Bevezetés a Gröbner-bázisok elméletébe

Oktatási segédlet a Komputer algebra c. tárgyhoz

Felszeghy Bálint

Tartalomjegyzék

1. Bevezetés

Ebben a jegyzetben a Gröbner-bázisok elméletével foglalkozunk. Az alapok bemutatásán kívül a téma néhány újabb eredményét is tárgyaljuk. Később természetesen a pontos definíciók is szerepelnek, egyelőre annyit mondunk, hogy egy polinomideál Gröbner-bázisa az ideál egy jó fajta generátorrendszere.

A Gröbner-bázis fogalma Bruno Buchberger osztrák matematikustól származik, aki mintegy 40 éve [5] Ph. D. tézisében (az angol fordítást nemrég adták ki [6]) és valamivel később megjelent [7] (angol nyelven [8] kiadványban) 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 [8] ezeknek egy jó összefoglalóját adja: ismertet alkalmazásokat a kódelméletben, az egész programozásban, az automatikus tételbizonyításokban, a szimbolikus számítások elméletében, a statisztikában, a parciális differenciálegyenletek elméletében és a numerikus módszerekben. 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 megoldásából ismert Gauss-eliminációnak és az egyismeretlenes polinomiális egyenletrendszerek megoldhatóságának eldöntéséhez szükséges euklideszi algoritmusnak.[1]

A Gröbner-bázisok elmélete nagyon is élő kutatási terület, minden évben temérdek új cikk jelenik meg a témakörben. Jelen jegyzetben igyekeztünk a már klasszikusnak számító eredmények bemutatása után a modern alkalmazásokból is ízelítőt adni. A 2. fejezetben ismertetjük az elmélet alapjait. A felépítésben a szokásos szemléletet ötvözzük egy, a legtöbb bevezető jellegű könyvben kevéssé hangsúlyos, modernebb hozzáállással: az ideálok standard monomjainak fontos szerepet szánunk.

A 3. fejezet algoritmusokról szól. Buchberger eredeti módszere, amellyel

[1] 2006 tavaszán a linzi Kepler Egyetemen került megrendezésre egy Gröbner-bázisokról szóló speciális félév (Buchbergerrel a szervezők között), amelyen én is eltöltöttem egy hónapot. A rengeteg szakmai jellegű információ mellett azt is megtudtam, hogy Linzben a mérnök hallgatók matematika tananyagának részét képezik a Gröbner-bázisokról, mint polinom-egyenletrendszereket megoldó módszerről szóló ismeretek. Meggyőződésem, hogy nem csupán a hely szelleme miatt van ennek létjogosultsága, a Gröbner-bázisok széleskörű alkalmazhatósága és az alapok egyszerű elsajátíthatósága okán érdemes lenne más egyetemeknek is követniük ezt a példát.

egy általános polinomideál Gröbner-bázisa számítható ki, szerepel minden a témába bevezető könyvben. Itt Adams és Loustaunau [2] munkáját választottuk a leírás alapjául. Tárgyalunk egy további algoritmust, amely egy véges pontrendszerhez tartozó Gröbner-bázist számol; az általánosság megszorításáért kárpótlásul algoritmuselméleszi szemmel nézve is igen hatékonyan. A Buchberger–Möller-algoritmus néven ismert módszer bemutatásában főként Teo Mora és Lorenzo Robbiano [23] összefoglaló cikkére hagyatkozunk.

Végül az utolsó fejezetben alkalmazásokról írunk. Két nagy területet választottunk erre: kommutatív algebrai számolgatásokról – beleértve polinomiális egyenletrendszerek megoldását is –, és kombinatorikai alkalmazásokról szólunk. Utóbbiak között sort kerítünk egy általánosabb módszerre, amely segítségével sok kombinatorikai probléma lefordítható algebrai kérdéssé. Erre mutatunk példát a nemrégiben született [15] cikk (néhány számolósabb részletet mellőző) bemutatásával.

A legtöbb matematikai program – így a Maple és a Mathematica is – tartalmaz Gröbner-bázist számoló algoritmust, és használ Gröbner-bázisokat más jellegű kérdések eldöntésére. Kifejezetten polinom-számítások végzésére fejlesztették ki a Singular és a C++ alapú CoCoA programcsomagokat; az Olvasónak a jegyzetben tanultak gyakorlásához mindenképpen ez utóbbiakat javasoljuk. A legújabb algoritmusok a publikásukkal szinte egyidőben megjelennek ezekben (ami az előbbi két programra nem igaz), ráadásul mindkét program szabadon letölthető (`http://www.singular.uni-kl.de` és `http://cocoa.dima.unige.it`).

A témában komolyabban elmélyedni szándékozóknak elsősorban a komputer algebrai számítások szemszögéből, de egyúttal kellő elméleti mélységgel megírt [19] könyvet ajánljuk. Alapos és az általunk leírtnál általánosabb tárgyalást találhatunk például [2] és [3] könyvekben is.

2. Alapfogalmak és a Gröbner-bázisok elemi tulajdonságai

Mielőtt rátérnénk a legfontosabb fogalmak definiálására, bevezetünk néhány jelölést, amelyeket végig használni fogunk.

2.1. Jelölések

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. A jegyzetben $\mathbb{F}$ mindvégig egy tetszőleges test lesz, n pedig egy 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.

Monomok 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 egy 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.

2.2. Tagsorrendek

2.1. Definíció. Egy, az $\mathbb{F}[\mathbf{x}]$ 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.

Gröbner-bázisról mindig egy rögzített tagsorrendet feltételezve beszélünk, más rendezéshez általában más polinomhalmaz lesz Gröbner-bázis. 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 leggyakrabban használt három tagsorrendet.

2.2. Definíció. 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 $w_i \neq u_i$, arra

$w_i < u_i$ tejesül. Nyilvánvaló, hogy a lexikografikus rendezés tagsorrend. Ezt a rendezést ezentúl röviden *lex*nek fogjuk nevezni.

2.3. Definíció. A másik gyakran használt tagsorrend a *fok-kompatibilis lexikografikus rendezés*, az angol degree compatible lexicographic rövidítéseként *deglex*. Egy $\mathbf{x^w}$ deglex-kisebb mint $\mathbf{x^u}$, amennyiben $\mathbf{x^w}$ foka kisebb, mint $\mathbf{x^u}$ foka (azaz $\sum_{i=1}^{n} w_i < \sum_{i=1}^{n} u_i$) vagy pedig azonos fokúak, és $\mathbf{x^w}$ megelőzi $\mathbf{x^u}$-t a lexikografikus rendezés szerint. A tagsorrendtől megkívánt tulajdonságok a deglex rendezésre is triviálisan teljesülnek.

Végül egy, az első pillantásra különös tagsorrend a degrevlex:

2.4. Definíció. Monomok *fok-kompatibilis fordított lexikografikus* – gyakoribb nevén *degrevlex* – sorrendje a következő. A kisebb fokú monom kisebb, azonos fokok esetén pedig $\mathbf{x^w}$ kisebb, mint $\mathbf{x^u}$ pontosan akkor, ha a legnagyobb i indexnél, amelynél $w_i \neq u_i$, ott $w_i > u_i$ teljesül.

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

2.1. Feladat. Igazoljuk, hogy $n = 1$-re minden tagsorrend megegyezik, $n = 2$-re pedig pontosan két különböző fok-kompatibilis rendezés létezik.

Például $n = 3$ esetén az első néhány monom lex rendezése:

$$1 \prec x_3 \prec x_3^2 \prec x_3^3 \prec \cdots \prec x_2 \prec x_2x_3 \prec x_2x_3^2 \prec \cdots \prec x_2^2 \prec x_2^2x_3 \prec x_2^2x_3^2 \prec \\ \cdots \prec x_1 \prec x_1x_3 \prec x_1x_3^2 \prec \ldots,$$

deglex rendezése:

$$1 \prec x_3 \prec x_2 \prec x_1 \prec x_3^2 \prec x_2x_3 \prec x_2^2 \prec x_1x_3 \prec x_1x_2 \prec x_1^2 \prec x_3^3 \prec \ldots$$

és degrevlex rendezése:

$$1 \prec x_3 \prec x_2 \prec x_1 \prec x_3^2 \prec x_2x_3 \prec x_1x_3 \prec x_2^2 \prec x_1x_2 \prec x_1^2 \prec x_3^3 \prec \ldots$$

2.2. Feladat. Mutassuk meg, hogy a lex, deglex, és degrevlex rendezések valóban tagsorrendek. Definiáljuk a revlex rendezést értelemszerűen, és lássuk be, hogy ez nem tagsorrend. (A revlex lokális rendezés. Bizonyos gyűrűkben ilyenek segítségével definiálható Gröbner-bázis, amely az általunk tárgyalt általánosítása.)

A változók sorrendjének variálásával nyilván további tagsorrendeket kaphatunk. Ez természetesen még nem az összes. Mielőtt rátérünk a tagsorrendek számunkra fontos tulajdonságainak tárgyalására, bizonyítás nélkül közöljük ezen rendezések egy szép jellemzését.

Legyen $\mathbf{a}$ egy nemnegatív 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 nemnegatív valós elemekből álló invertálható 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 [24] (vagy vázlatosan [25]) 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

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

mátrix.

2.3. Feladat. Írjuk fel a degrevlex egy mátrix-reprezentációját!

A következő tételben bebizonyítjuk a tagsorrendek két alapvető tulajdonságát. A jólrendezésről szóló állítás Dickson-lemma néven ismert. Vegyük észre, hogy – bár eddig is monomokról beszéltünk – még sehol sem használtuk fel, hogy polinomokkal dolgozunk: nyilván definiálhattuk volna mindent természetes számokból álló n hosszú vektorok rendezésére is. Dickson lemmája eredetileg ilyenekről szólt (és egyébként Leonard Dickson 1913-as [11] cikke előtt is ismert volt). Érdemes megpróbálkozni az elemi bizonyítással – utána bizonyára jobban fogjuk tudni értékelni az alább leírtat, amely Hilbert bázis tételét használja, tehát most kihasználjuk, hogy monomok rendezéséről beszélünk.

2.5. 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 indirekt, 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. □

2.3. Standard monomok és főtagok

Rögzítsünk egy $\prec$ tagsorrendet.

2.6. Definíció. 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 pedig $\operatorname{lm}(f)$ együtthatóját hívjuk.

2.7. Definíció. 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 $\mathbf{x}^{\mathbf{w}} = \operatorname{lm}(f(\mathbf{x}))$ és $f(\mathbf{x}) \in I$, úgy $\mathbf{x}^{\mathbf{u}} = \operatorname{lm}\left(\frac{\mathbf{x}^{\mathbf{u}}}{\mathbf{x}^{\mathbf{w}}} f(\mathbf{x})\right)$ és $\frac{\mathbf{x}^{\mathbf{u}}}{\mathbf{x}^{\mathbf{w}}} f(\mathbf{x}) \in I$

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

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

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

Néha fogjuk használni ideálok helyett tetszőleges $F \subseteq \mathbb{F}\,[\mathbf{x}]$ polinomhalmazra is az $\mathrm{Sm}\,(F)$ és $\mathrm{Lm}\,(F)$ jelöléseket.

2.8. Definíció.

$$\mathrm{Lm}\,(F) = \{\mathbf{x}^{\mathbf{w}} \,:\, \exists\, f \in F \;\; \mathrm{lm}\,(f) \mid \mathbf{x}^{\mathbf{w}}\}\,,$$
$$\mathrm{Sm}\,(F) = \{\mathbf{x}^{\mathbf{w}} \in \mathbb{F}\,[\mathbf{x}]\} \setminus \mathrm{Lm}\,(F)$$

Amennyiben F ideál, akkor az újonnan definiált $\mathrm{Lm}\,(F)$ (és $\mathrm{Sm}\,(F)$) megegyezik az ideálokra definiált korábbi fogalommal. Pusztán azért nem az általánosabban működő utóbbi definíciót mondtuk ki ideálokra, mert az elsőt valamivel szemléletesebbnek tartjuk. Ezek után pedig gondolhatunk $\mathrm{Lm}\,(F)$-re úgy is, mint az F-ben szereplő polinomok főtagjainak halmazának (az oszthatóságra nézve) felszállóvá tétele.

Fontos megjegyezni, hogy általában $\mathrm{Lm}\,(F) \neq \mathrm{Lm}\,(\langle F \rangle)$. Hamarosan látni fogjuk, hogy ez épp a Gröbner-bázisokat karakterizáló egyik tulajdonság.

2.4. Feladat. Mutassuk meg, hogy $\mathrm{lm}\,(g \cdot h) = \mathrm{lm}\,(g) \cdot \mathrm{lm}\,(h)$.

2.5. Feladat. Igazoljuk, hogy $I \subseteq J$ ideálokra $\mathrm{Sm}\,(I) \supseteq \mathrm{Sm}\,(J)$.

2.4. A Gröbner-bázis

2.9. Definíció. Az I ideál *Gröbner-bázis*ának olyan véges $G \subseteq I$ halmazt nevezünk, amelyre teljesül, hogy minden $f \in I$, $f \neq 0$ polinomhoz létezik $g \in G$, amelyre $\mathrm{lm}\,(g)$ osztója $\mathrm{lm}\,(f)$-nek. Másképpen megfogalmazva, $G \subseteq I$ véges halmaz I Gröbner-bázisa, ha $\mathrm{Lm}\,(I) = \mathrm{Lm}\,(G)$.

Fontos megjegyezni, hogy miután egy polinom vezető tagja függ a választott tagsorrendtől, ezért általában a Gröbner-bázis sem független tőle.

2.10. Példa. Tegyük fel, hogy az $\mathbb{F}$ alaptest nem 2 karakterisztikájú. Az $I = \langle x_1 - x_2, x_1 + x_2 \rangle$ ideálnak egy Gröbner-bázisa $G = \{x_1, x_2\}$ (tetszőleges tagsorrendre nézve). Egyrészt könnyű látni, hogy $G \subseteq I$ (itt kell, hogy nem 2 a karakterisztika). Másrészt ha egy f polinom vezető tagját nem osztja G semelyik elemének vezető tagja (azaz sem x_1, sem x_2), akkor $\mathrm{lm}\,(f) = 1$,

tehát f konstans $c \neq 0$. Azt kell csak látni, hogy $c \notin I$. Ez például azért igaz, mert az $x_1 = 0$, $x_2 = 0$ behelyettesítéskor a fenti két generátorelem 0-t ad, tehát I minden elemére igaz kell legyen ugyanez.

