Algoritmi na polinomima

Zlodi, Ivana

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Ivana Zlodi

ALGORITMI NA POLINOMIMA

Diplomski rad

Voditelj rada:
prof. dr. sc. Goran Muić

Zagreb, srpanj 2014.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Sadržaj

Uvod

U ovom radu proučavat ćemo metodu Groebnerovih baza, pomoću koje možemo riješiti problem polinomijalnih ideala u nekom algoritamskom i kompjuterskom trendu. Metoda Groebnerovih baza je jedna od najpraktičnijih metoda za pronalaženje rješenja sustava polinomijalnih jednadžbi. Groebnerove baze za ideale u polinomijalnim prstenima uvedene su 1965. godine, a uveo ih je Bruno Buchberger u svojoj doktorskoj disertaciji i nazvao ih u čast svom mentoru Wolfgangu Gröbneru (1899-1980). Buchberger je u tom radu također definirao algoritam, dalje poznat kao Buchbergerov algoritam, za njihov izračun. Ovaj algoritam se danas javlja u modificiranoj varijanti u većini sistema kompjuterske algebre, i predstavlja veoma efikasno riješenje za veliki broj problema sa kojim se programeri pri kreiranju takvih sistema mogu susresti.

U prvom poglavlju definiramo prsten polinoma u više varijabli i ideale u tom prstenu, te uvodimo pojmove i teoreme potrebne za razumijevanje rada.

U drugom poglavlju, definiramo monomijalni uređaj i dajemo algoritam za dijeljenje polinoma u više varijabli. Algoritam smo dobili tako što smo proširili algoritam dijeljenja polinoma u jednoj varijabli. Definiramo monomijalne ideale i uvodimo problem eksplicitnog opisa ideala, odnosno da li za svaki ideal u prstenu polinoma postoji konačni generirajući skup. Dalje, dajemo definiciju Groebnerove baze koja u ovom radu ima važnu ulogu. U matematici, točnije u računalnoj algebri Groebnerova baza je posebna vrsta generirajućeg skupa idela u prstenu polinoma. Pokazujemo koja svojstva ima Groebnerova baza i kako provjeriti je li dana baza Groebnerova. Na kraju, dajemo Buchbergerov algoritam za konstrukciju Groebnerovih baza.

Poglavlje 1

Preliminarni rezultati

1.1 Polinomi

Do sada smo se već sigurno susreli s polinomima u jednoj ili dvije varijable, no sada ćemo raditi s polinomima u n varijabli $x_1, \ldots, x_n$ s koeficijentima u nekom proizvoljnom polju k. Prije nego definiramo osnovne pojmove ovog odjeljka spomenimo pojam polja. Osnovna intuicija nam govori da je polje skup gdje se može definirati zbrajanje, oduzimanje, množenje i djeljenje s uobičajenim svojstvima. Standardni primjeri polja su skup realnih brojeva $\mathbb{R}$ i skup kompleksnih brojeva $\mathbb{C}$, dok skup cijelih brojeva $\mathbb{Z}$ nije polje zbog operacije dijeljenja (2 i 3 su cijeli brojevi, ali njihov kvocijent $\frac{2}{3}$ nije).

Definicija 1.1.1. ***Monom*** *u $x_1, \ldots, x_n$ je produkt oblika*

$$x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_n^{\alpha_n},$$

gdje su svi eksponenti $\alpha_1, \ldots, \alpha_n$ nenegativni cijeli brojevi. Totalni stupanj ovog monoma je suma $\alpha_1 + \ldots + \alpha_n$.

Neka je $\alpha = (\alpha_1, \ldots, \alpha_n)$ n-torka nenegativnih cijelih brojeva. Tada zapis monoma možemo pojednostaviti na sljedeći način

$$x^\alpha = x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_n^{\alpha_n}.$$

Kada je $\alpha = (0, \ldots, 0)$, primjetimo da je $x^\alpha = 1$. Nadalje, za totalni stupanj monoma x^α koristimo oznaku $|\alpha| = \alpha_1 + \ldots + \alpha_n$.

Definicija 1.1.2. ***Polinom*** *f u $x_1, \ldots, x_n$ s koeficijentima u k je konačna linearna kombinacija (s koeficijentima u k) monoma. Polinom f ćemo pisati u obliku*

$$f = \sum_{\alpha} a_\alpha x^\alpha, \quad a_\alpha \in k,$$

gdje je suma nad konačnim brojem n-torki $\alpha = (\alpha_1, \ldots, \alpha_n)$. Skup svih polinoma u $x_1, \ldots, x_n$ s koeficijentima u k pišemo $k[x_1, \ldots, x_n]$.

Kada radimo s polinomima s manjim brojem varijabli koristit ćemo se oznakama x, y, z, tako npr. polinomi u jednoj, dvije, i tri varijable leže u $k[x]$, $k[x, y]$ i $k[x, y, z]$. Za oznaku polinoma koristit ćemo se slovima f, g, h, p, q, r.

Definicija 1.1.3. *Neka je $f = \sum_\alpha a_\alpha x^\alpha$ polinom u $k[x_1, \ldots, x_n]$.*

1. *a_α zovemo **koeficijent** monoma x^α.*
2. *Ako je $a_\alpha \neq 0$, tada $a_\alpha x^\alpha$ zovemo **član** od f.*
3. ***Totalni stupanj** od f, oznaka deg(f), je maksimalni $|\alpha|$ takav da je koeficijent $a_\alpha \neq 0$.*

Na primjer, dani polinom $f = x^3y + 2x^2z + \frac{1}{3}y^3z^2 + xz^4$ leži u $\mathbb{Q}[x, y, z]$, ima četiri člana i totalni stupanj pet. Primjetimo da su dva člana maksimalnog totalnog stupnja, što se u slučaju polinoma jedne varijable ne može dogoditi.

Za polinom kažemo da je *nul-polinom* ako su svi njegovi koeficijenti jednaki nuli.

1.2 Ideali

U ovom odjeljku definiramo glavni objekt ovog rada.

Definicija 1.2.1. *Podskup $I \subseteq k[x_1, \ldots, x_n]$ je **ideal** ako zadovoljava:*

1. *$0 \in I$.*
2. *Ako je $f, g \in I$, tada je $f + g \in I$.*
3. *Ako je $f \in I$ i $h \in k[x_1, ..., x_n]$, tada je $hf \in I$.*

Prvi prirodni primjer ideala je ideal generiran konačnim brojem polinoma.

Definicija 1.2.2. *Neka su $f_1, \ldots, f_s$ polinomi u $k[x_1, \ldots, x_n]$. Definiramo:*

$$\langle f_1, \ldots, f_s \rangle = \Big\{ \sum_{i=1}^{s} h_i f_i : h_1, \ldots, h_s \in k[x_1, \ldots, x_n] \Big\}.$$

Lema 1.2.3. *Ako su $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$, tada je $\langle f_1, \ldots, f_s \rangle$ ideal u $k[x_1, \ldots, x_n]$. $\langle f_1, \ldots, f_s \rangle$ zvat ćemo ideal generiran sa $f_1, \ldots, f_s$.*

Dokaz. Prvo, $0 \in \langle f_1, \ldots, f_s \rangle$, jer je $0 = \sum_{i=1}^{s} 0 \cdot f_i$. Dalje, pretpostavimo da je $f = \sum_{i=1}^{s} p_i f_i$ i $g = \sum_{i=1}^{s} q_i f_i$, i neka je $h \in k[x_1, \ldots, x_n]$. Iz jednakosti

$$\begin{aligned} f + g &= \sum_{i=1}^{s} (p_i + q_i) f_i, \\ hf &= \sum_{i=1}^{s} (h p_i) f_i \end{aligned}$$

slijedi da je $\langle f_1, \ldots, f_s \rangle$ ideal. □

1.3 Algoritam dijeljenja polinoma u jednoj varijabli

U ovom odjeljku razmotrit ćemo polinome u jednoj varijabli i algoritam dijeljenja. Spomenimo prvo pojam algoritma. Neformalno, algoritam je specifičan skup instrukcija za rukovanje simboličkim ili numeričkim znakovima. U algoritmu postoje ulazni podaci (ili inputs), objekti kojima se koristi algoritam, i izlazni podaci (ili outputs) koji su rezultat algoritma. U svakom koraku algoritma mora biti točno specificirano koji je sljedeći korak. Algoritam ćemo pisati u pseudokodu.

Počinjemo sa definiranjem "vodećeg člana" polinoma u jednoj varijabli, koji ima ključnu ulogu u algoritmu dijeljenja.

