi a lexikografikus standard monomok rekurzív szerkezetéről szóló megállapításainkkal.

Az algoritmus során S_v halmazokat számolunk, végül minden v csúcsra

$$S_v = \mathrm{Sm}\left(I(V_{\beta_n\beta_{n-1}\ldots\beta_i})\right)$$

fog teljesülni, ahol a gyökérből v-be vezető út $\beta_n\beta_{n-1}\ldots\beta_i$ elemekkel indexelt és a standard monomokat a lexikografikus rendezésre tekintjük. Amennyiben

v a T fa $(n-i)$. szintjén van, akkor $I(V_{\beta_n\beta_{n-1}\ldots\beta_i}) \subseteq \mathbb{F}[x_1,\ldots,x_i]$, ezért S_v minden eleme $x_1,\ldots,x_i$ változók monomja lesz.

A 3.10. következmény alapján S_v elemei megkaphatóak, feltéve, hogy már ismerjük az $S_{v_j} = \mathrm{Sm}\left(I(V_{\beta_n\beta_{n-1}\ldots\beta_i\beta_{i-1,j}})\right)$ standard monom halmazokat $j = 1,\ldots,r$ esetén, ahol $v_1,\ldots,v_r$ a v csúcs összes gyermeke. Valóban, minden olyan $x_1^{w_1}\ldots x_{i-1}^{w_{i-1}}$-re, amely legalább egy S_{v_j} halmazban szerepel, az $x_1^{w_1}\ldots x_{i-1}^{w_{i-1}}x_i^w$ monom benne van S_v-ben, feltéve hogy van legalább $w+1$ olyan v_j a v csúcs gyermekei között, amelyre $x_1^{w_1}\ldots x_{i-1}^{w_{i-1}} \in S_{v_j}$. Ha speciálisan v a gyökér, akkor $S_v = \mathrm{Sm}\,(I(V))$, amit ki szeretnénk számolni.

Az algoritmus alábbi naiv változata ezt a tervet valósítja meg. Megjegyezzük, hogy $i = 1$ esetén az $x_1^{w_1}\ldots x_{i-1}^{w_{i-1}}$ üres szorzatot 1-nek értelmezzük.

```
For v ∈ {T levele} do S_v := {1}; endfor;
For i = 1 to n do
   For v ∈ {T (n − i). szintjén levő csúcs} do
      S_v := ∅;
      r := (v fiainak száma); {v_1, ..., v_r} := (v fiai);
      For j = 1 to r do
         For x_1^{w_1} ... x_{i-1}^{w_{i-1}} ∈ S_{v_j} do
            w := 1 + max({ℓ ≥ 0 : x_1^{w_1} ... x_{i-1}^{w_{i-1}} x_i^ℓ ∈ S_v} ∪ {−1});
            S_v := S_v ∪ {x_1^{w_1} ... x_{i-1}^{w_{i-1}} x_i^w};
         endfor;
      endfor;
   endfor;
endfor;
```

A helyesség a fent elmondottak alapján nagyjából világos, csupán egy egyszerű további észrevételt kell tennünk: minden szóba jövő rögzített i érték mellett j-re vonatkozó indukcióval igazoljuk, hogy S_v-hez pontosan akkor vesszük hozzá a j. lépésig az $x_1^{w_1}\ldots x_{i-1}^{w_{i-1}}x_i^w$ monomot, ha $S_{v_1},\ldots,S_{v_j}$ halmazokban $w+1$-szer előfordul az $x_1^{w_1}\ldots x_{i-1}^{w_{i-1}}$ monom.

Ez $j = 1$-re igaz, hiszen ez esetben a tekintett maximum -1 lesz, tehát akkor és csak akkor vesszük be $x_1^{w_1}\ldots x_{i-1}^{w_{i-1}}x_i^w = x_1^{w_1}\ldots x_{i-1}^{w_{i-1}}$ monomot S_v-be, ha az szerepel S_{v_1}-ben. Tegyük most fel, hogy az állítás $j-1$-ig igaz. Amikor a j. lépésben $x_1^{w_1}\ldots x_{i-1}^{w_{i-1}}x_i^w$-t hozzávesszük S_v-hez, akkor ($w > 0$ esetén) tudjuk, hogy $x_1^{w_1}\ldots x_{i-1}^{w_{i-1}}x_i^{w-1}$ már eleme S_v-nek, ezért $x_1^{w_1}\ldots x_{i-1}^{w_{i-1}}$ az indukciós feltétel szerint legalább w-szer előfordult már $S_{v_1}\ldots S_{v_{j-1}}$-ek között. Ez viszont az S_{v_j}-beli előfordulásával együtt éppen a kívánt $w+1$-et adja. □

Vegyük észre, hogy bár négy egymásba ágyazott `For` ciklust használunk, mégis mindössze nm alkalommal fut le a legbelső `For` ciklusban szereplő két utasítás, ugyanis könnyű látni, hogy T minden szintjén az S_v

halmazok elemszámának összege pont m. Ahhoz azonban, hogy az algoritmust igazán hatékonnyá tegyük, kellően gyors módszert kellene találni a $\max\{\ell \geq 0 : x_1^{w_1} \dots x_{i-1}^{w_{i-1}} x_i^{\ell} \in S_v\}$ mennyiségek számolására. Ennek érdekében egy újabb szófát fogunk használni, és külsőségeiben jócskán megváltoztatjuk az algoritmust.

Hatékony megvalósítás

Legyen $\mathrm{Sm}\,(I(V))$ szófája S. Pontosabban, S éleire természetes számok kerülnek, amelyeket a gyökérből a levelekbe vezető utak mentén összeolvasva éppen az $\mathrm{Sm}\,(I(V))$-ben szereplő monomok kitevővektorait kapjuk. Az i. szinten levő csúcshoz vezető út $x_1, \dots, x_i$ változók egy monomjának kitevővektora.

Az algoritmusunk javított változata ezt a szófát fogja elkészíteni, amiből $I(V)$ lexikografikus standard monomjai tehát könnyen leolvashatóak. A konstrukcióhoz szükségünk lesz egy megfeleltetésre. A készülő S fa minden csúcsához hozzárendeljük T bizonyos leveleit. A hozzárendelés olyan lesz, hogy T minden l levelét S minden szintjén pontosan egy csúcshoz rendeljük, ráadásul úgy, hogy ezek a csúcsok S-ben egy utat alkotnak. Kényelmi okokból nem fogjuk azonban a teljes hozzárendelést eltárolni. Ehelyett T minden l levelére $A[l]$ érték S azon csúcsa, amelyhez legutóbb hozzárendeltük l-et. Az algoritmus a gyökértől szintenként lefele haladva készíti S szófát.

```
S := (egyetlen gyökérből álló fa); g := S gyökere;
For l ∈ {T levelei} do A[l] := g; endfor;
For i = 1,...,n do
   For v ∈ {T csúcsai az (n − i). szinten} do
      For u ∈ {S csúcsai az (i − 1). szinten} do b[u] := 0; endfor;
      For l ∈ {T azon levelei, amelyek v leszármazottai} do
         b[A[l]] := b[A[l]] + 1;
         A[l] := (A[l] azon gyermeke, amelybe vezető élen
                  (b[A[l]] − 1) szám szerepel);
         //Létrehozunk egy ilyen gyermeket, ha még nem létezik
      endfor;
   endfor;
endfor;
```

Az algoritmus helyességének igazolásához, azaz annak belátásához, hogy S valóban $\mathrm{Sm}\,(I(V))$ (a fenti értelemben vett) szófája, először bebizonyítjuk a hozzárendelésnek három alapvető tulajdonságát.

4.5. Lemma. *T tetszőleges l levelére igaz, hogy S azon csúcsai, amelyekhez l-et hozzárendeltük S-ben egy levelétől a gyökérig tartó utat alkotnak.*

Bizonyítás: Kezdetben l levelet a gyökérhez rendeltük, majd S minden újabb szintjének készítésekor az utolsó eltárolt helyének egy gyermekéhez tettük. □

4.6. Lemma. *Ha S egy i. szinten levő csúcsához hozzárendeltük T-nek l_1 és l_2 különböző leveleit, akkor a T-beli $(n-i)$. szintű felmenője nem lehet azonos l_1 és l_2-nek.*

Bizonyítás: Ha l_1 és l_2 a lemma feltételeinek eleget tesz, akkor 4.5. lemma szerint az $(i-1)$. szinten is azonos csúcshoz vannak rendelve. Így S fa i. szintjének építésekor, ha a

$$\texttt{For } v \in \{T \texttt{ csúcsai az } (n-i)\texttt{. szinten}\} \texttt{ do}$$

ciklusban közös $(n-i)$. szintű v felmenőre kerülne a sor, akkor $A[l_1] = A[l_2]$ lenne, és ezért a b számláló gondoskodna róla, hogy S szófa i. szintjén már ne kerüljenek azonos csúcsba. □

4.7. Lemma. *Legyen l a T egy levele, amely a $(\beta_1, \ldots, \beta_n) \in V$ ponthoz tartozik, és tegyük fel, hogy l-et S azon leveléhez rendeltük, amelyhez a gyökérből a $(w_1, \ldots, w_n)$ egészekkel jelzett úton lehet eljutni. Ekkor minden $1 \leq i \leq n$ esetén*

$$x_1^{w_1} \ldots x_i^{w_i} \in \mathrm{Sm}\left(I(V_{\beta_n \beta_{n-1} \ldots \beta_{i+1}})\right). \tag{6}$$

Bizonyítás: Az állítást i-re vonatkozó indukcióval látjuk be.

Legyen először $i > 1$, és tegyük fel, hogy (6) igaz $(i-1)$-re. Legyen l, $(\beta_1, \ldots, \beta_n)$ és $(w_1, \ldots, w_n)$ a feltételeknek megfelelő, és S fa $(w_1, \ldots, w_{i-1})$-hez tartozó ($(i-1)$. szinten levő) csúcsa u. A 4.5. lemma szerint l levél S szófa $(i-1)$. szintjén u-hoz van rendelve, az i. szinten pedig u-nak w_i-hez tartozó fiához. Az algoritmus alapján ez csak úgy lehetséges, ha vannak olyan $l_0, l_1, \ldots, l_{w-1}, l_w = l$ különböző levelei T-nek, amelyek S fa $(i-1)$. szintjén ugyancsak u-hoz rendeltek, és amelyek $(n-i)$. szintű felmenője T-ben közös, az a csúcs, amelyhez a gyökérből a $(\beta_n, \beta_{n-1}, \ldots, \beta_{i+1})$-gyel jelölt út vezet. Legyen l_j csúcs $(n-i+1)$. szintű felmenője T-ben v_j. A 4.6. lemma miatt ezek páronként különbözőek. A T gyökeréből a v_j-kbe vezető út tehát $(\beta_n, \beta_{n-1}, \ldots, \beta_{i+1}, \beta_{i,j})$, valamilyen páronként különböző $\beta_{i,j}$ számokra. Alkalmazva az indukciós feltevést,

$$x_1^{w_1} \ldots x_{i-1}^{w_{i-1}} \in \mathrm{Sm}\left(I(V_{\beta_n \beta_{n-1} \ldots \beta_{i+1}, \beta_{i,j}})\right)$$

minden $0 \leq j \leq w_i$ esetén. Így a 3.10. következmény szerint

$$x_1^{w_1} \ldots x_i^{w_i} \in \mathrm{Sm}\left(I(V_{\beta_n \beta_{n-1} \ldots \beta_{i+1}})\right),$$

amint állítottuk.

Az indukció $i = 1$ kezdőlépésének belátásához vegyük észre, hogy minden, amit az indukciós feltétel alkalmazása előtt mondtunk, működik $i = 1$-re is. A bizonyítást tehát onnan folytatjuk, felhasználva, hogy van $w_1 + 1$ olyan $\beta_{1,j}$, amire $(\beta_{1,j}, \beta_2, \ldots, \beta_n) \in V$. Ez azt jelenti, hogy $\left|V_{\beta_n\beta_{n-1}\ldots\beta_2}\right| \geq w_1 + 1$, ezért $x_1^{w_1} \in \mathrm{Sm}\left(I(V_{\beta_n\beta_{n-1}\ldots\beta_2})\right)$. Ezt kellett megmutatnunk. □

A helyesség bizonyítása most már nem lesz nehéz.

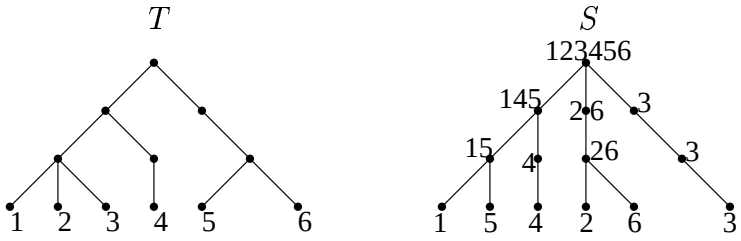
Először is, a 4.6. lemmát $i = n$ választással alkalmazva – miután T gyökere közös felmenője minden l levélnek – azt kapjuk, hogy S minden leveléhez legfeljebb egy l-et rendelhettünk hozzá. Az algoritmusból világos, hogy S minden csúcsához T-nek legalább egy levelét hozzárendeltük, tehát S-nek pontosan annyi levele van, mint T-nek.

Most $i = n$-re alkalmazva a 4.7. lemmát, látható, hogy S tetszőleges levele által megadott $(w_1, \ldots, w_n)$ kitevővektorra $x_1^{w_1} \ldots x_n^{w_n} \in \mathrm{Sm}\,(I(V))$, azaz S levelei valóban standard monomokat határoznak meg. Végül az is igaz, hogy minden standard monomot megad S, ugyanis

$$|\mathrm{Sm}\,(I(V))| = |V| = (T \text{ leveleinek száma}) = (S \text{ leveleinek száma}).$$

□

Az alábbi ábra a $V = \{(2,1,1), (3,1,1), (4,1,1), (4,2,1), (1,1,3), (3,1,3)\}$ pontrendszerhez tartozó T fordított szófát, és a hozzá tartozó S szófát ábrázolja. Beszámoztuk T leveleit, hogy S csúcsainál látható legyen a hozzárendelés. Elhagytuk ugyanakkor S éleinek számozását, amely könnyen rekonstruálható: egy csúcs gyerekeit balról jobbra haladva kell 0-tól kezdve számozni. Az S szófa alapján $\mathrm{Sm}\,(I(V)) = \{1, x_3, x_2, x_1, x_1x_3, x_1^2\}$.



4.8. Tétel. *Legyen $r + 1$ a T szófa maximális fokszáma és $|V| = m$. A fent bemutatott módszer ekkor $O(mnr)$ elemi művelettel, a testben csak egyenlőség tesztelésével, tehát aritmetikai operáció nélkül meghatározza $I(V)$ lexikografikus standard monomjait. Ha a test elemein van konstans időben ellenőrizhető rendezés, akkor ugyanez megvalósítható $O(mn \log r)$ időben is.*

Bizonyítás Az algoritmus két fő lépése – T, illetve S elkészítése – közül az első bizonyul időigényesebbnek.

Utóbbi $O(nm)$ költséggel megoldható. Vegyük észre ugyanis, hogy S szófa i. szintjének megépítéséhez $O(m)$ munkát végzünk, miután T minden levelével csak egyszer foglalkozunk, és T alkalmas előfeldolgozásával a T-ben $(n-i)$. szinten levő pontokhoz tartozó levelek konstans időben megkaphatóak.

A T-t rekurzívan építjük, V pontjait sorra szúrjuk be a készülő fordított szófába. A fa mélysége n, és m beszúrást kell elvégeznünk, ezért a költség $O(mn)$-szerese az egy csúcsban töltött időnek. Egy csúcsban, ha össze kell hasonlítanunk egy elemet az összes ott található másikkal, akkor nyilván $O(r)$ időt töltünk. Ha ismert gyorsan tesztelhető rendezés $\mathbb{F}$-ben, akkor – ha a csúcsokat rendezve tároljuk – bináris kereséssel megy ugyanez $O(\log r)$ lépésben. □

5. Számolások konkrét pontrendszerekre

Most rátérünk néhány speciálisan választott véges V pontrendszer standard monomjainak, illetve bizonyos esetekben egy Gröbner-bázisának konkrét kiszámolására. Leginkább szimmetrikus pontrendszerekkel fogunk foglalkozni, azaz olyan V véges halmazokkal, amelyekre teljesül, hogy $\mathbf{y} \in V$ esetén $\mathbf{y}$ koordinátáit tetszőlegesen permutálva a kapott vektor is V-ben van. Teljes általánosságban viszonylag keveset fogunk tudni róluk mondani, azonban több speciális esetben pontosan meg tudjuk adni a standard monomokat illetve egy Gröbner-bázist, amelyeket aztán a következő fejezetben különböző feladatok megoldásában alkalmazni is fogunk. Egy olyan példát is bemutatunk, ahol V nem szimmetrikus, nevezetesen az irányított fák esetét.

5.1. Szimmetrikus pontrendszerekről általában

Legyen $V \subseteq \{\alpha_1, \ldots, \alpha_k\}^n \subseteq \mathbb{F}^n$ véges pontrendszer. Egy $\mathbf{y} \in V$ pont *típus*a $\boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_k)$, ha $\mathbf{y}$ koordinátái között pontosan λ_i-szer szerepel α_i minden 1 és k közötti i-re. Egy $\boldsymbol{\lambda} \in \mathbb{Z}^k$ egészekből álló vektor *típus*, ha valamely $\mathbf{y} \in \{\alpha_1, \ldots, \alpha_k\}^n$-nek a típusa, azaz pontosan akkor, ha minden $1 \leq i \leq k$-ra $\lambda_i \geq 0$ és $\sum_{i=1}^{k} \lambda_i = n$.

