Univerzitet u Beogradu
Elektrotehnički fakultet

Master rad

JAVA APLETI ZA VIZUELIZACIJE U TEORIJI GREBNER-OVIH BAZA

Mentor:
Dr. Branko Malešević, doc.

Student:
Bojan Banjac
Br. indeksa: 2010/3153

Beograd, septembar 2011

Sadržaj

Uvod

Inženjerska struka je od samog početka bila vezana za matematiku. Već u srednjem veku je bilo jasno da bez temeljnog poznavanja matematike nije moguće precizno izvesti zaključke iz usvojenih saznanja. Sa daljim razvojem prirodnih nauka ovo je bilo sve vidljivije. Nijedan zakon fizike nije mogao proći kao definicija ako nije bio jasno definisan kao matematička formula. Hemijski ogledi su konstantno koristili procentni račun. Arhitekte su se oslanjale na formule koje su im prikazivale parametre objekta koji grade. U današnje vreme, kada se primena ovih nauka ogleda u inženjerskim disciplinama, nemoguće je zamisliti obrazovanog stručnjaka koji nema makar dobre osnove u matematici.

Ovo je dovelo do toga da svaki fakultet u svetu svoje inženjerske kurseve započinje na matematici. Ipak, od samih početaka pa do danas je došlo do velikog pomaka u metodama. Dok je pre sto godina matematika bilo objašnjavana putem primera, auditivnih predavanja, i vežbanja algoritama za rešavanje zadataka unutar stručne literature, danas je dostupan daleko širi asortiman pomagala. Studentima je dostupan širi izbor literature putem interneta. Komunikacija sa nastavnicima se odvija daleko efikasnije zbog pojave emaila. Predavanja se više ne vrše samo kredom i tablom, već postoji veliki broj pomagala koja korišćenjem mogućnosti kompjutera vizuelno predstavljaju pojmove. Mnogi kompjuterski sistemi studentima omogućavaju proveru rezultata proračuna.

Aplikacije koje su razvijene u okviru ovog master rada su kreirane kao pomoćno nastavno sredstvo. Buchbegerov algoritam, koji je korišćen u nekoliko njih, danas je jedan od standardnih načina rešavanja sistema jednačina, i koristi se u većini sistema kompjuterske algebre. Zbog svoje važnosti ovaj algoritam se predaje na većini fakulteta sa višim kursevima matematike. Ipak, postoji veoma mali broj aplikacija koje prikazuju način funkcionisanja ovog algoritma, i načine njegove primene. Namera autora je bila da se kreira aplikacija koja će moći da prikaže način funkcionisanja ovog algoritma i grafički prikaže određene elemete ove oblasti matematike, kako bi studentima približio ovu oblast.

U okviru prve glave ovog rada je dat prikaz teorije na osnovu koje su bazirane aplikacije. Buchbergerov algoritam pripada oblasti simboličke algebre, te su date osnove teoreme i definicije koje spadaju u ovu oblast. Takođe je prikazana jedna od primena Buchbergerovog algoritma, odnosno teorija na kojoj se ona zasniva, kako bi u okviru prikaza aplikacija bilo definisano na čemu se bazira.

Glava I : Grebnerove baze i Buchbergerov algoritam

U današnjim matematičkim kompjuterskim sistemima možemo sresti rešenja za mnoge složene proračune. Kao jedna od najpraktičnijih metoda za nalaženje rešenja sistema polinomijalnih jednačina u većini sistem možemo sresti Grebnerove baze. Teoriju Grebnerovih baza je još 1932. predstavio Wolfgang Gröbner u okviru svoje doktorske disertacije *Ein Beitrag zum Problem der Minimalbasen.* U toku svog daljeg rada on se bavio računskom algebrom, ali je teorija koju je predstavio dobila ime Grebnerove baze tek 1965. godine kada je student Wolfganga Gröbnera Bruno Buchberger u svojoj doktorskoj disertaciji *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenrings nach einem nulldimensionalen Polynomideal* po svom mentoru imenovao pojam Grebnerovih baza. Buchberger je u tom radu takođe definisao algoritam dalje poznat kao Buchbergerov algoritam, kojim se može doći do Grebnerove baze. Ovaj algoritam se u modifikovanoj varijanti javlja i danas u većini sistema kompjuterske algebre, i predstavlja veoma efikasno rešenje za veliki broj problema sa kojim se programeri pri kreiranju takvih sistema mogu sresti.

1. Ideali prstena

Definicija 1.1 Neka je **R**$=(R,+,\cdot)$ prsten, tada podskup $I \subseteq R$ određuje ideal prstena ukoliko je ispunjeno:

a) $(\forall x \in I)(\forall y \in I)x - y \in I$
b) $(\forall x \in I)(\forall r \in R)r \cdot x, x \cdot r \in I$

Teorema 1.2 Neka je **R**$=(R,+,\cdot)$ prsten i neka su $I, J \subseteq R$ ideali prstena R. Tada sledeći skupovi predstavljaju ideale u prstenu R:

a) $I + J = \{r \mid r = x + y \wedge x \in I \wedge y \in J\}$
b) $I \cdot J = \{r \mid (\exists n \in N)r = \sum_{i=1}^{n} x_i y_i \wedge (x_i)_{i=1}^{n} \subseteq I, (y_i)_{i=1}^{n} \subseteq J\}$
c) $I \cap J = \{r \mid r \in I \wedge r \in J\}$
d) $I : J = \{r \mid r(\forall y \in J)r \cdot y, y \cdot r \in I\}$