Viszont a $G' = \{x_1 - x_2, x_1 + x_2\}$ halmaz nem Gröbner-bázis, hiszen $x_2 \in I$, de x_2-t nem osztja semelyik G'-beli polinom főtagja.

2.6. Feladat. Lássuk be, hogy ha I főideál, akkor $\{g\}$ pontosan akkor Gröbner-bázisa, ha $\langle g \rangle = I$.

Gröbner-bázis létezése

A definícióban megköveteltük, hogy G véges halmaz legyen, ezért nem teljesen világos, hogy létezik-e tetszőleges ideálnak Gröbner-bázisa. Belátjuk, hogy a válasz szerencsére igen.

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

2.12. Lemma. *Ha I monomiális ideál, és H ennek monomokból álló generátorrendszere, valamint $f \in I$, 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. □

2.13. 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. (Utóbbi tulajdonságot $\mathrm{Lm}(H) = \mathrm{Lm}(I)$-nek rövidíthetjük.)*

Bizonyítás: Tekintsük az $\mathrm{In}(I) := \langle \mathrm{Lm}(I) \rangle$ monomiális ideál egy monomokból álló véges H generátorrendszerét, amely a 2.12 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 2.12 lemma alapján 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 2.12 lemma alapján valamely H-beli monom osztja őt. Ezek szerint H megfelel a követelményeknek. □

Az előbb definiált $\mathrm{In}\,(I)$ ideált *kezdő* vagy *kezdeti ideál*nak szokás hívni, jelölése az angol initial ideal elnevezésből ered.

Vegyük észre, hogy a 2.13 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 G halmaza I egy Gröbner-bázisa, miután $\mathrm{Lm}\,(G) = \mathrm{Lm}\,(H) = \mathrm{Lm}\,(I)$.

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.

2.14. Definíció. Ha G polinomok egy 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

$$f(\mathbf{x}) = \sum_{i=1}^{m} g_i(\mathbf{x}) h_i(\mathbf{x}) + \hat{f}(\mathbf{x}) \tag{2}$$

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 $\mathrm{lm}\,(g_i h_i) \preceq \mathrm{lm}\,(f)$.

2.15. Definíció. Azt mondjuk, hogy $\hat{f}$ *az* f *(egy) redukáltja* G*-re nézve,* (vagy f *(egy)* G *szerinti redukáltja,*) amennyiben létezik (2) előállítás a fenti tulajdonságú $h_1, \ldots, h_m$ polinomokkal. Hangsúlyozzuk, hogy a definícióban nem követeljük meg, hogy $\hat{f}$ redukciós lépésekkel legyen megkapható f-ből.

2.16. 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.

2.17. Tétel. *Ha* I *egy 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 az $\mathbb{F}[\mathbf{x}]/I$ faktorban, 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. □

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

Bizonyítás: Ha $\hat{f}_1$ és $\hat{f}_2$ is f redukáltja G-vel, akkor $\hat{f}_1 - \hat{f}_2 \in I$, ugyanakkor $\hat{f}_1 - \hat{f}_2$ standard monomok lineáris kombinációja, tehát $\hat{f}_1 - \hat{f}_2 = 0$. 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 most igazolt következmény adja a Gröbner-bázisok erejét. A redukált számolásához ezek szerint használhatunk (1) szerinti redukciós lépéseket, tetszőleges sorrendben véve G elemeit: ugyanazt fogjuk kapni. Egyszerű lépésekkel eldönthető például, hogy egy polinom redukáltja nulla-e, tehát hogy benne van-e az ideálban.

A 2.18 következmény alábbi megfordításai is igazak (bár a gyakorlatban nem igazán használhatóak annak tesztelésére, hogy G Gröbner-bázis).

2.19. 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, $\langle G \rangle = I$ és minden $f \in \mathbb{F}[\mathbf{x}]$ polinom G szerinti redukáltja egyértelmű, akkor G Gröbner-bázis.

Bizonyítás: 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 $\operatorname{lm}(g_i h_i) \preceq \operatorname{lm}(f)$. Ráadásul valamely i-re biztosan teljesül $\operatorname{lm}(f) = \operatorname{lm}(g_i h_i) = \operatorname{lm}(g_i)\operatorname{lm}(h_i)$, így ez az $\operatorname{lm}(g_i)$ osztja $\operatorname{lm}(f)$-et.

A második állítás bizonyításához először azt látjuk be, hogy tetszőleges $f, h \in \mathbb{F}[\mathbf{x}]$ és $g \in G$ polinomok esetén f és $f - gh$ redukáltja (ami a feltétel szerint egyértelmű) megegyezik. Ha $\operatorname{lm}(f - gh) \preceq \operatorname{lm}(f)$, akkor legyen $f - gh$ redukáltja $\hat{f}$ és a redukciót leíró egyenlet

$$f - gh = \sum_{i=1}^{m} g_i h_i + \hat{f},$$

ahol természetesen $\operatorname{lm}(g_i h_i) \preceq \operatorname{lm}(f - gh)$. Ekkor f is redukálható $\hat{f}$-re, ugyanis

$$f = \sum_{i=1}^{m} g_i h_i + gh + \hat{f}$$

redukció megfelelő: annyit kell csak észrevennünk, hogy $\operatorname{lm}(g_i h_i) \preceq \operatorname{lm}(f)$ és $\operatorname{lm}(gh) \preceq \operatorname{lm}(f)$. Ha pedig $\operatorname{lm}(f) \preceq \operatorname{lm}(f - gh)$ a helyzet, akkor legyen

$f' = f - gh$, $h' = -h$, és így $f = f' - gh'$, tehát $\mathrm{lm}\,(f' - gh') \preceq \mathrm{lm}\,(f')$, ezért az előbbiek szerint $f' = f - gh$ és $f' - gh' = f$ redukáltja ugyanaz.

Most már egyszerűen következik, hogy G Gröbner-bázis, ugyanis elegendő annyit belátni, hogy $f \in I$ esetén f redukáható G-vel 0-ra. De $\langle G \rangle = I$ miatt $f = \sum_{g \in G} g h_g$, tehát a fenti lépést többször alkalmazva arra jutunk, hogy f redukáltja azonos 0 redukáltjával, azaz 0-val. □

Ideje, hogy összefoglaljuk a Gröbner-bázis eddig tanult ekvivalens definícióit.

2.20. Tétel. *Egy $I \trianglelefteq \mathbb{F}[\mathbf{x}]$ ideál véges G részhalmazára az alábbiak ekvivalensek.*

1. *Minden $f \in I \setminus \{0\}$-ra létezik $g \in G$, hogy $\mathrm{lm}\,(g) \mid \mathrm{lm}\,(f)$.*
2. $\mathrm{Lm}\,(G) = \mathrm{Lm}\,(I)$
3. *Minden $f \in I$ redukálható 0-ra G-vel.*
4. *$\langle G \rangle = I$ és minden f redukáltja G-vel egyértelmű.*

Ilyenkor G az I egy Gröbner-bázisa. □

A 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.

2.21. Definíció. Ha az I ideál G Gröbner-bázisára teljesül, hogy minden $g \in G$ redukált $G \setminus \{g\}$-re nézve és főegyüttható 1, akkor G az *I redukált Gröbner-bázisa*. Más szóval G Gröbner-bázis pontosan akkor redukált, ha minden $g \in G$-ben $\mathrm{lm}\,(g)$-től eltekintve csupa $\mathrm{Sm}\,(G)$-beli monom szerepel és g főegyüttható 1.

2.22. 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 $\mathbf{x}^{\mathbf{w}}$ elemé-hez pontosan egy $g \in G$-t tartottunk meg, aminek főtagja $\mathbf{x}^{\mathbf{w}}$.

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

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

Ekkor G_2 szintén Gröbner-bázis, hiszen pontosan ugyanazok G_1 és G_2 elemeinek főtagjai, továbbá $\operatorname{lm}(g) + \hat{g}$ és g modulo I azonos, azaz $\operatorname{lm}(g) + \hat{g} \in I$. 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 $\operatorname{Lm}(I)$ minimális elemei, így $|G| = |H|$. Legyen $g \in G$ és $h \in H$, amelyre $\operatorname{lm}(g) = \operatorname{lm}(h)$. 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 $\operatorname{Lm}(I)$ *minimális generátorai*nak hívjuk, hiszen – amint az előbbi bizonyításban is láttuk – ezek éppen az oszthatóságra nézve minimális I-beli vezető tagok.

2.5. Eltűnő ideálok

Ebben az alfejezetben olyan ideálokkal fogunk foglalkozni, amelyek egyrészt központi szerepet játszanak az alkalmazásokban, másrészt egyszerűbb meghatározni Gröbner-bázisaikat.

Ha $f(x_1, \ldots, x_n) \in \mathbb{F}[\mathbf{x}]$ egy 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 egy $\mathbb{F}^n \to \mathbb{F}$ függvénynek.

2.23. Definíció. Legyen $V \subseteq \mathbb{F}^n$ és jelölje $I(V)$ a V-n eltűnő polinomok halmazát, azaz

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

Azt mondjuk, hogy $I(V)$ a *V halmaz eltűnő ideálja*.

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 $\mathbb{F}[\mathbf{x}]/I(V)$ izomorf a $V \to \mathbb{F}$ függvények vektorterével, ugyanis tetszőleges $V \to \mathbb{F}$ függvény reprezentálható polinommal. Ez a Lagrange-interpolációval egyszerűen látható: elég annyit megmutatni, hogy minden $\mathbf{y} \in V$ pontra $\mathbf{y}$ karakterisztikus függvénye $\chi_{\mathbf{y}}$

(amely $\mathbf{y}$-ban 1, mindenütt másutt V-n pedig 0) reprezentálható polinommal, hiszen tetszőleges függvény előáll $\chi_{\mathbf{y}}$ alakú függvények lineáris kombinációjaként. Jelölje $F \subseteq \mathbb{F}$ azon testelemek halmazát, amelyek előfordulnak V valamely pontjának valamely koordinátájában. Ha $y \in F$, akkor legyen

$$\chi_y(x) = \prod_{z \in F \setminus \{y\}} \frac{x - z}{y - z},$$

és $\mathbf{y} \in V$ esetén pedig $\chi_{\mathbf{y}}(\mathbf{x}) := \prod_{i=1}^{n} \chi_{y_i}(x_i)$.

2.24. Következmény. *Ha valamelyik oldal véges, akkor*

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

Bizonyítás: A $V \to \mathbb{F}$ függvények vektortere $|V|$ dimenziós, $\mathbb{F}[\mathbf{x}]/I(V)$ faktortér pedig a 2.17 tétel szerint éppen $|\mathrm{Sm}\,(I(V))|$ dimenziós. Fent láttuk, hogy ha V véges, akkor ez a két vektortér izomorf. Annyit kell tehát még látnunk, hogy ha V végtelen, akkor $\mathrm{Sm}\,(I(V))$ is az. Ez azért igaz, mert ha V végtelen, akkor az előbb látott interpolációs módszerrel készítsünk f_i polinomot minden i pozitív egészre, amely V első $i-1$ pontján eltűnik, az i. pontján pedig 1-et vesz fel. Világos, hogy ez végtelen sok lineárisan független polinomfüggvény, tehát $\mathbb{F}[\mathbf{x}]/I(V)$ dimenziója végtelen. □

Végül bebizonyítunk egy lemmát, amely jól használható annak bizonyítására, hogy egy $G = \{g_1, \ldots, g_m\}$ polinomhalmaz Gröbner-bázis.

2.25. Lemma. *Legyen I ideál, $G \subseteq I$ és tegyük fel, hogy $\mathrm{Sm}\,(I)$ véges. Ekkor teljesül, hogy G pontosan akkor Gröbner-bázisa I-nek, ha $|\mathrm{Sm}\,(I)| = |\mathrm{Sm}\,(G)|$.*

Bizonyítás: A definícióból nyilvánvaló, hogy $\mathrm{Sm}\,(I) \subseteq \mathrm{Sm}\,(G)$ mindig teljesül. A végességi feltétel miatt az elemszámok egyenlősége tehát ekvivalens a halmazok egyenlőségével. Az $\mathrm{Sm}\,(I) = \mathrm{Sm}\,(G)$ egyenlőség mindkét oldalának komplementerét véve, kapjuk, hogy $\mathrm{Lm}\,(I) = \mathrm{Lm}\,(G)$, tehát G Gröbner-bázis. □

Ezt a lemmát leginkább véges V halmazon eltűnő polinomok $I(V)$ ideáljára kényelmes alkalmazni. Vegyük észre ugyanis, hogy ilyenkor $|\mathrm{Sm}\,(I(V))| = |V|$, ezért a 2.25 lemma feltétele könnyen ellenőrizhető.

2.26. Következmény. *Ha V véges, $G \subseteq I(V)$, akkor G pontosan akkor $I(V)$ Gröbner-bázisa, ha $|V| = |\mathrm{Sm}\,(G)|$.*

3. Algoritmusok

Két Gröbner-bázist számoló 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, a Buchberger–Möller-algoritmus csak speciális ideálokra működik: véges V pontrendszerekhez tartozó $I(V)$ ideálok redukált Gröbner-bázisainak meghatározására szolgál. Sok alkalmazáshoz viszont ez éppen elég. Az irodalomban számtalan egyéb algoritmust – amelyek közül sok az itt tárgyalt általánosítása, vagy valamilyen javítása – lehet találni, közöttük olyanokat, amelyek általánosabban nulla dimenziós ideálokra (a definíciót lásd a 4.2 alfejezetben) működnek. A Buchberger–Möller-algoritmust egyszerűsége és ugyanakkor gyors futásideje miatt választottuk ki bemutatásra. Az általános algoritmussal szemben ez is a fő előnye: a Buchberger-algoritmus futásidejéről nehéz bármi pontosat állítani, azon túl, hogy véges sok lépésben véget ér.

3.1. Buchberger algoritmusa

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

3.1. Definíció. 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 főegyüttható ja 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.