Azt mondjuk, hogy $V \subseteq \{\alpha_1, \ldots, \alpha_k\}^n$ szimmetrikus, ha teljesül rá, hogy $\mathbf{y} \in V$ esetén $\{\alpha_1, \ldots, \alpha_k\}^n$ minden $\mathbf{y}$-nal megegyező típusú eleme V-ben van. Más szóval létezik olyan D típusokból álló halmaz, amelyre

$$V = V_{D,n} := \{\mathbf{y} \in \{\alpha_1, \ldots, \alpha_k\}^n : \ \mathbf{y} \text{ típusa } D\text{-ben van}\}.$$

Természetesen $V_{D,n}$ definíciója akkor is értelmes, ha $D \subseteq \mathbb{Z}^k$ tetszőleges, azaz nem feltétlen csak típusokból áll.

A következőkben a lex standard monomok rekurzív tulajdonsága segítségével megadjuk szimmetrikus pontrendszerhez tartozó lexikografikus standard monomoknak egy jellemzését. A tételt valójában csak a $k = 2$ esetre fogjuk alkalmazni, azonban az általános eset bizonyítása semmivel sem bonyolultabb.

Szükségünk lesz néhány jelölésre. Legyen $\boldsymbol{\mu}_j \in \mathbb{Z}^k$ a j. egységvektor, azaz $\boldsymbol{\mu}_j$ minden koordinátája 0, kivéve a j-ediket, amely 1. Emlékeztetünk, hogy $[k] = \{1, 2, \ldots, k\}$. Ha $D \subseteq \mathbb{Z}^k$ és $w \in \mathbb{N}$, akkor legyen

$$D^{(w)} = \bigcup_{\substack{H \subseteq [k] \\ |H| = w+1}} \bigcap_{j \in H} (D - \boldsymbol{\mu}_j),$$

ahol $D-\boldsymbol{\mu}_j=\{\boldsymbol{\lambda}-\boldsymbol{\mu}_j\,:\,\boldsymbol{\lambda}\in D\}$. Speciálisan $w\geq k$ esetén $D^{(w)}=\emptyset$. Ha $\mathbf{w}\in\mathbb{N}^n$, akkor

$$D^{(\mathbf{w})}:=\left(\ldots\left(\left(D^{(w_1)}\right)^{(w_2)}\right)^{\cdots}\right)^{(w_n)}.$$

5.1. Tétel. $\mathbf{x^w}$ *pontosan akkor lexikografikus standard monomja az* $I\left(V_{D,n}\right)$ *ideálnak, ha* $\mathbf{0}\in D^{(\mathbf{w})}$.

Bizonyítás: Legyen

$$A=\left\{\boldsymbol{\mu}\in\mathbb{Z}^k\,:\,\mathbf{x}^{\mathbf{w}}\in\mathrm{Sm}\left(I\left(V_{D-\boldsymbol{\mu},n}\right)\right)\right\}.$$

A bizonyítást n-re vonatkozó teljes indukcióval végezzük: megmutatjuk, hogy $A=D^{(\mathbf{w})}$. Nyilvánvaló, hogy ebből következik a tétel állítása.

Tekintsük először az $n=1$ esetet. Pontosan akkor teljesül $\boldsymbol{\mu}\in A$, azaz $x^w\in\mathrm{Sm}\left(I\left(V_{D-\boldsymbol{\mu},1}\right)\right)$, ha $\left|V_{D-\boldsymbol{\mu},1}\right|>w$, ami akkor és csak akkor áll fenn, ha van legalább $w+1$ olyan $j\in[k]$, amelyre $\boldsymbol{\mu}_j\in D-\boldsymbol{\mu}$, hiszen $n=1$ hosszon az összes lehetséges típus $\boldsymbol{\mu}_1,\ldots,\boldsymbol{\mu}_k$. Ezek szerint $\boldsymbol{\mu}\in A$ ekvivalens azzal, hogy létezik $H\subseteq[k]$, $|H|=w+1$, hogy $\forall\, j\in H$ esetén $\boldsymbol{\mu}_j\in D-\boldsymbol{\mu}$. Miután $\boldsymbol{\mu}_j\in D-\boldsymbol{\mu}\iff\boldsymbol{\mu}\in D-\boldsymbol{\mu}_j$, ezért beláttuk, hogy $\boldsymbol{\mu}\in A$ ugyanakkor áll fent, mint $\boldsymbol{\mu}\in D^{(w)}$.

Tegyük most fel, hogy $n>1$ és az állítás igaz $n-1$-re, azaz

$$D^{(w_1,\ldots,w_{n-1})}=\left\{\boldsymbol{\mu}\in\mathbb{Z}^k\,:\,x_1^{w_1}\ldots x_{n-1}^{w_{n-1}}\in\mathrm{Sm}\left(I\left(V_{D-\boldsymbol{\mu},n-1}\right)\right)\right\}=:B.$$

Ekkor $B^{(w_n)}=D^{(\mathbf{w})}$ miatt elegendő belátni, hogy $A=B^{(w_n)}$.

A 3.10. következmény szerint $\boldsymbol{\mu}\in A$ akkor és csak akkor teljesül, ha létezik olyan w_n+1 elemű $H\subseteq[k]$ halmaz, amelyre $j\in H$-ból következik

$$x_1^{w_1}\ldots x_{n-1}^{w_{n-1}}\in\mathrm{Sm}\left(I\left(\left(V_{D-\boldsymbol{\mu},n}\right)_{\alpha_j}\right)\right).\tag{7}$$

Vegyük észre, hogy $\left(V_{D-\boldsymbol{\mu},n}\right)_{\alpha_j}=V_{D-(\boldsymbol{\mu}+\boldsymbol{\mu}_j),n-1}$ és emiatt (7) ekvivalens $\boldsymbol{\mu}+\boldsymbol{\mu}_j\in B$-vel, ami pedig $\boldsymbol{\mu}\in B-\boldsymbol{\mu}_j$-vel. Azt kaptuk, hogy $\boldsymbol{\mu}\in A$ akkor és csak akkor, ha van w_n+1 elemű $H\subseteq[k]$ halmaz, amelyre $j\in H\Rightarrow\boldsymbol{\mu}\in B-\boldsymbol{\mu}_j$, ezért $A=B^{(w_n)}$. □

5.2. Egy szimmetrikus eset: modulo r ℓ-széles pontrendszer

A $V_{D,n}$ pontrendszert, amelyet ebben a fejezetben vizsgálni fogunk, a következő alakú $D\subseteq\mathbb{Z}^2$ definiálja:

$$D=D(d,\ell,r)=\left\{(\lambda,n-\lambda)\in\mathbb{N}^2\,:\,d\leq\lambda\bmod r\leq d+\ell-1\right\},$$

ahol d, r és ℓ rögzített egészek, amelyekre fennáll, hogy $0 \leq d \leq n$, $d < r$ és $1 \leq \ell < r$. Szavakban: $V_{D,n} \subseteq \{\alpha_1, \alpha_2\}^n$ azon pontokat tartalmazza, amelyekben a koordináták között α_1 előfordulásának száma modulo r a d és $d + \ell - 1$ egészek közé esik. A $V_{D,n}$-t *modulo r ℓ-széles pontrendszer*nek nevezzük.

Ki fogjuk számolni ezen pontrendszer lexikografikus standard monomjait, majd megmutatjuk, hogy a pontosan ℓ-széles pontrendszer (tehát amelyet nem modulárisan tekintünk) redukált Gröbner-bázisa minden $x_1 \succ x_2 \succ \cdots \succ x_n$-nek eleget tevő tagsorrendre megegyezik. Speciálisan tehát a standard monomok is azonosak ilyen rendezésekre a lex standard monomokkal. A redukált Gröbner-bázist is megadjuk.

Hasonló állítás egyébként a modulo r esetben nem igaz: nem nehéz megmutatni, hogy a paraméterekre vonatkozó néhány egyszerű feltétel teljesülése esetén a lex és deglex rendezésre vonatkozó standard monomok eltérnek az olyan $\mathbb{F}$ testek felett, amelyek karakterisztikája nem osztója r-nek.

A nem moduláris esetre vonatkozó eredmények közül Anstee, Sali és Rónyai [2] munkája volt az első, amelyben az $\ell = 1$ esetre kiszámolták a lexikografikus standard monomokat. Hegedűs és Rónyai [22] később meghatározták az $x_1 \succ x_2 \succ \cdots \succ x_n$ tulajdonságot kielégítő rendezésekre vonatkozó redukált Gröbner-bázist is. A – továbbra is nem moduláris – ℓ-széles esetet az utóbbi szerzőpáros Friedl Katalinnal együtt térképezte fel [20]. Eredményük jelen dolgozatban az 5.7. tételben szerepel, amely igazolásához is az ő cikküket vettem alapul. Az alfejezet további tételei korábban nem voltak ismertek.

Mielőtt belekezdenénk $\mathrm{Sm}\,(I(V_{D,n}))$ kiszámolásába, megmutatjuk $V_{D,n}$ egy másik leírását. Álljon $\mathcal{F}$ halmazcsalád $[n]$ azon részhalmazaiból, amelyek elemszáma modulo r a d és $d + \ell - 1$ egészek között van. Ekkor az $\mathcal{F}$ elemeinek karakterisztikus vektoraiból álló pontrendszer éppen $V_{D,n}$, feltéve, hogy $\alpha_1 = 1$ és $\alpha_2 = 0$. Az alkalmazásokról szóló fejezetben mutatunk példákat, hogy egy halmazcsaládhoz ilyen módon megfeleltethető pontrendszer ideálja (illetve annak standard monomjai és Gröbner-bázisa) miként segít a halmazcsalád kombinatorikus tulajdonságainak leírásában.

Lexikografikus standard monomok

Tekintsünk egy négyzetrácsot, amely vízszintes tengelye (X irány) az 1, függőleges tengelye (Y irány) a 0 számokhoz tartozik. Egy olyan töröttvonalat, amely az origóból indul, és a rácson egységnyit lépdelve halad *rácspoligon*nak nevezzük. Egy lépés kizárólag felfele vagy jobbra történhet. Kölcsönösen egyértelmű módon megfeleltethetünk egy $\mathbf{w} \in \{0,1\}^n$ vektornak egy $\hat{\mathbf{w}}$ rácspoligont. Minden i-re ($1 \leq i \leq n$) legyen az i. szakasza vízszintes $\hat{\mathbf{w}}$-nak, ha

$w_i = 1$, és legyen függőleges egyébként.

A következő tétel $D^{(\mathbf{w})}$ explicit kiszámolásával karakterizálja a $V_{D,n}$ modulo r ℓ-széles pontrendszer lexikografikus standard monomjait. Vegyük észre, hogy egy $\boldsymbol{\lambda} = (\lambda_1, \lambda_2)$ típus megadásához elegendő λ_1-et elárulni, hiszen $\lambda_2 = n - \lambda_1$. Egyszerűbb lesz a számolás, ha ennek megfelelően D-ben is csak az első koordinátákat tároljuk. Az új jelölés szerint tehát

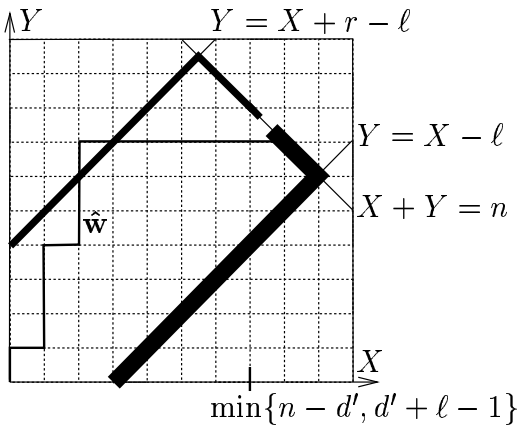
$$D^{(0)} = (D-1) \cup D \text{ és}$$
$$D^{(1)} = (D-1) \cap D.$$

5.2. Tétel. *Legyen* $\mathbf{w} \in \{0,1\}^n$ *és* $d' \in \mathbb{Z}$, *amelyre* $d' \equiv d \pmod r$ *és*

$$\frac{n-r-\ell}{2} < d' \leq \frac{n+r-\ell}{2}.$$

Ekkor $0 \in D^{(\mathbf{w})}$ *pontosan akkor, ha* $\hat{\mathbf{w}}$ *nem metszi előbb az* $Y = X - \ell$ *egyenest, mint az* $Y = X+r-\ell$*-et, és amennyiben* $\hat{\mathbf{w}}$ *végig a két egyenes között marad, akkor a végpontjának* n_1*-gyel jelölt* X *koordinátájára (ami valójában a* $\mathbf{w}$*-ben szereplő* 1 *koordináták száma) teljesül*

$$n_1 \leq \min\{n - d', d' + \ell - 1\}.$$



A példában $n = 15$, $r = 7$, $\ell = 3$ és $d = 1$ vagy $d = 5$. A tétel szerint $\mathbf{x}^{\mathbf{w}} = x_2x_6x_{10}x_{11}x_{12}x_{13}x_{14}x_{15}$ standard monom.

Tetszőleges $\mathbf{w} \in \{0,1\}^n$ esetén $\hat{\mathbf{w}}$ metszi az ábra szerinti vastag vonalak egyikét. Az 5.2. tétel azt állítja, hogy ha $\hat{\mathbf{w}}$ előbb a vékonyabbik vonalat érinti, akkor $\mathbf{x}^{\mathbf{w}}$ a lex rendezésre főtag, egyébként pedig $\mathbf{x}^{\mathbf{w}}$ standard monom. Ha $\mathbf{w}$ kitevővektornak van egynél nagyobb koordinátája, akkor természetesen $\mathbf{x}^{\mathbf{w}}$ főtag. Ezzel tehát jellemeztük a modulo r ℓ-széles pontrendszer lexikografikus standard monomjait.

5.2. tétel bizonyítása: Legyenek a és b egészek, ekkor az $[a,b]$ *egész intervallum*

$$[a,b] := \{c \in \mathbb{Z} \,:\, a \le c \le b\}\,.$$

Speciálisan, ha $a > b$, akkor $[a,b] = \emptyset$. Ha $[a,b] \neq \emptyset$, akkor $[a,b]^{(0)} = [a-1,b]$ és $[a,b]^{(1)} = [a,b-1]$. Általánosabban, tegyük fel, hogy a $\mathbf{w} \in \{0,1\}^n$ vektorban az 1 koordináták száma n_1, a nulláké pedig $n - n_1 = n_0$, és $\mathbf{w}$ minden $\mathbf{w}'$ prefixére teljesül $[a,b]^{(\mathbf{w}')} \neq \emptyset$. Ekkor

$$[a,b]^{(\mathbf{w})} = [a - n_0, b - n_1], \tag{8}$$

és $[a-n_0, b-n_1]$ akkor és csak akkor üres, ha $a - n_0 > b - n_1$, azaz az $[a,b]$ intervallum $b-a+1$ hossza kisebb vagy egyenlő, mint $n_1 - n_0$. Miután $[a,b]^{(w_1,\ldots,w_{n-1})} \neq \emptyset$ és $[a,b]^{(\mathbf{w})} = \emptyset$, ezért $w_n = 1$ és $a - n_0 \le b - (n_1 - 1)$. Tehát, ha $\mathbf{w}$ olyan, mint fent, akkor $[a-n_0, b-n_1] = \emptyset$ akkor és csak akkor, ha $b - a + 1 = n_1 - n_0$. Megállapíthatjuk azt is, hogy ha $\mathbf{w}^*$ a legrövidebb kezdőszelete $\mathbf{w} \in \{0,1\}^n$-nek, amelyre $[a,b]^{(\mathbf{w}^*)} = \emptyset$, akkor $\mathbf{w}^*$ koordinátái között pontosan $b-a+1$-gyel több egyes van, mint 0.

Tegyük most fel, hogy $A \subseteq \mathbb{Z}$ különálló intervallumok uniója, azaz $A = \bigcup_{i\in\Gamma} [a_i, b_i]$, és különböző $i, j \in \Gamma$ esetén $[a_i,b_i] \cup [a_j,b_j]$ nem intervallum. Ekkor világos, hogy

$$A^{(w)} = \bigcup_{i\in\Gamma} [a_i,b_i]^{(w)}. \tag{9}$$

Ha $A \subseteq \mathbb{Z}$, $r \in \mathbb{Z}$ és $\mathbf{w} \in \{0,1\}^n$, akkor az $A - r = \{a - r \,:\, a \in A\}$ halmazra nyilvánvaló, hogy

$$(A-r)^{(\mathbf{w})} = A^{(\mathbf{w})} - r. \tag{10}$$

A mi esetünkben $D = \bigcup_{i\in\mathbb{Z}} (A - ir)$ és $A = [d, d+\ell-1]$. Az $\ell < r$ feltevés miatt az $A - ir = [d-ir, d+\ell-1-ir]$ intervallumok valóban különállóak. Kihasználva (9) és (10) összefüggéseket, n-re vonatkozó indukcióval egyszerűen adódik

$$D^{(\mathbf{w})} = \bigcup_{i\in\mathbb{Z}} \left(A^{(\mathbf{w})} - ir\right), \tag{11}$$

feltéve, hogy $\left|A^{(\mathbf{w}')}\right| < r$ fennáll $\mathbf{w}$ minden $\mathbf{w}'$ kezdőszeletére. Ha van olyan $\mathbf{w}'$ prefix, amire $\left|A^{(\mathbf{w}')}\right| = r$, akkor D intervallumai összeesnek $D^{(\mathbf{w}')}$-ben, azaz $D^{(\mathbf{w}')} = \mathbb{Z}$. Miután $\mathbb{Z}^{(0)} = \mathbb{Z}^{(1)} = \mathbb{Z}$, ezért ilyenkor $D^{(\mathbf{w})} = \mathbb{Z}$ is teljesül.