Teorema 1.3 Neka je **R**$=(R,+,\cdot)$ prsten i neka su $I, J, M \subseteq R$ u idelu prstena. Tada važi:

a) $I \cdot J \subseteq I \bigcap J$
b) $(I \cap M) + (J \cap M) \subseteq (I + J) \cap M$
c) $(I : M) + (J : M) \subseteq (I + J) : M$
d) $I : (J + M) = (I : J) \cap (I : M)$

Teorema 1.4 Neka je **R**=$(R,+,\cdot)$ prsten i neka je $A \subseteq R$ podskup. Tada skup konačnih suma:

1. $I = \{r \mid r = \sum_{i=1}^{n} x_i a_i y_i + \sum_{j=1}^{m} k_j b_j \wedge (x_i)_{i=1}^{n}, (y_i)_{i=1}^{n} \subseteq R \wedge (a_i)_{i=1}^{n}, (b_j)_{j=1}^{m} \subseteq A \wedge (k_j)_{j=1}^{m} \subseteq Z\}$

Određuje jedan ideal prstena **R**. Posebno ako je **R** komutativni prsten sa jedinicom, tada ideal I se može predstaviti sledećim skupom:

2. $I = \{r \mid r = \sum_{i=1}^{n} x_i a_i \wedge (x_i)_{i=1}^{n} \subseteq R \wedge (a_i)_{i=1}^{n} \subseteq A\}$

Definicija 1.5 U prethodnoj teoremi ideal I nazivamo ideal generisan skupom A, što zapisujemo $I = \langle A \rangle$ .Pri tom ideal I određen sa (1) nazivamo dvostranim idealom, a ideal I određen sa (2) nazivamo dvostranim idealom.

Teorema 1.6 Neka su u prstenu **R**=$(R,+,\cdot)$ dati ideali I i J generisani skupovima $A \subseteq R$ i $B \subseteq R$ respektivno. Tada važi:

a) $I + J = \langle A \cup B \rangle$

b) $I \cdot J = \langle \{a \cdot b \mid a \in A \wedge b \in B\} \rangle$

Napomena 1.7 Ideal $I \cap J$ je najveći ideal sadržan u idealima I i J. Unija dva ideala $I \cup J$ ne mora biti ideal, međutim ideal $I + J$ je najmanji ideal koji sadrži ideale I i J. Odatle skup ideala nekog prstena u odnosu na presek i sumu ideala predstavlja mrežu.

Napomena 1.8 Za ma koji rastući lanac ideala $I_1 \subseteq I_2 \subseteq \ldots$ unija $J' = \bigcup_{k=0}^{\infty} J_k$ određuje jedan ideal.

Teorema 1.9 Neka je **R**=$(R,+,\cdot)$ prsten. Tada su sledeći iskazi međusobno ekvivalentni.

a) Svaki ideal I prstena **R** je generisan konačnim skupom.

b) Svaki rastući lanac ideala $I_1 \subseteq I_2 \subseteq \ldots$ prstena **R** postaje stacionaran, tj. Važi $I_m = I_{m+1} = \ldots$ počev od nekog m.

Definicija 1.10 Prsten **R**=$(R,+,\cdot)$ koji ispunjava bilo koji uslov prethodne teoreme naziva se Noetherin prsten.

2. Prsten polinoma

Neka je **K**=$(K,+,\cdot)$ polje. Ako je x promenjiva nad K i ako su $a_0, a_1 ... a_n \in K$ elementi polja takvi da $a_n \neq 0$ uobičajeno je da se izraz $a_n x^n + ... + a_1 x + a_0$ naziva polinomom stepena n po promenjivoj x. Drugi način definisanja polinoma je definisanje nizom koeficijenata $(a_0, a_1, ..., a_n, ...)$ gde su $a_i \in K (i = 0,1,....)$ elementi polja takvi da vaši postoji n takvo da $a_i = 0$ za $i > n$.

Neka je dat polinom P nizom koeficienata, tada stepen polinoma *dg(P)* je najveći broj n takav da $a_n \neq 0$. Tada elemente $a_0, a_1 ... a_n \in K$ nazivamo koeficientima polinoma, a koeficijent a_n nazivamo vodeći koeficijent polinoma. Dalje, za polinom P dat se beskonačnim nizom koeficijenata koristimo zapis konačnim nizom $(a_0, a_1, ..., a_n)$ podrazumevajući da $a_i = 0$ za $i > n$. Jedinica polja $1 \in K$ može se poistovetiti sa polinomom (1) nultog stepena i uopšte svaki element polja $c \in K$ može se poistovetiti sa polinomom (c) nultog stepena. Polinom $x = (0,1)$ nazivamo promenljivom. Uvedimo skup polinoma jedne promenljive:

$$K[x] = \{P = P(x) \mid p - polinom\ nad\ K\}$$

U skupu $K[x]$ uvedimo binarne operacije:

a) $(a_0, a_1, ..., a_i, ...) + (b_0, b_1, ..., b_i, ...) = (a_0 + b_0, a_1 + b_1, ..., a_i + b_i, ...)$

b) $(a_0, a_1, ..., a_i, ...) \cdot (b_0, b_1, ..., b_i, ...) = (c_0, c_1, ..., c_i, ...)$
gde je $c_i = \sum_{j=0}^{i} a_j a_{b-j} (i = 0,1,2,...)$

Dva polinoma su jednaka ako imaju jednake koeficijente. Prethodna definicija jednakosti polinoma se podudara sa jednakošću dve uređene n-torke.