3.2. Lemma. *Legyenek $f_1, \ldots, f_s$ közös $\mathbf{x}^{\mathbf{w}}$ főtagú és 1 főegyütthatójú polinomok. Tegyük fel továbbá, hogy $f = \sum_{i=1}^{s} c_i f_i$ valamilyen $c_i \in \mathbb{F}$ együtthatókkal. Ha $\mathrm{lm}(f) \prec \mathbf{x}^{\mathbf{w}}$, 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 $f(\mathbf{x})$-ben 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

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

□

3.3. 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 2.18 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 főegyütthatója 1. A 2.19 állítás első része szerint elegendő megmutatni, hogy minden $f \in \langle G \rangle$ redukálható 0-ra. Indirekt tegyük fel, hogy f ellenpélda. Tekintsünk egy olyan

$$f = \sum_{i=1}^{m} g_i h_i \tag{3}$$

előállítást, amelyben $\mathbf{x}^{\mathbf{w}} := \max_{i=1\ldots m} \mathrm{lm}(g_i h_i)$ minimális. Ilyen létezik, hiszen $f \in \langle G \rangle$ miatt van megfelelő előállítás, továbbá minden tagsorrend jólrendezés (így a minimum létezik). Nyilván $\mathrm{lm}(f) \preceq \mathbf{x}^{\mathbf{w}}$, ráadásul egyenlőség sem állhat fenn, különben a 2.15. definíció értelmében (3) azt mutatná, hogy f redukálható 0-ra.

Megkonstruáljuk f-nek egy (3)-hoz hasonló előállítását, amelyben azonban a szereplő monomok mind $\mathbf{x}^{\mathbf{w}}$-nél kisebbek lesznek, ellentmondva $\mathbf{x}^{\mathbf{w}}$ minimalitásának. Jelölje L azon i indexek nemüres halmazát, amelyre $\mathbf{x}^{\mathbf{w}} = \mathrm{lm}(g_i h_i)$. 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 $\operatorname{lm}(g_i(\mathbf{x})\mathbf{x}^{\mathbf{w_i}}) = \mathbf{x}^{\mathbf{w}}$. Ekkor $\sum_{i\in L} c_i = 0$ teljesül, 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 a g_i polinomok $\mathbb{F}[\mathbf{x}]$-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 3.2 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

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

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.

3.4. Algoritmus (BUCHBERGER)**.** *Legyen I ideál $\mathbb{F}[\mathbf{x}]$-ben és $F \subseteq I$ egy tetszőleges véges generátorrendszere. A következő eljárás véges lépésben véget ér, a végén F az I ideál egy Gröbner-bázisa lesz.*

`While` $\exists f_1, f_2 \in F$, amelyeket együtt még nem vizsgáltunk `do`
  $r :=$ ($S(f_1, f_2)$ redukáltja F-fel)`;`
  `If` $r \neq 0$ `then` $F := F \cup \{r\}$`; endif;`
`endwhile;`

Bizonyítás: A helyesség bizonyítása a 3.3 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 3.3 tétel szerint tehát I egy Gröbner-bázisát kapjuk így.

Végül megmutatjuk, hogy az eljárás véges sok lépésben véget ér. Tegyük fel indirekt az ellenkezőjét. Legyen $F_1 = F$ és $F_{i+1} = F_i \cup \{r_i\}$ az F halmaz $(i+1)$-edik állapota, speciálisan r_i redukált F_i-re. Megkaptuk tehát I generátorrendszereinek egy $F_1 \subsetneq F_2 \subsetneq \dots$ végtelen sorozatát. Teljesül $\mathrm{Lm}(F_i) \subsetneq \mathrm{Lm}(F_{i+1})$ is, hiszen $\mathrm{lm}(r_i) \in \mathrm{Lm}(F_{i+1}) \setminus \mathrm{Lm}(F_i)$. Legyen $\mathrm{In}(F_i) = \langle \mathrm{Lm}(F_i) \rangle$. Ekkor $\mathrm{lm}(r_i) \in \mathrm{In}(F_{i+1}) \setminus \mathrm{In}(F_i)$ szintén igaz, ugyanis $\mathrm{In}(F_i)$ monomiális ideál, tehát a 2.12 lemma miatt ha $\mathrm{lm}(r_i) \in \mathrm{In}(F_i)$ lenne, akkor $\mathrm{lm}(r_i) \in \mathrm{Lm}(F_i)$ is fennállna. Így viszont

$$\mathrm{In}(F_1) \subsetneq \mathrm{In}(F_2) \subsetneq \dots$$

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. Sok múlik például azon, hogy F elemeit milyen sorrendben tekintjük. Az érdeklődő Olvasó találhat javításokat [2] 3.3. alfejezetében, Giovini, Mora, Niesi, Robbiano és Traverso [18] munkájában. Érdemes megnézni Faugère [12] és [13] cikkeit is. A két leggyorsabban futó algoritmus a kutatások mai állása szerint az utóbbi és Brickenstein [4] eljárása, amely számos trükköt – köztük a „sovány polinomokkal" való számolást – sorakoztat fel.

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

3.2. A Buchberger–Möller-algoritmus

Az algoritmus változatai több cikkben megtalálhatóak, az eredeti Buchberger és Möller 1982-ben megjelent [9] munkája. Részletes költségelemzést tartal-

maz és elég általános Marinari, Möller és Mora [22] dolgozata, jó összefoglalót ad Mora és Robbiano [23] és végül a nulla dimenziós esetre általánosítja Abott, Kreuzer és Robbiano [1]. Ugyanezen az alapötleten múlik Faugère, Gianni, Lazard és Mora [14] algoritmusa, amely a számításhoz felteszi, hogy valamely más tagsorrendre már ismert a redukált Gröbner-bázis.

A Buchberger–Möller-algoritmus egy V véges pontrendszerhez tartozó ideál redukált Gröbner-bázisát számolja ki. Mielőtt nekikezdenénk az algoritmus ismertetésének, vizsgáljuk meg, hogy hogyan járhatnánk el, ha azt a – látszólag – egyszerűbb feladatot tűznénk ki, hogy V segítségével adjuk meg $I(V)$ egy tetszőleges generátorrendszerét.

Tekintsük a következő, végtelenszer $|V|$-es A „mátrixot". Az A sorait monomokkal, oszlopait V elemeivel indexeljük. Az $\mathbf{x}^{\mathbf{w}}$ és $\mathbf{v}$-hez tartozó elem legyen $\mathbf{x}^{\mathbf{w}}(\mathbf{v}) = \mathbf{v}^{\mathbf{w}}$, azaz $\mathbf{x}^{\mathbf{w}}$ helyettesítési értéke a $\mathbf{v}$ helyen. Sorműveletek segítségével az A mátrixot „felső háromszög" alakra lehet hozni, azaz kaphatunk egy

$$\begin{bmatrix} 1 & * & \dots & * \\ 0 & 1 & \dots & * \\ & & \ddots & \\ 0 & 0 & \dots & 1 \\ 0 & 0 & \dots & 0 \\ & & \dots & \end{bmatrix}$$

alakú A' mátrixot. A sorműveletek során megőrizhetjük A azon tulajdonságát, hogy minden sor egy-egy polinom V-n felvett helyettesítési értékeiből áll: például ha az $f(\mathbf{x})$-hez tartozó sorhoz hozzáadjuk a $g(\mathbf{x})$-hez tartozó sor α skalárszorosát, akkor mostantól az előbbi sor az $f(x) + \alpha g(\mathbf{x})$ polinom helyettesítési értékeiből áll.

Ezek szerint a csupa 0 sorok V-n eltűnő polinomokhoz tartoznak. Miután az összes monom lineáris bázisa $\mathbb{F}[\mathbf{x}]$ vektortérnek, ezért az A' soraihoz tartozó polinomok halmaza szintén lineáris bázisa $\mathbb{F}[\mathbf{x}]$-nek. Ebből viszont következik, hogy a csupa nulla sorokhoz tartozó polinomok lineáris kombinációjával előállítható tetszőleges $f \in I(V)$. Ezek szerint a csupa nulla sorok polinomjai közül kiválasztható $I(V)$ egy véges generátorrendszere.

Ennek az eljárásnak a *hatékony* megvalósítása a Buchberger–Möller-algoritmus. Végtelen sok sor kinullázása helyett pontosan annyival fogunk foglalkozni, amennyire feltétlenül szükség van.

Egyetlen sorral – az 1 monomhoz tartozóval – kezdünk és az algoritmus futása közben határozzuk meg azon monomokat, amelyekhez tartozó sorokat érdemes lesz vizsgálni. (Ezek szerepelnek majd az M halmazban.) Egy új sor (azaz egy $\mathbf{x}^{\mathbf{w}} \in M$ monom) vizsgálatakor megpróbáljuk kinullázni azt a korábbi sorok segítségével. Jelölje $p(\mathbf{x})$ az ezen sorhoz tartozó polinomot

(tehát először $p(\mathbf{x}) = \mathbf{x}^{\mathbf{w}}$, majd a sorműveletek során $p(\mathbf{x})$ változik). Nagyon lényeges, hogy egy új sorhoz a kizárólag a *korábbiak* skalárszorosát adhatjuk hozzá. Miután az adott tagsorrendre nézve egyre nagyobb monomokkal fogunk foglalkozni, ezzel garantáljuk, hogy a sorműveletek során változatlan $\mathbf{x}^{\mathbf{w}}$ marad $p(\mathbf{x})$ főtagja.

Ha az új sort sikerült kinullázni, akkor a kapott $p(\mathbf{x})$ épp a redukált Gröbner-bázis $\mathbf{x}^{\mathbf{w}}$ főtagú eleme. Ha nem sikerült, akkor viszont $p(\mathbf{x})$ egy alkalmas skalárszorosa az A' mátrix egyik nem csupa 0 sorának felel majd meg. Ha eddig i ilyen sorunk volt, akkor a megfelelő polinomot $q_{i+1}(\mathbf{x})$ jelöli. A V pontrendszer elemeinek a sorrendjének esetleges megváltoztatása árán feltehető, hogy a nemnulla elem a főáltóban van. Képletben tehát: $q_{i+1}(\mathbf{v}_j) = 0$ (ha $j \leq i$) és $q_{i+1}(\mathbf{v}_{i+1}) = 1$ (az előbb említett skalár tehát $\frac{1}{p(\mathbf{v}_{i+1})}$ lesz). Belátjuk majd, hogy ilyenkor teljesül $\mathbf{x}^{\mathbf{w}} \in \mathrm{Sm}\,(I(V))$.

Lássuk tehát az algoritmus pontos működését.

3.5. Algoritmus (Buchberger–Möller)**.** *Legyen $V \subseteq \mathbb{F}^n$ véges pontrendszer. A következő eljárás előállítja az $I(V) \trianglelefteq \mathbb{F}[\mathbf{x}]$ ideál G redukált Gröbner-bázisát (az inputként megadandó) $\prec$ tagsorrendre. Melléktermékként megkapjuk az $I(V)$ standard monomjait (az S halmazban), továbbá a fent részletezett tulajdonságú q_i polinomokat is.*

$G := \emptyset$; $S := \emptyset$; $M := \{1\}$; $i := 0$;
`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`
      `legyen` $\mathbf{v}_{i+1} \in V$, `amire` $p(\mathbf{v}_{i+1}) \neq 0$;
      $q_{i+1}(\mathbf{x}) := \frac{p(\mathbf{x})}{p(\mathbf{v}_{i+1})}$;
      $S := S \cup \{\mathbf{x}^{\mathbf{w}}\}$;
      $M := M \cup \{x_j \cdot \mathbf{x}^{\mathbf{w}} \,:\, j = 1 \ldots n\}$;
      $i := i + 1$;
    `endif`;
  `endif`;
`endwhile`;

Bizonyítás: Könnyű látni (i-re vonatkozó indukció), hogy q_{i+1} eleget tesz a kívánalmaknak, azaz $j \leq i$ esetén $q_{i+1}(\mathbf{v}_j) = 0$ és $q_{i+1}(\mathbf{v}_{i+1}) = 1$. Vegyük észre, hogy a `For` ciklus pontosan a Gauss-elimináció azon lépését valósítja

meg, amelyben a $p(\mathbf{x}) = \mathbf{x}^{\mathbf{w}}$ polinomhoz tartozó sort a korábbiakkal megpróbáljuk kinullázni: $q_1, \ldots, q_i$ segítségével tehát elérjük, hogy p helyettesítési értéke 0 legyen a $\mathbf{v}_1, \ldots, \mathbf{v}_i$ pontokon. Ha $p(\mathbf{x}) \notin I(V)$, akkor van olyan V-beli $\mathbf{v}_{i+1}$ pont, amire $p(\mathbf{v}_{i+1}) \neq 0$. Ekkor $q_{i+1}(\mathbf{x})$ definíciójára tekintve az állítás világos.

Az algoritmus véges sok lépésben leáll, ugyanis ha már $i = |V|$, akkor minden újabb $p(\mathbf{x})$ polinom eltűnik V-n (a megfelelő sor kinullázható), ezért M-be több elem már nem kerül, tehát előbb-utóbb kiürül.

Rátérünk annak igazolására, hogy G redukált Gröbner-bázis, és $S = \mathrm{Sm}\,(I(V))$.

Először is bebizonyítjuk, hogy $\mathrm{lm}\,(p) = \mathbf{x}^{\mathbf{w}}$. 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. Nyilvánvaló 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 $\mathrm{lm}\,(p) = \mathbf{x}^{\mathbf{w}}$.

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. Az algoritmusra tekintve az is világos, hogy S és $\mathrm{Lm}\,(G)$ diszjunkt, tehát $S = \mathrm{Sm}\,(G)$.

Látható, hogy $G \subseteq I(V)$, ezért az algoritmus végén $|S| = |\mathrm{Sm}\,(G)| \geq |\mathrm{Sm}\,(I(V))| = |V|$. De az algoritmus során mindvégig $|S| = i \leq |V|$, tehát az előbbi összefüggésben valójában egyenlőség áll fenn, speciálisan $|\mathrm{Sm}\,(G)| = |V|$. A 2.26 következmény szerint G tehát Gröbner-bázis és így persze $S = \mathrm{Sm}\,(G) = \mathrm{Sm}\,(I(V))$ is igaz.

Végül következik, 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. □

3.1. Feladat. Igazoljuk, hogy $\mathrm{Sm}\,(I(\{v_1,\ldots,v_i\})) = S$ az algoritmus során végig igaz.

3.6. Példa. Legyen $V = \{(1,2,3),(2,2,3),(0,3,2)\} \in \mathbb{Q}^3$ és tekintsük a deglex rendezést. Végig fogjuk nézni az algoritmus futását. Gyakorlás végett érdemes párhuzamosan az A' mátrix alakulását is számolni.