Tehát (11) segítségével $D^{(\mathbf{w})}$ kiszámolását vissza tudjuk vezetni az $A^{(\mathbf{w})}$ intervalluméra. Speciálisan $D^{(\mathbf{w})} = \emptyset$ pontosan akkor, ha $A^{(\mathbf{w})} = \emptyset$ és nincs olyan $\mathbf{w}'$ kezdőszelete $\mathbf{w}$-nek, amelyre $\left|A^{(\mathbf{w}')}\right| = r$. Legyen $\mathbf{w}^*$ a $\mathbf{w}$ legrövidebb

prefixe, amelyre $A^{(\mathbf{w}^*)} = \emptyset$. Láttuk, hogy $\mathbf{w}^*$-ban ℓ-lel több 1 koordináta van, mint 0, azaz $\hat{\mathbf{w}}^*$ eléri az $Y = X - \ell$ egyenest (pont az utolsó lépésben). Az a feltétel, hogy $\mathbf{w}^*$ minden $\mathbf{w}'$ kezdőszeletére $\left|A^{(\mathbf{w}')}\right| < r$, ekvivalens azzal, hogy $\mathbf{w}'$-ben kevesebb, mint $r - \ell$-lel több 0 van, mint 1, azaz azzal, hogy a $\hat{\mathbf{w}}'$ rácspoligon az $Y = X + r - \ell$ egyenes alatt marad.

Összegezve, $D^{(\mathbf{w})}$ akkor és csak akkor üres, ha $\hat{\mathbf{w}}$ eléri az $Y = X - \ell$ egyenest, méghozzá előbb, mint az $Y = X+r-\ell$-et. Ilyenkor persze $0 \notin D^{(\mathbf{w})}$. Ha $\hat{\mathbf{w}}$ előbb $Y = X + r - \ell$-et éri el, akkor $D^{(\mathbf{w})} = \mathbb{Z}$, ezért $0 \in D^{(\mathbf{w})}$.

Már csak azt az esetet kell megnéznünk, amikor $\hat{\mathbf{w}}$ végig szigorúan a két egyenes között marad. Legyenek $\hat{\mathbf{w}}$ végpontjának koordinátái (n_1, n_0). Ekkor $D^{(\mathbf{w})}$ kiszámolható (11) segítségével. A (8) összefüggés miatt

$$A^{(\mathbf{w})} = [d, d + \ell - 1]^{(\mathbf{w})} = [d - n_0, d + \ell - 1 - n_1],$$

tehát azt kaptuk, hogy

$$D^{(\mathbf{w})} = \bigcup_{i \in \mathbb{Z}} [d + ir - n_0, d + ir + \ell - 1 - n_1]. \tag{12}$$

Az $Y = X + r - \ell$ és $X + Y = n$ egyenesek metszéspontja $\left(\frac{n-r+\ell}{2}, \frac{n+r-\ell}{2}\right)$. Miután (n_1, n_0) az $X + Y = n$ egyenesen, az $Y = X + r - \ell$ alatt van, ezért következik, hogy

$$n_0 \leq \frac{n + r - \ell}{2} \quad \text{és} \tag{13}$$

$$n_1 \geq \frac{n - r + \ell}{2}. \tag{14}$$

Tehát (12) alapján $0 \in D^{(\mathbf{w})}$ pontosan akkor, ha van olyan $i \in \mathbb{Z}$, amelyre $d + ir - n_0 \leq 0 \leq d + \ell - 1 + ir - n_1$. Miután

$$d + ir \leq n_0 \leq \frac{n + r - \ell}{2}$$

(13) miatt, és

$$d + ir \geq n_1 - \ell + 1 \geq \frac{n - r + \ell}{2} - \ell + 1 > \frac{n - r - \ell}{2}$$

(14) miatt, ezért $d' = d + ir$. Azaz $0 \in D^{(\mathbf{w})}$ akkor és csak akkor, ha $d' - n_0 \leq 0 \leq d' + \ell - 1 - n_1$, ami $n_0 = n - n_1$ miatt éppen megegyezik a kívánt $n_1 \leq \min\{n - d', d' + \ell - 1\}$ feltétellel. □

Lex főtagok minimális generátorai

A rácspoligonos megfeleltetés és az 5.2. tétel segítségével könnyű meghatározni a modulo r ℓ-széles pontrendszer főtagjainak minimális generátorait. Emlékeztetünk, hogy $\mathrm{Lm}\,(I(V_{D,n}))$ minimális generátorai éppen a redukált Gröbner-bázis vezető tagjai. Jellemezhetőek ugyanakkor úgy is, mint azok a vezető tagok, amelyek minden valódi osztója standard monom.

5.3. Lemma. *Az 5.2. tétel jelöléseit használva*

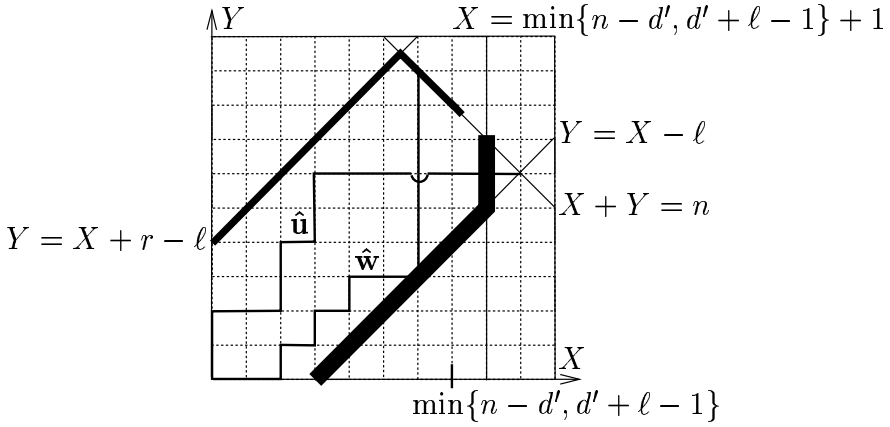
$$\min\{n-d', d'+\ell-1\}+1 \geq \frac{n+\ell-r}{2},$$

azaz az 5.2. tétel utáni ábrán a vastag vonal utolsó rácspontja az $Y = X+r-\ell$ egyenes alatt van.

Bizonyítás: Ha d'-t $\frac{n-r-\ell}{2} < d' \leq \frac{n+r-\ell}{2}$ segítségével becsüljük, akkor pont a bizonyítandó egyenlőtlenséget kapjuk. Miután $Y = X + r - \ell$ és $X + Y = n$ egyenesek metszéspontjának X koordinátája éppen $\frac{n+\ell-r}{2}$, ezért az értelmezés is igaz. □

5.4. Következmény. *Azon $\hat{\mathbf{w}}$ rácspoligonok tartoznak a lexikografikus értelemben vett $\mathrm{Lm}\,(I(V_{D,n}))$ minimális generátoraihoz, amelyek elérik az $Y = X - \ell$ vagy az $X = \min\{n-d', d'+\ell-1\}+1$ egyenest, mielőtt metszenék az $Y = X+r-\ell$-et, továbbá az $Y = X-\ell$, illetve $X = \min\{n-d', d'+\ell-1\}+1$ egyenes elérése után már kizárólag felfele (Y irányba) haladnak.*

A következmény szemléltetésére tekintsük az alábbi ábrát.



A példán $n = 15$, $r = 7$, $\ell = 3$ és $d = 1$ vagy $d = 5$. Az 5.4. következmény alapján $\mathbf{x}^{\mathbf{w}} = x_1x_2x_4x_6x_8x_9$ minimális, míg $\mathbf{x}^{\mathbf{u}} = x_3x_4x_7x_{10}x_{11}x_{12}x_{13}x_{14}x_{15}$, bár főtag, nem minimális. Valóban, ha utóbbiból elhagyjuk az x_{11}, x_{12}, x_{13}, x_{14}, x_{15} változók valamelyikét, akkor (minimális) főtagot kapunk.

A következmény rácspoligonokra vonatkozó része azt állítja, hogy $\mathbf{w} \in \{0,1\}^n$ esetén $\mathbf{x}^{\mathbf{w}}$ pontosan akkor van $\mathrm{Lm}\,(I(V_{D,n}))$ minimális generátorai között, ha $\hat{\mathbf{w}}$ előbb érinti a fenti ábra vastagabb vonalát, mint a vékonyat, és az érintési ponttól kezdve felfele halad.

5.4. következmény bizonyítása: Az 5.2. tétel miatt világos, hogy ha egy $\mathbf{x}^{\mathbf{w}}$ négyzetmentes monom minimális vezető tag, akkor a fenti alakú, valahol ugyanis érintenie kell $\hat{\mathbf{w}}$-nak az $Y = X - \ell$ vagy az $X = \min\{n - d', d' + \ell - 1\} + 1$ egyeneseket: mondjuk, hogy az i. szakaszának vége teszi ezt először. Ekkor $x_1^{w_1} \dots x_i^{w_i}$ a tétel szerint már főtag, és miután osztója $\mathbf{x}^{\mathbf{w}}$-nek, csak az lehet, hogy egyenlőek $\mathbf{x}^{\mathbf{w}}$ minimalitása miatt. Tehát $w_{i+1} = w_{i+2} = \dots = w_n = 0$, ami pont azt jelenti, hogy $\hat{\mathbf{w}}$ az i. lépés után csak felfele halad.

Megfordítva, megint az 5.2. tételből látható, hogy az ilyen alakú $\mathbf{x}^{\mathbf{w}}$ monomok főtagok, kihasználva az 5.3. lemmát is, hiszen amiatt az $X = \min\{n - d', d' + \ell - 1\} + 1$ egyenest elérő rácspoligonok nem érinthetik már az $Y = X + r - \ell$-et.

A minimalitás igazolásához megmutatjuk, hogy $\mathbf{x}^{\mathbf{w}}$ minden valódi osztója standard monom. Tudjuk, hogy $\hat{\mathbf{w}}$ rácspoligon végpontjának X koordinátája, tehát a $\mathbf{w}$-ben szereplő egyesek száma legfeljebb $\min\{n - d', d' + \ell - 1\} + 1$. Így $\mathbf{x}^{\mathbf{w}}$ tetszőleges valódi osztójára ugyanez maximum $\min\{n - d', d' + \ell - 1\}$, tehát vezető tag az 5.2. tétel szerint csak úgy lehetne, ha érintené valahol az $Y = X - \ell$ egyenest. Azonban ez sem fordulhat elő, tekintve, hogy egyrészt minden valódi osztó rácspoligonja $\hat{\mathbf{w}}$-től balra kell legyen, másrészt néhány lépés után szigorúan balra halad, ezért ugyanott sem érintheti $Y = X - \ell$ egyenest, mint $\hat{\mathbf{w}}$. □

A valamely változó négyzetét is tartalmazó monomok közül x_1^2, x_2^2, …, x_n^2 lehet esetleg minimális főtag. A következő állítás lényegében azt mondja, hogy $x_2^2, \dots, x_n^2$ a degenerált esetek kivételével mindig minimális főtag, x_1^2-re pedig $\ell > 1$ esetén igaz ugyanez.

5.5. Állítás. *A következő állítások karakterizálják a nem négyzetmentes minimális főtagokat.*

- *Ha vagy $d = n < r$, vagy $d = 0$, $\ell = 1$ és $n < r$, akkor a minimális vezető tagok mind négyzetmentesek.*
- *Ha $d = 0$, $\ell = 1$ és $n = r$, akkor x_n^2 az egyetlen minimális nem négyzetmentes főtag.*
- *Minden egyéb esetben $x_2^2, \dots, x_n^2$ minimális vezető tag, továbbá $\ell > 1$ esetén x_1^2 is az.*

Bizonyítás: Azt kell vizsgálnunk, hogy mely x_i monomok lesznek főtagok. Az első állítás nyilvánvaló, miután mindkét esetben $|V_{D,n}| = 1$, tehát az egyetlen standard monom az 1. A második esetben az 5.2. tétel alkalmazásával kapjuk, hogy $\mathrm{Sm}\,(I(V_{D,n})) = \{1, x_n\}$, ezért ez is igaz.

Amennyiben $\min\{n - d', d' + \ell - 1\} > 0$, úgy világos, hogy $x_2, \ldots, x_n$ standard monom, és $\ell > 1$ esetén pedig x_1 is. Az utolsó állítás igazolásához tehát azt mutatjuk meg, hogy ha $\min\{n - d', d' + \ell - 1\} \leq 0$ akkor a korábbi esetek valamelyike teljesül. Az 5.3. lemma és az 5.2. tétel szerint ha $\min\{n - d', d' + \ell - 1\} \leq 0$, akkor legfeljebb az 1 és az x_n monom lehet lex standard, azaz $|V_{D,n}| \leq 2$.

A $V_{D,n} \neq \emptyset$-t még a definícióban kikötöttük (mivel $0 \leq d \leq n$). Látható, hogy $|V_{D,n}| = 1$ csak a korábbi esetekben fordulhat elő. Tehát $|V_{D,n}| = 2$. De ez is – kizárva az első két állításban szereplő pontrendszereket – csak úgy lehet, ha $n = 2$, $d = 1$, $\ell = 1$ és $r \geq 2$ vagy pedig $n = 1$, $d = 0$, $\ell = 2$, $r > 2$. Viszont mindkét esetben $\min\{n - d', d' + \ell - 1\} = 1$. □

ℓ-széles pontrendszer Gröbner-bázisa

A fentiek azon speciális esetével fogunk foglalkozni, amikor $d + r > n$, azaz valójában nem moduláris esetben nézzük az ℓ-széles pontrendszereket. Tehát ebben a részben

$$D = \{a \in \mathbb{N} : \ d \leq a \leq d + \ell - 1\} = [d, d + \ell - 1],$$

ahol $0 \leq d \leq n$ és $1 \leq \ell$. Más szóval $V_{D,n} \subseteq \{\alpha_1, \alpha_2\}^n$ azon elemeket tartalmazza, amelyekben a koordinátaértékek között α_1 előfordulásainak száma a d és $d + \ell - 1$ közé esik. Nem kötöttük ki, hogy a teljes intervallum lehetséges típusokat ad, azaz előfordulhat $d + \ell - 1 > n$, ettől még minden további megállapításunk érvényes.

Célunk ebben a részben, hogy kiszámoljuk $I(V_{D,n})$ lexikografikus redukált Gröbner-bázisát, és bebizonyítsuk, hogy ez minden más $x_1 \succ x_2 \succ \cdots \succ x_n$ feltételt kielégítő tagsorrendre nézve is redukált Gröbner-bázis. Ebből azonnal következne, hogy ilyen rendezésekre a standard monomok halmaza is megegyezik.

Az egyszerűbbség kedvéért feltesszük, hogy $\alpha_1 = 1$ és $\alpha_2 = 0$. Láttuk már a 3.8. következményben, hogy a lex standard monomokon ilyen feltevés nem változtat; most ráadásul igaz ugyanez tetszőleges rendezésre vett standard monomok esetén is. Ezt egyszerű látni, ha ugyanis $f(\mathbf{x})$ a $\{0,1\}^n$ bizonyos elemein eltűnő polinom, akkor $\boldsymbol{\alpha_1} := (\alpha_1, \ldots, \alpha_1)$ jelöléssel $\hat{f}(\mathbf{x}) := f\left(\frac{\mathbf{x} - \boldsymbol{\alpha_1}}{\alpha_2 - \alpha_1}\right)$ polinom $\{\alpha_1, \alpha_2\}^n$ megfelelő elemein tűnik el, főtagja pedig azonos f vezető tagjával. Ebből az is világos, hogy a 0-1 eset redukált Gröbner-bázisa hogyan transzformálható át az általános esetre.

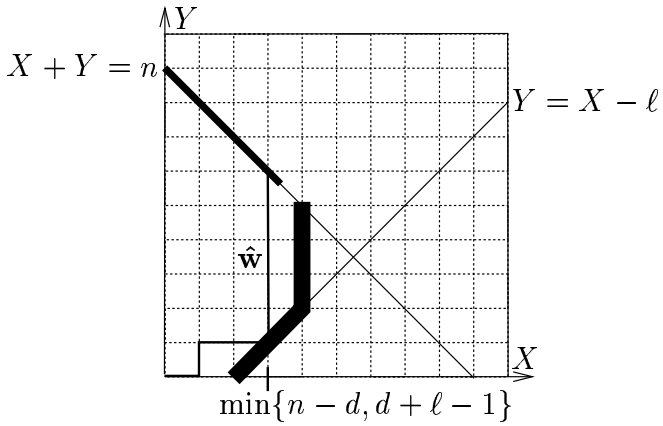
Egyik előnye az $\alpha_1 = 1$ és $\alpha_2 = 0$ egyszerűsítésnek, hogy $\{\alpha_1, \alpha_2\}^n$ elemeit gondolhatjuk $[n]$ bizonyos részhalmazainak a karakterisztikus vektorainak. Ha $F \subseteq [n]$, akkor jelölje $\mathbf{v}_F$ az F karakterisztikus vektorát, azaz $i \in F \iff$ $\mathbf{v}_F$ i. koordinátája 1. Így $V_{D,n}$ elemeihez azok az F halmazok tartoznak, amelyekre $d \leq |F| \leq d + \ell - 1$.

Először kimondjuk az 5.2., az 5.4. tételek és az 5.5. állítás most tekintett esetünkre specializált változatát, amelyek így némileg egyszerűbb alakot öltenek.