Teorema 2.1 Neka je **K**=$(K,+,\cdot)$ polje, tada je **K**[x]= $(K[x],+,\cdot)$ komutativan prsten sa jedinicom bez delitelja nule.

Napomena 2.2 Prethodna teorema važi ukoliko je **K** komutativan prsten sa jedinicom bez delitelja nule, tada je je **K**[x]= $(K[x],+,\cdot)$ takođe komutativan prsten sa jedinicom bez delitelja nule.

Teoreme 2.3 Ako su dva polinoma nad poljem **K** jednaka tada su jednake i odgovarajuće polinomske funkcije. Obratno tvrđenje važi za beskonačno polje K.

Teorema 2.4 Ako je dato konačno polje Galoisa K=GF(m) sa $m = p^n$ elemenata (za p-prost broj i $n \in N$). Ako su data dva polinoma P_r i Q_s stepena r i s respektivno, pri

čemu je ispunjeno: $m > \max\{r,s\}$, tada su polinomi P_r i Q_s sa jednakim koeficijentima ako i samo ako su im jednake odgovarajuće polinomske funkcije.

Teorema 2.5 Neka su dati polinomi $P,Q,\in K[x]$ gde Q nije nula polinom, nad prstenom $K[x]$. Tada postoje jedinstveno određei polinomi $G,R \in K[x]$ takvi da važi $P = G \cdot Q + R$, takvi da $dg(R) < dg(Q)$ ili R=0.

Teorema 2.6 Neka je I ideal u prstenu polinoma $K[x]$, tada je ideal I generisan jednim elementom, tj. postoji polinom $g \in K[x]$ takav da važi $I = \langle\{g\}\rangle$. Na osnovu ovoga zaključujemo da je algebarska struktura **K**[x]= $(K[x],+,\cdot)$ Noetherin prsten.

Neka je **K**=$(K,+,\cdot)$ polje. Polazeći od prstena polinoma jedne pomenljive $K[x]$, saglasno sa napomenom 2.2, prsten polinoma više promenljivih definišemo induktivno:

$$\mathbf{K}[x_1,...,x_n] = (K[x_1,...,x_{n-1}])[x_n]$$

Teorema 2.7 Neka je **K**=$(K,+,\cdot)$ polje, tada za svako $n \in N$ algebarska struktura $\mathbf{K}[x_1,...,x_n]=(K[x_1,...,x_n],+,\cdot)$ je komutativan prsten sa jedinicom bez delitelja nule.

Teorema 2.8 U prstenu polinoma jedne i više promenljivih, usled komutativnosti i postojanja jedinice, svi ideali su jednostrani

Neka je dat polinom $P = P(x_1,...,x_n) \in K[x_1,...,x_n]$, tada važi jednakost:

$$P(x_1,...,x_n) = \sum_{\alpha \in A_0} c_\alpha x_1^{\alpha_1}...x_n^{\alpha_n}$$

gde je $A_0 \subset N_0^n$ konačan skup n-torki $\alpha = (\alpha_1,...,\alpha_n)$ prirodnih brojeva i gde je $c_\alpha \in K \setminus \{0\}$. Izrazi $M_\alpha = x_1^{\alpha_1}...x_n^{\alpha_n}$ u prethodnoj sumi nazivaju se monomima. Samim tim, polinom P predstavlja linearnu kombinaciju monoma nad poljem K. Pojedinačne sabirke $c_\alpha x_1^{\alpha_1}...x_n^{\alpha_n}$ za $\alpha \in A_0$, koji učestvuju u polinomu P nazivamo još i termima polinoma. Dalje, n-torku $\alpha = (\alpha_1,...,\alpha_n)$ nazivamo multistepen monoma, a sumu eksponenata $\sum_{k=1}^{n} \alpha_k$ određuje stepen monoma, koji označavamo $dg(M)$. Primetimo da se jedinica polja $1 \in K$ može predstaviti na jedinstven način kao monom $1 = x_1^0...x_n^0$, dakle kao monom nultog multistepena **0**=(0,.....,0)

3. Monomijalni ideali

Neka je $M_\alpha = x_1^{\alpha_1}...x_n^{\alpha_n}$ monom u prstenu polinoma više promenljivih $\mathbf{K}[x_1,...,x_n]$ gde je $\alpha = (\alpha_1,...,\alpha_n) \in N_0^n$ multistepen. Tada koristimo kraći zapis $x^\alpha = x_1^{\alpha_1}...x_n^{\alpha_n}$.
Za skup multistepenova $A \subseteq N_0^n$ skup monoma $\{x^\alpha : \alpha \in A\}$ određuje ideal generisan tim skupom monoma $I = \langle x^\alpha : \alpha \in A \rangle$. Takav ideal se naziva monomijani ideal i on se može odrediti kao skup konačnih suma :

$$I = \{ \sum_{\alpha \in A_0} q_\alpha x^\alpha : q_\alpha \in K[x_1,..., x_n] \wedge \alpha \in A_0 \wedge A_0 \in A \}$$