$\min M = 1$, tehát $p(\mathbf{x}) := 1$.
$p(\mathbf{x}) \notin I(V)$, mert $p(1,2,3) = 1 \neq 0$, így
$q_1(\mathbf{x}) := 1$, $\mathbf{v}_1 := (1,2,3)$, $S = \{1\}$ és
$M = \{x_1, x_2, x_3\}$.
$\min M = x_3$, tehát $p(\mathbf{x}) := x_3$,
$p(\mathbf{x}) := x_3 - q_1(\mathbf{x})(x_3(1,2,3)) = x_3 - 3$.
$p(\mathbf{x}) \notin I(V)$, mert $p(0,3,2) = -1 \neq 0$, így
$q_2(\mathbf{x}) := \frac{x_3-3}{-1} = -x_3 + 3$, $\mathbf{v}_2 := (0,3,2)$, $S = \{1, x_3\}$ és
$M = \{x_1, x_2, x_1x_3, x_2x_3, x_3^2\}$.
$\min M = x_2$, tehát $p(\mathbf{x}) := x_2$,
$p(\mathbf{x}) := x_2 - q_1(\mathbf{x})(x_2(1,2,3)) = x_2 - 2$,
$p(\mathbf{x}) := x_2 - 2 - q_2(\mathbf{x})((x_2-2)(0,3,2)) = x_2 + x_3 - 5$.
$p(\mathbf{x}) \in I(V)$, így
$g_1(\mathbf{x}) := x_2 + x_3 - 5$ és
$M = \{x_1, x_1x_3, x_2x_3, x_3^2\}$.
$\min M = x_1$, tehát $p(\mathbf{x}) := x_1$,
$p(\mathbf{x}) := x_1 - q_1(\mathbf{x})(x_1(1,2,3)) = x_1 - 1$,
$p(\mathbf{x}) := x_1 - 1 - q_2(\mathbf{x})((x_1-1)(0,3,2)) = x_1 - x_3 + 2$.
$p(\mathbf{x}) \notin I(V)$, mert $p(2,2,3) = 1 \neq 0$, így
$q_3(\mathbf{x}) := \frac{x_1-x_3+2}{1} = x_1 - x_3 + 2$, $\mathbf{v}_3 := (2,2,3)$, $S = \{1, x_3, x_1\}$,
$M = \{x_1x_3, x_2x_3, x_3^2, x_1^2, x_1x_2\}$.
$\min M = x_3^2$, tehát $p(\mathbf{x}) := x_3^2$,
$p(\mathbf{x}) := x_3^2 - q_1(\mathbf{x})(x_3^2(1,2,3)) = x_3^2 - 9$,
$p(\mathbf{x}) := x_3^2 - 9 - q_2(\mathbf{x})((x_3^2-9)(0,3,2)) = x_3^2 - 5x_3 + 6$,
$p(\mathbf{x}) := x_3^2 - 5x_3 + 6 - q_3(\mathbf{x})((x_3^2-5x_3+6)(2,2,3)) = x_3^2 - 5x_3 + 6$.
$p(\mathbf{x}) \in I(V)$, így
$g_2(\mathbf{x}) := x_3^2 - 5x_3 + 6$ és
$M = \{x_1x_3, x_2x_3, x_1^2, x_1x_2\}$.
$\min M = x_2x_3$, de $\mathrm{lm}\,(g_1) = x_2 \mid x_2x_3$, ezért nem foglalkozunk vele és
$M = \{x_1x_3, x_1^2, x_1x_2\}$.
$\min M = x_1x_3$, tehát $p(\mathbf{x}) := x_1x_3$,
$p(\mathbf{x}) := x_1x_3^2 - q_1(\mathbf{x})((x_1x_3)(1,2,3)) = x_1x_3 - 3$,
$p(\mathbf{x}) := x_1x_3 - 3 - q_2(\mathbf{x})((x_1x_3-3)(0,3,2)) = x_1x_3 - 3x_3 + 6$,
$p(\mathbf{x}) := x_1x_3 - 3x_3 + 6 - q_3(\mathbf{x})((x_1x_3-3x_3+6)(2,2,3)) = x_1x_3 - 3x_1$.
$p(\mathbf{x}) \in I(V)$, így

$g_3(\mathbf{x}) := x_1x_3 - 3x_1$ és
$M = \{x_1^2, x_1x_2\}$.
$\min M = x_1^2$, tehát $p(\mathbf{x}) := x_1^2$,
$p(\mathbf{x}) := x_1^2 - q_1(\mathbf{x})(x_1^2(1,2,3)) = x_1^2 - 1$,
$p(\mathbf{x}) := x_1^2 - 1 - q_2(\mathbf{x})((x_1^2 - 1)(0,3,2)) = x_1^2 - x_3 + 2$,
$p(\mathbf{x}) := xx_1^2 - x_3 + 2 - q_3(\mathbf{x})((x_1^2 - x_3 + 2)(2,2,3)) = x_1^2 + 3x_1 - 4x_3 + 8$.
$p(\mathbf{x}) \in I(V)$, így
$g_3(\mathbf{x}) := x_1^2 + 3x_1 - 4x_3 + 8$ és
$M = \{x_1x_2\}$.
$\min M = x_1x_2$, de $\operatorname{lm}(g_1) = x_2 \mid x_1x_2$, ezért nem foglalkozunk vele és
$M = \emptyset$, azaz végeztünk.

Tehát $\operatorname{Sm}(I(V)) = \{1, x_3, x_1\}$ és $G = \{x_2 + x_3 - 5, x_3^2 - 5x_3 + 6, x_1x_3 - 3x_1, x_1^2 + 3x_1 - 4x_3 + 8\}$ a redukált Gröbner-bázis.

3.7. Tétel. *Tegyük fel, hogy az aritmetikai műveletek $\mathbb{F}$ testben a, két n változós monom $\prec$ szerinti összehasonlítása pedig nb költségűek. Legyen továbbá $m = |V|$. Ekkor a Buchberger–Möller-algoritmus $O(am^3n + bmn^2 \log(mn))$ 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. Itt ebből annyit használunk, hogy $O(\log |M|)$ összehasonlítással tudunk M-ben keresni, ennyi idő alatt megkapjuk M minimális elemét, illetve ugyanekkora költséggel tudunk M-ből törölni és M-be beszúrni elemeket.

Ahelyett, hogy valamiféle kereséssel direkt módon próbálnánk eldönteni, hogy $\mathbf{x}^{\mathbf{w}} \in \operatorname{Lm}(G)$ fennáll-e, a következőt tesszük. Feljegyezzük M elemei mellé, hogy hány alkalommal szúrtuk be őket. (Ehhez kell, hogy keresni is tudjunk gyorsan M-ben.) Bebizonyítjuk, hogy ha $\mathbf{x}^{\mathbf{w}}$ az M minimális eleme egy lépésben, akkor pontosan akkor teljesül $\mathbf{x}^{\mathbf{w}} \notin \operatorname{Lm}(G)$, 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 $\operatorname{Lm}(I)$ 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 $\mathbf{v_i}^{\mathbf{w}}$ 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 $\mathbf{v_i}^{\mathbf{w}'}$ értékeket (és persze ℓ-et se feledjük). Így minden egyes $\mathbf{v_i}^{\mathbf{w}}$ kiszámolható egyetlen szorzással, ez összesen tehát $i \leq m$ aritmetikai művelet.

Amikor p polinommal dolgozunk, $p \in I(V)$ eldöntéséhez szükségünk lesz rá, hogy minden pontban kiszámoljuk p helyettesítési értékét. Érdemes emiatt a sokat emlegetett A' mátrixot ténylegesen tárolni, így a `For` ciklus után kapott p polinom V-n felvett értékeit néhány sorművelettel megkaphatjuk. Pontosan tehát azt mondhatjuk, hogy p számolásakor az alábbi

$$\left[\begin{array}{cccc|ccc|c} 1 & q_1(\mathbf{v}_2) & \dots & q_1(\mathbf{v}_{i-1}) & q_1(\mathbf{v}_i) & \dots & q_1(\mathbf{v}_m) & q_1(\mathbf{x}) \\ 0 & 1 & \dots & q_2(\mathbf{v}_{i-1}) & q_2(\mathbf{v}_i) & \dots & q_2(\mathbf{v}_m) & q_2(\mathbf{x}) \\ & \dots & & & & \dots & & \\ 0 & 0 & \dots & 1 & q_{i-1}(\mathbf{v}_i) & \dots & q_{i-1}(\mathbf{v}_m) & q_{i-1}(\mathbf{x}) \\ \mathbf{v_1}^{\mathbf{w}} & \mathbf{v_2}^{\mathbf{w}} & \dots & \mathbf{v_{i-1}}^{\mathbf{w}} & \mathbf{v_i}^{\mathbf{w}} & \dots & \mathbf{v_m}^{\mathbf{w}} & \mathbf{x}^{\mathbf{w}} \end{array}\right]$$

mátrixot ismerjük. 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 $p(\mathbf{v}_j)$ $(j = 1 \dots m)$ 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, a 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. Alkalmazások

4.1. Elemi kommutatív algebrai kérdések

Ideál egy elemének megadása generátorokkal

Komputer algebra rendszerekben természetesnek vesszük, hogy találunk beépített függvényt annak tesztelésére, hogy egy elem benne van-e egy adott (véges) halmazban. A hasonló kérdés, hogy egy polinomot tartalmaz-e egy ideál, nem ilyen egyszerű, hiszen egy ideál tipikusan végtelen elemszámú. Erre az elemi kérdésre a választ az ideál egy Gröbner-bázisának segítségével lehet megadni.

Tegyük fel, hogy $I = \langle f_1, \ldots, f_s \rangle$ és $f \in \mathbb{F}[\mathbf{x}]$. Legyen egy Gröbner bázisa I-nek $G = \{g_1, \ldots, g_m\}$. Számítsuk ki f-nek $\hat{f}$ redukáltját G-re. Erre, mint láttuk, jó a „mohó" algoritmus: f-ből kiindulva az aktuális polinom legnagyobb monomját redukáljuk, amely még redukálható G valamely elemével. A 2.18 következmény szerint $f \in I$ pontosan akkor, ha $\hat{f} = 0$.

Jogos igény, hogy $f \in I$ esetén adjuk is meg f előállítását a generátorokkal. Először is, a redukció során megkapjuk f egy

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

alakú előállítását. Elegendő ezért G elemeit kifeljezni az eredeti f_j generátorokkal.

Egy lehetséges megoldás – amennyiben G-t a Buchberger-algoritmussal számoljuk –, hogy $F = \{f_1, \ldots, f_s\}$-ből kiindulva, amikor F két elemének S-polinomjának redukáltját számoljuk, rögtön $\{f_1, \ldots, f_s\}$ polinom-lineáris kombinációjával kifejezzük. Pontosabban, ha az aktuális $F = \{f_1, \ldots, f_{s'}\}$ halmaz elemeinek a kezdeti generátorokkal való előállítása például

$$f_i = \sum_{j=1}^{s} f_j h_{i,j} \quad (1 \leq i \leq s'),$$

akkor az újonnan hozzáveendő $f_{s'+1}$ polinomot a következő módon tudjuk kifejezni. Tegyük fel, hogy ebben a lépésben épp f_k, f_ℓ polinomokkal dolgozunk. Ekkor

$$S(f_k, f_\ell) = \sum_{i=1}^{s'} f_i h_i + f_{s'+1},$$

összefüggésből kapjuk, hogy

$$f_{s'+1} = \frac{\mathbf{x}^{\mathbf{w}}}{c_{f_k} \operatorname{lm}(f_k)} f_k - \frac{\mathbf{x}^{\mathbf{w}}}{c_{f_\ell} \operatorname{lm}(f_j)} f_\ell - \sum_{i=1}^{s'} f_i h_i =$$

$$\frac{\mathbf{x}^{\mathbf{w}}}{c_{f_k} \operatorname{lm}(f_k)} \sum_{j=1}^{s} f_j h_{k,j} - \frac{\mathbf{x}^{\mathbf{w}}}{c_{f_\ell} \operatorname{lm}(f_\ell)} \sum_{j=1}^{s} f_j h_{\ell,j} - \sum_{i=1}^{s'} \sum_{j=1}^{s} f_j h_{i,j} h_i =$$

$$\sum_{j=1}^{s} f_j \left(\frac{\mathbf{x}^{\mathbf{w}}}{c_{f_k} \operatorname{lm}(f_k)} h_{k,j} - \frac{\mathbf{x}^{\mathbf{w}}}{c_{f_\ell} \operatorname{lm}(f_\ell)} h_{\ell,j} - \sum_{i=1}^{s'} h_{i,j} h_i \right),$$

azaz $h_{s'+1,j} = \frac{\mathbf{x}^{\mathbf{w}}}{c_{f_k} \operatorname{lm}(f_k)} h_{k,j} - \frac{\mathbf{x}^{\mathbf{w}}}{c_{f_\ell} \operatorname{lm}(f_\ell)} h_{\ell,j} - \sum_{i=1}^{s'} h_{i,j} h_i$.

Ideálok egyenlősége

Ha $I = \langle F \rangle$ és $J = \langle H \rangle$ ideálok, akkor $I \stackrel{?}{=} J$ eldöntésére használhatjuk az előző alfejezetben tanultakat: $I \subseteq J$ akkor és csak akkor, ha F minden eleme J-ben van.

Egy másik – talán kevesebb számolást igénylő – eljárás, ha meghatározzuk I és J redukált Gröbner-bázisát. Ez, a redukált Gröbner-bázis egyértelműségéről szóló, 2.22 tétel bizonyításában leírtak alapján gyorsan megtehető, tetszőleges Gröbner-bázisból kiindulva. A két ideál pontosan akkor egyenlő, ha a redukált Gröbner-bázisok megegyeznek.

Fontos speciális eset az $I \stackrel{?}{=} \mathbb{F}[\mathbf{x}]$ kérdés, amit természetesen $1 \in I$ tesztelésével dönthetünk el, ami ekvivalens kérdés azzal, hogy G-ben van-e nem nulla konstans polinom (bármilyen G Gröbner-bázis esetén).

Számítások $\mathbb{F}[\mathbf{x}]/I$-ben

A 2.17 tételben láttuk, hogy $\operatorname{Sm}(I)$ elemeinek I szerinti mellékosztályai a faktor lineáris bázisát adják. Másrészt azt is igazoltuk, hogy egy Gröbner-bázis segítségével tetszőleges $f \in \mathbb{F}[\mathbf{x}]$ polinom redukálható $\hat{f}$ polinommá, amely standard monomok lineáris kombinációja. Másképpen mondva, tetszőleges polinom mellékosztályának egy kanonikus reprezentációja a polinom redukáltja.