5.6. Következmény. *Legyen* $\mathbf{w} \in \{0,1\}^n$, *D, mint fent, és tekintsük a lex rendezést. Akkor és csak akkor teljesül* $\mathbf{x}^{\mathbf{w}} \in \mathrm{Sm}\,(I(V_{D,n}))$, *ha* $\hat{\mathbf{w}}$ *nem metszi az* $Y = X - \ell$ *egyenest, és végpontjának* n_1*-gyel jelölt* X *koordinátájára (ami valójában a* $\mathbf{w}$*-ben szereplő* 1 *koordináták száma) teljesül*

$$n_1 \leq \min\{n - d, d + \ell - 1\}.$$

Pontosan akkor minimális eleme $\mathbf{x}^{\mathbf{w}}$ *monom* $\mathrm{Lm}\,(I(V_{D,n}))$*-nek, ha* $\hat{\mathbf{w}}$ *érinti az* $Y = X - \ell$ *vagy az* $X = \min\{n-d, d+\ell-1\}+1$ *egyenest és az első érintési pont után már kizárólag felfele halad. Ha* $d = n$ *és* ℓ *tetszőleges, vagy* $d = 0$ *és* $\ell = 1$, *akkor csakis négyzetmentes monomok vannak* $\mathrm{Lm}\,(I(V_{D,n}))$ *minimális generátorai között, egyébként* $x_2^2, \ldots, x_n^2$ *is minimális elem, továbbá, ha* $\ell > 1$, *akkor* x_1^2 *is.*



Az ábrán $n = 9$, $\ell = 2$ és $d = 6$ vagy $d = 2$. A következmény szerint $\mathbf{x}^{\mathbf{w}} = x_1x_3x_4$ minimális vezető tag.

Nincs más feladatunk, mint az 5.6. következmény által megadott $\mathbf{x}^{\mathbf{w}}$ minimális főtagokhoz mutatni polinomokat, amelyek eltűnnek $I(V_{D,n})$ ideálon, és $\mathbf{x}^{\mathbf{w}}$ vezető tagjuktól eltekintve standard monomok lineáris kombinációi.

Miután $V_{D,n} \subseteq \{0,1\}^n$, ezért az

$$x_i^2 - x_i \ \ (i \in [n]) \tag{15}$$

polinomok $I(V_{D,n})$-ben vannak. Következésképpen, amennyiben x_i^2 minimális főtag, akkor a hozzá tartozó elem a redukált Gröbner-bázisból éppen a fenti.

Legyen most $\mathbf{x}^{\mathbf{w}}$ olyan minimális lex főtag, amelyre $\hat{\mathbf{w}}$ az $X = \min\{n - d, d+\ell-1\}+1$ egyenest érinti, azaz $\mathbf{x}^{\mathbf{w}}$ éppen $\min\{n-d, d+\ell-1\}+1$-edfokú monom. Tegyük fel először, hogy $\min\{n-d, d+\ell-1\} = d+\ell-1$. Ekkor maga

$$\mathbf{x}^{\mathbf{w}} \tag{16}$$

is eltűnik $V_{D,n}$-en, ugyanis utóbbi elemei legfeljebb $d+\ell-1$ egyest tartalmaznak, míg $\mathbf{x}^{\mathbf{w}}$ pontosan $d+\ell$ változó szorzata. A másik esetben, ha $\min\{n-d, d+\ell-1\} = n-d$, akkor a

$$\prod_{i=1}^{n} (x_i - 1)^{w_i} \tag{16'}$$

polinom lesz a redukált Gröbner-bázis $\mathbf{x}^{\mathbf{w}}$ főtagú eleme. Ez nyilvánvalóan $I(V_{D,n})$-ben van, mivel $\mathbf{v} \in V_{D,n}$-ben legalább d egyes van a (16′) polinom viszont $n-d+1$ olyan szorzatot tartalmaz, amely bármelyikébe 1-et helyettesítve az egész polinom értéke 0. Az is igaz, hogy (16′) főtagjától eltekintve standard monomokból áll, a feltevés szerint ugyanis $\mathbf{x}^{\mathbf{w}}$ minimális vezető tag, ezért minden valódi osztója standard monom.

Végül tegyük fel, hogy $\mathbf{x}^{\mathbf{w}}$ minimális lex főtag, amely az $Y = X - \ell$ egyeneshez tartozik. Legyen $\mathbf{x}^{\mathbf{w}}$ foka t, így tehát $\hat{\mathbf{w}}$ az $X = t$, $Y = t - \ell$ pontban érinti először az $Y = X - \ell$ egyenest, onnan pedig csak felfele halad. Miután az $X + Y = n$ egyenesen levő $(t, n-t)$ végpontjáig még $(n-t)-(t-\ell) = n-2t+\ell$ lépést halad felfele, ezért $w_{2t-\ell} = 1$, és minden $i > 2t-\ell$ esetén $w_i = 0$. Legyen

$$W = \{i \in [n] \,:\, w_i = 1\} \cup \{2t-\ell+1, 2t-\ell+2, \ldots, n\},$$

és

$$l_{\mathbf{w}}(\mathbf{x}) := \sum_{i \in W} x_i = \sum_{i=1}^{2t-\ell} x_i^{w_i} + \sum_{i=2t-\ell+1}^{n} x_i.$$

Vegyük észre, hogy minden $F \subseteq \{0,1\}^n$ esetén $l_{\mathbf{w}}(\mathbf{v}_F) = |W \cap F|$. (Pontosabban, ha a test $p > 0$ karakterisztikájú, akkor $(|W \cap F| \mod p)$-vel igaz ugyanez.) Legyen

$$f_{\mathbf{w}}(\mathbf{x}) :=$$
$$\frac{1}{t!}\left(\prod_{j=1}^{t} (l_{\mathbf{w}} - (d+\ell-j)) \text{ redukáltja } x_i^2 - x_i \ (i \in [n]) \text{ polinomokkal}\right). \tag{17}$$

Nem látszik rögtön, hogy $f_{\mathbf{w}}$ definíciója $p < t$ karakterisztika esetén is értelmes volna. Ha viszont igazoljuk, hogy 0 karakterisztikájú testek esetén $f_{\mathbf{w}}$ a redukált Gröbner-bázis eleme, akkor a 3.9. következmény alapján $f_{\mathbf{w}}$ egész együtthatós, tehát értelmes p karakterisztikában is. Ezt fogjuk tenni.

Miután $x_i^2 - x_i \in I(V_{D,n})$, ezért $f_{\mathbf{w}} \in I(V_{D,n})$ igazolásához azt kell megmutatni, hogy $\prod_{j=1}^{t} (l_{\mathbf{w}} - (d + \ell - j))$ eltűnik minden $\mathbf{v}_F \in V_{D,n}$ elemen. Ehhez az $l_{\mathbf{w}}$-ről szóló észrevétel miatt elegendő $d + \ell - t \leq |W \cap F| \leq d + \ell - 1$. A felső becslés $|F| \leq d + \ell - 1$ miatt nyilvánvaló, az alsó pedig

$$|W \cap F| = |F \setminus ([n] \setminus W)| \geq |F| - |[n] \setminus W| \geq d + \ell - t$$

szerint következik $|[n] \setminus W| = t - \ell$ és $|F| \geq d$-ből.

Megmutatjuk, hogy $f_{\mathbf{w}}$ főtagját leszámítva standard monomok lineáris kombinációja. Ha $\mathbf{x}^{\mathbf{u}}$ tetszőleges monomja $f_{\mathbf{w}}$-nek, akkor négyzetmentes, legfeljebb t-edfokú és W-beli indexű változók szorzata. Világos, hogy ilyenek közül $\mathbf{x}^{\mathbf{w}}$ a legnagyobb minden $x_1 \succ x_2 \succ \cdots \succ x_n$-nek eleget tevő tagsorrendre, és hogy $\mathbf{x}^{\mathbf{w}}$ együtthatója 1. Az is látszik, hogy minden $f_{\mathbf{w}}$-ben szereplő monom rácspoligonja $\hat{\mathbf{w}}$-tól balra-fel halad, tehát az $\mathbf{x}^{\mathbf{w}}$-től különböző $\mathbf{x}^{\mathbf{u}}$-k rácspoligonjai nem érinthetik az $Y = X - \ell$ vagy az $X = \min\{n-d, d+\ell-1\}+1$ egyenest, azaz mind standard monomok.

Ezzel bebizonyítottuk, hogy a (15), (16), (16′) és (17) polinomok közül a megfelelőket kiválasztva $I(V_{D,n})$ lexikografikus redukált Gröbner-bázisát kapjuk. Sőt, már majdnem bebizonyítottuk az alábbi tételt is.

5.7. Tétel. *Az ℓ-széles pontrendszerhez tartozó ideálnak redukált Gröbner-bázisát kapjuk minden $x_1 \succ x_2 \succ \cdots \succ x_n$ feltételnek eleget tevő rendezésre, ha a (15), (16), (16′) és (17) polinomok közül a fent leírtak szerint a megfelelőket választjuk ki, továbbá minden ilyen rendezésre az ℓ-széles pontrendszerhez tartozó standard monomok ugyanazok, mint a lexikografikus esetben.*

Bizonyítás: Az állítás igaz a lex rendezésre. Láttuk viszont, hogy a fenti polinomoknak minden $x_1 \succ x_2 \succ \cdots \succ x_n$-nek eleget tevő tagsorrendre ugyanazok a vezető tagjaik. Ha tehát $\prec$ most egy tetszőleges ilyen rendezés, akkor igaz, hogy minden lex szerinti főtag $\prec$ szerint is főtag. Miután a standard monomok száma minden rendezésre ugyanaz, ezért ez csak úgy lehet, ha a $\prec$ rendezés és a lex tagsorrendhez tartozó standard monomok ugyanazok. Így viszont a (15), (16), (16′) és (17) polinomok közül a megfelelőek redukált Gröbner-bázist alkotnak $\prec$-re nézve is. □

5.3. Partíciók és egy elem generálta szimmetrikus pontrendszerek

Olyan szimmetrikus pontrendszerrel foglalkozunk ebben az alfejezetben, amelyet egyetlen típus generál, azaz a $V_{D,n}$-et definiáló D pontosan egy típust tartalmaz. Az itt tárgyalt eredmények – némileg eltérő bizonyítással – szerepelnek Hegedűs és Rónyai [23] cikkében. A lex standard monomok rekurzív szerkezetére vonatkozó állítás azért ebben az esetben is lehetővé tesz némi egyszerűsítést. Az alfejezet utolsó, $(1,\dots,1)$ típussal foglalkozó része Hegedűs, Nagy és Rónyai [21] cikkéből ismert, illetve hasonló esetet vizsgált Kézdy és Snevily [25] is.

A könnyebb érthetőség kedvéért kicsit eltérünk az eddig használt jelölésektől: azt tesszük fel, hogy $V \subseteq \{\alpha_0,\dots,\alpha_{k-1}\}^n$, és ennek megfelelően a típus koordinátáit is 0-tól $k-1$-ig indexeljük. Miután most D egyetlen $\boldsymbol{\lambda} = (\lambda_0,\dots,\lambda_{k-1})$ típust tartalmaz, így a rövidebb $V_{\boldsymbol{\lambda}}$ jelölést használjuk $V_{D,n}$ helyett.

Indexeljük át úgy $\boldsymbol{\lambda}$ koordinátáit, és ennek megfelelően az α_i elemeket is, hogy teljesüljön

$$\lambda_0 \geq \lambda_1 \geq \cdots \geq \lambda_{k-1}.$$

Az ilyen tulajdonságú k-asokat n *partíciójá*nak nevezzük.

Azt mondjuk, hogy egy $\mathbf{w} \in \{0,\dots,k-1\}^n$ sorozat *rácsszó*, ha minden $(w_1,\dots,w_j)$ kezdőszeletére igaz, hogy benne legalább annyiszor szerepel az $u \in \{0,\dots,k-2\}$ egész szám, mint ahányszor az $u+1$. Ha egy $\mathbf{w} \in \{0,\dots,k-1\}^n$ sorozatban minden i-re a koordináták között i pontosan λ_i-szer szerepel, akkor $\mathbf{w}$ *vektor* $\boldsymbol{\lambda}$ *típusú*. Eddig olyan $\mathbb{F}^n$-beli sorozatokat neveztünk $\boldsymbol{\lambda}$ típusúnak, amely koordinátái között pontosan λ_i-szer szerepel α_i. Ezt a továbbiakban is fenntartjuk, mindig világos lesz, hogy egész számok, vagy testelemek sorozatairól beszélünk. Legyen

$$b_{\boldsymbol{\lambda}} := \{\mathbf{w} \in \{0,\dots,k-1\}^n : \\ \exists \mathbf{w}' \in \{0,\dots,k-1\}^n \ \boldsymbol{\lambda} \text{ típusú rácsszó, hogy } \forall\, j \in [n]\text{-re } w_j \leq w'_j\}.$$

Vegyük észre, hogy $b_{\boldsymbol{\lambda}}$ pontosan azokra a típusokra nem üres, amelyek partíciók, hiszen egy rácsszó típusa szükségképpen partíció.

Fő célunk ebben az alfejezetben, hogy tetszőleges $\boldsymbol{\lambda}$ partícióra megmutassuk, hogy $b_{\boldsymbol{\lambda}}$ elemei pontosan a lexikografikus rendezés szerinti $\mathrm{Sm}\left(I\left(V_{\boldsymbol{\lambda}}\right)\right)$ kitevővektorai. Igaz az is, hogy a deglex standard monomok is ugyanezek, ezt azonban itt nem bizonyítjuk. Gröbner-bázist csupán egy speciális esetben számolunk ki.

Az alfejezet fő állítását indukcióval fogjuk bizonyítani, amihez szükségünk lesz néhány további jelölésre. Legyen $u \in \{0,\dots,k-1\}$; ekkor $\boldsymbol{\lambda}^{(u)}$ az $n-1$

azon partíciója, amelyet $\boldsymbol{\lambda}$-ból úgy kapunk, hogy eggyel csökkentjük az első u-nál nagyobb vagy egyenlő indexű koordinátáját, amelyet csökkentve még partíciót kapunk, azaz amely nagyobb az utána következőnél. Formulával: legyen $i \geq 0$ olyan, hogy $\lambda_u = \lambda_{u+1} = \cdots = \lambda_{u+i} > \lambda_{u+i+1}$, vagy $\lambda_u = \lambda_{u+1} = \cdots = \lambda_{u+i} = \lambda_{k-1}$ és $u+i = k-1$, ha az előbbi nem létezik. Ekkor

$$\boldsymbol{\lambda}^{(u)} := (\lambda_0, \ldots, \lambda_u, \ldots, \lambda_{u+i-1}, \lambda_{u+i} - 1, \lambda_{u+i+1}, \ldots, \lambda_{k-1}) .$$

Megjegyezzük, hogy a

$$\left(V_{\boldsymbol{\lambda}}\right)_{\alpha_u} = \left\{(v_1, \ldots, v_{n-1}) \in \mathbb{F}^{n-1} \ : \ (v_1, \ldots, v_{n-1}, \alpha_u) \in V_{\boldsymbol{\lambda}}\right\}$$

halmaz, bár általában nem egyenlő $V_{\boldsymbol{\lambda}^{(u)}}$-val, mégis a lex esetben teljesíti, hogy

$$\mathrm{Sm}\left(I\left(\left(V_{\boldsymbol{\lambda}}\right)_{\alpha_u}\right)\right) = \mathrm{Sm}\left(I\left(V_{\boldsymbol{\lambda}^{(u)}}\right)\right). \tag{18}$$

Valóban, $\boldsymbol{\lambda}' := (\lambda_0, \ldots, \lambda_u - 1, \ldots, \lambda_{k-1})$, definícióval $\left(V_{\boldsymbol{\lambda}}\right)_{\alpha_u} = V_{\boldsymbol{\lambda}'}$. Ugyanakkor $\boldsymbol{\lambda}'$ és $\boldsymbol{\lambda}^{(u)}$ koordinátáinak halmaza megegyezik, tehát a 3.8. következményből (18) világos.

A következő két egyszerű lemma lesz segítségünkre az alfejezet fő tételének igazolásában.

5.8. Lemma. *Legyen $\boldsymbol{\lambda} = (\lambda_0, \ldots, \lambda_{k-1})$ az n egész egy partíciója és $0 \leq u < k-1$ egész. Ekkor $b_{\boldsymbol{\lambda}^{(u+1)}} \subseteq b_{\boldsymbol{\lambda}^{(u)}}$. Ezért igaz minden $0 \leq u < w \leq k-1$-re is*

$$b_{\boldsymbol{\lambda}^{(w)}} \subseteq b_{\boldsymbol{\lambda}^{(u)}}.$$

Bizonyítás: A második állítás az első nyilvánvaló következménye, ezért csak az elsővel fogunk foglalkozni.

Amennyiben $\lambda_u = \lambda_{u+1}$, akkor $\lambda^{(u)} = \lambda^{(u+1)}$ is, így nincs mit bizonyítani. Tegyük fel tehát, hogy valamely $i \geq 1$-re $\lambda_u > \lambda_{u+1} = \lambda_{u+2} = \cdots = \lambda_{u+i} > \lambda_{u+i+1}$ vagy $\lambda_u > \lambda_{u+1} = \lambda_{u+2} = \cdots = \lambda_{u+i} = \lambda_{k-1}$ és $u+i = k-1$.