Teorema 3.1 Neka su $x_1^{\alpha_1}...x_n^{\alpha_n}$ monomi u prstenu polinoma više promenljivih $\mathbf{K}[x_1,...,x_n]$ sa međusobno različitim stepenima. Tada je skup monoma $\{x_1^{\alpha_1}...x_n^{\alpha_n}\}$ linearno nezavistan skup.

Teorema 3.2 Neka je za skup multistepenova $A \subseteq N_0^n$ u prstenu polinoma više promenljivih $\mathbf{K}[x_1,...,x_n]$ određen monomijalni ideal $I = \langle x^\alpha : \alpha \in A \rangle$. Tada za multistepen $\beta = (\beta_1,...,\beta_n) \in N_0^n$ važi $x^\beta \in I$ ako i samo ako $(\exists \alpha \in A) x^\alpha \mid x^\beta$.

Teorema 3.3 Neka je skup multistepenova $A \subseteq N_0^n$ u prstenu polinoma više promenljivih $\mathbf{K}[x_1,...,x_n]$ određen monomijalni ideal $I = \langle x^\alpha : \alpha \in A \rangle$. Tada za polinom $P = \sum_{k=1}^{m} b_k x^{\beta k} \in K[x_1,...,x_n](b_k \in K \setminus \{0\} \wedge b_k \in N_0^n)$ važi $\sum_{k=1}^{m} b_k x^{\beta k} \in I \Rightarrow (\forall k) x^{\beta k} \in I$

Teorema 3.4 U prstenu polinoma više promenljivih $\mathbf{K}[x_1,...,x_n]$ dva monomijalna ideala su jednaka ako i samo ako se sastoje od jednakih skupova monoma.

Definicija 3.5 Neka su data dva monoma x^α i x^β iz prstena polinoma više promenljivih $\mathbf{K}[x_1,...,x_n]$. Najveći zajednički delilac (GCD) prethodnih monoma je sledeći monom $x^\gamma = GCD(x^\alpha, x^\beta)$, takav da je $(\forall k \in \{1,....n\})\gamma_k = \min\{\alpha_k, \beta_k\}$

Definicija 3.6 Najmanji zajednički sadržalac prethodno posmatranih monoma je sledeći monom $x^\delta = LCM(x^\alpha, x^\beta)$, takav da je $(\forall k \in \{1,....n\})\delta_k = \max\{\alpha_k, \beta_k\}$

Teorema 3.7 Neka su $I = \langle m_1,...,m_r \rangle$ i $J = \langle n_1,...,n_s \rangle$ dva monomijalna ideala u prstenu polinoma više promenljivih **K**[$x_1,...,x_n$]. Tada važi:

a) $I + J = \langle m_1,...,m_r, n_1,...,n_s \rangle$

b) $I \cap J = \sum_{i=1}^{r} \sum_{j=1}^{s} \langle GCD(m_i, n_j) \rangle$

c) $I \cdot J = \langle m_1 n_1,..., m_1 n_s, m_2 n_1,..., m_r n_s \rangle$

d) $I : J = \bigcap_{j=1}^{s} \left\langle \frac{m_1}{LCM(m_1, n_j)},..., \frac{m_r}{LCM(m_r, n_j)} \right\rangle$

Teorema 3.8 Diksonova lema[1](Mašević,2000) Svaki monomijalni ideal $I = \langle x^\alpha : \alpha \in A \rangle$ gde je $A \subseteq N_0^n$ u prstenu polinoma više promenljivih **K**[$x_1,...,x_n$] je konačno generisan ideal.

4. Monomijalni poretci

Za neprazan skup $S \neq 0$ relacija dužine n je neprazan podskup $\rho \subseteq S^n$. Ukoliko je relacija dužine $n = 2$, tu relaciju nazivamo binarna relacija. Osobine relacija mogu biti:

a) Refleksivnost: $(\forall x \in S)\ x \rho x$
b) Simetričnost: $(\forall x, y \in S)\ x \rho y \Rightarrow y \rho x$
c) Antisimetričnost: $(\forall x, y \in S)\ x \rho y \wedge y \rho x \Rightarrow x = y$
d) Tranzitivnost: $(\forall x, y, z \in S)\ x \rho y \wedge y \rho z \Rightarrow x \rho z$

Definicija 4.1 Binarna relacija koja refleksivna, simetrična i tranzitivna se naziva relacija ekvivalencije.

Definicija 4.2 Binarna relacija koja je refleksivna, antisimetrična i tranzitivna naziva se relacija poretka.