Redukált polinomok összege nyilván redukált. A szorzásra ugyanez nem mondható el: itt a Gröbner-bázisunkkal még redukálnunk kell az eredményt. Az inverz számítása már érdekesebb feladat.

4.1. Állítás. *Egy f polinommal reprezentált $\mathbb{F}[\mathbf{x}]/I$-beli elem pontosan akkor invertálható, ha $\langle f, I \rangle = \mathbb{F}[\mathbf{x}]$.*

Bizonyítás: Világos, hogy $\langle f, I\rangle = \mathbb{F}[\mathbf{x}]$ akkor és csak akkor teljesül, ha valamely $g \in I$ és $h \in \mathbb{F}[\mathbf{x}]$ polinomokra $1 = hf + g$. Utóbbi egyenlőséget az $\mathbb{F}[\mathbf{x}]/I$ faktorban tekintve kapjuk, hogy h épp f inverze modulo I. □

Ha $g_1, \ldots, g_m$ egy generátorrendszere I-nek, akkor $f, g_1, \ldots, g_m$ generátorrendszere az $\langle f, I\rangle$ ideálnak. Számoljuk ki az utóbbi egy Gröbner-bázisát úgy, hogy az $f, g_1, \ldots, g_m$ polinomokból indulunk ki és a számítás közben megjegyezzük az új elemek előállítását $f, g_1, \ldots, g_m$ polinomokkal. Ha a kapott Gröbner-bázisban nem szerepel 1, akkor az előbbi állítás szerint f mellékosztálya nem invertálható. Ha szerepel, akkor viszont a számítás mentén megkaptunk egy $1 = fh + \sum_{i=1}^{m} g_i h_i$ előállítást, amiből látszik, hogy f modulo I inverze éppen h.

Ideálok metszetének generátorrendszere

4.2. Állítás. *Legyen $I, J \trianglelefteq \mathbb{F}[\mathbf{x}]$ és tekintsük a $\langle zI, (1-z)J\rangle \trianglelefteq \mathbb{F}[z, x_1, \ldots, x_n]$ ideált, ahol z egy új változó. Ekkor*

$$I \cap J = \langle zI, (1-z)J\rangle \cap \mathbb{F}[\mathbf{x}].$$

Bizonyítás: Ha $f \in I \cap J$, akkor $f = zf + (1-z)f$ miatt f a jobb oldalon is szerepel. Megfordítva, tegyük fel, hogy $f(\mathbf{x})$ a jobb oldali metszet egy eleme. Ha $I = \langle f_1, \ldots, f_s\rangle$ és $J = \langle g_1, \ldots, g_m\rangle$, akkor $\langle zI, (1-z)J\rangle = \langle zf_1, \ldots, zf_s, (1-z)g_1, \ldots, (1-z)g_m\rangle$, ezért

$$f(\mathbf{x}) = \sum_{i=1}^{s} z f_i(\mathbf{x}) h_i(z, \mathbf{x}) + \sum_{i=1}^{m} (1-z) g_i(\mathbf{x}) h_i'(z, \mathbf{x}).$$

Innen $z = 1$ helyettesítéssel adódik $f \in I$ és $z = 0$-val $f \in J$. □

Legyen $\mathbb{F}[\mathbf{x}]$ monomjain egy rögzített tagsorrend $\prec$. Definiáljunk egy $\prec'$ rendezést $\mathbb{F}[z, \mathbf{x}]$ monomjain a következő módon. Akkor és csak akkor teljesül $z^w \mathbf{x}^{\mathbf{w}} \prec' z^u \mathbf{x}^{\mathbf{u}}$, ha $w < u$, vagy $w = u$ és $\mathbf{x}^{\mathbf{w}} \prec \mathbf{x}^{\mathbf{u}}$. Könnyű látni, hogy $\prec'$ tagsorrend.

4.3. Állítás. *Legyen $I' \trianglelefteq \mathbb{F}[z, \mathbf{x}]$ ideál egy Gröbner-bázisa G' a $\prec'$ tagsorrendre. Ekkor $I = I' \cap \mathbb{F}[\mathbf{x}]$ ideálnak $G := G' \cap \mathbb{F}[\mathbf{x}]$ Gröbner-bázisa a $\prec$ rendezésre.*

Bizonyítás: Legyen $f \in I$. Ekkor $f \in I'$ is, ezért van olyan $g \in G'$, amelyre $\mathrm{lm}(g) \mid \mathrm{lm}(f)$. Megmutatjuk, hogy $g \in G$ is teljesül, ami bizonyítja, hogy G valóban Gröbner-bázis. Miután $f \in \mathbb{F}[\mathbf{x}]$, ezért speciálisan $\mathrm{lm}(f)$-ben nem szerepel a z változó. Így viszont ugyanez igaz osztójára, $\mathrm{lm}(g)$-re is. Ha z szerepelne g egy másik monomjában, akkor ez a monom $\prec'$ definíciója szerint

nagyobb lenne $\mathrm{lm}\,(g)$-nél, ami lehetetlen. Tehát z nem szerepel g semelyik monomjában, azaz $g \in G$. □

A két fenti állítás segítségével meghatározható I, J ideálok metszetének egy generátorrendszere, amely ráadásul a metszet Gröbner-bázisa is egyben. Valóban, ha G' az $\langle zI, (1-z)J\rangle$ ideál Gröbner-bázisa akkor $G' \cap \mathbb{F}[\mathbf{x}]$ a 4.3 állítás szerint Gröbner bázisa $\langle zI, (1-z)J\rangle \cap \mathbb{F}[\mathbf{x}]$ ideálnak, amely a 4.2 állítás alapján pontosan $I \cap J$.

4.2. Polinom-egyenletrendszerek megoldása

Az előző fejezetben ízelítőt kaptunk a Gröbner-bázisok alkalmazására különböző szimbolikus számítási feladatok elvégzésében. Bár ezek kétségtelenül igen hasznosak, mégis valószínűleg senki sem vitatkozik azzal a kijelentéssel, hogy a Gröbner-bázisok legfontosabb alkalmazási területe a többváltozós polinomiális egyenletek megoldása.

Az ilyen jellegű szimbolikus számításoknak jól ismert korlátja, hogy nem létezik képlet, amely megadná például tetszőleges ötödfokú polinom gyökeit. Ez nyilván a többváltozós esetnek is határokat szab, a szimbolikus számítások egy bizonyos pontján elő kell vegyünk numerikus megoldási módszereket.

Az alapprobléma tehát a következő. Adott $f_1, \ldots, f_s \in \mathbb{F}[\mathbf{x}]$ polinom. Létezik-e olyan $\mathbf{y} \in \mathbb{F}^n$, esetleg $\mathbf{y} \in \overline{\mathbb{F}}^n$ elem ($\overline{\mathbb{F}}$ az $\mathbb{F}$ algebrai lezártja), amely kielégíti az

$$\begin{aligned} f_1(\mathbf{x}) &= 0 \\ &\ldots \\ f_s(\mathbf{x}) &= 0 \end{aligned} \tag{4}$$

egyenletrendszert? Ha igen, szeretnénk tudni legalább egy, de inkább az összes megoldást. Esetleg megelégszünk a megoldások számának meghatározásával.

Ebben az alfejezetben I végig az $f_1, \ldots, f_s$ polinomok által generált ideált jelöli.

Kommutatív algebrai alapok

A 2.5 alfejezetben megismerkedtünk az $I(V)$ jelöléssel. Az $I(.)$ operátor $\mathbb{F}^n$ részhalmazaihoz ideálokat rendelt. Most definiáljuk a duális fogalmat, amely polinomiális egyenletrendszerek vizsgálatakor kulcsszerepet játszik.

4.4. Definíció. Jelölje $V(I)$ az I ideál elemeinek közös gyökeinek a halmazát, azaz

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

4.5. Lemma. *A $(I(.), V(.))$ pár Galois-kapcsolat, azaz teljesül $I \subseteq I(V(I))$, $V \subseteq V(I(V))$, $I \subseteq J \Rightarrow V(I) \supseteq V(J)$ és $V \subseteq U \Rightarrow I(V) \supseteq I(U)$. Ebből következik, hogy $I(V(I(V))) = I(V)$ és $V(I(V(I))) = V(I)$.*

Bizonyítás: Legyen $f \in I$. Ahhoz, hogy $f \in I(V(I))$ legyen, meg kell mutatni, hogy f eltűnik $V(I)$ tetszőleges $\mathbf{y}$ elemén. Csakhogy $V(I)$ definíciója miatt $\mathbf{y} \in V(I)$-ből következik $f(\mathbf{y}) = 0$. Teljesen analóg módon megy $V \subseteq V(I(V))$ bizonyítása is. A második állításpár triviális.

Végül egyrészt alkalmazzuk a $V \subseteq V(I(V))$ összefüggésre az $I(.)$ operátort, így $I(V) \supseteq I(V(I(V)))$. Másrészt az $I := I(V)$ ideálra írjuk fel az $I \subseteq I(V(I))$ egyenlőtlenséget, amiből kapjuk, hogy $I(V) \subseteq I(V(I(V)))$. A másik állítás ugyanígy igazolható. □

4.1. Feladat. Bizonyítsuk be, hogy ha V véges halmaz, akkor $V(I(V)) = V$.

Ahhoz, hogy polinomok közös gyökei közül ne csak az alaptestben levőket tudjuk vizsgálni, szükségünk lesz a következő definícióra.

4.6. Definíció. Legyen az $\mathbb{F}'$ test az $\mathbb{F}$ egy bővítése, és

$$V_{\mathbb{F}'}(I) := \{\mathbf{y} \in \mathbb{F}'^n \,:\, f(\mathbf{y}) = 0 \text{ minden } f \in I\text{-re}\}$$

az $\mathbb{F}'^n$-ben levő közös gyökök halmaza. Az $I(V)$ ideált szó szerint ugyanúgy értelmezzük $V \subseteq \mathbb{F}'^n$ esetén, tehát $I(V) \trianglelefteq \mathbb{F}[\mathbf{x}]$ továbbra is.

Speciálisan, ha $\overline{\mathbb{F}}$ az $\mathbb{F}$ algebrai lezártja, akkor $V_{\overline{\mathbb{F}}}(I)$ az algebrai lezárt feletti összes gyökök halmaza.

Könnyű látni, hogy $\sqrt{I} \subseteq I(V(I))$, ahol $\sqrt{I}$ az *I ideál radikál*ja, azaz $f \in \sqrt{I} \iff$ valamely e pozitív egészre $f^e \in I$. Valóban, ha $f \in \sqrt{I}$, azaz $f^e \in I$, akkor tetszőleges $\mathbf{y} \in V(I)$-n f eltűnik, hiszen f^e is eltűnik $V(I)$ definíciója szerint. Ez azt jelenti, hogy $f \in I(V(I))$. A megfordítás általában nem igaz, algebrailag zárt test felett azonban igen. Erről szól a kommutatív algebra egyik legfontosabb állítása, Hilbert nullhelytétele, amelyet itt nem bizonyítunk.

4.7. Tétel (Hilbert Nullstellensatz). $\sqrt{I} = I(V_{\overline{\mathbb{F}}}(I))$.

A megoldások száma, nulla dimenziós ideálok

4.2. Feladat. Bizonyítsuk be, hogy $V(I)$ egyenlő I tetszőleges generátorrendszerében szereplő polinomok közös gyökeinek a halmazával.

A (4) egyenletrendszer megoldásainak halmaza az előbbi feladat szerint éppen $V(I)$. Természetesen az is igaz, hogy az algebrai lezárt feletti megoldások éppen $V_{\overline{\mathbb{F}}}(I)$ elemei.

A fő kérdések tehát: $V_{\overline{\mathbb{F}}}(I) \stackrel{?}{=} \emptyset$, $V(I) \stackrel{?}{=} \emptyset$, illetve $|V_{\overline{\mathbb{F}}}(I)| =?$, $|V(I)| =?$, végül pedig, hogy pontosan mik $V_{\overline{\mathbb{F}}}(I)$ és $V(I)$ elemei. Nem túl meglepő módon az algebrai lezártban levő megoldásokkal kapcsolatos kérdésekre tudunk egyszerűbben választ adni.

Az első probléma eldöntése Gröbner-bázisok segítségével egészen könnyű.

4.8. Állítás. *Legyen az I ideál egy Gröbner-bázisa G. Pontosan akkor teljesül $V_{\overline{\mathbb{F}}}(I) = \emptyset$, ha G-ben szerepel egy nem nulla konstans polinom.*

Bizonyítás: Hilbert nullhelytételéből következik, hogy $V_{\overline{\mathbb{F}}}(I) = \emptyset$ akkor és csak akkor, ha $1 \in I$ (tehát $I = \mathbb{F}[\mathbf{x}]$). Ha ugyanis $V_{\overline{\mathbb{F}}}(I) = \emptyset$, akkor $I(V_{\overline{\mathbb{F}}}(I)) = I(\emptyset) = \mathbb{F}[\mathbf{x}]$, tehát a Nullstellensatz szerint $\sqrt{I} = \mathbb{F}[\mathbf{x}]$, ezért $1 \in \sqrt{I}$, tehát $1 \in I$ is igaz. A megfordítás nyilvánvaló: az 1 polinomnak nincs gyöke.

Ha G-ben van nemnulla konstans polinom, akkor ez I-ben is benne van, tehát $1 \in I$. Fordítva: ha $1 \in I$, akkor G-ben kell legyen g polinom, amely főtagja osztja az 1 monomot, tehát amely főtagja 1. Miután 1 a legkisebb monom, ezért g ebből az egyetlen monomból áll, tehát konstans. □

Ez persze speciális esete az algebrai lezárt feletti megoldások számára vonatkozó kérdésnek. A következő tétel két módon jellemzi azon polinomegyenletrendszereket, amelyeknek véges sok megoldása van az algebrai lezárt felett. Vegyük észre, hogy tetszőleges Gröbner-bázis kiszámításával el lehet tehát dönteni, hogy $V_{\overline{\mathbb{F}}}$ véges-e.