Definicija 1.3.1. *Neka je f različit od nul-polinoma, $f \in k[x]$, te neka je*

$$f = a_0 x^m + a_1 x^{m-1} + \ldots + a_m,$$

*gdje je $a_i \in k$ i $a_0 \neq 0$ (prema tome, $m = deg(f)$). Tada kažemo da je $a_0 x^m$ **vodeći član** od f, i pišemo LT(f) = $a_0 x^m$.*

Na primjer, ako je $f = 2x^3 - 5x^2 + 1$, tada je $LT(f) = 2x^3$. Primjetimo da ako su f i g različiti od nul-polinoma, tada je

$$deg(f) \leq deg(g) \Leftrightarrow LT(f) \; dijeli \; LT(g). \tag{1.1}$$

Propozicija 1.3.2. *Neka je k polje i neka je g polinom različit od nul-polinoma u $k[x]$. Tada svaki $f \in k[x]$ možemo zapisati kao*

$$f = qg + r,$$

gdje su q i $r \in k[x]$, i ili je $r = 0$ ili $deg(r) < deg(g)$. Nadalje, q i r su jedinstveni, i postoji algoritam za pronalaženje q i r.

Dokaz. Algoritam za određivanje q i r opisan je pseudokodom:

Input: g, f
Output: q, r
$q := 0$; $r := f$
while *($r \neq 0$* **and** *LT(g) dijeli LT(r))* **do**
  $q := q + LT(r)/LT(g)$
  $r := r - (LT(r)/LT(g))g$
end while

while...do izraz znači da uvučene operacije q i r računamo sve dok uvjet između *while* i *do* više ne vrijedi. Izrazi $q := \ldots$ i $r := \ldots$ znače da definiramo i redefiniramo vrijednosti od q i r. q i r su varijable u algoritmu i one mijenjaju vrijednost u svakom koraku. Moramo pokazati da algoritam završava i da konačne vrijednosti od q i r imaju tražena svojstva.

Primjetimo da jedankost $f = qg + r$ vrijedi za inicijalne vrijednosti od q i r, te svaki puta kada redefiniramo q i r. To se vidi iz sljedeće jednakosti:

$$f = qg + r = (q + LT(r)/LT(g))g + (r - (LT(r)/LT(g))g).$$

Primjetimo da *while...do* petlja završava kad uvjet ($r \neq 0$ *and* $LT(g)$ *dijeli* $LT(r)$) više ne vrijedi, to znači da je ili $r = 0$ ili $LT(g)$ ne dijeli $LT(r)$. Po (1.1), zadnja tvrdnja ekvivalentna je $deg(r) < deg(g)$. Kad algoritam završi, imamo q i r sa traženim svojstvima.

Sada ćemo pokazati da algoritam završava tj. uvjet između *while...do* na kraju prestaje vrijediti (inače bi zapeli u beskonačnoj petlji). To će se dogoditi kada je $r-(LT(r)/LT(g))g$ jednako 0 ili ima stupanj manji od r. Pretpostavimo da je za $m \geq k$

$$r = a_0x^m + \ldots + a_m, \quad LT(r) = a_0x^m,$$
$$g = b_0x^k + \ldots + b_k, \quad LT(g) = b_0x^k,$$

Tada je

$$r - (LT(r)/LT(g))g = (a_0x^m + \ldots + a_m) - (a_0/b_0)x^{m-k}(b_0x^k + \ldots + b_k),$$

i slijedi da se stupanj od r mora smanjiti (ili cijeli izraz nestaje). S obzirom na to da je stupanj konačan, može se smanjiti najviše konačno mnogo puta, što dokazuje da algoritam završava.

Još moramo pokazati da su q i r jedinstveni. Stoga pretpostavimo da je $f = qg + r = q'g + r'$ gdje su r i r' manjeg stupnja od g (osim ako je jedan 0 ili su oba 0). Ako je $r \neq r'$, tada je $deg(r' - r) < deg(g)$. S druge strane, jer je

$$(q - q')g = r' - r, \tag{1.2}$$

vrijedilo bi da je $q - q' \neq 0$, te

$$deg(r' - r) = deg((q - q')g) = deg(q - q') + deg(g) \geq deg(g).$$

To je kontradikcija sa $r = r'$, i iz (1.2) slijedi da je $q = q'$. Time smo dokazali jedinstvenost. □

Poglavlje 2

Groebnerove baze

2.1 Monomijalni uređaj

U algoritmu dijeljenja u $k[x]$ prije nego smo krenuli sa samim dijeljenjem zahtjevali smo da se članovi polinoma napišu u silazećem poretku, tj. tražili smo da se odredi vodeći član. Stoga, možemo reći da je ideja "uređivanja" članova u polinomima ključni dio ovog algoritma.

Kako je polinom zbroj monoma, želimo moći rasporediti članove polinoma nedvosmisleno u silazećem poretku. Da bismo to učinili, moramo znati usporediti svaki par monoma tako da se uspostave njihove odgovarajuće relativne pozicije. Moramo uzeti u obzir i efekt zbrajanja i množenja polinoma monom.

Uzevši u obzir ove zahtjeve, slijedi definicija.

Definicija 2.1.1. ***Monomijalni uređaj*** *na $k[x_1, \ldots, x_n]$ je bilo koja relacija $>$ na $\mathbb{Z}^n_{\geq 0}$, ili ekvivalentno, bilo koja relacija na skupu monoma x^α, $\alpha \in \mathbb{Z}^n_{\geq 0}$, koja zadovoljava:*

(i) *$>$ je totalni (ili linearni) uređaj na $\mathbb{Z}^n_{\geq 0}$.*

(ii) *Ako je $\alpha > \beta$ i $\gamma \in \mathbb{Z}^n_{\geq 0}$, tada je $\alpha + \gamma > \beta + \gamma$.*

(iii) *$>$ je "dobar" uređaj na $\mathbb{Z}^n_{\geq 0}$. To znači da svaki neprazni podskup od $\mathbb{Z}^n_{\geq 0}$ ima najmanji element pod uređajem $>$.*

Za jednostavni primjer monomijalnog uređaja, primjetimo da obični numerički uređaj

$$\ldots > m+1 > m > \ldots > 3 > 2 > 1 > 0$$

na elementima u $\mathbb{Z}_{\geq 0}$ zadovoljava sva tri uvjeta prethodne definicije. Dakle, uređaj po stupnjevima

$$\ldots > x^{m+1} > x^m > \ldots > x^2 > x > 1$$

monoma u $k[x]$ je monomijalni uređaj. Prvi primjer uređaja na n-torki bit će leksikografski uređaj (ili lex uređaj).

Definicija 2.1.2. *Neka je $\alpha = (\alpha_1, \ldots, \alpha_n)$ i $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$. Kažemo da je $\alpha >_{lex} \beta$, ako je vektor razlike $\alpha - \beta \in \mathbb{Z}^n_{\geq 0}$, i prvi element s lijeve strane različit od nule je pozitivan. Pisat ćemo $x^\alpha >_{lex} x^\beta$ ako je $\alpha >_{lex} \beta$.*

Slijedi nekoliko primjera:

(a) (1,2,0) $>_{lex}$ (0,3,4) jer je $\alpha - \beta$ = (1,-1,-4).

(b) (3,2,4) $>_{lex}$ (3,2,1) jer je $\alpha - \beta$ = (0,0,3).

(c) varijable $x_1, \ldots, x_n$ su poredane na uobičajeni način leksikografskim uređajem:

$$(1, 0, \ldots, 0) >_{lex} (0, 1, 0, \ldots, 0) >_{lex} \ldots >_{lex} (0, \ldots, 0, 1)$$

pa je $x_1 >_{lex} x_2 >_{lex} \ldots >_{lex} x_n$.

Abecedni uređaj $a > b > c > \ldots > x > y > z$ na varijablama koristimo za definiranje leksikografskog uređaja, osim ako nije eksplicitno drugačije rečeno. Primjetimo da je leksikografski uređaj analogan uređaju riječi korištenih u riječniku.

Propozicija 2.1.3. *Leksikografski uređaj na $Z^n_{\geq 0}$ je monomijalni uređaj.*

U leksikografskom uređaju, primjetimo da kod određivanja poretka monoma ne uzimamo u obzir totalni stupanj, tako na primjer za $x > y > z$ vrijedi $x >_{lex} y^5z^3$. Za neke svrhe, možda ćemo željeti uzeti u obzir totalni stupanj monoma i poredati monome prvo s većim stupnjom. To možemo napraviti koristeći gradirani leksikografski uređaj.

Definicija 2.1.4. ***(Gradirani lex uređaj)*** *Neka je $\alpha,\ \beta \in Z^n_{\geq 0}$. Kažemo da je $\alpha >_{grlex} \beta$ ako*

$$|\alpha| = \sum_{i=1}^{n} \alpha_i > |\beta| = \sum_{i=1}^{n} \beta_i,\ \textit{ili}\ |\alpha| = |\beta|\ i\ \alpha >_{lex} \beta.$$

Slijedi nekoliko primjera:

(a) $(1,2,3) >_{grlex} (3,2,0)$ jer je $|(1,2,3)| = 6 > |(3,2,0)| = 5$.