Definicija 4.3 Binarna relacija je totalna ili linearna ako važi $(\forall x, y \in S)\ x \rho y \vee y \rho x$

Definicija 4.4 Binarna relacija koja je totalna, antisimetrična i tranzitivna naziva se relacijom totalnog poretka. Za relaciju totalnog poretka ρ nad skupom S uobičajeno je da koristimo oznaku $\succeq$, i tada je za svaka dva elementa $x, y \in S$ moguće izvršiti poređenje elemenata $x \succeq y$ ili $y \succeq x$

Defininicija 4.5 Element $a \in A \subseteq S$ je minimalni element skupa $A \subseteq S$ ako važi $(\forall \alpha \in A)(a \succ \alpha \Rightarrow \alpha = a)$

Definicija 4.6 Binarna relacija totalnog poretka nad skupom S je relacija dobrog uređenja ukoliko svaki neprazan podskup $A \subseteq S$ ima minimalni element $a = \min(A)$.

Definicija 4.7 Na skupu N_0^n relacija $\succeq$ naziva se relacijom monomijalnog poretka ako ispunjava sledeće uslova:

a) $\succeq$ je relacija totalnog poretka na N_0^n
b) $(\forall \alpha, \beta, \gamma \in N_0^n)\alpha \succeq \beta \Rightarrow \alpha + \gamma \succeq \beta + \gamma$
c) $\succeq$ je relacija dobrog uređenja na N_0^n

Lema 4.8 Dicksonova lema je ekvivalentna tvrđenju da u skupu monoma ne postoji beskonačan opadajući niz monoma u odnosu na fiksirani monomijalni poredak $\succeq$

Definicija 4.8 [1](Malešević,2000) Relacija leksikografskog poretka $\succ_{lex}$ na skupu N_0^n uvodimo na način koji sleduje. Za $\alpha, \beta \in N_0^n$ smatramo da je $\alpha \succ_{lex} \beta$ ako je u vektoru razlike $\gamma = \alpha - \beta \in Z^n$ prva nenulta pozicija sa leve strane pozitivna . Tada takođe pišemo i $x^\alpha \succ_{lex} x^\beta$, čime prenosimo relaciju $\succ_{lex}$ na skup monoma više promenljivih.

Teorema 4.9 Relacija leksikografskog poretka $\succ_{lex}$ je relacija monomijalnog poretka

Primer 4.10 U leksikografskom poretku važi:

a) $x \succ_{lex} y \succ_{lex} z$ jer je $(1,0,0) \succ_{lex} (0,1,0) \succ_{lex} (0,0,1)$
b) $xy^2 \succ_{lex} y^3z^4$ jer je $\alpha = (1,2,0) \succ_{lex} \beta = (0,3,4)(\alpha - \beta = (\underset{(>0)}{1}, -1, -4))$
c) $x^3y^2z^4 \succ_{lex} x^3y^2z$ jer je $\alpha = (3,2,4) \succ_{lex} \beta = (3,2,1)(\alpha - \beta = (0,0, \underset{(>0)}{3}))$

Definicija 4.11 Relaciju obrnutog leksikografskog poretka $\succ_{invlex}$ na skupu N_0^n uvodimo na način koji sleduje. Za $\alpha, \beta \in N_0^n$ smatramo da je $\alpha \succ_{invlex} \beta$ ako je u vektoru razlike $\gamma = \alpha - \beta \in Z^n$ poslednja nenulta pozicija sa desne strane pozitivna. Tada takođe pišemo i $x^\alpha \succ_{invlex} x^\beta$, čime prenosimo relaciju $\succ_{invlex}$ na skup monoma više promenljivih.

Teorema 4.12 Relacija obrnutog leksikografskog poretka $\succ_{invlex}$ je relacija monomijalnog poretka.

Primer 4.13 U obrnutom leksikografskom poretku važi:

a) $z \succ_{invlex} y \succ_{invlex} x$ jer je $(0,0,1) \succ_{invlex} (0,1,0) \succ_{invlex} (1,0,0)$
b) $y^3z^4 \succ_{invlex} xy^2$ jer je $\alpha = (0,3,4) \succ_{invlex} \beta = (1,2,0)(\alpha - \beta = (-1,1, \underset{(>0)}{4}))$
c) $x^5y^3z \succ_{invlex} x^3y^2z^1$ jer je $\alpha = (5,3,1) \succ_{invlex} \beta = (3,2,1)(\alpha - \beta = (2, \underset{>0}{1}, 0))$

Definicija 4.14 Relaciju gradiranog leksikografskog poretka $\succ_{grlex}$ na skupu N_0^n uvodimona način koji sledjuje. Za $\alpha, \beta \in N_0^n$ smatramo da je $\alpha \succ_{grlex} \beta$ ako je tačno $(|\alpha| = \sum_{i=1}^{n} \alpha_i > |\beta| = \sum_{i=1}^{n} \beta_i) \vee (|\alpha| = |\beta| \wedge \alpha \succ_{lex} \beta)$. Tada takođe pišemo i $x^{\alpha} \succ_{grlex} x^{\beta}$, čime prenosimo relaciju $\succ_{grlex}$ na skup monoma više promenljivih.

Teorema 4.15 Relacija gradiranog leksikografskog poretka $\succ_{grlex}$ je relacija monomijalnog poretka.