Bebizonyítjuk, hogy minden $\boldsymbol{\lambda}^{(u+1)}$ típusú $\mathbf{w} = (w_1, \ldots, w_{n-1})$ rácsszó $b_{\boldsymbol{\lambda}^{(u)}}$-ban van, így a definíció alapján nyilvánvaló ugyanez $b_{\boldsymbol{\lambda}^{(u+1)}}$ tetszőleges elemére. A bizonyításhoz konstruálunk egy $\boldsymbol{\lambda}^{(u)}$ típusú $\mathbf{w}' = (w'_1, \ldots, w'_{n-1})$ rácsszót, amely minden koordinátájára $w_j \leq w'_j$.

Először legyen $\mathbf{w}' = \mathbf{w}$, majd módosítsuk még $\mathbf{w}'$ néhány koordinátáját a következőek szerint. Ha j_1 a legnagyobb index, amelyre $w'_{j_1} = u$, akkor $w'_{j_1} := u+1$. Az így kapott $\mathbf{w}'$-re legyen j_2 legnagyobb index, amelyre $w'_{j_2} = u+1$, és ekkor $w'_{j_2} := u+2$. Hasonlóan járjunk el egészen j_i-ig, tehát végül $w'_{j_i} := u+i$. Világos, hogy $1 \leq j_1 \leq j_2 \leq \cdots \leq j_i \leq n-1$.

Megmutatjuk, hogy a kapott $\mathbf{w}'$ megfelelő. Minden lépésben növeltük $\mathbf{w}'$ koordinátáit, ezért $w_j \le w'_j$ teljesül. A konstrukcióból az is látszik, hogy $\mathbf{w}'$ sorozatban eggyel kevesebb u és eggyel több $u+i$ van, mint a $\boldsymbol{\lambda}^{(u+1)}$ típusú $\mathbf{w}$-ben, ezért $\mathbf{w}'$ típusa $\boldsymbol{\lambda}^{(u)}$. Azt kell csak igazolni, hogy $\mathbf{w}'$ rácsszó.

Tekintsük egy $(w'_1, \dots, w'_j)$ kezdőszeletét. Ha $j < j_1$, akkor $(w'_1, \dots, w'_j) = (w_1, \dots, w_j)$, tehát a rácsszó-feltétel teljesül rá. Legyen $\ell \le i$ a legnagyobb index, amelyre $j_\ell \le j$. Így ennek a kezdőszeletnek és $(w_1, \dots, w_j)$-nek a típusa csak annyiban tér el, hogy előbbiben egy u helyett $u+\ell$ szerepel. Emiatt a rácsszó-feltétel is csak kétféleképpen sérülhet. Egyrészt lehet, hogy több $u+1$ szerepel, mint u. Azonban az u-k száma $(w'_1, \dots, w'_j)$-ben $j_1 \le j$ miatt $\lambda_u - 1$, míg az $u+1$-ek száma legfeljebb λ_{u+1}, tehát ilyen probléma nincs. Másrészt $\ell > 1$ esetén előfordulhatna még, hogy több $u+\ell$ szerepel, mint $u+\ell-1$. Viszont $\ell > 1$ és $j_\ell \le j$ alapján $u+\ell-1$-ből mind a $\lambda_{u+\ell-1}$ példány $(w'_1, \dots, w'_j)$-ben van, ami egyenlő $\lambda_{u+\ell}$-lel, tehát $u+\ell$-ek maximális számával. A lemmát ezzel igazoltuk. □

5.9. Lemma. *Tetszőleges $(w_1, \dots, w_n) \subseteq \{0, \dots, k-1\}^n$ vektorra és $\boldsymbol{\lambda}$ partícióra*

$$(w_1, \dots, w_{n-1}) \in b_{\boldsymbol{\lambda}^{(w_n)}} \iff (w_1, \dots, w_{n-1}, w_n) \in b_{\boldsymbol{\lambda}}.$$

Bizonyítás: Legyen először $(w_1, \dots, w_{n-1})$ egy $\boldsymbol{\lambda}^{(w_n)}$ típusú rácsszó. Ha $\boldsymbol{\lambda}^{(w_n)}$-et a $\boldsymbol{\lambda}$ partícióból λ_{w_n+i} $(i \ge 0)$ csökkentésével kaptuk, akkor következik, hogy $(w_1, \dots, w_{n-1}, w_n + i)$ épp $\boldsymbol{\lambda}$ típusú rácsszó, és így teljesül $(w_1, \dots, w_{n-1}, w_n) \in b_{\boldsymbol{\lambda}}$. Ha $(w_1, \dots, w_{n-1}) \in b_{\boldsymbol{\lambda}^{(w_n)}}$ tetszőleges, akkor van nála koordinátánként nagyobb $(w'_1, \dots, w'_{n-1})$, amely $\boldsymbol{\lambda}^{(w_n)}$ típusú rácsszó, így $(w'_1, \dots, w'_{n-1}, w_n)$ a fentiek alapján eleme $b_{\boldsymbol{\lambda}}$ halmaznak, ezért ugyanez igaz $(w_1, \dots, w_{n-1}, w_n)$-re is.

Megfordítva, legyen most $(w_1, \dots, w_{n-1}, w_n)$ egy $b_{\boldsymbol{\lambda}}$ típusú rácsszó. Ilyenkor $\lambda_{w_n} > \lambda_{w_n+1}$, máskülönben a $(w_1, \dots, w_{n-1})$ kezdőszelet nem teljesíthetné a rácsszó-feltételt. Így viszont nyilvánvaló, hogy $(w_1, \dots, w_{n-1})$ épp $\boldsymbol{\lambda}^{(w_n)}$ típusú rácsszó, tehát $b_{\boldsymbol{\lambda}^{(w_n)}}$-ben van. Ha pedig $(w_1, \dots, w_{n-1}, w_n) \in b_{\boldsymbol{\lambda}}$ tetszőleges és $(w'_1, \dots, w'_{n-1}, w'_n)$ nála koordinátánként nagyobb vagy egyenlő $\boldsymbol{\lambda}$ típusú rácsszó, akkor az előbbiek szerint $(w'_1, \dots, w'_{n-1}) \in b_{\boldsymbol{\lambda}^{(w'_n)}}$, és ezért $(w_1, \dots, w_{n-1}) \in b_{\boldsymbol{\lambda}^{(w'_n)}}$. Ugyanakkor $w'_n \ge w_n$, tehát az 5.8. lemma szerint $b_{\boldsymbol{\lambda}^{(w'_n)}} \subseteq b_{\boldsymbol{\lambda}^{(w_n)}}$, amivel állításunkat beláttuk. □

Ennyi előkészület után a $V_{\boldsymbol{\lambda}}$ lexikografikus standard monomjait karakterizáló tétel bizonyítása már könnyű lesz.

5.10. Tétel. *Minden* $\mathbf{w} = (w_1, \ldots, w_n) \subseteq \mathbb{N}^n$ *vektorra és* $\boldsymbol{\lambda}$ *partícióra teljesül, hogy a lex rendezésre nézve*

$$\mathbf{x}^{\mathbf{w}} \in \mathrm{Sm}\left(I\left(V_{\boldsymbol{\lambda}}\right)\right) \iff \mathbf{w} \in b_{\boldsymbol{\lambda}}.$$

Bizonyítás: Amint ígértük, n-re vonatkozó indukcióval bizonyítunk. Ha $n = 1$, akkor $\left|V_{\boldsymbol{\lambda}}\right| = 1$, ezért $\mathrm{Sm}\left(I\left(V_{\boldsymbol{\lambda}}\right)\right) = \{1\}$, és $b_{\boldsymbol{\lambda}} = \{(0)\}$, tehát az állítás igaz.

Ha $n > 1$, és a tétel $n-1$-re igaz, akkor a lex standard monomok rekurzív szerkezetére vonatkozó 3.10. következmény szerint $\mathbf{x}^{\mathbf{w}} \in \mathrm{Sm}\left(I\left(V_{\boldsymbol{\lambda}}\right)\right)$ akkor és csak akkor, ha van legalább $w_n + 1$ olyan $u \in \{0, \ldots, k-1\}$, amelyre

$$x_1^{w_1} \ldots x_{n-1}^{w_{n-1}} \in \mathrm{Sm}\left(I\left(\left(V_{\boldsymbol{\lambda}}\right)_{\alpha_u}\right)\right) = \mathrm{Sm}\left(I\left(V_{\boldsymbol{\lambda}^{(u)}}\right)\right),$$

utóbbi egyenlőséghez a (18) összefüggést kihasználva.

Az indukciós feltevés szerint $\mathrm{Sm}\left(I\left(V_{\boldsymbol{\lambda}^{(u)}}\right)\right)$ kitevővektorai éppen $b_{\boldsymbol{\lambda}^{(u)}}$ elemei. Azokra viszont teljesül az 5.8. lemma szerinti tartalmazás, ezért

$$\mathrm{Sm}\left(I\left(V_{\boldsymbol{\lambda}^{(0)}}\right)\right) \supseteq \mathrm{Sm}\left(I\left(V_{\boldsymbol{\lambda}^{(1)}}\right)\right) \supseteq \cdots \supseteq \mathrm{Sm}\left(I\left(V_{\boldsymbol{\lambda}^{(k-1)}}\right)\right).$$

Ezek alapján igaz, hogy $\mathbf{x}^{\mathbf{w}} \in \mathrm{Sm}\left(I\left(V_{\boldsymbol{\lambda}}\right)\right)$ ekvivalens $x_1^{w_1} \ldots x_{n-1}^{w_{n-1}} \in \mathrm{Sm}\left(I\left(V_{\boldsymbol{\lambda}^{(w_n)}}\right)\right)$-nel. Most megint az indukciós feltételt használva, utóbbi pontosan akkor áll fent, ha $(w_1, \ldots, w_{n-1}) \in b_{\boldsymbol{\lambda}^{(w_n)}}$. Végül ez, az 5.9. lemma szerint, $\mathbf{w} = (w_1, \ldots, w_{n-1}, w_n) \in b_{\boldsymbol{\lambda}}$-val egyenértékű. Készen vagyunk tehát a bizonyítással. □

Egyebek mellett az 5.10. tétel felhasználásával mutatható meg, hogy a partíciók lex és deglex standard monomjai megegyeznek, tehát

$$\mathbf{x}^{\mathbf{w}} \in \mathrm{Sm}_{\mathrm{lex}}\left(I\left(V_{\boldsymbol{\lambda}}\right)\right) = \mathrm{Sm}_{\mathrm{deglex}}\left(I\left(V_{\boldsymbol{\lambda}}\right)\right) \iff \mathbf{w} \in b_{\boldsymbol{\lambda}}.$$

A bizonyítás Hegedűs és Rónyai [23] cikkében található meg.

Megjegyezzük, hogy $k = 2$ esetén a minden $V_{\boldsymbol{\lambda}}$ éppen egy $\ell = 1$-széles pontrendszer. Az olvasó könnyen ellenőrizheti, hogy a standard monomok ott tárgyalt leírása megegyezik az imént bizonyítottal. Most egy másik speciális esetet vizsgálunk részletesebben. Legyen ezentúl $n = k$, így természetesen az egyetlen lehetséges típus az $(1, \ldots, 1) \in \mathbb{Z}^n$.

Az $(1, \ldots, 1)$ típus

Legyenek tehát $\alpha_0, \ldots, \alpha_{n-1}$ különböző elemek $\mathbb{F}$ testből, $\boldsymbol{\lambda} = (1, \ldots, 1)$, és legyen $V_{\boldsymbol{\lambda}}$ a vizsgált pontrendszer.

Az egyetlen $(1,\dots,1)$ típusú rácsszó a $(0,1,\dots,n-1)$, így az 5.10. tétel alapján a lexikografikus standard monomok éppen $x_2x_3^2\dots x_n^{n-1}$ osztói. Ebből az is jól látszik, hogy a minimális vezető tagok az x_t^t $(t\in[n])$ monomok. Megadjuk az ezen pontrendszerhez tartozó redukált lex Gröbner-bázist, amiről ki fog derülni, hogy redukált Gröbner-bázis minden olyan rendezésre is, amire $x_1\succ x_2\succ\dots\succ x_n$.

Legyen $0\le i$, és az *i-edfokú teljes szimmetrikus polinom*

$$h_i(\mathbf{x}) := \sum_{w_1+\dots+w_n=i} \mathbf{x}^{\mathbf{w}}.$$

Ha $0\le i\le n$, akkor legyen az *i-edik elemi szimmetrikus polinom*

$$\sigma_i(\mathbf{x}) := \sum_{\substack{S\subseteq[n]\\ |S|=i}} \prod_{j\in S} x_j.$$

Bizonyítás nélkül felhasználjuk a következő összefüggést (ld például [11] vagy [21]), amely minden $t\in[n]$ esetén igaz.

$$\sum_{i=0}^{t}(-1)^i h_{t-i}(x_t,\dots,x_n)\sigma_i(x_1,\dots,x_n)=0 \tag{19}$$

Legyen $t\in[n]$ és

$$f_t(\mathbf{x}) := \sum_{i=0}^{t}(-1)^i h_{t-i}(x_t,\dots,x_n)\sigma_i(\alpha_0,\dots,\alpha_{n-1}).$$

5.11. Tétel. *Az $\{f_t : t\in[n]\}$ polinomhalmaz $\boldsymbol{\lambda}=(1,\dots,1)$ esetén redukált Gröbner-bázisa a $V_{\boldsymbol{\lambda}}$ pontrendszernek tetszőleges olyan rendezésre, amire a változók sorrendje $x_1\succ x_2\succ\dots\succ x_n$.*

Bizonyítás: Világos, hogy ha $x_1\succ x_2\succ\dots\succ x_n$ fennáll egy tagsorrendre, akkor $\mathrm{lm}\,(f_t)=x^t$ és az is, hogy $f_t(\mathbf{x})$ minden monomja lex standard. A (19) összefüggés miatt f_t eltűnik a teljes $V_{\boldsymbol{\lambda}}$ pontrendszeren. Miután fent azt is megjegyeztük, hogy a főtagok halmazának $\{x_t^t : t\in[n]\}$ generátora, ezzel igazoltuk is, hogy $\{f_t : t\in[n]\}$ lex redukált Gröbner-bázis. Csakhogy minden tekintett $\prec$ rendezésre f_t vezető tagja ugyanaz, így $\mathrm{Sm}_{\mathrm{lex}}\left(I\left(V_{\boldsymbol{\lambda}}\right)\right)\supseteq \mathrm{Sm}_{\prec}\left(I\left(V_{\boldsymbol{\lambda}}\right)\right)$. Az elemszámok egyenlősége miatt tehát ugyanazok a standard monomok, ezért $\{f_t : t\in[n]\}$ redukált Gröbner-bázis $\prec$ rendezésre is. □

5.4. Irányított fák

A halmazrendszerek után ebben az alfejezetben egy újabb példát mutatunk arra, hogy miként lehet kombinatorikus objektumhoz pontrendszert rendelni. Adott csúcshalmazon tekintett irányított fák karakterisztikus vektoraiból fog állni V, amelynek meghatározzuk a lexikografikus rendezésre vett redukált standard monomjait és Gröbner-bázisát. Az alfejezet [21] alapján készült.

Legyen r pozitív egész és legyen F az $[r] = \{1, 2, \ldots, r\}$ csúcshalmazon *irányított fa*, azaz olyan irányított gráf, amely nem tartalmaz kört, és van egy olyan – *gyökér*nek nevezett – csúcs, amely minden más csúcsból irányított úton elérhető. Ekkor, az $r(r-1)$ lehetséges élet valamilyen rögzített sorrendben tekintve, F leírható a karakterisztikus vektorával, azaz $\{0,1\}^{r(r-1)}$ részeként. Álljon V az összes irányított fa karakterisztikus vektoraiból. Eddigi szokásunktól eltérően az $n = r(r-1)$ változót nem egészekkel indexeljük, hanem a megfelelő élekkel, azaz $\mathbb{F}[\mathbf{x}] = \mathbb{F}[x_{(i,j)} : 1 \leq i, j \leq r, i \neq j]$. A lexikografikus tagsorrenddel fogunk dolgozni, ahol a változók sorrendje

$$x_{(2,1)} \succ x_{(3,1)} \succ \cdots \succ x_{(r,1)} \succ x_{(1,2)} \succ x_{(1,3)} \succ \cdots \succ x_{(1,r)} \succ x_{(3,2)} \succ \ldots,$$

tehát legnagyobbak az 1-be mutató élek, őket követik az 1-ből kilépőek, majd következnek a még nem tekintett 2-be mutató élek, utánuk a 2-ből kilépőek, és így tovább $r-1$-ig; legkisebb az $x_{(r-1,r)}$ változó. Megjegyezzük, hogy amikor az irányított fák karakterisztikus vektorait tekintjük, akkor az éleket természetesen ugyanilyen sorrendben vesszük figyelembe.

Ha H tetszőleges irányított gráf az $[r]$ ponthalmazon, akkor

$$\mathbf{x}_H := \prod_{(i,j) \text{ a } H \text{ éle}} x_{(i,j)}.$$

Triviális észrevétel, de sokszor fogjuk használni, hogy $\mathbf{x}_H$ pontosan akkor nem tűnik el egy F gráf karakterisztikus vektorán, ha H részgráfja F-nek. Ha H összefüggő komponensei irányított fák, akkor H-t *irányított erdő*nek nevezzük.

A következőkben definiálunk polinomokat, amelyekről később ki fog derülni, hogy a redukált Gröbner-bázishoz tartoznak. Ha $1 < i \leq r$ egész, akkor legyen

$$g_i(\mathbf{x}) = \sum_L \mathbf{x}_L - \left(\sum_{j \in [r] \setminus i} x_{(i,j)} - 1 \right) \left(\sum_P \mathbf{x}_P - 1 \right),$$

ahol P végigfut az $[r]$ csúcshalmazú teljes irányított gráf összes lehetséges 1-ből i-be vezető irányított útján, L pedig az olyan *hurok*nak nevezett részgráfjain, amelyek egy 1-ből i-be vezető irányított Q útból és egy (i,j) élből állnak, ahol j a Q egy csúcsa.