(b) $(1,2,4) >_{grlex} (1,1,5)$ jer je $|(1,2,4)| = |(1,1,5)|$ i $(1,2,4) >_{lex} (1,1,5)$.

(c) varijable su poredane prema lex uređaju, tj. $x_1 >_{grlex} \ldots >_{grlex} x_n$.

S obzirom na zadani monomijalni uređaj koristit ćemo sljedeću terminologiju.

Definicija 2.1.5. *Neka je $f = \sum_\alpha a_\alpha x^\alpha$ različit od nul-polinoma u $k[x_1, ..., x_n]$ i neka je $>$ monomijalni uređaj.*

1. ***Multistupanj** od f je*

$$multideg(f) = max(\alpha \in Z^n_{\geq 0} : a_\alpha \neq 0).$$

2. ***Vodeći koeficijent** od f je*

$$LC(f) = a_{multideg(f)} \in k.$$

3. ***Vodeći monom** od f je*

$$LM(f) = x^{multideg(f)}$$

(s koeficijentom 1).

4. ***Vodeći član** od f je*

$$LT(f) = LC(f) \cdot LM(f).$$

Pokažimo prethodno na primjeru, neka je $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2$ i neka je sa $>$ označen leksikografski uređaj. Tada je

$$multideg(f) = (3,0,0),$$
$$LC(f) = -5,$$
$$LM(f) = x^3,$$
$$LT(f) = -5x^3.$$

Multistupanj polinoma ima sljedeća korisna svojstva.

Lema 2.1.6. *Neka su $f, g \in k[x_1, \ldots, x_n]$ polinomi različiti od nul-polinoma. Tada:*

(i) multideg(f · g) = multideg(f) + multideg(g).

(ii) Ako je $f + g \neq 0$*, tada*

$$multideg(f + g) \leq max(multideg(f), multideg(g)).$$

Dodatno, ako je multideg(f) $\neq$ *multideg(g) , tada vrijedi jednakost.*

2.2 Algoritam dijeljenja

U prošlom poglavlju, vidjeli smo kako funkcionira algoritam dijeljenja polinoma u jednoj varijabli. Sada želimo algoritam za dijeljenje polinoma u $k[x_1, \ldots, x_n]$ koji proširuje algoritam za *k[x]*. Cilj je podijeliti $f \in k[x_1, \ldots, x_n]$ sa $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. To znači da f želimo napisati u obliku

$$f = a_1 f_1 + \ldots + a_s f_s + r$$

gdje su $a_1, \ldots, a_s$ "kvocijenti", a r ostatak koji leži u $k[x_1, \ldots, x_n]$. Osnovna ideja algoritma je ista kao i u slučaju jedne varijable. Želimo poništiti vodeći član u f (s obzirom na fiksni monomijalni uređaj) množenjem nekog f_i s odgovarajućim monomom i oduzimanjem. Tada taj monom postaje član s odgovarajućim a_i. Prije samog algoritma dijeljenja pogledajmo primjer.

Primjer 2.2.1. *Podijelit ćemo* $f = x^2y + xy^2 + y^2$ *sa* $f_1 = xy - 1$ *i* $f_2 = y^2 - 1$ *koristeći leksikografski uređaj sa* $x > y$*. Želimo upotrijebiti istu šemu za dijeljenje polinoma u jednoj varijabli, razlika je u tome što sada imamo nekoliko djelitelja i kvocijenta. Nabrajanjem djelitelja* f_1*,* f_2 *i kvocijenta* a_1*,* a_2 *imamo sljedeću postavu*

$$\begin{array}{rl} & a_1: \\ & a_2: \\ xy - 1 & \\ y^2 - 1 & \sqrt{x^2y + xy^2 + y^2} \end{array}$$

Gledamo vodeće članove polinoma f_1 *i* f_2*,* $LT(f_1) = xy$ *i* $LT(f_2) = y^2$*. Vidimo da samo* $LT(f_1)$ *dijeli* $LT(f) = x^2y$*, stoga dijelimo* x^2y *sa* xy*, ostavljajući* x*, i onda oduzimamo* $x \cdot f_1$ *od* f*:*

$$
\begin{array}{rll}
 & a_1: & x \\
 & a_2: & \\
xy-1 & & \sqrt{x^2y+xy^2+y^2} \\
y^2-1 & & \underline{x^2y-x} \\
 & & \quad xy^2+x+y^2
\end{array}
$$

Sada ponovimo isti postupak na $xy^2 + x + y^2$. Vodeći članovi $LT(f_1) = xy$ i $LT(f_2) = y^2$ dijele vodeći član $LT(xy^2 - x + y^2) = xy^2$. Kako je f_1 prvi nabrojan uzimamo prvo njega. Pa dobijemo:

$$
\begin{array}{rll}
 & a_1: & x+y \\
 & a_2: & \\
xy-1 & & \sqrt{x^2y+xy^2+y^2} \\
y^2-1 & & \underline{x^2y-x} \\
 & & \quad xy^2+x+y^2 \\
 & & \quad \underline{xy^2-y} \\
 & & \qquad x+y^2+y
\end{array}
$$

Primjetimo da $LT(f_1) = xy$ ni $LT(f_2) = y^2$ ne dijeli $LT(x + y^2 + y) = x$. Međutim, $x + y^2 + y$ nije ostatak kako $LT(f_2)$ dijeli y^2. Prema tome, ako premjestimo x u ostatak, možemo nastaviti dijeliti. Desno od korijena, kreiramo stupac ostataka r, gdje stavljamo članove koji pripadaju ostatku. Također, polinom ispod korijena zovemo srednji djeljenik. Nastavljamo dijeliti sve dok srednji djeljenik nije nula. Prije nastavka dijeljenja, x stavljamo u stupac ostatka kao što je naznačeno strelicom:

$$
\begin{array}{rll}
a_1: & x+y & \\
a_2: & & r \\
xy-1 & & \\
y^2-1 & \sqrt{x^2y+xy^2+y^2} & \\
 & x^2y-x & \\
 & \hline
 & \quad xy^2+x+y^2 & \\
 & \quad xy^2-y & \\
 & \quad \hline
 & \qquad x+y^2+y & \\
 & \qquad \hline
 & \qquad\quad y^2+y & \to x
\end{array}
$$

Ako možemo podijeliti srednji djeljenik s $LT(f_1)$ ili $LT(f_2)$, nastavljamo uobičajeno, a ako nijedan ne dijeli, maknemo vodeći član srednjeg djeljenika u stupac ostatka. Ovdje je ostatak dijeljenja:

$$
\begin{array}{rll}
a_1: & x+y & \\
a_2: & 1 & r \\
xy-1 & & \\
y^2-1 & \sqrt{x^2y+xy^2+y^2} & \\
 & x^2y-x & \\
 & \hline
 & \quad xy^2+x+y^2 & \\
 & \quad xy^2-y & \\
 & \quad \hline
 & \qquad x+y^2+y & \\
 & \qquad \hline
 & \qquad\quad y^2+y & \to x \\
 & \qquad\quad y^2-1 & \\
 & \qquad\quad \hline
 & \qquad\qquad y+1 & \\
 & \qquad\qquad \hline
 & \qquad\qquad\quad 1 & \to x+y \\
 & \qquad\qquad\quad \overline{0} & \to x+y+1
\end{array}
$$

Na kraju, ostatak je zbroj monoma $x+y+1$, od kojih niti jedan nije djeljiv s vodećim članovima $LT(f_1)$ i $LT(f_2)$. Dakle, f možemo zapisati na sljedeći način:

$$x^2y+xy^2+y^2 = (x+y)\cdot(xy-1)+1\cdot(y^2-1)+x+y+1.$$

Sada možemo iznijeti generalnu formu algoritma dijeljenja.

Teorem 2.2.2. ***(Algoritam dijeljenja u $k[x_1, \ldots, x_n]$)*** *Fiksirajmo monomijalni uređaj $>$ na $Z^n_{\geq 0}$, i neka je $F = (f_1, \ldots, f_s)$ uređena s-torka polinoma u $k[x_1, \ldots, x_n]$. Tada svaki $f \in k[x_1, \ldots, x_n]$ možemo zapisati kao*

$$f = a_1 f_1 + \ldots + a_s f_s + r$$

gdje su a_i, $r \in k[x_1, \ldots, x_n]$, i ili je $r = 0$ ili je linearna kombinacija s koeficijentima u k, od monoma, od kojih ni jedan nije djeljiv sa $LT(f_1), \ldots, LT(f_s)$. r ćemo zvati ostatak od f pri dijeljenju sa F. Nadalje, ako je $a_i f_i \neq 0$, tada imamo

$$multideg(f) \geq multideg(a_i f_i).$$

Dokaz. Dokazujemo egzistenciju $a_1, \ldots, a_s$ i r dajući algoritam za njihovu konstrukciju i pokazujemo da radi točno za bilo koji $f, f_1, \ldots, f_s$.