Primer 4.16 U gradiranom leksikografskom poretku važi:

a) $x \succ_{grlex} y \succ_{grlex} z$ jer je $(1,0,0) \succ_{grlex} (0,1,0) \succ_{grlex} (0,0,1)$

b) $y^3 z^4 \succ_{grlex} xy^2$ jer je $\alpha = (0,3,4) \succ_{grlex} \beta = (1,2,0)(|\alpha| = 7 > 3 = |\beta|)$

c) $x^3 y^4 z^2 \succ_{grlex} x^3 y^2 z^4$ jer je
$\alpha = (3,4,2) \succ_{grlex} \beta = (3,2,4)(|\alpha| = 9 = |\beta| \wedge \alpha - \beta = (0, \underset{(>0)}{2}, -2))$

Definicija 4.17 Definišimo relaciju $\alpha \succeq_{rinvlex} \beta$ ako i samo ako $\beta \succeq_{invlex} \alpha$ (sa uslovom da je u vektoru razlike: $\gamma = \alpha - \beta \in Z^n$ poslednja nenulta koordinata negativna). Relacija $\succeq_{rinvlex}$ nije relacija monomijalnog poretka i služi za definisanje gradiranog obrnutog leksikografskog poretka. Za $\alpha, \beta \in N_0^n$ smatramo da važi $\alpha \succeq_{grevlex} \beta$ ukoliko je tačna disjunkcija $(|\alpha| = \sum_{i=1}^{n} \alpha_i > |\beta| = \sum_{i=1}^{n} \beta_i) \vee (|\alpha| = |\beta| \wedge \alpha \succeq_{rinvlex} \beta)$. Tada takođe u skupu monoma važi $x^{\alpha} \succeq_{grevlex} x^{\beta}$

Teorema 4.18 Relacija obrnutog gradiranog leksikografskog poretka $\succ_{grevlex}$ je relacija monomijalnog poretka.

Primer 4.19 U obrnuto gradiranom leksikografskom poretku važi:

a) $z \succ_{grevlex} y \succ_{grevlex} x$ jer je $(0,0,1) \succ_{grevlex} (0,1,0) \succ_{grevlex} (1,0,0)$

b) $y^3 z^4 \succ_{grevlex} xy^2$ jer je $\alpha = (0,3,4) \succ_{grlex} \beta = (1,2,0)(|\alpha| = 7 > 3 = |\beta|)$

c) $x^3 y^4 z^2 \succ_{grevlex} x^3 y^2 z^4$ jer je
$\alpha = (3,4,2) \succ_{grevlex} \beta = (3,2,4)(|\alpha| = 9 = |\beta| \wedge \alpha - \beta = (0,2, \underset{(<0)}{-2}))$

Neka je fiksiran jedan monomijalni poredak $\succ$ i neka je u prstenu polinoma više pormenljivih $\mathbf{K}[x_1,...,x_n]$ dat polinom $P = \sum_{k=0}^{m} c_k x^{\alpha_k}$ za neke monome x^{α_k} i neke koeficijente $c_k \in K (k = 0,1,...,m)$. Smatramo da je polinom P sređen u datom monomijalnom poretku $P = c_{\pi 0} x^{\alpha_{\pi 0}} + ... + c_{\pi m} x^{\alpha_{\pi m}}$ ako za neku permutaciju π skupa

indeksa $I_m = \{0,1,...,m\}$ ispunjeno $\alpha_{\pi 0} \succ \alpha_{\pi 1} \succ ... \succ \alpha_{\pi m}$ tj. ako su termovi polinoma P zapisani u opadajućem poretku multistepena. Svaki polinom se može srediti u datom poretku. Tada definišemo polinom P pojmove koji su vezani za sređivanje polinoma u datom monomijalnom poretki:

a) multistepen: $MD(P) = \alpha_{\pi 0}$
b) vodeći koeficijent: $LC(P) = c_{\pi 0}$
c) vodeći monom: $LM(P) = x^{\alpha_{\pi 0}}$
d) vodeći term: $LT(P) = c_{\pi 0} x^{\alpha_{\pi 0}}$

5. Deljenje u prstenu više promenljivih i redukcija polinoma

Teorema 5.1 Ideali u prstenu polinoma više promenljivih $\mathbf{K}[x_1,...,x_n]$ za $n \geq 2$ u opštem slučaju nisu generisani jednim elementom.

Algoritam deljenja

Input: $f_1, \ldots, f_k, f$
Output: $a_1, \ldots, a_k, r$
$a_1 := 0, \ldots, a_k := 0, r := 0$
$p := f$
WHILE $p \neq 0$ *DO*
    $i := 1$
    divisionoccured := false
    WHILE $i \leq k$ *and divisionoccured = false DO*
        IF $LT(f_i)$ *divides* $LT(p)$ *THEN*
            $a_i := a_i + LT(p)/LT(f_i)$
            $p := p - LT(p)/LT(f_i) \cdot f_i$
            divisionoccured := true
        ELSE
            $i := i + 1$
    IF divisionoccured = false THEN
        $r := r + LT(p)$
        $p := p - LT(p)$
(STOP)