4.9. Tétel. *Legyen I egy Gröbner-bázisa G. Ekkor az alábbiak ekvivalensek.*

1. *Minden $i \in [n]$-hez létezik $g_i \in G$ és $w_i \in \mathbb{N}$, hogy* $\operatorname{lm}(g_i) = x_i^{w_i}$.
2. $|\operatorname{Sm}(I)| < \infty$
3. $|V_{\overline{\mathbb{F}}}(I)| < \infty$

Az ilyen ideálokat 0 dimenziós *ideáloknak nevezzük.*

Bizonyítás: $1 \Rightarrow 2$: Egy $\mathbf{x}^{\mathbf{u}}$ monom legfeljebb akkor lehet $\operatorname{Sm}(I)$-ben, ha minden i-re $u_i < w_i$ (hiszen $x_i^{w_i} \in \operatorname{Lm}(I)$), ilyenből viszont csak véges sok $(w_1 \cdot w_2 \dots w_n)$ van.

$2 \Rightarrow 3$: Az $1, x_i, x_i^2, \dots$ monomok modulo I lineárisan összefüggőek, hiszen $\dim(\mathbb{F}[\mathbf{x}]/I) = |\operatorname{Sm}(I)|$ véges. Ezek szerint van olyan $f_i(x_i) \in \mathbb{F}[x_i]$, amely

I-ben van. Ennek csak véges sok gyöke van, azaz $V_{\overline{\mathbb{F}}}(I)$ elemeinek i-edik koordinátája csak véges sok féle lehet.

$3 \Rightarrow 1$: Miután $V_{\overline{\mathbb{F}}}(I)$ véges, az i-edik koordinátában csak véges sok elem fordulhat elő, legyenek ezek $\alpha_{i,1}, \ldots, \alpha_{i,s_i} \in \overline{\mathbb{F}}$. Ha $f_{i,j}(x_i)$ az $\alpha_{i,j}$ minimálpolinomja $\mathbb{F}$ felett, akkor legyen $f_i(x_i) = \prod_{j=1}^{s_i} f_{i,j}(x_i)$. Világos, hogy $f_i(x_i) \in \mathbb{F}[\mathbf{x}]$ eltűnik $V_{\overline{\mathbb{F}}}(I)$ minden elemén, azaz $f_i(x_i) \in I(V_{\overline{\mathbb{F}}}(I)) = \sqrt{I}$ a Hilbert Nullstellensatz szerint. Tehát valamilyen e_i-re $f_i^{e_i}(x_i) \in I$. Ha $g_i \in G$ egy polinom, amelyre $\mathrm{lm}(g_i) \mid \mathrm{lm}(f_i^{e_i})$, akkor miután $f_i^{e_i}$ főtagja x_i hatványa (pontosan $\mathrm{lm}(f_i^{e_i}) = x_i^{e_i \cdot \deg f_i}$), ezért $\mathrm{lm}(g_i)$ is x_i-hatvány. □

Ebben a jegyzetben nem foglalkozunk ideálok dimenziójával, kizárólag a nulla dimenziós esetet különböztetjük meg, ezért magasabb dimenziókra pontos definíciót sem adunk. Szemléletesen azonban egyszerű magyarázni az elnevezést. Legyen például $I = \langle x_1^2 - x_2 - x_3 \rangle$ és $n = 3$. Ekkor I két dimenziós, miután $V(I)$ a három dimenziós tér egy felületének pontjaiból áll. A tér véges sok pontja természetesen 0 dimenziós halmaz, tehát ilyenkor jogos 0 dimenziós ideálnak nevezni I-t.

4.10. Példa. Legyen $\mathbb{F} = \mathbb{R}$, $n = 2$ és $I = \langle x_1^2 + x_2^2 \rangle$. Ekkor $V(I) = \{(0,0)\}$, de $V_{\mathbb{C}}(I)$ végtelen sok pontot tartalmaz, egész pontosan $V_{\mathbb{C}}(I)$ az $x_1 + x_2\sqrt{-1} = 0$ és $x_1 - x_2\sqrt{-1} = 0$ komplex egyenesek uniója. Tehát I nem 0 dimenziós (hanem 1).

Utóbbi egyben arra is példa, hogy előfordulhat, hogy az algebrai lezárt felett végtelen sok megoldás van, míg az alaptestben véges sok.

A következő cél, hogy pontosabbat mondjunk a megoldások számáról a 0 dimenziós esetben, tehát amikor véges sok megoldás van.

Ha $\mathbb{F}'$ test az $\mathbb{F}$ bővítése, akkor jelölje $I_{\mathbb{F}'}$ az I által $\mathbb{F}'[\mathbf{x}]$-ben generált ideált, azaz $I_{\mathbb{F}'} = I \cdot \mathbb{F}'[\mathbf{x}]$.

4.11. Lemma. $V_{\mathbb{F}'}(I_{\mathbb{F}'}) = V_{\mathbb{F}'}(I)$

Bizonyítás: Nyilvánvaló, hogy $\mathbf{y}$ pontosan akkor közös gyöke egy ideál összes polinomjának, ha az ideál egy generátorrendszerének gyöke. Válasszunk I-ben egy $f_1, \ldots, f_s$ generátorrendszert. Ezek a polinomok $\mathbb{F}'[\mathbf{x}]$-ben természetesen $I_{\mathbb{F}'}$ ideált generálják. Tehát az állításban szereplő két ideálnak ugyanaz a polinomhalmaz generátorrendszere, így az ideálok $\mathbb{F}'^n$-beli gyökei is megegyeznek. □

4.12. Lemma. $\mathrm{Sm}(I_{\mathbb{F}'}) = \mathrm{Sm}(I)$, *sőt* $G \subseteq \mathbb{F}[\mathbf{x}]$ *pontosan akkor Gröbner-bázisa* I*-nek, ha Gröbner-bázisa az* $I_{\mathbb{F}'}$ *ideálnak.*

Bizonyítás: Miután tetszőleges Gröbner-bázis meghatározza a standard monomokat, ezért elegendő a második állítást igazolni.

Ehhez a Buchberger-algoritmus kapcsán tanult, a Gröbner-bázist S-polinomok segítségével jellemző 3.3 tételt használjuk. Jelölje $\langle G\rangle_{\mathbb{F}}$, illetve $\langle G\rangle_{\mathbb{F}'}$ a G által $\mathbb{F}[\mathbf{x}]$, illetve $\mathbb{F}'[\mathbf{x}]$ gyűrűben generált ideált. Az idézett tétel szerint G pontosan akkor Gröbner bázis $\langle G\rangle_{\mathbb{F}}$ ideálban, ha G bármely két elemének S-polinomja 0-ra redukálható G-vel. Ez a feltétel viszont független a testtől, ezért újra alkalmazva a tételt, utóbbi azzal ekvivalens, hogy G Gröbner bázisa $\langle G\rangle_{\mathbb{F}'}$-nek.

Annyit kell még látni, hogy G pontosan akkor generálja az egyik gyűrűben I-t, ha a másikban $I_{\mathbb{F}'}$-t. Ha G az $I_{\mathbb{F}'}$ ideál generátorrendszere, akkor $I_{\mathbb{F}'} \cap \mathbb{F}[\mathbf{x}] = I$ miatt (és mert $G \subseteq \mathbb{F}[\mathbf{x}]$) teljesül $\langle G\rangle_{\mathbb{F}} = I$. Fordítva: miután $I_{\mathbb{F}'}$ az I által $\mathbb{F}[\mathbf{x}]$-ben generált ideál, ezért I bármely generátorrendszere $\mathbb{F}'[\mathbf{x}]$-ben $I_{\mathbb{F}'}$ ideált generálja. Az állítást ezzel beláttuk. □

Készen állunk a megoldások számáról szóló második tételünk bizonyítására.

4.13. Tétel. *Ha valamelyik oldal véges, akkor*

$$|V_{\overline{\mathbb{F}}}(I)| = \left|\mathrm{Sm}\left(\sqrt{I}\right)\right|.$$

Bizonyítás: Tegyük fel először, hogy $\mathbb{F} = \overline{\mathbb{F}}$, azaz az alaptestünk algebrailag zárt. Ekkor a 2.24 következmény és a Hilbert Nullstellensatz miatt

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

amint állítottuk.

Az általános esetben az előbbi összefüggést $I_{\overline{\mathbb{F}}}$ ideálra alkalmazva azt kapjuk, hogy

$$|V_{\overline{\mathbb{F}}}(I_{\overline{\mathbb{F}}})| = \left|\mathrm{Sm}\left(\sqrt{I_{\overline{\mathbb{F}}}}\right)\right|$$

A 4.11 lemma miatt a bal oldal egyenlő $|V_{\overline{\mathbb{F}}}(I)|$-vel. A jobb oldal pedig egyrészt $\sqrt{I_{\overline{\mathbb{F}}}} = \sqrt{I \cdot \overline{\mathbb{F}}[\mathbf{x}]} = \sqrt{I} \cdot \overline{\mathbb{F}}[\mathbf{x}] = \left(\sqrt{I}\right)_{\overline{\mathbb{F}}}$, másrészt a 4.12 lemma miatt éppen $\mathrm{Sm}\left(\sqrt{I}\right)$ elemszámával egyezik meg. □

4.3. Feladat. Lássuk be az állítást direkt módon, ha $n = 1$.
(Segítség: Ilyenkor I főideál, mondjuk $I = \langle f\rangle$. Az f polinom irreducibilis felbontása segítségével $\sqrt{I}$ generátorát könnyű megadni.)

Jogos ezek után a kérdés, hogy nyertünk-e valamit, azaz I ismeretében meg tudjuk-e határozni I radikáljának standard monomjait. A válasz igen,

ráadásul a módszer Gröbner-technikákkal működik, de ezen jegyzetben nem tárgyaljuk. A nulla karakterisztikájú alaptest esete egyébként nem különösebben nehéz, pozitív karakterisztika esetén a megoldás viszont egyáltalán nem magától értetődő, az ismert algoritmusok mindössze néhány évesek. Egy jó kiindulópont ezek felkutatására [20], és az ott hivatkozott cikkek. Mindenesetre $\sqrt{I} \supseteq I$ miatt $\mathrm{Sm}\left(\sqrt{I}\right) \subseteq \mathrm{Sm}\,(I)$, tehát felső becslést egyszerűen tudunk mondani a megoldások számára pusztán I egy Gröbner-bázisának kiszámításával.

Mielőtt továbblépnénk, érdemes megjegyezni, hogy $\mathbb{F}$ tetszőleges $\mathbb{F}'$ bővítése esetén $V_{\mathbb{F}'}(I) = V_{\mathbb{F}'}(\sqrt{I})$, hiszen egy polinomnak és hatványainak ugyanazok a gyökei.

Polinom-egyenletrendszerek normálformája

Az alfejezet tételeiben eddig nem tettünk fel semmit a Gröbner-bázishoz tartozó tagsorrendről. A továbbiakban viszont a lexikografikus rendezést fogjuk használni.

4.14. Definíció. A (4) *egyenletrendszer normálformája* a

$$\begin{aligned} g_1(\mathbf{x}) &= 0 \\ &\dots \\ g_m(\mathbf{x}) &= 0 \end{aligned}$$

egyenletrendszer, ahol $G = \{g_1, \dots, g_m\}$ az $f_1, \dots, f_s$ polinomok által generált I ideál redukált Gröbner-bázisa a lexikografikus tagsorrendre nézve.

4.15. Állítás. *Ha I nulla dimenziós (tehát az algebrai lezárt felett is csak véges sok közös gyöke van I elemeinek) és G egy lexikografikus Gröbner-bázisa, akkor minden $i \in [n]$ számra van olyan $g_i \in G$ polinom, amely csak x_i, x_{i+1}, $\dots x_n$ változóktól függ, és g_i vezető tagja x_i-hatvány.*

Bizonyítás: A 4.9 tétel szerint minden 0 dimenziós ideál és bármely $i \in [n]$ számra tetszőleges Gröbner-bázis tartalmaz olyan g_i polinomot, amelyre $\mathrm{lm}\,(g_i)$ épp x_i-hatvány. A lexikografikus rendezés tulajdonságai miatt g_i semelyik monomjában nem szerepelhet olyan x_j, amelyre $j < i$, hiszen ez a monom nagyobb volna x_i bármely hatványánál. □

Ez az egyszerű megfigyelés lehetőséget ad nulla dimenziós ideálok elemei közös gyökeinek meghatározására. Jelölje tehát az I ideál lexikografikus Gröbner-bázisának a tételben szereplő n elemét $g_n(x_n)$, …, $g_i(x_i, \dots, x_n)$, …, $g_1(x_1, \dots, x_n)$. Ekkor a közös gyökök utolsó koordinátája biztosan $g_n(x_n)$

egyváltozós polinom gyökei közül kerül ki. Ha y_n a g_n egy gyöke, akkor ezt g_{n-1}-be helyettesítve egy egyváltozós $\hat{g}(x_{n-1}) = g_{n-1}(x_{n-1}, y_n)$ polinomot kapunk, amelynek egy gyöke legyen y_{n-1}. Az eljárást y_{n-1} és y_n elemek g_{n-2}-be helyettesítésével folytathatjuk. A $g_1, \dots, g_n$ polinomok ilyen vizsgálata után meg kell nézni még, hogy a kapott gyökök kielégítik-e a további $g_{n+1}, \dots g_m$ polinomokat is.

4.16. Példa. Tekintsük az

$$\begin{aligned} x_1x_2 + x_3 - 11 &= 0 \\ x_1x_3 + x_2 - 13 &= 0 \\ x_2x_3 + x_1 - 17 &= 0. \end{aligned}$$

egyenletrendszert $\mathbb{Q}$ felett. A megfelelő I ideál egy lex Gröbner-bázisa

$$\begin{aligned} g_3(x_3) &= x_3^5 - 11x_3^4 - 2x_3^3 + 243x_3^2 - 457x_3 + 210 \\ g_2(x_2, x_3) &= \frac{1}{120}\left(120x_2 - 13x_3^4 + 126x_3^3 + 200x_3^2 - 2999x_3 + 2010\right) \\ g_1(x_1, x_2, x_3) &= x_1 + x_2x_3 - 17. \end{aligned}$$

A g_3 polinom racionális gyökeit 210 egész osztói között kell keresnünk. Ellenőrizhető, hogy az egyetlen racionális gyök az 5. Ekkor $g_2(x_2, 5) = x_2 - 3$, tehát x_2 csakis 3 lehet. Végül $g_2(x_1, 3, 5) = x_1 - 2$, azaz $V(I) = \{(2, 3, 5)\}$. Ha kíváncsiak vagyunk $V_{\overline{\mathbb{Q}}}(I)$-re is, kénytelenek vagyunk megoldani a $\frac{g(x_3)}{x_3-5} = x_3^4 - 6x_3^3 - 32x_3^2 + 83x_3 - 42 = 0$ egyenletet, akár a megoldóképlettel, akár valamilyen numerikus módszerrel (a négy gyök mindegyike valós). Annyit mindenesetre bonyolultabb számolások nélkül is látunk, hogy g_3-nak öt különböző gyöke van, amelyek mindegyikéhez pontosan egy $V_{\overline{\mathbb{Q}}}(I)$-beli pont tartozik (hiszen g_2 az x_2-ben, g_3 az x_3-ban lineáris) azaz $\left|V_{\overline{\mathbb{Q}}}(I)\right| = 5$. Vegyük észre, hogy $|\mathrm{Sm}\,(I)| = 5$ szintén teljesül.