Input: $f_1, \ldots, f_s, f$
Output: $a_1, \ldots, a_s, r$
$a_1 := 0, \ldots, a_s := 0, r := 0$
$p := f$
while $(p \neq 0)$ **do**
  $i := 1$
  $divisionoccured := false$
  while $(i \leq s$ **and** $divisionoccured = false)$ **do**

    if $(LT(f_i)\ divides\ LT(p))$ **then**
      $a_i := a_i + LT(p)/LT(f_i)$
      $p := p - (LT(p)/LT(f_i))f_i$
      $divisionoccured := true$
    else
      $i := i + 1$
    end if
    if $(divisionoccured = false)$ **then**
      $r := r + LT(p)$
      $p := p - LT(p)$
    end if
  end while
end while

Možemo povezati ovaj algoritam s prethodnim primjerom tako da primjetimo da varijabla p predstavlja *"srednji djeljenik"* u svakoj fazi, varijabla r predstavlja stupac na desnoj

strani, i varijable $a_1, \ldots, a_s$ su kvocijenti nabrojani iznad korijena. Konačno, varijabla *"divisionoccured"* pokazuje nam kada neki $LT(f_i)$ dijeli vodeći član srednjeg djeljenika. To treba provjeriti svaki puta kad prolazimo kroz *while...do* petlju, točno jedan od dva slučaja se dogodi:

1. (KORAK DIJELJENJA) Ako neki $LT(f_i)$ dijeli $LT(p)$, tada algoritam radi kao u slučaju jedne varijable.
2. (KORAK OSTATKA) Ako $LT(f_i)$ ne dijeli $LT(p)$, tada algoritam dodaje $LT(p)$ u ostatak.

Ovi koraci odgovaraju točno onom što smo radili u Primjeru 2.2.1. Da bi dokazali da algoritam radi, prvo moramo pokazati da

$$f = a_1 f_1 + \ldots + a_s f_s + p + r \tag{2.1}$$

vrijedi u svakoj fazi. Ovo je očito točno za inicijalne vrijednosti $a_1, \ldots, a_s,\ p,\ r$. Sada, pretpostavimo da gornja jednakost vrijedi u nekom koraku algoritma. Ako je sljedeći korak "korak dijeljenja", tada neki $LT(f_i)$ dijeli $LT(p)$, i jednakost

$$a_i f_i + p = (a_i + LT(p)/LT(f_i))f_i + (p - (LT(p)/LT(f_i))f_i)$$

pokazuje da $a_i f_i + p$ ostaje nepromijenjen. Kako su sve ostale varijable nepromijenjene, jednakost (2.1) još uvijek vrijedi u ovom slučaju. S druge strane, ako je sljedeći korak "korak ostatka", tada će p i r biti promijenjeni, ali suma $p + r$ ostaje nepromijenjena jer je:

$$p + r = (p - LT(p)) + (r + LT(p)).$$

Kao i prije, jednakost (2.1) još uvijek vrijedi. Sljedeće, primjetimo da se algoritam zaustavlja kada je $p = 0$. U toj situaciji, (1.1) postaje

$$f = a_1 f_1 + \ldots + a_s f_s + r.$$

Kako se članovi dodaju u ostatak r samo kada nisu djeljivi s niti jednim od vodećih članova $LT(f_i)$, slijedi da $a_1, \ldots, a_s$ i r imaju poželjna svojstva kada algoritam završava.

Na kraju, moramo pokazati da je algoritam konačan. Svaki puta kada redefiniramo

varijablu p, njezin stupanj pada ili postaje 0. Da bismo to vidjeli, pretpostavimo da se tijekom "koraka dijeljenja" p redefinira

$$p' = p - \frac{LT(p)}{LT(f_i)} f_i.$$

Po Lemi 2.1.6 imamo

$$LT(\frac{LT(p)}{LT(f_i)} f_i) = \frac{LT(p)}{LT(f_i)} LT(f_i) = LT(p)$$

tako da p i $(LT(p)/LT(f_i))f_i$ imaju isti vodeći član. Dakle, njihova razlika p' mora imati strogo manji multistupanj kada je $p' \neq 0$. Dalje, pretpostavimo da se tijekom "koraka ostatka" p redefinira

$$p' = p - LT(p).$$

Očito je da je $multideg(p') < multideg(p)$ kada je $p' \neq 0$. Prema tome, u svakom slučaju, multistupanj se mora smanjiti. Ako algoritam nikad ne završava, dobili bismo beskonačni padajući niz multistupnjeva. Svojstvo 'dobrog uređaja' > pokazuje da se ovo ne može dogoditi. Prema tome, na kraju mora biti $p = 0$, tako da algoritam završava nakon konačno mnogo koraka.

Ostaje pokazati odnos između *multideg(f)* i $multideg(a_i f_i)$. Svaki član u a_i je oblika $LT(p)/LT(f_i)$ za neku vrijednost varijable p. Algoritam počinje s $p = f$, i upravo smo završili s dokazivanjem da multistupanj od p pada. Ovo pokazuje da $LT(p) \leq LT(f)$, i onda lako slijedi (koristeći uvjet (ii) iz definicije za monomijalni uređaj) da $multideg(a_i f_i) \leq multideg(f)$ kada $a_i f_i \neq 0$. □

Prvo važno svojstvo algoritma dijeljenja u $k[x]$ je da je ostatak jedinstveno određen. Da bismo vidjeli da ovo ne vrijedi u slučaju više od jedne varijable pogledajmo sljedeći primjer.

Primjer 2.2.3. *Želimo podijeliti* $f = xy^2 + xy^2 + y^2$ *sa* $f_1 = xy + 1$ *i* $f_2 = y + 1$ *koristeći leksikografski uređaj* $x > y$. *Primjetimo da su polinomi zadani isto kao i u prethodnom primjeru, osim što smo sada promijenili poredak djelitelja. Uzimajući u obzir novi poredak dobijemo sljedeće rješenje:*

$$
\begin{array}{rll}
a_1: & x+1 & \\
a_2: & x & r \\
y^2-1 & \sqrt{x^2y+xy^2+y^2} & \\
xy-1 & x^2y-x & \\
\hline
 & xy^2+x+y^2 & \\
 & xy^2-x & \\
\hline
 & 2x+y^2 & \\
\hline
 & y^2 & \to 2x \\
 & y^2-1 & \\
\hline
 & 1 & \to 2x+1 \\
\hline
 & 0 & \to 2x+1
\end{array}
$$

Ovo pokazuje da je

$$x^2y + xy^2 + y^2 = (x+1)(y^2-1) + x(xy-1) + 2x + 1.$$

Ako ovo usporedimo s rezultatom iz prethodnog primjera vidimo da ostatak nije jedinstveno okarakteriziran uz uvjet da nijedan od članova ostatka nije djeljiv sa $LT(f_1)$ i $LT(f_2)$.

2.3 Monomijalni ideali

U ovom odjeljku uvest ćemo *Problem eksplicitnog opisa ideala* u slučaju monomijalnih ideala. Ovaj problem postavlja pitanje da li svaki ideal $I \subseteq k[x_1, \ldots, x_n]$ ima konačni generirajući skup. Drugim riječima, možemo li pisati $I = \langle f_1, \ldots, f_s \rangle$ za neki $f_i \in k[x_1, \ldots, x_n]$?

Za početak, definiramo monomijalne ideale u $k[x_1, \ldots, x_n]$.

Definicija 2.3.1. *Ideal $I \subseteq k[x_1, \ldots, x_n]$ je **monomijalni ideal** ako postoji podskup $A \subseteq \mathbb{Z}^n_{\geq 0}$ takav da I sadrži sve polinome koji su konačna suma oblika $\sum_{\alpha \in A} h_\alpha x^\alpha$, gdje je $h_\alpha \in k[x_1, \ldots, x_n]$. U ovom slučaju, pišemo $I = \langle x^\alpha : \alpha \in A \rangle$.*

Primjer monomijalnih ideala dan je sa $I = \langle x^4y, x^2y^3, xy \rangle \subseteq k[x, y]$. Slijedi karakterizacija za sve monome koji leže u danom monomijalnom idealu.