5.12. Lemma. *g_i-t különböző monomok lineáris kombinációjaként írva a szereplő monomok négyzetmentesek, így $\mathbf{x}_F$ alakúak valamely F irányított gráfra. Ekkor F vagy egyetlen (i,j) él, vagy 1-ből induló irányított út. Teljesül $\mathrm{lm}\,(g_i) = x_{(i,1)}$ és utóbbi monom együtthatója 1.*

Bizonyítás: Végezzük el a beszorzásokat, így g_i előáll monomok lineáris kombinációjaként. Mivel P egy 1-ből i-be vezető irányított út, ezért nem tartalmazhat (i,j) élet, tehát a kapott $\mathbf{x}_P \cdot x_{(i,j)}$ szorzat valóban négyzetmentes, és egyenlő $\mathbf{x}_{P\cup\{(i,j)\}}$-vel. Ha $P \cup \{(i,j)\}$ nem irányított út, akkor $P \cup \{(i,j)\} = L$ hurok, azaz a bal oldali összegzésben tekintett típusú részgráf, tehát kiesik. Továbbá minden $\mathbf{x}_L$ típusú monom a bal oldali összegből $P \cup \{(i,j)\}$ alakú, így szintén kiesik. Megkaptuk tehát, hogy a g_i-ben szereplő $\mathbf{x}_F$ monomok irányított utakhoz tartoznak. Miután egy 1-ből induló irányított út nem tartalmazhatja az $(i,1)$ élet, ezért a változók fent definiált rendezésével $x_{(i,1)}$ a g_i főtagja, és a főegyüttható pedig 1. □

Legyen

$$\mathcal{A} = \left\{x_{(i,j)}^2 - x_{(i,j)} \,:\, i,j \in [r], \text{ különbözőek, } j > 1\right\},$$
$$\mathcal{B} = \left\{x_{(i,j)}x_{(i,k)} \,:\, i,j,k \in [r], \text{ különbözőek, } j,k > 1\right\},$$
$$\mathcal{C} = \left\{\mathbf{x}_C \,:\, C \text{ 1-et elkerülő irányított kör a teljes irányított gráfban}\right\},$$
$$\mathcal{D} = \left\{g_i \,:\, i \in [r], i > 1\right\} \quad \text{és}$$
$$G = \mathcal{A} \cup \mathcal{B} \cup \mathcal{C} \cup \mathcal{D}.$$

Utóbbi G-ről be fogjuk látni, hogy $I(V)$ redukált Gröbner-bázisa.

5.13. Lemma. $G \subseteq I(V)$

Bizonyítás: V 0-1 vektorokból áll, ezért $\mathcal{A}$ elemei valóban eltűnnek V-n. Ha F irányított fa, akkor a definícióból könnyű látni, hogy minden pontjából legfeljebb egy él lép ki, azaz nem tartalmaz $(i,j) \cup (i,k)$ alakú részgráfot. Hasonlóan $\mathcal{C}$ elemei is eltűnnek V-n, hiszen irányított kör szintén nincsen irányított fában.

Legyen F irányított fa, $\mathbf{v}_F$ a karakterisztikus vektora és $g_i \in \mathcal{D}$. Miután a g_i definíciójában szereplő L hurkok nem körmentesek, így $\sum_L \mathbf{x}_L$ eltűnik $\mathbf{v}_F$-en. Ha F-ben i gyökér, akkor pontosan egy 1-ből i-be vezető utat tartalmaz, ezért $\sum_P \mathbf{x}_P - 1$ értéke $\mathbf{v}_F$-en 0, tehát $g_i(\mathbf{v}_F) = 0$. Ha viszont i nem az F gyökere, akkor F-ben pontosan egy (i,j) alakú él van, ezért $\sum_{j\in[r]\setminus i} x_{(i,j)} - 1$ tűnik el $\mathbf{v}_F$-en. □

Jelöljük $\mathcal{F}$-fel az összes olyan $[r]$ csúcshalmazú irányított erdők halmazát, amelyek nem tartalmaznak 1-be mutató éleket. Belátjuk, hogy $|\mathcal{F}| = |V|$.

Valóban, egyrészt egy irányított fából az 1-be mutató éleket törölve egy $\mathcal{F}$-ben levő gráfot kapunk, másrészt ez a leképezés invertálható: $\mathcal{F}$ egy eleméből irányított fát kapunk, ha minden 1-et nem tartalmazó komponens i gyökerére hozzávesszük a gráfhoz az $(i,1)$ élet.

5.14. Tétel. *A lexikografikus rendezésre vett redukált Gröbner-bázisa az irányított fák karakterisztikus vektoraiból álló V pontrendszerhez tartozó $I(V)$ ideálnak pontosan a fent definiált G.*

Bizonyítás: Megmutatjuk, hogy $\mathrm{Sm}\,(G) \subseteq \{\mathbf{x}_F : F \in \mathcal{F}\}$. Ebből következik, hogy

$$|\mathrm{Sm}\,(G)| \leq |\mathcal{F}| = |V| = |\mathrm{Sm}\,(I(V))|\,.$$

Ugyanakkor $G \subseteq I(V)$, így $\mathrm{Sm}\,(I(V)) \subseteq \mathrm{Sm}\,(G)$, és ezért $|\mathrm{Sm}\,(I(V))| \leq |\mathrm{Sm}\,(G)|$ is igaz, tehát egyenlőség áll fenn, ezért a 2.8. lemma miatt készen leszünk azzal, hogy G Gröbner-bázis.

Tekintsünk egy $\mathbf{x}^{\mathbf{w}}$ monomot, ami G-re nézve redukált. Mivel az $\mathcal{A}$-beli polinomok főtagjai $x^2_{(i,j)}$ alakúak ($j > 1$), $g_i \in \mathcal{D}$ főtagja pedig $x_{(i,1)}$ ezért a monom négyzetmentes, és nem tartalmaz $x_{(i,1)}$ változót. Ezek szerint $\mathbf{x}^{\mathbf{w}} = \mathbf{x}_H$ egy olyan H irányított gráfra, amelyben nincs 1-be mutató él. A $\mathcal{B}$ polinomhalmaz biztosítja továbbá, hogy H-ban minden pontból legfeljebb egy él mutat ki, $\mathcal{C}$ pedig, hogy H irányított kör mentes. Világos, hogy ekkor H csakis irányított erdő lehet, sőt $H \in \mathcal{F}$.

Az elemszámok egyenlősége miatt azt is igazoltuk, hogy $\mathrm{Sm}\,(I(V)) = \mathrm{Sm}\,(G) = \{\mathbf{x}_F : F \in \mathcal{F}\}$. Így viszont ($\mathcal{D}$-hez az 5.12. lemmát használva) látható, hogy G minden eleme a főtagjától eltekintve standard monomok lineáris kombinációja. Végül G különböző elemeinek főtagjai nem oszthatóak egymással, azaz G valóban redukált. □

6. Alkalmazások

A Gröbner-bázisok alkalmazási területe hihetetlenül szerteágazó. Ahol a felmerülő problémák megfogalmazhatóak többváltozós polinomok halmazaira vonatkozó kérdésként, ott nagy eséllyel segíthet ez a módszer.

Ebben a fejezetben zömében olyan elméleti alkalmazásokat válogattunk össze, amelyek kombinatorikus tételek bizonyításával illusztrálják véges pontrendszerek Gröbner-bázisainak és a kapcsolódó fogalmaknak a jelentőségét. A 6.2. fejezetben egy kicsit más alkalmazást is ismertetünk, megmutatjuk, hogy meglepő módon a szimmetrikus polinomok alaptétele kiterjeszthető tetszőleges polinomokra.

6.1. Alkalmazás halmazrendszerekre

Amint az előző fejezetben már utaltunk rá, érdemes néha halmazrendszer helyett az elemeinek karakterisztikus vektorai alkotta halmazt vizsgálni. Bizonyos tulajdonságok így kezelhetővé válnak lineáris algebrai, algebrai módszereket használva. Talán a legismertebb kombinatorikai probléma, amire lineáris algebrai technikákkal adható egyszerű megoldás a Páratlanváros feladat, de számtalan hasonlót találhat az Olvasó Babai és Frankl [3] könyvében. A fő cél ebben az alfejezetben rokon problémák megoldása: bizonyos tulajdonságú halmazrendszerek elemszámára adunk (felső) becslést. A szükséges segédtételek azonban önmagukban is érdekes és másra is használható eszközök.

Jelölje az $[n] = \{1, \dots, n\}$ halmaz összes részhalmazainak halmazát $2^{[n]}$. Egy d egészre az $[n]$ összes d elemű halmazaiból álló halmazrendszert *teljes d-uniform halmazcsalád*nak fogjuk nevezni és $\binom{[n]}{d}$-vel jelöljük, a legfeljebb d elemű halmazok alkotta családra pedig az $\binom{[n]}{\leq d}$ jelölést használjuk. Azt mondjuk, hogy $\mathcal{F} \subseteq 2^{[n]}$ halmazrendszer *d-uniform*, ha a teljes d-uniform halmazcsalád része, tehát ha minden eleme d elemű.

Egy $\mathcal{F}$ családot *ℓ-széles*nek nevezünk, ha valamilyen d egész számra minden $F \in \mathcal{F}$ elemszáma d és $d + \ell - 1$ közé esik. Ha $0 \leq d \leq n$ és $1 \leq \ell$ egészek, akkor az

$$\mathcal{F} = \bigcup_{i=d}^{d+\ell-1} \binom{[n]}{i} = \binom{[n]}{\leq d+\ell-1} \setminus \binom{[n]}{\leq d-1}$$

halmazrendszert *teljes ℓ-széles halmazrendszer*nek nevezzük.

Végül $q = p^\alpha > 1$ prímhatványokra vizsgálni fogunk *modulo q d-uniform halmazcsalád*okat, tehát olyan $\mathcal{F}$ halmazrendszereket, amelyekre $F \in \mathcal{F}$-

ből következik $|F| \equiv d \pmod{q}$. A *teljes modulo q d-uniform halmazcsalád* értelemszerűen $[n]$ összes fenti tulajdonságú részhalmazából áll.

Tartalmazási mátrix

A már ismertetetteken kívül a legfontosabb fogalom, amelyet e fejezetben lépten-nyomon használni fogunk a tartalmazási mátrix. Legyen $\mathcal{F}$ és $\mathcal{G}$ két halmazrendszer. Ekkor az $I(\mathcal{F},\mathcal{G})$ *tartalmazási mátrix* olyan $|\mathcal{F}| \times |\mathcal{G}|$-es mátrix, amely sorai $\mathcal{F}$, oszlopai $\mathcal{G}$ elemeivel vannak indexelve, és amennyiben $F \in \mathcal{F}$, $G \in \mathcal{G}$, akkor az (F,G)-hez tartozó érték a mátrixban 1, ha $G \subseteq F$, 0 egyébként. Például az $I\left(\mathcal{F}, \binom{[n]}{1}\right)$ mátrix az $\mathcal{F}$ halmazrendszer szokásos illeszkedési mátrixa.

Legyen $\mathcal{F} \subseteq 2^{[n]}$ egy halmazrendszer. Az $\mathcal{F}$ elemeinek karakterisztikus vektoraiból álló halmaz legyen $V_{\mathcal{F}}$, azaz

$$V_{\mathcal{F}} := \{\mathbf{v}_F \in \{0,1\}^n \,:\, F \in \mathcal{F} \text{ és } i \in F \iff \mathbf{v}_F \text{ } i. \text{ koordinátája } 1\}\,.$$

Tetszőleges $\mathbb{F}$ test esetén tekinthetjük $V_{\mathcal{F}}$-et $\mathbb{F}^n$-beli pontrendszernek. Az ehhez tartozó $I(V_{\mathcal{F}})$ ideál jól leírja $\mathcal{F}$ néhány kombinatorikus tulajdonságát. A továbbiakban is használni fogjuk a $\mathbf{v}_F$ jelölést F karakterisztikus vektorára.

Ha $G \subseteq [n]$, akkor legyen x_G a G-ben szereplő indexű változók szorzata, azaz $x_G := \prod_{i \in G} x_i$. Miután tetszőleges $\mathcal{F}$ halmazrendszerre $x_i^2 - x_i \in I(V_{\mathcal{F}})$ minden $i \in [n]$ esetén, ezért világos, hogy $\mathrm{Sm}\,(I(V_{\mathcal{F}}))$ csakis négyzetmentes monomokból állhat. Legyen

$$\mathcal{S}(\mathcal{F}) = \{S \subseteq [n] \,:\, x_S \in \mathrm{Sm}\,(I(V_{\mathcal{F}}))\}$$

a standard monomokat természetes módon leíró halmazrendszer.

Vegyük észre, hogy amennyiben $F \subseteq [n]$ egy halmaz, akkor az x_G polinom értéke az F karakterisztikus vektorán, $\mathbf{v}_F$-en, pontosan akkor 1, ha $G \subseteq F$ és 0 egyébként. Tehát

$$x_G(\mathbf{v}_F) = \begin{cases} 1, \text{ ha } G \subseteq F \\ 0 \text{ egyébként} \end{cases}.$$

Ez viszont azt jelenti, hogy $I(\mathcal{F},\mathcal{G})$ tartalmazási mátrix $G \in \mathcal{G}$ oszlopára tekinthetünk úgy, mint az $x_G \colon V_{\mathcal{F}} \to \mathbb{F}$ függvényre. Ez a szemlélet hasznos lesz többek között a következő – [2] cikkből ismert – egyszerű állítás igazolására.

6.1. Állítás. *Az $I(\mathcal{F},\mathcal{S}(\mathcal{F}))$ négyzetes mátrix reguláris.*

Bizonyítás: Miután

$$|\mathcal{F}| = |V_{\mathcal{F}}| = |\mathrm{Sm}\,(I(V_{\mathcal{F}}))| = |\mathcal{S}(\mathcal{F})|\,,$$

ezért a szóban forgó mátrix valóban négyzetes. Azt mutatjuk meg, hogy oszlopai lineárisan függetlenek. Az állítás kimondása előtti észrevételt felhasználva ehhez az kell, hogy az $x_S\colon V_{\mathcal{F}} \to F$ $(S \in \mathcal{S}(\mathcal{F}))$ függvények ne legyenek lineárisan összefüggőek. Ezek azonban pontosan az $\mathrm{Sm}\,(I(V_{\mathcal{F}}))$-ben szereplő monomok $I(V_{\mathcal{F}})$ szerinti ekvivalenciaosztályai $\mathbb{F}[\mathbf{x}]\,/I(V_{\mathcal{F}})$-ben, amik a 2.4. tétel szerint lineárisan függetlenek. □

Hilbert-függvény

Tetszőleges s nemnegatív egész esetén legyen $\mathbb{F}[\mathbf{x}]_{\leq s}$ a legfeljebb s-edfokú $\mathbb{F}[\mathbf{x}]$-beli polinomok vektortere. Ha $I \trianglelefteq \mathbb{F}[\mathbf{x}]$, akkor az $\mathbb{F}[\mathbf{x}]\,/I$ algebra *Hilbert-függvénye* a $h(0)$, $h(1)$, ... sorozat, ahol

$$h(s) = \dim_{\mathbb{F}} \left(\mathbb{F}[\mathbf{x}]_{\leq s}\,/(I \cap \mathbb{F}[\mathbf{x}]_{\leq s})\right).$$

Egyszerűbb a definíció, ha valamely véges $V \subseteq F^n$ pontrendszerhez tartozó $I(V)$ ideálra tekintjük, ekkor $h(s)$ a legfeljebb s-edfokú polinommal reprezentálható $V \to \mathbb{F}$ függvények terének dimenziója.

6.2. Állítás. *Legyen $I = I(V)$ véges pontrendszerhez tartozó ideál. Tetszőleges fok-kompatibilis rendezésre tekintve a legfeljebb s-edfokú standard monomok száma megegyezik $h(s)$-sel.*

Bizonyítás: A standard monomok lineárisan független $V \to \mathbb{F}$ függvények. Ha megmutatjuk, hogy generálják is a legfeljebb s-edfokú polinomfüggvények terét, akkor készen leszünk. Legyen f egy legfeljebb s fokú polinom, és legyen a redukáltja $I(V)$ egy Gröbner-bázisa szerint $\hat{f}$. Miután fok-kompatibilis rendezést használunk, a redukció nem növelheti a fokszámot, ezért $\hat{f}$ legfeljebb s-edfokú standard monomok lineáris kombinációja. Ha $V \to \mathbb{F}$ függvények tekintjük, akkor f és $\hat{f}$ megegyezik, tehát f előáll a fenti monomfüggvények lineáris kombinációjaként. □

Ha $\mathcal{F} \subseteq 2^{[n]}$ halmazrendszer, akkor jelöljük $\mathbb{F}[\mathbf{x}]\,/I(V_{\mathcal{F}})$ Hilbert-függvényét $h_{\mathcal{F}}$-fel. Az alábbi állítás összekapcsolja az $I(V_{\mathcal{F}})$ típusú ideálok Hilbert-függvényét bizonyos tartalmazási mátrixokkal.