4.4. Feladat. Mutassuk meg, hogy amennyiben $f_1, \dots, f_s$ lineáris polinomok, úgy az egyenletrendszer normálalakja az egyenletrendszerhez tartozó mátrix felső háromszög alakjának felel meg (minden sor első nullától különböző eleme 1, és ennek oszlopindexe nagyobb, mint a felette levő sorban található első nemnulla elem oszlopindexe). A fenti gyökkereső eljárás tehát a Gauss-elimináció általánosítása.

A módszer többé-kevésbé használható nem nulla dimenziós ideál esetén is: ha x_n egy hatványa főtag, akkor ugyanúgy találunk egy megfelelő tulajdonságokkal rendelkező $g_n(x_n)$ polinomot, mint a 4.15 állítás bizonyításában. Ha x_n semelyik hatványa sem főtag, akkor viszont véges sok kivételtől eltekintve

$\overline{\mathbb{F}}$ minden eleme előfordul, mint egy $\overline{\mathbb{F}}^n$-beli megoldás i-edik koordinátája, tehát a behelyettesítgetést ilyenkor szinte bármerre folytathatjuk. A részletek kidolgozását az Olvasóra bízzuk.

A tisztesség kedvéért meg kell említeni, hogy a fenti eljárás a numerikus számítások tekintetében korántsem olyan jó, mint gondolnánk. Egyrészt a lexikografikus Gröbner-bázis együtthatói nem mindig „szépek", elég csak megnézni a 4.16 példát: az aránylag kis egész számokból nagyobb egészek, néhol pedig törtek lettek a normálformára hozás során. Másrészről, ha például valós együtthatós polinomokkal kell számolnunk, akkor a Gröbner-számításhoz feltehetően kerekíteni kell ezeket, ami a Gröbner-bázisban már komoly eltéréseket okozhat. (Nagyon nem mindegy, hogy egy polinom egyik monomjának 10^{-100} az együtthatója, vagy 0, ezen múlhat például, hogy mi a főtag.) A módszer tehát ebben a formájában numerikusan instabil. Végül – ha a normálformát pontosan ki is tudtuk számolni –, az egyváltozós polinomok közelítéssel meghatározott gyökeit más polinomokba helyettesítve a közelítés hibája esetleg túlságosan megnőhet. Ezen kérdések egyik legnagyobb szakértője Hans J. Stetter, akinek a honlapján[2] találhat útbaigazítást a numerikus számítások iránt érdeklődő Olvasó.

Egy polinom-egyenletrendszer megoldásának más értelmezését is szokás vizsgálni. A közös gyökök halmazán túl azt is célként tűzhetjük ki, hogy a gyökök multiplicitását határozzuk meg. Például az $x_1x_2 - x_1 - x_2 + 1 = 0$ egyenletnek az $(1, 1)$ gyöke és az $(y, 1)$, illetve $(1, y)$ gyökei (ahol $y \neq 1$) között lényeges különbség van. A legáltalánosabb megoldásfogalom az egyenletrendszernek megfelelő ideál primér felbontásának meghatározása. A témának nagy irodalma van (lásd például [17], vagy az újabb [10] és [21]), a módszerek legtöbbször Gröbner-számításokat használnak.

4.3. Kombinatorikai alkalmazások

Bemelegítésként mutatunk egy példát, hogyan lehet kombinatorikai problémákat polinomokra vonatkozó kérdéssé átfogalmazni, és ezután Gröbner-bázisok segítségével megoldani.

Gráfok 3-színezhetősége Legyen adott n ponton egy $\mathcal{G}$ gráf. A kérdés, hogy kiszínezhetőek-e a pontjai három színnel, úgy, hogy szomszédos csúcsok különböző színűek.

[2] `http://www.math.tuwien.ac.at/~stetter/`

Legyen $\mathbb{F} = \mathbb{C}$ és ebben ε egy primitív harmadik egységgyök. A három „szín" 1, ε és ε^2 lesz. A $\mathcal{G}$ gráf i-edik csúcsához rendeljünk egy x_i változót, x_i értéke mutatja majd az i csúcs színét.

Fogalmazzuk meg a színezés szabályait polinomok eltűnési feltételeként!

- Csak 1, ε és ε^2 lehet szín: $x_i^3 - 1 = 0$.
- Szomszédos i és j csúcsok különböző színűek kell legyenek: $x_i^2 + x_i x_j + x_j^2 = 0$. Ez az egyenlet – az előző feltétellel együtt – a kért tulajdonságot garantálja. Valóban: $x_i^3 = 1 = x_j^3$, ezért $0 = x_i^3 - x_j^3 = (x_i - x_j)(x_i^2 + x_i x_j + x_j^2)$, tehát x_i és x_j pontosan akkor különböző, ha a szorzat második tényezője tűnik el.

Legyen I az ezen polinomok által generált ideál. Az eddigiekből világos, hogy $\mathcal{G}$ pontosan akkor színezhető 3 színnel, ha az I-beli polinomoknak van közös gyöke, azaz $V(I) \neq \emptyset$. A polinomiális egyenletek megoldhatóságáról szóló 4.8 állítás szerint $V(I) \neq \emptyset \iff G$-ben nincs konstans polinom, ahol G az ideál tetszőleges Gröbner-bázisa.

Ez az alkalmazás szépen mutatja a polinom-módszernek nevezett eljárás erejét kombinatorikában. Ugyanakkor a Gröbner-bázis számítás szempontjából negatív eredmény, hiszen egy NP-teljes problémát oldottunk meg Gröbner-bázis számolás segítségével.

A Hilbert-függvény

Bevezetünk egy igen fontos fogalmat, amely gyakran használható kombinatorikai tulajdonságok algebrai átfogalmazására.

4.17. Definíció. Ha m nemnegatív egész, jelölje $\mathbb{F}[\mathbf{x}]_{\leq m}$ az $\mathbb{F}$ feletti legfeljebb m-edfokú polinomok vektorterét. Hasonlóan, egy $I \trianglelefteq \mathbb{F}[\mathbf{x}]$ ideál esetén $I_{\leq m} = I \cap \mathbb{F}[\mathbf{x}]_{\leq m}$ az előbbi vektortér azon altere, amely az I-beli legfeljebb m-edfokú polinomokból áll.

Az $\mathbb{F}[\mathbf{x}]/I$ algebra *Hilbert-függvénye*

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

Most megadjuk a 2.17 tétel egy általánosítását fok-kompatibilis rendezésekre.

4.18. Állítás. *Legyen $\prec$ tetszőleges fok-kompatibilis rendezés (például deglex, vagy degrevlex). Ekkor a legfeljebb m-edfokú standard monomok $I_{\leq m}$ szerinti mellékosztályai lineáris bázisát alkotják az $\mathbb{F}[\mathbf{x}]_{\leq m} / I_{\leq m}$ vektortérnek*

Bizonyítás: Miután a standard monomok modulo I lineárisan függetlenek és $I_{\leq m} \subseteq I$, ezért modulo $I_{\leq m}$ is azok. Azt kell még megmutatnunk, hogy generálják is a legfeljebb m fokú polinomokat modulo $I_{\leq m}$.

Legyen $f \in \mathbb{F}[\mathbf{x}]$ legfeljebb m fokú és legyen $\hat{f}$ az f egy $\prec$-hez tartozó Gröbner-bázis szerinti redukáltja. Vegyük észre, hogy a redukálás során csak legfeljebb m fokú polinomokat használhatunk, hiszen a fok-kompatibilitás miatt a nagyobb fokú polinomok főtagjai nagyobbak volnának, mint $\operatorname{lm}(f)$. Így $\hat{f}$ és $f - \hat{f}$ szintén legfeljebb m fokú, utóbbiból adódik $f - \hat{f} \in I_{\leq m}$. Elegendő ezért $\hat{f}$ polinomot előállítani legfeljebb m fokú standard monomok lineáris kombinációjaként. De miután $\hat{f}$ monomjai redukáltak egy Gröbner-bázisra nézve, ezért $\hat{f}$ standard monomok lineáris kombinációja, a fokszámkorlát miatt pedig ezek legfeljebb m fokúak. □

4.19. Következmény. *Ha $\prec$ egy fok-kompatibilis rendezés, I egy ideál, akkor $H(m)$ éppen a legfeljebb m-edfokú, $\prec$-re nézve standard monomok száma.*

Ha I nulla dimenziós, akkor van olyan m_0, hogy $m \geq m_0$-ra $H(m) = |\operatorname{Sm}(I)|$, tehát nem függ m-től.

Bizonyítás: Az első állítás világos a 4.18 állításból. A másodikhoz emlékezzünk vissza, hogy I nulla dimenziós voltának egy ekvivalens megfogalmazása az volt, hogy $\operatorname{Sm}(I)$ véges, így m_0 választható a legmagasabb fokú standard monom fokának. □

Láttuk, hogy egy konkrét ideál Hilbert-függvények kiszámításához nem kell mást tennünk, mint meghatározni valamely fok-kompatibilis rendezésre vonatkozó Gröbner-bázist. Most megnézzük, hogy ennek mi köze van a kombinatorikához.

4.20. Definíció. Legyen $\mathcal{F} \subseteq 2^{[n]}$ egy *halmazrendszer* (avagy *halmazcsalád*), azaz az $[n]$ halmaz bizonyos részhalmazaiból álló halmaz. Az $\mathcal{F}$ *család ideálja* $I(V_{\mathcal{F}})$, ahol $V_{\mathcal{F}} = \{\mathbf{v}_F : F \in \mathcal{F}\}$ és $\mathbf{v}_F$ pedig F karakterisztikus vektora, tehát az i-edik koordinátája 1, ha $i \in F$ és 0 különben. Miután e jegyzetben nincs szükségünk algebrák Hilbert-függvényére teljes általánosságban, ezért nem okoz keveredést, hogy $\mathbb{F}[\mathbf{x}]/I(V_{\mathcal{F}})$ Hilbert-függvényét ezentúl röviden $\mathcal{F}$ Hilbert-függvényének fogjuk nevezni.

Megjegyezzük, hogy a definíció elég általános, például gráfok is kezelhetőek vele. Egy s pontú gráfot kódolhatunk egy $\binom{s}{2}$ dimenziós 0-1 vektorral: minden pontpárhoz egy koordinátát rendelünk, amelynek értéke 0 vagy 1, attól függően, hogy az adott gráfban van-e él a két pont között. A $V_{\mathcal{F}}$ halmazrendszer ilyen alkalmazásokban valamilyen közös tulajdonsággal (k-színezhető, k-összefüggő) rendelkező összes s pontú gráfok vektorainak halmaza.

4.21. Definíció. Ha $G \subseteq [n]$, akkor legyen $x_G = \prod_{i \in G} x_i$. Világos, hogy tetszőleges négyzetmentes monom valamely $G \subseteq [n]$ halmazra x_G alakú, továbbá hogy $\deg x_G = |G|$.

4.22. Definíció. Két $\mathcal{F}, \mathcal{G} \subseteq 2^{[n]}$ halmazrendszer $I(\mathcal{F}, \mathcal{G})$ *tartalmazási mátrix*a egy $|\mathcal{F}| \times |\mathcal{G}|$ mértetű mátrix, amely sorai $\mathcal{F}$, oszlopai $\mathcal{G}$ elemeivel vannak indexelve. Az (F, G)-hez tartozó érték a mátrixban 1, ha $G \subseteq F$, 0 különben.

4.23. Tétel. *Jelölje az $[n]$ összes legfeljebb m elemű részhalmazából álló halmazcsaládot $\binom{[n]}{\leq m}$. Ekkor $\mathcal{F}$ halmazrendszer Hilbert-függvénye*

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

Bizonyítás: Miután minden $i \in [n]$ esetén $x_i^2 - x_i \in I_{\mathcal{F}}$, ezért $I_{\mathcal{F}}$ standard monomjai négyzetmentesek.

Tekintsük az összes legfeljebb m fokú négyzetmentes monomot. A 4.18 állítás miatt ezek közül a modulo $I(V_{\mathcal{F}})$ lineárisan függetlenek maximális száma épp egyenlő a legfeljebb m-edfokú standard monomok számával, ami a 4.19 következmény szerint éppen $H(m)$. Tehát

$$\begin{aligned} H(m) = \operatorname{rang}_{\mathbb{F}} \left\{ \mathbf{x}^{\mathbf{w}} + I(V_{\mathcal{F}}) \,:\, \deg \mathbf{x}^{\mathbf{w}} \leq m \text{ és } \mathbf{x}^{\mathbf{w}} \text{ négyzetmentes} \right\} \\ = \operatorname{rang}_{\mathbb{F}} \left\{ x_G + I(V_{\mathcal{F}}) \,:\, |G| \leq m \right\}, \quad (5) \end{aligned}$$

ahol a halmaz rangján a lineárisan függetlenek maximális számát értjük.

Láttuk, hogy $\mathbb{F}[\mathbf{x}]/I(V_{\mathcal{F}})$ izomorf a $V_{\mathcal{F}}$-en értelmezett függvények vektorterével. Másképpen, izomorf az $\mathbb{F}^{|\mathcal{F}|}$ oszlopvektorok terével, ahol $f(\mathbf{x})$ függvénynek az az $\mathbf{f}$ vektor felel meg, amely $F \in \mathcal{F}$-fel indexelt koordinátája $f(\mathbf{v}_F)$. Ezen izomorfizmus mentén átírva (5) egyenlőséget, kapjuk, hogy

$$H(m) = \operatorname{rang}_{\mathbb{F}} \left\{ (x_G(\mathbf{v}_F))_{F \in \mathcal{F}} \,:\, G \in \binom{[n]}{\leq m} \right\}.$$

Végül vegyük észre, hogy $x_G(\mathbf{v}_F)$ pontosan akkor 1, ha $G \subseteq F$ és 0 különben. Ezek szerint $(x_G(\mathbf{v}_F))_{F \in \mathcal{F}}$ éppen a tartalmazási mátrix $G \in \binom{[n]}{\leq m}$-hez tartozó oszlopa. □

Egy extremális halmazelméleti eredmény

A kombinatorikai alkalmazások lezárásaként bemutajuk Hegedűs Gábor, Rónyai Lajos és e sorok írójának egy 2006-os eredményét. A bizonyítás egy részét kihagyjuk, a részletek megtalálhatóak [15] cikkben.