Lema 2.3.2. *Neka je $I = \langle x^\alpha : \alpha \in A \rangle$ monomijalni ideal. Tada monom x^β leži u I ako i samo ako je x^β djeljiv sa x^α za neki $\alpha \in A$.*

Primjetimo da je x^β djeljiv sa x^α točno onda kada je $x^\beta = x^\alpha \cdot x^\gamma$ za neki $\gamma \in \mathbb{Z}^n_{\geq 0}$. To je ekvivalentno $\beta = \alpha + \gamma$.

Lema 2.3.3. *Neka je I monomijalni ideal, i neka je $f \in k[x_1, \ldots, x_n]$. Tada je sljedeće ekvivalentno:*

(a) $f \in I$.

(b) Svaki član od f leži u I.

(c) f je k-linearna kombinacija monoma u I.

Neposredna posljedica trećeg dijela leme je da je monomijalni ideal jedinstveno određen njegovim monomima. Stoga, imamo sljedeći korolar.

Korolar 2.3.4. *Dva monomijalna ideala su ista ako i samo ako sadrže iste monome.*

Glavni rezultat ovog odjeljka je da su svi monomijalni ideali u $k[x_1, \ldots, x_n]$ konačno generirani.

Teorem 2.3.5. ***(Dicksonova lema)*** *Monomijalni ideal $I = \langle x^\alpha : \alpha \in A \rangle \subseteq k[x_1, \ldots, x_n]$ može biti zapisan u obliku $I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$ gdje su $\alpha(1), \ldots, \alpha(s) \in A$. Posebno, I ima konačnu bazu.*

2.4 Hilbertov teorem o bazi i Groebnerove baze

Vidjeli smo da vodeći članovi imaju vrlo važnu ulogu u algoritmu dijeljenja. Jednom kad izaberemo monomijalni uređaj, svaki $f \in k[x_1, \ldots, x_n]$ ima jedinstven vodeći član $LT(f)$. Tada za bilo koji ideal I, možemo definirati njegov ideal vodećih članova.

Definicija 2.4.1. *Neka je $I \subseteq k[x_1, \ldots, x_n]$ ideal različit od $\{0\}$.*

*(i) Sa **LT(I)** označavamo skup vodećih članova elemenata od I. Prema tome,*

$$LT(I) = \{cx^\alpha : postoji\ f \in I\ sa\ LT(f) = cx^\alpha\}.$$

(ii) Sa $\langle LT(I) \rangle$ označavamo ideal generiran elementima od $LT(I)$.

Neka je $I = \langle f_1, \ldots, f_s \rangle$ ideal, tada $\langle LT(f_1), \ldots, LT(f_s) \rangle$ i $\langle LT(I) \rangle$ mogu biti različiti ideali. Vrijedi da je $LT(f_i) \in LT(I) \subseteq \langle LT(I) \rangle$ po definiciji, što povlači $\langle LT(f_1), \ldots, LT(f_s) \rangle \subseteq \langle LT(I) \rangle$. Međutim, iz sljedećeg primjera se vidi da $\langle LT(I) \rangle$ može biti strogo veći.

Primjer 2.4.2. *Neka je $I = \langle f_1, f_2 \rangle$, gdje su $f_1 = x^3 - 2xy$ i $f_2 = x^2y - 2y^2 + x$ i koristimo grlex uređaj u $k[x, y]$. Tada zbog*

$$x \cdot (x^2y - 2y^2 + x) - y \cdot (x^3 - 2xy) = x^2$$

vidimo da je $x^2 \in I$. Prema tome, $x^2 = LT(x^2) \in \langle LT(I) \rangle$. Kako x^2 nije djeljiv sa $LT(f_1) = x^3$ ili $LT(f_2) = x^2y$, tako da $x^2 \notin \langle LT(f_1), LT(f_2) \rangle$ po Lemi 2.3.2.

Propozicija 2.4.3. *Neka je $I \subseteq k[x_1, \ldots, x_n]$ ideal.*

(i) $\langle LT(I) \rangle$ je monomijalni ideal.

(ii) Postoje $g_1, \ldots, g_s \in I$ tako da je $\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_s) \rangle$.

Teorem 2.4.4. ***(Hilbertov teorem o bazi)*** *Svaki ideal $I \subseteq k[x_1, \ldots, x_n]$ ima konačno generirajući skup. To jest, $I = \langle g_1, \ldots, g_s \rangle$ za neki $g_1, \ldots, g_s \in I$.*

Baza $\{g_1, \ldots, g_s\}$ iz prethodnog teorema ima specijalno svojstvo da je $\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_s) \rangle$. Ovakvim specijalnim bazama dati ćemo sljedeće ime.

Definicija 2.4.5. *Fiksirajmo monomijalni uređaj. Za konačan podskup $G = \{g_1, ..., g_t\}$ nekog ideala I kažemo da je* ***Groebnerova baza*** *(ili standardna baza) ako vrijedi*

$$\langle LT(g_1), \ldots, LT(g_t) \rangle = \langle LT(I) \rangle.$$

Korolar 2.4.6. *Fiksirajmo monomijalni uređaj. Tada svaki ideal $I \subseteq k[x_1, \ldots, x_n]$ različit od $\{0\}$ ima Groebnerovu bazu. Štoviše, bilo koja Groebnerova baza za ideal I je baza od I.*

Uzlazni lanac ideala u $k[x_1, \ldots, x_n]$ ugniježđen je u rastući niz

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

Na primjer, niz

$$\langle x_1 \rangle \subseteq \langle x_1, x_2 \rangle \subseteq \ldots \subseteq \langle x_1, \ldots, x_n \rangle \tag{2.2}$$

čini uzlazni lanac ideala. Ako pokušamo proširiti ovaj lanac ideala priključujući mu ideal s daljnim generatorom, jedna od dvije alternative će se dogoditi. Pokažimo na primjeru. Neka je $\langle x_1, \ldots, x_n, f\rangle$ ideal gdje je $f \in k[x_1, \ldots, x_n]$. Ako je $f \in k[x_1, \ldots, x_n]$ tada opet dobijemo $\langle x_1, \ldots, x_n\rangle$ i ništa se ne mijenja. Ako, $f \notin \langle x_1, \ldots, x_n\rangle$ tada tvrdimo da je $\langle x_1, \ldots, x_n, f\rangle = k[x_1, \ldots, x_n]$. Kao rezultat uzlazni lanac (2.2) može se nastaviti na dva načina, u prvom slučaju ponavljajući zadnji ideal "do beskonačnosti", a u drugom slučaju dodavanjem $k[x_1, \ldots, x_n]$ i onda njegovim ponavljanjem "do beskonačnosti". U svakom slučaju uzlazni lanac stabilizirat će se nakon konačnog broja koraka.

Teorem 2.4.7. *Neka je $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ uzlazni lanac ideala u $k[x_1, \ldots, x_n]$. Tada postoji $N \geq 1$ takav da je*

$$I_N = I_{N+1} = I_{N+2} = \ldots$$

2.5 Svojstva Groebnerovih baza

Do sada smo naučili da svaki ideal $I \subseteq k[x_1, \ldots, x_n]$ ima Groebnerovu bazu. Sada ćemo vidjeti koja svojstva ima Groebnerova baza te kako odrediti je li dana baza Groebnerova. Također ćemo dati odgovor na *Problem pripadnosti idealu* koji postavlja pitanje kako možemo provjeriti za dani $f \in k[x_1, \ldots, x_n]$ i ideal $I = \langle f_1, \ldots, f_s\rangle$ je li $f \in I$?

Prvo važno svojstvo koje ćemo pokazati je jedinstvenost ostatka u algoritmu dijeljenja u $k[x_1, \ldots, x_n]$ kada dijelimo elementima Groebnerove baze.

Propozicija 2.5.1. *Neka je $G = \{g_1, \ldots, g_t\}$ Groebnerova baza za ideal $I \subseteq k[x_1, \ldots, x_n]$ i neka je $f \in k[x_1, \ldots, x_n]$. Tada postoji jedinstveni $r \in k[x_1, \ldots, x_n]$ sa sljedeća dva svojstva:*

(i) Nijedan član od r nije djeljiv s bilo kojim od $LT(g_1), \ldots, LT(g_t)$.

(ii) Postoji $g \in I$ takav da je $f = g + r$.

Specijalno, r je ostatak od f pri dijeljenju s G bez obzira kako su elementi od G raspoređeni kada koristimo algoritam dijeljenja.