Teorema 5.2 Neka je data k-torka polinoma $F = (f_1 ... f_k)$ gde su polinomi $f_i \in K[x_1,...,x_n]$ svaki za sebe sređeni u istom monomijalnom poretku $\succ (i = 1,..,k)$. Tada primenom gore navedenog algoritma deljenja svaki polinom $f \in K[x_1,...,x_n]$ se može zapisati na sledeći način $f = a_1 \cdot f_1 + ... + a_k \cdot f_k + r$ za $a_i, r \in K[x_1,...,x_n](i = 1,..,k)$ pri čemu ili je $r = 0$ ili je r neka K- linearna kombinacija monoma od kojih ni jedan nije deljiv sa ma kojim od vodećih monoma $LT(f_1),...,LT(f_k)$ pri datom monomijalnom poretku $\succ$. Pri navedenim pretpostavkama važi $(\forall i \in \{1,...,s\}) LT(f) \geq LT(a_i f_i)$

Primer rada algoritma (leksikografski poredak)
Početne pripreme: Ulaz: $f=-x^3z+xz+y^2z-yz^2$ $f_1=x^2z$ $f_2=x-z^2$, $f_3=y-z$ $a_1=0$ $a_2=0$ $a_3=0$ $r=0$ $p=f=-x^3y+xz-yz$
Korak 1: $lt(p)\mid lt(f_1)$ $p=p-(-x^3z)=xz-yz^2$ $a_1=a_1+(-x)=-x$ $r=0$
Korak 2: $lt(p)\mid lt(f_2)$ $p=p-(-xz-z^3)=y^2z-yz^2+z^3$ $a_2=a_2+(z)=z$ $r=0$
Korak 3: $lt(p)\mid lt(f_3)$ $p=p-(y^2z-yz^2)=z^3$ $a_3=a_3+(yz)=yz$ $r=0$
Korak 4: $lt(p)\mid\{\}$ $r=r+lt(p)=z^3$ $p=p-lt(p)=0$
Korak 5: $p=0$ Algoritam završava sa izvršavanjem $a_1=-x$ $a_2=z$ $a_3=yz$ $r=z^3$

Definicija 5.3 Polinom *r=Rem(f,F)* nazivamo ostatkom pri deljenju polinoma f sa k-torkom sređenih polinoma F.

Napomena 5.4 Ostatak pri deljenju polinoma f sa k-torkom sređenih polinoma F zavisi od redosleda polinoma unutar F, i nije jedinstven.

Lema 5.5 Za polinom *f* i k-torku $F = (f_1 ... f_k)$ sređenih u istom monomijalnom poretku $\succ$ važi *r=Rem(f,F)=0* $\Rightarrow f \in \langle \{f_1,...,f_k\} \rangle$

Definicija 5.6 Za nenula polinome *f, g* i polinom $\hat{f}$ iz $\mathbf{K}[x_1,...,x_n]$, sređene u istom monomijalnom poretku $\succ$, smatramo da se polinom *f* redukuje na polinom $\hat{f}$ po modulu polinoma *g,* u oznaci $f \rightarrow_g \hat{f}$ ili $f \equiv \hat{f}$ *mod g* ako postoji term *h* polinoma *f* takav da važi: $lt(g) \mid h \wedge \hat{f} = f - \frac{h}{lt(g)} \cdot g$

Definicija 5.7 Neka je *f* polinom i neka je $G = \{g_1,...,g_k\}$ skup polinoma u $\mathbf{K}[x_1,...,x_n]$ sređenih u istom monomijalnom poretku $\succ$. Polinom *f* se redukuje na polinom $\hat{f}$ po modulu skupa polinoma *G*, u oznaci $f \rightarrow_G \hat{f}$, ako postoji polinom $g_i \in G$ takav da $f \rightarrow_{g_i} \hat{f}$ (pri tom je $\hat{f}$ je sređen u istom monomijalnom poretku $\succ$). Smatramo da se polinom *f* u potpunosti redukovao na polinom $\hat{f}$ po modulu skupa polinoma *G* ako je $f \rightarrow_G \hat{f} \rightarrow_G \hat{f}$. Navedeno označavamo $f \rightarrow_{*G} \hat{f}$.

Definicija 5.8 Polinom $\hat{f}$ je normalna forma polinoma *f* po modulu skupa polinoma *G* takav da $f \rightarrow_{*G} \hat{f}$. Normalnu formu polinoma označavamo $\hat{f} = normalf(f, G)$.

Teorema 5.9 Neka je dat skup polinoma $G = \{g_1,...,g_k\}$ u prstenu polinoma više promenljivih $\mathbf{K}[x_1,...,x_n]$. Tada za svaki polinom $f \in K[x_1,...,x_n]$ normalna forma $h = normalf(f, G)$ određuje se u konačnom broju koraka. Pri tom se polazni polinom *f* može zapisati na sledeći način $f = a_1 \cdot g_1 + ... + a_k \cdot g_k + h$ za neke polinome $a_i \in K[x_1,...,x_n](i = 1,...,k)$, pri čemu ili je *h=0* ili je *h* neka K-linearna kombinacija monoma od kojih ni jedan nije deljiv sa ma kojim od vodećih monoma $lt(g_1),...,lt(g_k)$. Pri tome važi $(\forall i \in \{1,...,s\}) lf(f) \succeq lt(a_i f_i)$.