6.3. Állítás. *Tetszőleges $\mathcal{F} \subseteq 2^{[n]}$ halmazrendszerre, és $0 \leq s \leq n$ egészre*

$$h_{\mathcal{F}}(s) = \mathrm{rang}_{\mathbb{F}}\, I\left(\mathcal{F}, \binom{[n]}{\leq s}\right).$$

Bizonyítás: A tartalmazási mátrix oszlopait megint tekintsük monomfüggvényeknek. Szerepel minden legfeljebb s-edfokú négyzetmentes monom, amik éppen a legfeljebb s-edfokú $V_{\mathcal{F}}$-en értelmezett függvények terét generálják. Az állítást ezzel beláttuk. □

Összefoglalva, $\mathcal{F}$ halmazrendszerre tetszőleges fok-kompatibilis rendezést rögzítve a 6.2. és 6.3. állítások szerint teljesül

$$\left|\mathcal{S}(\mathcal{F}) \cap \binom{[n]}{\leq s}\right| = h_{\mathcal{F}}(s) = \operatorname{rang}_{\mathbb{F}} I\left(\mathcal{F}, \binom{[n]}{\leq s}\right). \tag{20}$$

A következőkben speciális $\mathcal{F}$ családok Hilbert-függvényeivel foglalkozunk, így egyúttal a fenti illeszkedési mátrixok rangjáról is többet fogunk tudni.

Teljes ℓ-széles és teljes modulo q d-uniform családok

Legyen most $\mathcal{F}$ teljes ℓ-széles család. A kapcsolódó $V_{\mathcal{F}}$ pontrendszer éppen megegyezik az 5.2. alfejezetben a nem moduláris esetben tekintett ℓ-széles pontrendszerrel. A következő tételben az ott igazolt eredményeket felhasználva kiszámoljuk a $h_{\mathcal{F}}$ Hilbert-függvényt. Az eredeti bizonyítás Hegedűs, Friedl és Rónyai [20] munkája, amellyel általánosították Wilson [35] uniform halmazcsaládokra kimondott hasonló eredményét. Megjegyezzük, hogy $i < 0$ esetén az $\binom{n}{i}$ binomiális együtthatót e tételben és a továbbiakban is 0-nak definiáljuk.

6.4. Tétel. *Ha $0 \leq d \leq n$, $1 \leq \ell$ és $s \leq \min\{d+\ell-1, n-d\}$ egészek, továbbá a d-hez tartozó teljes ℓ-széles család $\mathcal{F}$, akkor*

$$h_{\mathcal{F}}(s) = \sum_{i=s-\ell+1}^{s} \binom{n}{i}.$$

Bizonyítás: Megszámoljuk a legfeljebb s-edfokú $I(V_{\mathcal{F}})$-hez tartozó deglex standard monomokat, ami (20) szerint éppen a Hilbert-függvény s helyen felvett értéke.

Legyen $d' = n - s$, és legyen $\mathcal{F}'$ a d'-höz tartozó teljes ℓ-széles család. Miután $s \leq \min\{d+\ell-1, n-d\}$, ezért s nem nagyobb ezek átlagánál sem, azaz $s \leq \frac{n+\ell-1}{2}$. Átrendezve: $s \leq n-s+\ell-1$, ezért $n-d' \leq d'+\ell-1$, tehát

$$s = \min\{d'+\ell-1, n-d'\}.$$

Az 5.6. következmény miatt az $\mathcal{F}$-hez tartozó legfeljebb s-edfokú lexikografikus standard monomok pontosan az $\mathcal{F}'$-höz tartozó lexikografikus standard monomok. Ráadásul az 5.7. tétel alapján a lex és a deglex standard

monomok teljes ℓ-széles családok esetén megegyeznek. Ezek szerint az $I(V_{\mathcal{F}})$ legfeljebb s-edfokú deglex standard monomjainak száma éppen

$$|\mathrm{Sm}\,(I(V_{\mathcal{F}'}))| = |\mathcal{F}'| = \sum_{i=d'}^{d'+\ell-1} \binom{n}{i} = \sum_{i=s-\ell+1}^{s} \binom{n}{i}.$$

□

A következő – Hegedűstől és Rónyaitól [24] származó – tétel a teljes modulo q d-uniform $\mathcal{F}$ halmazrendszer Hilbert-függvényét becsli kis s-ekre. Nagyobb értékekre itt nem határozzuk meg $h_{\mathcal{F}}$-et, miután az előző fejezetben csupán a $V_{\mathcal{F}}$-hez tartozó lexikografikus standard monomokat írtuk le, $h_{\mathcal{F}}$ számolásához pedig a deglex monomokra volna szükségünk. A 6.5. tétel így is általánosítja Frankl egy tételét [16], amely prímhatványok helyett csak prímekről szól.

6.5. Tétel. *Legyen p prím, $q = p^{\alpha} > 1$, és legyen $\mathcal{F}$ a teljes modulo q d-uniform család, ahol feltesszük, hogy a paraméterekre teljesülnek a szokásos $0 \le d \le n$, $d < q$ feltételek. Ha s egész, amelyre $s < q$ és $s \le \frac{n}{2}$, akkor a p elemű $\mathbb{F}_p$ test felett*

$$h_{\mathcal{F}}(s) \le \binom{n}{s},$$

sőt $\mathcal{F}$ legfeljebb s-edfokú $\mathbb{F}_p$ feletti deglex standard monomjai a teljes s-uniform családhoz tartozó standard monomok között vannak.

Bizonyítás: Világos, hogy az előbbi állítás az utóbbi következménye, tehát a másodikra fogunk koncentrálni. Jelölje $\mathcal{G}$ a teljes s-uniform családot, és tegyük fel indirekte, hogy a deglex rendezésre $\mathbf{x}^{\mathbf{u}} \in \mathrm{Sm}\,(I(V_{\mathcal{F}}))\backslash\mathrm{Sm}\,(I(V_{\mathcal{G}}))$ legfeljebb s-edfokú monom.

Az 5.7. tételben beláttuk, hogy $\mathrm{Sm}\,(I(V_{\mathcal{G}}))$ független attól, hogy a lex vagy a deglex rendezést tekintjük, ezért az 5.6. következmény leírja a $\mathcal{G}$-hez tartozó deglex monomokat is. Miután $s \le \frac{n}{2}$, ezért $s = \min\{s, n-s\}$, így az 5.6. következmény szerint a legfeljebb s-edfokú $\mathbf{x}^{\mathbf{u}}$ monom csakis úgy lehet vezető tag $I(V_{\mathcal{G}})$-ben, ha valamely $Y = X - 1$ egyeneshez tartozó minimális $\mathbf{x}^{\mathbf{w}}$ főtag osztja. Legyen az ehhez a főtaghoz tartozó (17) szerinti Gröbner-bázis elem $f_{\mathbf{w}}$.

Megmutatjuk, hogy $f_{\mathbf{w}} \in I(V_{\mathcal{F}})$ is, ami bizonyítja hogy $\mathbf{x}^{\mathbf{w}} \in \mathrm{Lm}\,(I(V_{\mathcal{F}}))$, tehát $\mathbf{x}^{\mathbf{u}}$ sem lehetne $\mathrm{Sm}\,(I(V_{\mathcal{F}}))$-ben, ellentétben a feltevésünkkel.

Ennek érdekében hasonlóan járunk el, mint $f_{\mathbf{w}} \in I(V_{\mathcal{G}})$ igazolásakor. Legyen $\mathbf{x}^{\mathbf{w}}$ foka $t \le s$, $W := \{i \in [n] : w_i = 1\} \cup \{2t-\ell+1, 2t-\ell+2, \ldots, n\}$ és $F \in \mathcal{F}$. Így

$$f_{\mathbf{w}}(\mathbf{v}_F) \equiv \frac{1}{t!} \prod_{j=1}^{t} (|F \cap W| - d - 1 + j)) \pmod{p}.$$

Ha $|F| = d + qa$ valamely $a \in \mathbb{N}$-re, akkor – amint korábban azt az $a = 0$ esetre már elvégeztük – megmutatható, hogy $d+aq+1-t \leq |F \cap W| \leq d+aq$, és emiatt

$$0 \leq |F \cap W| - d - 1 + t - aq \leq t - 1. \tag{21}$$

Ha belátnánk, hogy b egész számra

$$\binom{b+q}{t} \equiv \binom{b}{t} \pmod{p}, \tag{22}$$

akkor ezt a-szor alkalmazva

$$f_{\mathbf{w}}(\mathbf{v}_F) \equiv \binom{|F \cap W| - d - 1 + t}{t} \equiv \binom{|F \cap W| - d - 1 + t - aq}{t} = 0 \pmod{p},$$

az utolsó egyenlőséghez a (21) becslést használva.

Végül (22) a jól ismert

$$\binom{b+q}{t} = \sum_{j=0}^{t} \binom{b}{j}\binom{q}{t-j},$$

azonosságból következik, felhasználva, hogy $0 < t - j < q$ esetén $\binom{q}{t-j} \equiv 0 \pmod{p}$, ami $j = t$ kivételével az összeg minden tagjára teljesül, ugyanis $t - j \leq t \leq s < q$ a feltétel szerint. □

Néhány becslés halmazrendszerek elemszámára

Azt mondjuk, hogy egy $\mathcal{F} \subseteq 2^{[n]}$ *halmazrendszer szétzúzza a* $G \subseteq [n]$ *halmazt*, ha G minden G' részhalmazához létezik olyan $F \in \mathcal{F}$, amelyre $G \cap F = G'$. Világos, hogy amennyiben $\mathcal{F}$ szétzúzza G-t, akkor szétzúzza G minden részhalmazát is.

Megmutatható (ld [2]), hogy minden, a lexikografikus rendezésre tekintett, $S \in \mathcal{S}(\mathcal{F})$ standard monomhoz tartozó halmazt szétzúz $\mathcal{F}$. Ezzel az észrevétellel könnyű bizonyítani a következő, többek által más módon igazolt tételt.

6.6. Tétel. (Sauer[32], Perles, Shelah [33], Vapnik, Chervonenkis [34]) *Ha* $\mathcal{F}$ *olyan halmazrendszer, amely semmilyen* s *elemű halmazt sem zúz szét, akkor*

$$|\mathcal{F}| \leq \sum_{i=0}^{s-1} \binom{n}{i}$$

Bizonyítás:

A feltételből következik, hogy csakis $\binom{[n]}{\leq s-1}$-ben levő halmazt zúzhat szét $\mathcal{F}$, így a lex standard monomokat megadó S halmazok is ezek között vannak. Tehát

$$|\mathcal{F}| = |\mathcal{S}(\mathcal{F})| \leq \left| \binom{[n]}{\leq s-1} \right| = \sum_{i=0}^{s-1} \binom{n}{i},$$

amint azt igazolni akartuk. □

A 6.6. tételhez hasonló mondható ℓ-széles családokra, természetesen kisebb felső korláttal. A 6.7. tétel a 6.4. tétel egyszerű következménye, és ugyanazon [20] cikkből származik. Az állítást egyébként $\ell = 1$-re Frankl és Pach [15] más módszerekkel igazolta.

6.7. Tétel. *Legyen $\mathcal{F}$ egy ℓ-széles család, és tegyük fel, hogy valamely $s \leq d + \ell$ egészre $\mathcal{F}$ nem zúz szét s elemszámú halmazt. Ekkor*

$$|\mathcal{F}| \leq \sum_{i=s-\ell}^{s-1} \binom{n}{i}.$$

Bizonyítás: Legyen $\mathcal{F}' = \binom{[n]}{\leq d+\ell-1} \setminus \binom{[n]}{\leq d-1}$ a teljes ℓ-széles család, ami tartalmazza $\mathcal{F}$-et. Miután az $\mathcal{S}(\mathcal{F})$ halmazokat $\mathcal{F}$ szétzúzza, azért $\mathcal{S}(\mathcal{F}) \subseteq \binom{[n]}{\leq s-1}$. Ugyanakkor $\mathcal{S}(\mathcal{F}) \subseteq \mathcal{S}(\mathcal{F}')$ is igaz, így

$$|\mathcal{F}| = |\mathcal{S}(\mathcal{F})| \leq \left| \binom{[n]}{\leq s-1} \cap \mathcal{S}(\mathcal{F}') \right|.$$

Amennyiben $s - 1 \leq \min\{d + \ell - 1, n - d\}$, úgy a 6.4. tétel alkalmazható, hiszen az egyenlőség jobb oldalán egy teljes ℓ-széles család legfeljebb $s-1$-edfokú monomjainak száma szerepel, amiről ott igazoltuk, hogy pontosan $\sum_{i=s-\ell}^{s-1} \binom{n}{i}$. Ellenkező esetben a jobb oldal éppen

$$|\mathcal{S}(\mathcal{F}')| = |\mathcal{F}'| = \sum_{i=d}^{d+\ell-1} \binom{n}{i} \leq \sum_{i=s-\ell}^{s-1} \binom{n}{i}.$$

Az utolsó egyenlőtlenségnél azt használjuk, hogy $n - d \leq s - 1 \leq d + \ell - 1$, amiből következik $n-(d+\ell-1) \leq s-\ell \leq d$, és így a binomiális együtthatókat $\frac{n}{2}$-höz közelebb eső értékekre összegezzük. □

Az alábbi tétel Babai és Frankl ([3], 115. oldal) egy sejtése volt, amelyet Hegedűs és Rónyai [24] igazolt.

6.8. Tétel. *Legyen $q = p^\alpha > 1$ prímhatvány, amelyre $2(q-1) \leq n$, és legyen $\mathcal{F}$ modulo q d-uniform halmazrendszer, amelyre teljesül, hogy tetszőleges $F, G \in \mathcal{F}$ különböző halmazokra $F \cap G \not\equiv d \pmod q$. Ekkor*

$$|\mathcal{F}| \leq \binom{n}{q-1}.$$

A bizonyításhoz előbb belátunk egy lemmát.

6.9. Lemma. *Ha $f \in \mathbb{Q}[\mathbf{x}]$ polinomra minden $\mathbf{v} \in \{0,1\}^n$ esetén $f(\mathbf{v}) \in \mathbb{Z}$, akkor f redukáltja az $x_i^2 - x_i$ $(i = 1, \ldots, n)$ polinomokkal egész együtthatós.*

Bizonyítás: Legyen a redukált $\hat{f}(\mathbf{x}) = \sum_{G \subseteq [n]} \alpha_G x_G$ valamilyen $\alpha_G \in \mathbb{Q}$ együtthatókkal. A $|G|$ elemszámra vonatkozó indukcióval megmutatjuk, hogy $\alpha_G \in \mathbb{Z}$.

Miután $\alpha_\emptyset = \hat{f}(\mathbf{0}) = f(\mathbf{0}) \in \mathbb{Z}$, ezért a $|G| = 0$ esettel megvagyunk. Legyen most $|G| \geq 1$, és tegyük fel, hogy minden $H \subsetneq G$-re $\alpha_H \in \mathbb{Z}$. Ekkor

$$\alpha_G = \alpha_G x_G(\mathbf{v}_G) = \hat{f}(\mathbf{v}_G) - \sum_{\substack{H \subseteq [n] \\ H \neq G}} \alpha_H x_H(\mathbf{v}_G) = \hat{f}(\mathbf{v}_G) - \sum_{H \subsetneq G} \alpha_H \in \mathbb{Z}$$

az indukciós feltétel és $\hat{f}(\mathbf{v}_G) = f(\mathbf{v}_G) \in \mathbb{Z}$ miatt. □

6.8. tétel bizonyítása: A bizonyítás stratégiája a következő. Minden $F \in \mathcal{F}$ halmazhoz megkonstruáljuk az F karakterisztikus függvényének egy $\mathbb{F}_p$ feletti polinom reprezentációját, azaz olyan polinomot, amely $\mathbf{v}_F$-en 1, $\mathbf{v}_G$-n pedig eltűnik minden más $G \in \mathcal{F}$ esetén. Ezek ráadásul legfeljebb $q-1$ fokú, a teljes ℓ-széles családra tekintve standard monomok lineáris kombinációi lesznek. Az ilyen monomok számára a 6.5. tétel felső becslést ad, ami ezek szerint felülről becsli a karakterisztikus polinomjaink, és így az $F \in \mathcal{F}$ halmazok számát is.

Legyen $F \in \mathcal{F}$, és tekintsük az

$$f_F(\mathbf{x}) := \frac{1}{(q-1)!} \prod_{j=1}^{q-1} ((\mathbf{x} \cdot \mathbf{v}_F) - d - j) \in \mathbb{Q}[\mathbf{x}]$$

polinomot, ahol $(\mathbf{x} \cdot \mathbf{v}) = \sum_{i=1}^{n} x_i v_i$, és amelynek az $x_i^2 - x_i$ $(i = 1, \ldots, n)$ polinomokkal vett redukáltja legyen $\hat{f}_F$. Miután tetszőleges $\mathbf{v} \in \{0,1\}^n$ vektoron f_F értéke $\binom{(\mathbf{v} \cdot \mathbf{v}_A) - d - 1}{q-1} \in \mathbb{Z}$, ezért a 6.9. lemma alkalmazható és $\hat{f}_F \in \mathbb{Z}[\mathbf{x}]$.