Dokaz. Algoritam dijeljenja daje $f = a_1g_1 + \ldots + a_tg_t + r$, gdje r zadovoljava (i). Možemo zadovoljiti i (ii) stavljajući da je $g = a_1g_1 + \ldots + a_tg_t \in I$. Ovo dokazuje egzistenciju od r. Da bi dokazali jedinstvenost, pretpostavimo da $f = g+r = g'+r'$ zadovoljava (i) i (ii). Tada $r-r' = g'-g \in I$, pa onda ako je $r \neq r'$, vrijedi $LT(r-r') \in \langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_t)\rangle$. Po Lemi 2.3.2 slijedi da je $LT(r - r')$ djeljiv s nekim $LT(g_i)$. To je nemoguće jer niti jedan član od r, r' nije djeljiv s nekim od $LT(g_1), \ldots, LT(g_t)$. Prema tome, $r - r'$ mora biti nula,

time smo dokazali jedinstvenost.

Zadnji dio propozicije slijedi iz jedinstvenosti od r. □

Iako je ostatak r jedinstven, čak i za Groebnerovu bazu, "kvocijenti" a_i dobiveni algoritmom dijeljenja $f = a_1g_1 + \ldots + a_tg_t + r$ mogu se promijeniti ako stavimo drugačiji redoslijed generatora.

Korolar 2.5.2. *Neka je $G = \{g_1, \ldots, g_t\}$ Groebnerova baza za ideal $I \subseteq k[x_1, \ldots, x_n]$ i neka je $f \in k[x_1, \ldots, x_n]$. Tada je $f \in I$ ako i samo ako ostatak pri dijeljenju f sa G je nula.*

Dokaz. Ako je ostatak nula, tada već znamo da je $f \in I$. Obrnuto, za dani $f \in I$, $f = f + 0$ zadovoljava dva uvjeta Propozicije 2.5.1. Slijedi da je 0 ostatak od f pri djeljenju sa G. □

Koristeći prethodni korolar, dobivamo algoritam za rješavanje *Problema pripadnosti idealu* pod uvjetom da znamo Groebnerovu bazu G za ideal o kome je riječ, jedino moramo izračunati ostatak s obzirom na G da bi odredili je li $f \in I$.

Definicija 2.5.3. *Sa $\overline{f}^F$ označavat ćemo ostatak pri dijeljenju f sa uređenom s-torkom $F = (f_1, \ldots, f_s)$. Ako je F Groebnerova baza za $\langle f_1, \ldots, f_s \rangle$, tamo možemo F smatrati kao skup (bez ikakvog posebnog uređaja).*

Na primjer, sa $F = (x^2y - y^2, x^4y^2 - y^2) \subseteq k[x, y]$ koristeći lex uređaj, imamo

$$\overline{x^5y}^F = xy^3$$

zbog

$$x^5y = (x^3 + xy)(x^2y - y^2) + 0 \cdot (x^4y^2 - y^2) + xy^3.$$

Definicija 2.5.4. *Neka su $f, g \in k[x_1, \ldots, x_n]$ različiti od nul-polinoma.*

*(i) Ako je multideg$(f) = \alpha$ i multideg$(g) = \beta$, tada neka je $\gamma = (\gamma_1, ..., \gamma_n)$, gdje je $\gamma_i = max(\alpha_i, \beta_i)$ za svaki i. x^γ zovemo **najmanji zajednički višekratnik** od $LM(f)$ i $LM(g)$, i pišemo $x^\gamma = LCM(LM(f), LM(g))$.*

*(ii) **S-polinom** od f i g je kombinacija*

$$S(f, g) = \frac{x^\gamma}{LT(f)} \cdot f - \frac{x^\gamma}{LT(g)} \cdot g.$$

Na primjer, neka je $f = x^3y^2 - x^2y^3 + x$ i $g = 3x^4y + y^2$ u $\mathbb{R}[x, y]$ sa grlex uređajom. Tada je $\gamma = (4, 2)$ i

$$\begin{aligned} S(f,g) &= \frac{x^4y^2}{x^3y^2} \cdot f - \frac{x^4y^2}{3x^4y} \cdot g \\ &= x \cdot f - \frac{1}{3} \cdot y \cdot g \\ &= -x^3y^3 + x^2 - \frac{1}{3}y^3. \end{aligned}$$

S-polinom *S(f,g)* napravljen je da se ponište vodeći članovi. Sljedeća lema pokazuje nam da svako poništavanje vodećih članova među polinomima istog multistupnja proizlazi iz ove vrste poništavanja.

Lema 2.5.5. *Pretpostavimo da imamo sumu $\sum_{i=1}^{s} c_i f_i$, gdje je $c_i \in k$ i $multideg(f_i) = \delta \in \mathbb{Z}^n_{\geqslant 0}$ za sve i. Ako je $multideg(\sum_{i=1}^{s} c_i f_i) < \delta$, tada je $\sum_{i=1}^{s} c_i f_i$ linearna kombinacija, s koeficijentima u k, od S-polinoma $S(f_j, f_k)$ za $1 \leq j, k, \leq s$. Nadalje, svaki $S(f_j, f_k)$ ima multideg $< \delta$.*

Sljedeći teorem ponekad se zove "Buchbergerov par kriterija" i jedan je od ključnih rezultata Groebnerovih baza. Koristeći prethodnu lemu i S-polinome dokazat ćemo da vrijedi sljedeće.

Teorem 2.5.6. *Neka je I polinomijalni ideal. Tada je baza $G = \{g_1, \ldots, g_t\}$ Groebnerova baza za I ako i samo ako za sve parove $i \neq j$, ostatak pri dijeljenju $S(g_i, g_j)$ sa G je nula.*

Dokaz. $\Rightarrow$: Ako je G Groebnerova baza, tada je zbog $S(g_i, g_j) \in I$, ostatak pri dijeljenju sa G nula po Korolaru 2.5.2.
$\Leftarrow$: Neka je $f \in I$ različit od nul-polinoma. Moramo pokazati da ako svi S-polinomi imaju ostatak nula pri dijeljenju sa G, tada je $LT(f) \in \langle LT(g_1), \ldots, LT(g_t)\rangle$. Prije nego što damo detalje dokaza, opišimo prvo strategiju dokaza.

Za dani $f \in I = \langle g_1, \ldots, g_t\rangle$, postoje polinomi $h_i \in k[x_1, \ldots, x_n]$ takvi da je

$$f = \sum_{i=1}^{t} h_i g_i. \tag{2.3}$$

Po Lemi 2.1.6, slijedi da je

$$multideg(f) \leq max(multideg(h_i g_i)). \tag{2.4}$$

Ako ne vrijedi jednakost, tada se javlja poništavanje među vodećim članovim iz (2.3). Lema 2.5.5 omogućit će nam da napišemo jednakost u obliku S-polinoma. Tada će nam naša pretpostavka da S-polinomi imaju ostatke nula omogućiti da zamijenimo S-polinome sa izrazima koji uključuju manje poništavanje. Prema tome, dobit ćemo izraz za f koji ima manje poništavanja vodećih članova. Nastavljajući na ovaj način, na kraju ćemo naći izraz (2.3) za f gdje se dobije jednakost u (2.4). Tada $multideg(f) = multideg(h_i g_i)$ za neki i, i slijedit će da je $LT(f)$ djeljiv sa $LT(g_i)$. Ovo će pokazati da je $LT(f) \in \langle LT(g_1), \ldots, LT(g_t)\rangle$, a to smo htjeli dokazati.

Sada ćemo dati detalje dokaza. S obzirom na izraz (2.3) za f, neka je $m(i) = multideg(h_i g_i)$, i definiramo $\delta = max(m(1), \ldots, m(t))$. Tada nejednakost (2.4) postaje

$$multideg(f) \leq \delta.$$

Sada razmotrimo sve moguće načine na koje f može biti zapisan u obliku (2.3). Za svaki takav izraz, moguće da dobijemo različiti δ. Kako je monomijalni uređaj "dobar uređaj", možemo odabrati izraz (2.3) za f takav da je δ minimalan.

Pokazat ćemo da kad jednom odaberemo minimalni δ, imamo da je $multideg(f) = \delta$. Tada se jednakost pojavljuje u (2.4), i kao što smo promatrali, sllijedi da je $LT(f) \in \langle LT(g_1), \ldots, LT(g_t)\rangle$. Ovo će dokazati teorem.

Ostaje pokazati da je $multideg(f) = \delta$. Dokazat ćemo ovo pomoću kontradikcije. Jednakost ne vrijedi samo kada je $multideg(f) < \delta$. Da bi odvojili članove multistupnja δ, zapišimo f u sljedećem obliku:

$$\begin{aligned} f &= \sum_{m(i)=\delta} h_i g_i + \sum_{m(i)<\delta} h_i g_i \\ &= \sum_{m(i)=\delta} LT(h_i) g_i + \sum_{m(i)=\delta} (h_i - LT(h_i)) g_i + \sum_{m(i)<\delta} h_i g_i. \end{aligned} \tag{2.5}$$

Monomi koji se pojavljuju u drugoj i trećoj sumi u drugom redu imaju multistupanj $< \delta$. Prema tome, pretpostavka da $multideg(f) < \delta$ znači da prva suma također ima multistupanj $< \delta$.