4.24. Definíció. Legyen $L \subseteq \{0, \ldots, q-1\}$ halmaz és $\mathcal{F}$ egy halmazrendszer. Azt mondjuk, hogy $\mathcal{F}$ *modulo q L-kerülő*, ha $F \in \mathcal{F}$ és $f \in L$-ből következik, hogy $|F| \not\equiv f \pmod{q}$.

Ha pedig az teljesül, hogy bármely két különböző $F_1, F_2 \in \mathcal{F}$ esetén $|F_1 \cap F_2| \equiv f \pmod{q}$ fennáll valamely $f \in L$-re, akkor $\mathcal{F}$-et *modulo q L-metsző*nek nevezzük.

4.25. Definíció. Egy $L \subseteq \{0, \ldots, q-1\}$ halmaz *modulo q intervallum*, ha L vagy egész számok intervalluma, vagy olyan $L_1, L_2 \subseteq \{0, \ldots, q-1\}$ intervallumok uniója, amelyekre teljesül, hogy $0 \in L_1$ és $q-1 \in L_2$.

4.26. Tétel (Hegedűs, Rónyai, Felszeghy; 2006). *Legyen q egy prímhatvány, L modulo q intervallum és $\mathcal{F} \subseteq 2^{[n]}$ egy modulo q L-kerülő, L-metsző halmazcsalád. Ha $|L| \leq n - q + 2$, akkor*

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

A tétel bizonyításához előbb be kell vezetni egy újabb halmazrendszert.

4.27. Definíció. Legyenek q, d és ℓ egész számok, amelyekre teljesül $1 \leq \ell < q$. Ekkor a *modulo q teljes ℓ-széles család*:

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

Más szóval $\mathcal{G}$ az $[n]$ minden olyan részhalmazát tartalmazza, amely elemszáma modulo q beleesik a $[d, d+\ell-1]$ (ℓ hosszú) intervallumba. Az ℓ és q paraméterekre vonatkozó fenti feltételek éppen annyit mondanak, hogy ha $|G| \equiv d + \ell \pmod{q}$, akkor $G \notin \mathcal{G}$ (azaz $\mathcal{G}$ valóban ℓ-széles).

A következő tétel a 4.26 tétel bizonyításának az alapja. Csak vázoljuk, hogy hogyan juthatunk el ehhez az eredményhez, a részletes igazolás hosszadalmas volna.

4.28. Tétel. *Legyen p prímszám, $\mathbb{F}_p$ a p elemű test, q pedig p-hatvány. Jelölje $H(m)$ a modulo q teljes ℓ-széles $\mathcal{G}$ család Hilbert-függvényét. Ha $0 \leq m \leq \frac{n+\ell}{2}$, akkor*

$$H(m) \leq \sum_{i=0}^{\infty} \sum_{k=0}^{\ell-1} \binom{n}{m - iq - k}.$$

A bizonyítás vázlata a következő.

A „lex játék módszerrel” (lásd [16]) meg lehet határozni az $I(V_{\mathcal{G}})$ ideál lexikografikus standard monomjait. Ezek után maga a lexikografikus Gröbner-bázis is megkonstruálható: minden minimális főtaggal mutatunk egy-egy polinomot az ideálban. Kiderül, hogy ezen polinomok főtagjai a lex és a deglex rendezésre nézve is ugyanazok. Ebből viszont következik, hogy ők egyben egy deglex Gröbner-bázist is alkotnak, és a lex és deglex standard monomok ugyanazok. Ez azért jó hír, mert a legfeljebb m fokú deglex standard monomok összeszámolásával megkapjuk $H(m)$ pontos értékét. A 4.28 tételben szereplő felső korlát a pontos formula triviális becslésével adódik.

A 4.26 tétel bizonyításához fel fogjuk használni az alábbi lemmát.

4.29. Lemma. *Ha f egész és q a p prím egy hatványa, akkor*

$$\binom{f-1}{q-1} \equiv \begin{cases} 0 \pmod{p}, \text{ ha } f \not\equiv 0 \pmod{q} \\ 1 \pmod{p}, \text{ ha } f \equiv 0 \pmod{q}. \end{cases}$$

Bizonyítás: Egy erősebb állítást fogunk belátni, azt hogy amennyiben $f \equiv f' \pmod{q}$ és $0 \le s < q$ tetszőleges egész, akkor $\binom{f}{s} \equiv \binom{f'}{s} \pmod{p}$.

Utóbbihoz elég megmutatni, hogy $\binom{q+f}{s} \equiv \binom{f}{s} \pmod{p}$. Ez pedig fennáll, miután

$$\binom{q+f}{s} = \sum_{j=0}^{s} \binom{q}{j} \cdot \binom{f}{s-j} \equiv \binom{f}{s} \pmod{p},$$

ahol kihasználtuk, hogy $\binom{q}{j} \equiv 0 \pmod{p}$, ha $0 < j < q$.

Az eredeti állítás igazolásához tehát feltehetjük, hogy $0 \le f \le q-1$, így nyilvánvaló az egyenlőség. □

A 4.26 tétel bizonyítása: Legyen $\ell = q - |L|$. Ha L egészekből álló intervallum, akkor legyen $d = \max L + 1$, máskülönben – amikor L az L_1, L_2 intervallumok uniója, de maga nem intervallum – akkor legyen $d = \max L_1 + 1$, feltéve, hogy $0 \in L_1$. Jelölje $\mathcal{G}$ az ezen d paraméterrel definiált modulo q teljes ℓ-széles halmazrendszert. A definíciókból jól látszik, hogy $\mathcal{F} \subseteq \mathcal{G}$.

Minden $F \in \mathcal{F}$ halmazra definiáljuk az $\hat{f}_F(\mathbf{x}) \in \mathbb{Q}[\mathbf{x}]$ polinomot a következő módon:

$$\hat{f}_F(\mathbf{x}) = \left(\sum_{\substack{k=0 \\ k \notin L}}^{q-1} \binom{\mathbf{x} \cdot \mathbf{v}_F - k - 1}{q-1} \right) \text{ redukáltja } x_j^2 - x_j \text{ polinomokkal},$$

ahol $\mathbf{x} \cdot \mathbf{v} = \sum_{j=1}^{n} x_j v_j$ a vektorok szokásos skaláris szorzata.

Azt állítjuk, hogy $\hat{f}_F \in \mathbb{Z}[\mathbf{x}]$. Miután redukáltunk az $x_j^2 - x_j$ polinomokkal, így $\hat{f}_F(\mathbf{x})$ négyzetmentes, ezért írható $\hat{f}_F = \sum_{G \subseteq [n]} \alpha_G x_G$ valamilyen $\alpha_G \in \mathbb{Q}$ együtthatókkal. Ha $\hat{f}_F \notin \mathbb{Z}[\mathbf{x}]$, akkor legyen G a tartalmazásra nézve minimális olyan halmaz, amelyre $\alpha_G \notin \mathbb{Z}$. Világos, hogy a redukció $x_j^2 - x_j$ polinomokkal nem változtatja meg az eredeti polinom 0-1 vektorokon vett helyettesítési értékét, ezért $\hat{f}_F(\mathbf{v}_G)$ egész szám. De másrészt $x_{G'}(\mathbf{v}_G)$ pontosan akkor 1, ha $G' \subseteq G$ és 0 különben. Ezért $\hat{f}_F(\mathbf{v}_G) = \sum_{G' \subsetneq G} \alpha_{G'} + \alpha_G$. A G minimalitása miatt $\alpha_{G'}$ egész, ha $G' \subsetneq G$, így az előbbi egyenlőségből az következik, hogy α_G-nek is egésznek kellene lennie. Tehát valóban $\hat{f}_F \in \mathbb{Z}[\mathbf{x}]$.

Vegyünk egy $F' \in \mathcal{F}$ halmazt. Ekkor

$$\hat{f}_F(\mathbf{v}_{F'}) = \sum_{\substack{k=0 \\ k \notin L}}^{q-1} \binom{|F' \cap F| - k - 1}{q-1}. \tag{6}$$

Ha $F' \neq F$, akkor, miután $\mathcal{F}$ modulo q L-metsző, ezért $|F' \cap F| - k \not\equiv 0 \pmod{q}$, ha $k \notin L$.

Legyen p prím, amelynek q hatványa. A 4.29 lemmát alkalmazva kapjuk, hogy ha $F' \neq F$, akkor a (6) egyenlet jobb oldalán minden tag 0 modulo p. Ha viszont $F' = F$, akkor miután $\mathcal{F}$ modulo q L-kerülő, ezért pontosan egy modulo p nemnulla tag szepepel a jobb oldalon, ez a tag pedig modulo p éppen 1.

Jelölje $\mathbb{F}_p$ a p elemű testet és f_F azt az $\mathbb{F}_p[\mathbf{x}]$-beli polinomot, amelyet $\hat{f}_F$ (egész) együtthatóinak modulo p redukciójával kapunk. A fenti érvelés szerint tehát

$$f_F(\mathbf{v}_{F'}) = \begin{cases} 0 \text{ ha } F \neq F' \\ 1 \text{ ha } F = F'. \end{cases}$$

Miután $\hat{f}_F$ foka legfeljebb $q-1$, ezért ugyanezt elmondhatjuk f_F polinomról is. Ezt a korábbi jelöléseinkkel úgy írhatjuk, hogy $f_F \in \mathbb{F}_p[\mathbf{x}]_{\leq q-1}$. Azt állítjuk, hogy f_F polinomok $\overline{f}_F$ képei az $\mathbb{F}_p[\mathbf{x}]_{\leq q-1} / I(\mathcal{G})_{\leq q-1}$-re képező természetes faktorleképezésnél lineárisan függetlenek $\mathbb{F}_p$ felett. Tegyük ugyanis fel, hogy

$$\sum_{F \in \mathcal{F}} \alpha_F \overline{f}_F = 0 \tag{7}$$

valamely $\alpha_F \in \mathbb{F}_p$ együtthatókra. Többször használtuk, hogy $\mathbb{F}_p[\mathbf{x}] / I(\mathcal{G})$ elemei tekinthetőek $V_{\mathcal{G}}$ halmazon értelmezett függvényeknek. Speciálisan a (7) egyenlőség akkor is fennáll, ha behelyettesítjük $\mathbf{v}_F$ pontot valamely $F \in \mathcal{F} \subseteq \mathcal{G}$ halmazra. Innen azonnal következik $\alpha_F = 0$.

Végül annyit kell észrevennünk, hogy az $\overline{f}_F$ polinomok számának a lineáris függetlenség miatt felső korlátja $\mathbb{F}_p[\mathbf{x}]_{\leq q-1} / I(\mathcal{G})_{\leq q-1}$ dimenziója, tehát

$$|\mathcal{F}| \leq \dim\left(\mathbb{F}_p[\mathbf{x}]_{\leq q-1} / I(\mathcal{G})_{\leq q-1}\right) = H(q-1) \leq \sum_{i=0}^{\infty}\sum_{k=0}^{\ell-1}\binom{n}{q-1-iq-k} = \sum_{k=|L|}^{q-1}\binom{n}{k}.$$

a modulo q ℓ-széles család Hilbert-függvényéről szóló 4.28 tétel miatt. (Jegyezzük még meg, hogy $|L| \leq n-q+2$ egyenlőtlenségből következik a tétel $q-1 \leq \frac{n+\ell}{2}$ feltétele.) □

Köszönetnyilvánítás

Köszönettel tartozom Horváth Erzsébetnek, amiért lektorálta és számtalan hasznos megjegyzéssel javította jelen jegyzetet.

Hivatkozások

[1] J. Abott, M. Kreuzer, L. Robbiano, Computing zero-dimensional schemes, *J. Symbolic Computation* **39** (2005) 31–49.

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

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

[4] M. Brickenstein, Slimgb: Gröbner bases with slim polynomials, *Reports on Computer Algebra* **35**, *ZCA, University of Kaiserslautern*, (2005).

[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 Bruno Buchberger's PhD thesis 1965: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal *J. Symbolic Computation* **41** (2006) no. 3–4, 475–511.

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

[8] 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"*

[9] 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.

[10] W. Decker, G.-M. Greuel, G. Pfister, Primary decomposition: algorithms and comparisons, in Algorithmic Algebra and Number Theory (G.-M. Greuel, B. H. Matzat, G. Hiss editors), *Springer* 1998, 187–220.

[11] L. E. Dickson, Finiteness of the odd perfect and primitive abundant numbers with r distinct prime factors, *Amer. Journal Math* **35** (1913), 413–422.

[12] J.-C. Faugère, A New Efficient Algorithm for Computing Gröbner Bases without Reduction to Zero (F4), *Journal of Pure and Applied Algebra* **139** (1999) 61–88.

[13] J.-C. Faugère, A New Efficient Algorithm for Computing Gröbner Bases without Reduction to Zero (F5), *Proc ISSAC '02, ACM Press* (2002).

[14] 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.

[15] B. Felszeghy, G. Hegedűs, L. Rónyai, Algebraic properties of modulo q ℓ-wide families, *preprint* (2006)

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

[17] P. Gianni, B. Trager, G. Zacharias, Gröbner bases and Primary Decomposition of Polynomial Ideals, *J. Symbolic Computation* **6** (1988), 149–167.

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

[19] G.-M. Greuel, G. Pfister, A Singular Introduction to Commutative Algebra (with contributions by O. Bachmann, C. Lossen, and H. Schönemann), *Springer-Verlag* 2002.

[20] S. Laplagne, An algorithm for the computation of the radical of an ideal, *Proc ISSAC '06, ACM Press* (2006) 191–195.

[21] S. Laplagne, Computation of the Minimal Associated Primes, in Challenges in Symbolic Computation Software (W. Decker, M. Dewar, E. Kaltofen, S. Watt editors) *Dagstuhl Seminar Proceedings* 2006, `http://drops.dagstuhl.de/opus/volltexte/2006/774`

[22] 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.

[23] 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.

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

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