Ha az együtthatókat modulo p redukáljuk, akkor tekinthető $\hat{f}_F$ az $\mathbb{F}_p$ test feletti polinomnak is. Legyen $\overline{f}_F$ az a polinom, amelyet a teljes modulo p

d-uniform halmazrendszerhez tartozó $\mathbb{F}_p$ feletti deglex Gröbner-bázissal redukálva kapunk $\hat{f}_F$-ből. Miután $\mathcal{F}$ is modulo p d-uniform család, tehát a Gröbner-bázis része $I(V_\mathcal{F})$-nek, következésképp tetszőleges $G \in \mathcal{F}$ esetén

$$\overline{f}_F(\mathbf{v}_G) \equiv \hat{f}_F(\mathbf{v}_G) = f_F(\mathbf{v}_G) = \binom{|G \cap F| - d - 1}{q-1} \pmod{p}.$$

A (22) azonosságot $t = q-1$ választással alkalmazva láthatjuk, hogy tetszőleges $b \in \mathbb{Z}$-re $\binom{b-1}{q-1} \equiv 0 \pmod{p}$ pontosan akkor, ha $b \not\equiv 0 \pmod{q}$, ellenkező esetben pedig $\binom{b-1}{q-1} \equiv 1 \pmod{p}$. Az $\mathcal{F}$-re vonatkozó metszési feltétel miatt tehát $F \neq G$ esetén $\overline{f}_F(\mathbf{v}_G) \equiv 0 \pmod{p}$ és $\overline{f}_F(\mathbf{v}_F) \equiv 1 \pmod{p}$.

Tehát az $\{\overline{f}_F : F \in \mathcal{F}\}$ polinomok függvényként a $V_\mathcal{F}$-en értelmezett $\mathbb{F}_p$ értékű függvények terének egy lineáris bázisa, így viszont polinomként is lineárisan függetlenek $\mathbb{F}_p$ felett.

Az f_F polinomok foka $q-1$, ezért az $\overline{f}_F$ deglex redukáltjaik legfeljebb $q-1$-edfokú a teljes modulo p d-uniform családhoz tartozó deglex standard monomok lineáris kombinációi. Az ilyenek által kifeszített tér dimenzióját a 6.5. tétel szerint felülről becsli $\binom{n}{q-1}$, kihasználva a $2(q-1) \leq n$ feltételt. Ezek szerint az $\{\overline{f}_F : F \in \mathcal{F}\}$ lineárisan független polinomok száma sem lehet ennél több, azaz valóban

$$|\mathcal{F}| \leq \binom{n}{q-1}.$$

□

6.2. Egy változat a szimmetrikus polinomok alaptételére

Ebben az alfejezetben Hegedűs, Nagy és Rónyai [21] egyszerű bizonyítását mutatjuk be Garsia [18] egy tételére. A bizonyítás a $\boldsymbol{\lambda} = (1, \ldots, 1)$ típus generálta pontrendszer standard monomjainak és Gröbner-bázisának leírásán alapul.

Láttuk, hogy ha $V = V_{\boldsymbol{\lambda}}$, akkor tetszőleges $x_1 \succ x_2 \succ \cdots \succ x_n$-nek eleget tevő tagsorrendre

$$\mathrm{Sm}\,(I(V)) = \{\mathbf{x}^{\mathbf{w}} : \forall\, i \in [n]\ w_i \leq i-1\}.$$

A szimmetrikus polinomok alaptétele szerint, ha $f(\mathbf{y})$ szimmetrikus polinom, akkor egyértelműen írható a $\sigma_i(\mathbf{y})$ elemi szimmetrikus polinomok polinomjaként, azaz

$$f(\mathbf{y}) = \sum_{\mathbf{i} \geq \mathbf{0}} a_{\mathbf{i}} \prod_{j=1}^{n} \sigma(\mathbf{y})^{i_j}$$

alakban, ahol $a_{\mathbf{i}} \in \mathbb{F}$ és $\mathbf{i} \geq \mathbf{0}$ azt jelenti, hogy $i_j \geq 0$ minden $j \in [n]$-re. A következő általánosítás is igaz.

6.10. Tétel. *Tetszőleges $f(\mathbf{y}) \in \mathbb{F}[\mathbf{y}]$ polinom egyértelműen írható fel*

$$f(\mathbf{y}) = \sum_{\mathbf{x}^{\mathbf{w}} \in \mathrm{Sm}(I(V))} \sum_{\mathbf{i} \geq \mathbf{0}} a_{\mathbf{w},\mathbf{i}} \mathbf{y}^{\mathbf{w}} \prod_{j=1}^{n} \sigma(\mathbf{y})^{i_j}$$

alakban, ahol $a_{\mathbf{w},\mathbf{i}} \in \mathbb{F}$.

Bizonyítás: Legyen most az alaptest az n változós $\mathbb{F}(\mathbf{y})$ függvénytest, amiben válasszuk α_{i-1}-nek y_i-t, és tekintsük a kapott V pontrendszert. Emlékeztetünk, hogy a Gröbner-bázis $t \in [n]$-nel indexelt eleme

$$f_t(\mathbf{x}) = \sum_{i=0}^{t} (-1)^i h_{t-i}(x_t, \ldots, x_n) \sigma_i(y_1, \ldots, y_n),$$

ami ezek szerint $\mathbf{y}$ változóknak szimmetrikus polinomja.

Ha redukáljuk $f(\mathbf{x}) \in \mathbb{F}(\mathbf{y})[\mathbf{x}]$-et ezekkel, akkor $f(\mathbf{x})$-et $\mathbf{x}^{\mathbf{w}}$ standard monomok $\mathbb{F}(\mathbf{y})$-lineáris kombinációjaként állítjuk elő. Ráadásul, $f_t(\mathbf{x})$ konkrét alakjából az is látszik, hogy az együtthatók $\mathbf{y}$-ban szimmetrikus $\mathbb{F}[\mathbf{y}]$-beli polinomok lesznek. Tehát V-n értelmezett függvényként

$$f(\mathbf{x}) = \sum_{\mathbf{x}^{\mathbf{w}} \in \mathrm{Sm}(I(V))} \mathbf{x}^{\mathbf{w}} g_{\mathbf{w}}(\mathbf{y}),$$

ahol $g_{\mathbf{w}}(\mathbf{y}) \in \mathbb{F}[\mathbf{y}]$. Így viszont $\mathbf{x}$ helyébe $\mathbf{y}$-t írva igaz az egyenlőség, tehát

$$f(\mathbf{y}) = \sum_{\mathbf{x}^{\mathbf{w}} \in \mathrm{Sm}(I(V))} \mathbf{y}^{\mathbf{w}} g_{\mathbf{w}}(\mathbf{y}).$$

Most alkalmazva minden $g_{\mathbf{w}}(\mathbf{y})$-ra a szimmetrikus polinomok alaptételét, megkapjuk $f(\mathbf{y})$ kívánt előállítását.

Az egyértelműség következik, hiszen amennyiben

$$f(\mathbf{y}) = \sum_{\mathbf{x}^{\mathbf{w}} \in \mathrm{Sm}(I(V))} \sum_{\mathbf{i} \geq \mathbf{0}} a_{\mathbf{w},\mathbf{i}} \mathbf{y}^{\mathbf{w}} \prod_{j=1}^{n} \sigma(\mathbf{y})^{i_j}$$

egy előállítás, akkor a fenti V-n értelmezett függvényként

$$f(\mathbf{x}) = \sum_{\mathbf{x}^{\mathbf{w}} \in \mathrm{Sm}(I(V))} \sum_{\mathbf{i} \geq \mathbf{0}} a_{\mathbf{w},\mathbf{i}} \mathbf{x}^{\mathbf{w}} \prod_{j=1}^{n} \sigma(\mathbf{y})^{i_j} = \sum_{\mathbf{x}^{\mathbf{w}} \in \mathrm{Sm}(I(V))} \mathbf{x}^{\mathbf{w}} \hat{g}_{\mathbf{w}}(\mathbf{y}),$$

azaz megkaptuk $f(\mathbf{x})$ egy előállítását standard monomok $\mathbb{F}(\mathbf{y})$-lineáris kombinációjaként. Ez viszont egyértelmű, tehát $\hat{g}_{\mathbf{w}}(\mathbf{y}) = g_{\mathbf{w}}(\mathbf{y})$, és így a szimmetrikus polinomok alaptételében szereplő egyértelműség miatt $f(\mathbf{y})$ eredeti előállítása sem lehetett különböző. □

7. Összefoglalás

Dolgozatomban ismertettem ideálok Gröbner-bázisaival és standard monomjaival kapcsolatos alapvető definíciókat és tételeket, különös tekintettel véges pontrendszeren eltűnő többváltozós polinomok által alkotott ideálra.

A lexikografikus rendezésre tekintett standard monomok és főtagok ekvivalens jellemzését adtam, amely szerint a $\mathrm{Lex}(V, \mathbf{w})$ játékban pontosan akkor nyer Stan, ha $\mathbf{x}^{\mathbf{w}}$ standard monom a V pontrendszeren eltűnő polinomok $I(V)$ ideáljára. Ebből egyszerűen adódott, hogy az eggyel kevesebb változós polinomgyűrű bizonyos ideáljainak lex standard monomjai hogyan határozzák meg $I(V)$ lex standard monomjait. Ezen következményt a lexikografikus standard monomok rekurzív tulajdonságának neveztem és standard monomok kiszámolásához elsődleges eszközként használtam.

Bemutattam az általános ideálok Gröbner-bázisának kiszámítására használt Buchberger-algoritmust, majd két másik – véges V pontrendszerhez tartozó $I(V)$ ideál redukált Gröbner-bázisának meghatározására szolgáló – módszert: Farr és Gao illetve Buchberger és Möller algoritmusát. A lex standard monomok rekurzív tulajdonságára alapozó lex standard monom számoló algoritmus naiv és hatékony megvalósítását is tárgyaltam. Utóbbi nagyvonalú becsléssel is $O(|V|^2\, n)$ elemi lépést igényel (n a polinomok változóinak száma); ez kevesebb, mint a korábban ismert legjobb algoritmus futásideje.

A lex játékból adódó módszert konkrét pontrendszerek standard monomjainak kiszámolására is felhasználtam: meghatároztam a modulo r ℓ-széles pontrendszerekhez tartozó lexikografikus standard monomokat és lex minimális főtagokat. Ezt felhasználva az ismerttől részben eltérő utat mutattam ℓ-széles pontrendszer redukált Gröbner-bázisának kiszámolására. A lex monomok rekurzív szerkezetéről szóló megállapítás segítségével vizsgáltam az egy elem által generált szimmetrikus pontrendszer lex standard monomjait, ezzel egyszerűsítettem Hegedűs és Rónyai eredeti bizonyítását. További konkrét példaként ismertettem az irányított fákhoz tartozó Gröbner-bázist.

A Gröbner-bázis kombinatorikus alkalmazhatóságát néhány, az irodalomból válogatott példán szemléltettem. Ezek egy része az egy halmazrendszerhez tartozó bizonyos tartalmazási mátrixok rangja és a megfelelő pontrendszer fok-kompatibilis rendezésre tekintett standard monomjainak száma közötti összefüggésen múlt. Halmazcsaládok elemszámát is lehetett ilyen technikával becsülni. Egy más típusú alkalmazás a szimmetrikus polinomok alaptételének kiterjesztése volt. Mindezekhez szükség volt a megelőző fejezetben kiszámolt standard monomokra, illetve Gröbner-bázisra.

Remélem, hogy az alkalmazásokkal sikerült érzékeltetnem, hogy milyen erős algebrai eszközt adnak a Gröbner-bázisokkal kapcsolatos technikák a

kombinatorikában. Ugyanakkor dolgozatom fő célja az volt, hogy magát az eszköztárat mutassam be, és számítási módszereket adjak kombinatorikus problémák átfogalmazásakor felmerülő véges pontrendszerek standard monomjai és Gröbner-bázisai számolására. Bár bízom benne, hogy dolgozatom igen, a kutatás biztosan nem tekinthető lezártnak. Egyfelől további véges pontrendszerekre lehetne konkrétan megadni egy Gröbner-bázist, ez minden bizonnyal kombinatorikus alkalmazásokra is találna. Másrészt az elmélet szempontjából is több nyitott kérdés maradt.

Sok tárgyalt esetben a lex standard monomok megegyeztek a deglex standard monomokkal, sőt gyakran bármilyen $x_1 \succ x_2 \succ \cdots \succ x_n$-nek eleget tevő tagsorrendre ugyanazok voltak a standard monomok. Hasznos volna valahogyan karakterizálni az előbbi és az utóbbi pontrendszereket. A lex standard monomokat számoló algoritmus kapcsán láttuk, hogy két – V_1 és V_2 – pontrendszer standard monomjai azonosak, ha fordított szófáik gyökeres faként izomorfak. Ez azonban nem szükséges $\mathrm{Sm}\,(I(V_1)) = \mathrm{Sm}\,(I(V_2))$ teljesüléséhez. Érdekes lenne könnyen ellenőrizhető szükséges és elégséges feltételt adni.

Köszönetnyilvánítás

Szeretném ezúton is kifejezni hálámat témavezetőmnek, Rónyai Lajosnak, aki megismertetett véges pontrendszerek Gröbner-bázisainak elméletével, irányt mutatott a kutatásban, és dolgozatom elkészítéséhez is nélkülözhetetlen segítséget nyújtott.

Számtalan hasznos megjegyzéssel és problémafelvetéssel segítette munkámat Ráth Balázs. Szeretnék továbbá köszönetet mondani Rudas Annának és Rácz Balázsnak, amiért a témával kapcsolatos észrevételeiket megosztották velem.

Hivatkozások

[1] W. W. Adams, P. Loustaunau, An Introduction to Gröbner Bases, *American Mathematical Society*, 1994.

[2] R. P. Anstee, L. Rónyai, A. Sali, Shattering news, *Graphs and Combinatorics* **18** (2002), 59–73.

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

[4] T. Becker, V. Weispfenning, Gröbner bases – a computational approach to commutative algebra, *Springer-Verlag*, Berlin, Heidelberg, 1993.

[5] B. Buchberger Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal, *Ph. D. Thesis, Univ. of Innsbruck, Austria*, 1965.

[6] B. Buchberger, Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleischungssystem, *Aequationes Mathematicae*, **4** (1970), 374–383.

[7] B. Buchberger, F. Winkler (editors), Gröbner Bases and Applications, *London Mathematical Society Series*, Volume 251 (1998), Proc of the international conference "33 Years of Gröbner Bases"

[8] B. Buchberger, H. M. Möller, The construction of multivariate polynomials with preassigned zeros, *Proc EUROCAM '82, Lecture Notes In Computer Science* **144** (1982), 24–31.

[9] 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.

[10] T. H. Cormen, C. E. Leiserson, R. L. Rivest, Introduction to Algorithms, *Massachusetts Institute of Technology*, 1990. vagy Algoritmusok, *Műszaki könyvkiadó*, Budapest, 1997, 1999.

[11] D. Cox, J. Little, D. O'Shea, Ideals, varieties, and algorithms, *Springer-Verlag*, Berlin, Heidelberg, 1992

[12] J. Farr, S. Gao, Computing Gröbner bases for vanishing ideals of finite sets of points, *megjelenés alatt*, (2003).

[13] J. C. Faugère, P. Gianni, D. Lazard, T. Mora, Efficient computation of zero-dimensional Gröbner bases by change of ordering, *J. Symbolic Computation* **16** (1993) 329–344.

[14] B. Felszeghy, B. Ráth, L. Rónyai, The lexicographic game and some applications, *kézirat.*

[15] P. Frankl, J. Pach, On disjointly representable sets, *Graphs Comb.* **5** (1989) 295–299.

[16] P. Frankl, Intersection theorems and mod p rank of inclusion matrices, *J. Combin. Theory Ser. A* **54** (1990), 85–94.

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

[18] A. M. Garsia, Pebbles and expansions in the polynomial ring, *kézirat* 2002.

[19] A. Giovini, T. Mora, G. Niesi, L. Robbiano, C. Traverso, "One sugar cube, please" or selection strategies in Buchberger algorithm, *Proc ISSAC '91*, ACM (1991), 49–54.

[20] G. Hegedűs, K. Friedl, L. Rónyai, Gröbner bases for complete ℓ-wide families, *megjelenés alatt.*

[21] G. Hegedűs, A. Nagy, L. Rónyai, Gröbner bases for permutations and oriented trees, *megjelenés alatt.*

[22] G. Hegedűs, L. Rónyai, Gröbner bases for complete uniform families, *J. of Algebraic Combinatorics* **17** (2003), 171–180.

[23] G. Hegedűs, L. Rónyai, Standard monomials for partitions, *megjelenés alatt.*

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

[25] A. E. Kézdy, H. S. Snevily, Polynomials that vanish on distinct n^{th} roots of unity, *Combinatorics, Probability and Computing* **13** (2004), 37–59.

[26] D. E. Knuth, The art of computer programming, Volume 3., *Addison-Wesley*, Reading 1973.

[27] M. G. Marinari, H. M. Möller, T. Mora, Gröbner bases of ideals defined by functionals with an application to ideals of projective points, *Appl. Algebra Engrg. Comm. Comput.* **4** (1993), no. 2, 103–145.

[28] T. Mora, L. Robbiano, Points in affine and projective spaces, in Computational Algebraic Geometry and Commutative Algebra (D. Eisenbud, L. Robbiano editors), *Cambridge Univ. Press* (1993), 106–150.

[29] L. Robbiano, Term orderings on the polynomial ring, *Proceedings of EUROCAL '85, Lecture Notes In Computer Science* **204** (1985), 513–517.

[30] L. Robbiano, On the theory of graded structures, *J. Symbolic Comput.* **2** (1986), no. 2, 139–170.

[31] L. Rónyai, G. Ivanyos, R. Szabó, Algoritmusok, *Typotex*, 1999.

[32] N. Sauer, On the density of families of sets, *J. Combin. Theory, Ser. A* **13** (1972), 145–147.

[33] S. Shelah, A combinatorial problem: stability and order for models and theories in infinitary language, *Pac. J. Math.* **41** (1972), 247–261.

[34] V. N. Vapnik, A. Ya. Chervonenkis, On the uniform convergence of relative frequencies of events to their probabilities. *Theory Probab. Appl.* **16** (1971), 264–280.

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