Neka je $LT(h_i) = c_i x^{\alpha(i)}$. Tada prva suma $\sum_{m(i)=\delta} LT(h_i) g_i = \sum_{m(i)=\delta} c_i x^{\alpha(i)} g_i$ ima upravo oblik opisan u Lemi 2.5.5 sa $f_i = x^{\alpha(i)} g_i$. Pa Lema 2.5.5 povlači da je ova suma linearna kombinacija S-polinoma $S(x^{\alpha(j)} g_j, x^{\alpha(k)} g_k)$. Međutim,

$$\begin{aligned} S(x^{\alpha(j)}g_j, x^{\alpha(k)}g_k) &= \frac{x^\delta}{x^{\alpha(j)}LT(g_j)}x^{\alpha(j)}g_j - \frac{x^\delta}{x^{\alpha(k)}LT(g_k)}x^{\alpha(k)}g_k \\ &= x^{\delta-\gamma_{jk}}S(g_j, g_k) \end{aligned}$$

gdje je $x^{\gamma_{jk}} = LCM(LM(g_j), LM(g_k))$. Prema tome, postoje konstante $c_{jk} \in k$ takve da je

$$\sum_{m(i)=\delta} LT(h_i)g_i = \sum_{j,k} c_{jk}x^{\delta-\gamma_{jk}}S(g_j, g_k). \tag{2.6}$$

Sljedeći korak je koristiti pretpostavku da je ostatak od $S(g_j, g_k)$ pri dijeljenju sa $g_1, \ldots, g_t$ nula. Koristeći algoritam dijeljenja, ovo znači da svaki S-polinom možemo zapisati u obliku

$$S(g_j, g_k) = \sum_{i=1}^{t} a_{ijk}g_i \tag{2.7}$$

gdje su $a_{ijk} \in k[x_i, \ldots, x_n]$. Algoritam dijeljenja također nam kaže da je

$$mulitdeg(a_{ijk}g_i) \leq multideg(S(g_j, g_k)) \tag{2.8}$$

za sve i, j, k. Intuitivno, ovo znači da kada je ostatak nula, možemo pronaći izraz za $S(g_j, g_k)$ pomoću elemenata od G gdje se vodeći članovi ne poništavaju. Da bi iskoristili ovo, pomnožimo izraz za $S(g_j, g_k)$ sa $x^{\delta-\gamma_{jk}}$ da bi dobili

$$x^{\delta-\gamma_{jk}}S(g_j, g_k) = \sum_{i=1}^{t} b_{ijk}g_i \tag{2.9}$$

gdje je $b_{ijk} = x^{\delta-\gamma_{jk}}a_{ijk}$. Tada (2.8) i Lema 2.5.5 povlače da je

$$multideg(b_{ijk}g_i) \leq multideg(x^{\delta-\gamma_{jk}}S(g_j, g_k)) < \delta. \tag{2.10}$$

Ako zamijenimo gornji izraz sa $x^{\delta-\gamma_{jk}}S(g_j, g_k)$ u (2.6), dobijemo jednakost

$$\sum_{m(i)=\delta} LT(h_i)g_i = \sum_{j,k} c_{jk}x^{\delta-\gamma_{jk}}S(g_j,g_k) = \sum_{j,k} c_{jk}\Big(\sum_i b_{ijk}g_i\Big) = \sum_i \tilde{h}_i g_i \tag{2.11}$$

što po (2.10) ima svojstvo da za sve i vrijedi $multideg(\tilde{h}_i g_i) < \delta$. Za kraj dokaza, zamijenimo $\sum_{m(i)=\delta} LT(h_i)g_i = \sum_i \tilde{h}_i g_i$ u jednadžbi (2.5) da bi dobili izraz za f kao polinomijalnu kombinaciju g_i gdje su svi članovi multistupnja $< \delta$. To je kontradikcija sa minimalnošću od δ i dovršava dokaz teorema. □

Na primjeru ćemo pokazati kako koristiti prethodni teorem. Pogledajmo ideal $I = \langle y - x^2, z - x^3\rangle$. Tvrdimo da je $G = \{y - x^2, z - x^3\}$ Groebnerova baza za I za lex uređaj sa $y > z > x$. Pogledajmo S-polinom

$$S(y - x^2, z - x^3) = \frac{yz}{y}(y - x^2) - \frac{yz}{z}(z - x^3) = -zx^2 + yx^3.$$

Koristeći algoritam dijeljenja dobili smo

$$-zx^2 + yx^3 = x^3(y - x^2) + (-x^2)(z - x^3) + 0$$

tako da je $\overline{S(y - x^2, z - x^3)}^{G} = 0$. Prema Teoremu 2.5.6. G je Groebnerova baza za I.

2.6 Buchbergerov algoritam

Do sada smo naučili da svaki ideal u $k[x_1, \ldots, x_n]$ različit od $\{0\}$ ima Groebnerovu bazu, no nismo naučili kako je konstruirati. Prije samog algoritma za konstrukciju Groebnerove baze pogledajmo sljedeći primjer.

Primjer 2.6.1. *Neka je $I = \langle f_1, f_2\rangle \subseteq k[x, y]$ ideal gdje je $f_1 = x^3 - 2xy$ i $f_2 = x^2y - 2y^2 + x$. Koristit ćemo grlex uređaj. $\{f_1, f_2\}$ nije Groebnerova baza za I jer $LT(S(f_1, f_2)) = -x^2 \notin \langle LT(f_1), LT(f_2)\rangle$. Da bismo napravili Groebnerovu bazu, prirodna ideja je prvo pokušati proširiti originalni generirajući skup do Groebnerove baze dodavanjem još polinoma u I. Koje nove generatore trebamo dodati? Ideja je sljedeća. Imamo $S(f_1, f_2) = -x^2 \in I$ i njegov ostatak pri dijeljenju sa $F = (f_1, f_2)$ je $-x^2$, različit od nule. Dakle, trebali bismo uključiti ostatak u naš generirajući skup, kao novi generator dodajemo $f_3 = -x^2$. Ako*

stavimo $F = (f_1, f_2, f_3)$, možemo koristiti Teorem 2.5.6 za testiranje je li ovaj novi skup Groebnerova baza za I. Računamo

$$\begin{array}{rcl} S(f_1, f_2) & = & f_3, \ pa \\ \overline{S(f_1, f_2)}^F & = & 0, \\ S(f_1, f_3) & = & (x^3 - 2xy) - (-x)(-x^2) = -2xy, \ ali \\ \overline{S(f_1, f_3)}^F & = & -2xy \neq 0. \end{array}$$

Stoga, moramo dodati $f_4 = -2xy$ u naš generirajući skup. Ako stavimo $F = (f_1, f_2, f_3, f_4)$, tada

$$\begin{array}{rcl} \overline{S(f_1, f_2)}^F & = & \overline{S(f_1, f_3)}^F = 0, \\ S(f_1, f_4) & = & y(x^3 - 2xy) - (-\frac{1}{2})x^2(-2xy) = -2xy^2 = yf_4, \ pa \\ \overline{S(f_1, f_4)}^F & = & 0, \\ S(f_2, f_3) & = & (x^2y - 2y^2 + x) - (-y)(-x^2) = -2y^2 + x, \ ali \\ \overline{S(f_2, f_3)}^F & = & -2y^2 + x \neq 0. \end{array}$$

Prema tome, također moramo dodati $f_5 = -2y^2 + x$ u naš generirajući skup. Postavljajući $F = \{f_1, f_2, f_3, f_4, f_5\}$, može se izračunati da je

$$\overline{S(f_i, f_j)}^F = 0 \ za \ sve \ 1 \leq i \leq j \leq 5.$$

Po Teoremu 2.5.6, slijedi da je grlex Groebnerova baza za I dana sa

$$\{f_1, f_2, f_3, f_4, f_5\} = \{x^3 - 2xy, x^2y - 2y^2 + x, -x^2, -2xy, -2y^2 + x\}.$$

Teorem 2.6.2. *Neka je $I = \langle f_1, \ldots, f_s \rangle \neq \{0\}$ polinomijalni ideal. Tada se Groebnerova baza za I može konstruirati konačnim brojem koraka sljedećim algoritmom:*

Input : $F = (f_1, \ldots, f_s)$
Output : *Groebnerova baza* $G = (g_1, \ldots, g_t)$ *za* I, *sa* $F \subseteq G$
$G := F$
repeat
  $G' := G$
  for *za svaki par* $\{p, q\}$, $p \neq q$ *u* G' ***do***

$S := \overline{S(p,q)}^{G'}$
if $S \neq 0$ **then**
$G := G \cup \{S\}$
end if
end for
until $G = G'$

Dokaz. Ako je $G = \{g_1, \ldots, g_t\}$, tada će $\langle G \rangle$ i $\langle LT(G) \rangle$ označavati sljedeće ideale:

$$\langle G \rangle = \langle g_1, \ldots, g_t \rangle,$$

$$\langle LT(G) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle.$$

Prvo pokazujemo da $G \subseteq I$ vrijedi u svakom koraku algoritma. To je istina u početku, i svaki put kad povećamo G činimo to dodavanjem ostatka $S = \overline{S(p,q)}^{G'}$ za $p, q \in G$. Prema tome, ako je $G \subseteq I$, tada p, q i stoga $S(p,q)$ su u I, i kako dijelimo sa $G' \subseteq I$, dobijemo $G \cup \{S\} \subseteq I$. Također napomenimo da G sadrži danu bazu F od I tako da je G zapravo baza od I.

Algoritam završava kada je $G = G'$, što znači da $\overline{S(p,q)}^{G} = 0$ za sve $p, q \in G$. Prema tome, G je Groebnerova baza od $\langle G \rangle = I$ po Teoremu 2.5.6.

Ostaje pokazati da algoritam završava. Moramo razmotriti što se dogodi nakon svakog prolaza kroz glavnu petlju. Skup G se sastoji od G'(stoga G) zajedno sa nenul ostacima od S polinoma elemenata od G'. Tada je

$$\langle LT(G') \rangle \subseteq \langle LT(G) \rangle \tag{2.12}$$

zbog $G' \subseteq G$. Nadalje, ako je $G' \neq G$, tvrdimo da je $\langle LT(G') \rangle$ strogo manji od $\langle LT(G) \rangle$. Da bismo to vidjeli, pretpostavimo da je ostatak $r \neq 0$ S-polinoma pridružen u G. Jer je r ostatak pri dijeljenju sa G', $LT(r)$ nije dijeljiv s vodećim članovima elemenata od G', i prema tome, $LT(r) \notin \langle LT(G') \rangle$. Još $LT(r) \in \langle LT(G) \rangle$, što dokazuje našu tvrdnju.

Po (2.12), ideali $\langle LT(G') \rangle$ iz uzastopnih ponavljanja iz petlje čine uzlazni lanac ideala u $k[x_1, \ldots, x_n]$. Prema tome, Teorem 2.4.7 povlači da poslije konačnog broja iteracija lanac će se stabilizirati, tako da $\langle LT(G') \rangle = \langle LT(G) \rangle$ mora biti na kraju. Po prethodnom paragrafu, ovo povlači da je $G' = G$, tako da algoritam mora završiti nakon konačnog broja koraka. □

Groebnerove baze izračunate koristeći prethodni algoritam često su veće nego što je potrebno. Možemo eliminirati neke nepotrebne generatore koristeći sljedeću činjenicu.

Lema 2.6.3. *Neka je G Groebnerova baza za polinomijalni ideal I. Neka je $p \in G$ polinom takav da je $LT(p) \in \langle LT(G - \{p\}) \rangle$. Tada je $G - \{p\}$ također Groebnerova baza za I.*

Dokaz. Znamo da je $\langle LT(G)\rangle = \langle LT(I)\rangle$. Ako $LT(p) \in \langle LT(G - \{p\})\rangle$, tada je $\langle LT(G - \{p\})\rangle = \langle LT(G)\rangle$. Po definiciji, slijedi da je $G - \{p\}$ također Groebnerova baza za I. □

Definicija 2.6.4. ***Minimalna Groebnerova baza*** *za polinomijalni ideal I je Groebnerova baza G za I ako je*

(i) $LC(p) = 1$ *za sve* $p \in G$,

(ii) za sve $p \in G$, $LT(p) \notin \langle LT(G - \{p\})\rangle$.

Minimalnu Groebnerovu bazu za dani ideal I možemo konstruirati koristeći Teorem 2.6.2 i prethodnu lemu za eliminiranje nepotrebnih generatora koji su možda bili uključeni. Iskoristit ćemo prethodni primjer za računanje minimalne Groebnerove baze. Koristeći grlex uređaj, izračunali smo Groebnerovu bazu

$$\begin{aligned} f_1 &= x^3 - 2xy, \\ f_2 &= x^2y - 2y^2 + x, \\ f_3 &= -x^2, \\ f_4 &= -2xy, \\ f_5 &= -2y^2 + x. \end{aligned}$$

Primjetimo da su neki od vodećih koeficijenata generatora različiti od 1, tada te generatore moramo pomnožiti odgovarajućim koeficijentima. Dalje, primjetimo da je

$$\begin{aligned} LT(f_1) &= x^3 = -x \cdot LT(f_3), \\ LT(f_2) &= x^2y = -\frac{1}{2}x \cdot LT(f_4). \end{aligned}$$

Po Lemi 2.6.3 možemo eliminirati f_1 i f_2. Nemamo više slučajeva gdje vodeći član generatora dijeli vodeći član drugog generatora. Prema tome,

$$\begin{aligned} \tilde{f_3} &= x^2, \\ \tilde{f_4} &= xy, \\ \tilde{f_5} &= y^2 - \tfrac{1}{2}x \end{aligned}$$

je minimalna Groebnerova baza za I.

Međutim, dani ideal može imati puno minimalnih Groebnerovih baza. Lako se može provjeriti da je

$$\hat{f}_3 = x^2 + axy,\ \tilde{f}_4 = xy,\ \tilde{f}_5 = y^2 - \frac{1}{2}x$$

također minimalna Groebnerova baza, gdje je $a \in k$ bilo koja konstanta. Srećom, možemo izdvojiti jednu minimalnu bazu koja je bolja od ostalih. Slijedi definicija.

Definicija 2.6.5. ***Reducirana Groebnerova baza*** *za polinomijalni ideal I je Groebnerova baza G za I ako vrijedi*

(i) $LC(p) = 1$ *za sve* $p \in G$,

(ii) za sve $p \in G$, *nijedan monom od* p *ne leži u* $\langle LT(G - \{p\})\rangle$.

Primjetimo da u prethodnom primjeru jedino za $a = 0$ dobivamo reduciranu Groebnerovu bazu.

Propozicija 2.6.6. *Neka je* $I \neq \{0\}$ *polinomijalni ideal. Tada, za dani monomijalni uređaj, I ima jedinstvenu reduciranu Groebnerovu bazu.*

Bibliografija

[1] David Cox, *John Little, and Donal O'Shea. Ideals, varieties, and algorithms. Undergraduate Texts in Mathematics*, Springer-Verlag, New York,, 1997.

Sažetak

U ovom radu dokazali smo algoritam za dijeljenje polinoma u više varijabli s obzirom na fiksni monomijalni uređaj. Algoritam smo dobili proširenjem algoritma dijeljenja polinoma u jednoj varijabli. Vidjeli smo da ostatak nije jedinstveno okarakteriziran kao u slučaju jedne varijable. Uvođenjem Groebnerovih baza pokazali smo da algoritam postiže puni potencijal kada je u paru s Groebnerovim bazama. Zatim, smo vidjeli da svaki nenul ideal u prstenu polinoma ima Groebnerovu bazu, te smo naučili kako provjeriti je li dana baza Groebnerova. Pokazali smo kako pomoću algoritma dijeljenja i Groebnerovih baza provjeriti pripadnost polinoma idealu. Na kraju, pokazali smo kako Buchbergerovim algoritmom konstruirati Greobnerovu bazu.

Summary

In this thesis, we have proved the division algorithm for polynomials in several variables with respect to a fixed monomial order. We have got this algorithm by extending the division algorithm for polynomials in one variable. It was shown that the remainder is not uniquely characterized as in the case of one variable. By introduction Groebner's basis we have shown that the algorithm achieves full potential when it is paired with Groebner basis. Also, every nonzero ideal in a polynomial ring has Groebner base, and we learned how to check whether the base is Groebner. We showed by using a division algorithm and Groebner basis how to check if polynomial lies in the ideal. Finally, we showed how to construct Groebner base with Buchberger's algorithm.

Životopis

Rođena sam 29. prosinca 1987. godine u Zagrebu. 2002. godine završila sam osnovnu školu te sam upisala Ekonomsku školu Velika Gorica, smjer ekonomist. 2006. godine sam sudjelovala na državnom natjecanju iz područja računovodstva i knjigovodstva s bilanciranjem. Iste godine upisujem Prirodoslovno-matematički fakultet, Matematički odsjek Sveučilišta u Zagrebu. Nakon završenog preddiplomskog studija matematike upisujem Diplomski sveučilišni studij Financijske i poslovne matematike na istom odsjeku.