Teorema 5.10 Neka je dat skup polinoma $G = \{g_1,...,g_k\}$ u prstenu polinoma više promenljivih $\mathbf{K}[x_1,...,x_n]$. Polinom $f \in K[x_1,...,x_n]$ se u potpunosti redukuje na nulu po modulu skupa polinoma *G* ako i samo ako se polinom *f* može zapisati na sledeći način: $f = a_1 \cdot g_1 + ... + a_k \cdot g_k$ za neke polinome $a_i \in K[x_1,...,x_n](i = 1,...,k)$. Pri navedenim pretpostavkama važi $(\forall i \in \{1,...,s\}) lf(f) \succeq lt(a_i f_i)$

6. Hilbertova teorema o bazi

Definicija 6.1 Neka je I nenula ideal u prstenu polinoma više promenljivih $\mathbf{K}[x_1,...,x_n]$. Tada skupom vodećih termova ideala $lt(I)=\langle\{lt(f)\mid f\in I\}\rangle$ generišemo ideal vodećih termova $\langle lt(I)\rangle=\langle\{lt(f)\mid f\in I\}\rangle$

Teorema 6.2 Neka je I nenula ideal u $\mathbf{K}[x_1,...,x_n]$, tada važi:

a) $\langle lt(I)\rangle$ jeste monomijalni ideal u $\mathbf{K}[x_1,...,x_n]$

b) $(\exists g_1,...,g_s\in I)\langle lt(I)\rangle=\langle\{lt(g_1),...,lt(g_s)\}\rangle$

Teorema 6.3 Hilbertova teorema o bazi Svaki ideal I u prstenu polinoma više promenljivih $\mathbf{K}[x_1,...,x_n]$ jeste konačno generisan ideal

Napomena 6.4 Na osnovu Hilbertove teoreme o bazi zaključujemo da je algebarska struktura $\mathbf{K}[x_1,...,x_n]=(K[x_1,...,x_n],+,\cdot)$ Noetherin prsten.

7. Grebnerova baza

U razmatranju u ovom delu i narednim delovima koji se odnose na Grebnerove baze smatraćemo da je dat fiksiran monomijalni poredak $\succ$.

Teorema 7.1 Neka je $I=\langle f_1,...,f_s\rangle$ ideal u prstenu polinoma više promenljivih $\mathbf{K}[x_1,...,x_n]$ tada važi $\langle\{lt(f_1),...,lt(f_s)\}\rangle\subseteq\langle lt(I)\rangle$

Definicija 7.2 Konačan skup $G=\{g_1,...,g_k\}$ u idealu I prstena polinoma više promenljivih $\mathbf{K}[x_1,...,x_n]$ naziva se standardna Grebnerova baza ideala I ako važi $\langle lt(I)\rangle=\langle\{lt(g_1),...,lt(g_s)\}\rangle$

Primer 7.3 Za polinome $f_1=xy+1$ i $f_2=y^2+1$ postoje polinomi $g_1=f_2=y^2+1$ i $g_2=x\cdot f_2-y\cdot f_1=xy^2+x-xy^2-y=x-y$, takvi da $I=\langle\{g_1,g_2\}\rangle$ i da $\langle\{lt(f_1),lt(f_2)\rangle\subseteq\langle\{lt(g_1),lt(g_2)\rangle$

Napomena 7.4 Neka je $G=\{g_1,...,g_k\}$ baza ideala I prstena više promenljivih $\mathbf{K}[x_1,...,x_n]$. Uslov da je normalna forma po modulu skupa G jedinstveno određena je ekvivalentan sa uslovom da je *G* Grebnerova baza ideala I. Navedeni uslov je koristio B. Buchberger pri definiciji standardne Grebnerove baze.

Teorema 7.5 Svaki ideal I u prstenu polinoma više promenljivih $\mathbf{K}[x_1,...,x_n]$ ima bar jednu standardnu Grebnerovu bazu G koja jeste jedna baza za ideal I.

Teorema 7.6 Konačan skup $G=\{g_1,...,g_k\}$ u idealu I prstena više promenljivih $\mathbf{K}[x_1,...,x_n]$ jeste standardna Grebnerova baza ideala ako i samo ako za svako $f\in I$ važi $(\exists g_i\in G)lt(g_i)\,|\,lt(f)$

Teorema 7.7 Neka je $G=\{g_1,...,g_k\}$ Grebnerova baza ideala $I\subseteq K[x_1,...,x_n]$. Tada za svako $f\in K[x_1,...,x_n]$ postoji jedinstveno određen $r\in K[x_1,...,x_n]$ sa sledećim pretpostavkama:

a) Ako je $r\neq 0$, tada nijedan monom koji se javlja u r kao sabirak nije deljiva sa nekim od monoma $lt(g_1),...,lt(g_s)$
b) Postoji $g\in I$ tako da $f=g+r$

Definicija 7.8 Neka je $G=\{g_1,...,g_s\}$ Grebnerova baza ideala $I\subseteq K[x_1,...,x_n]$. Tada za svako $f\in K[x_1,...,x_n]$ jedinstveno određen polinom r iz prethodne teoreme nazivamo ostatakom polinoma f u odnosu na Grebnereovu bazu G.

Teorema 7.9 Neka je $G=\{g_1,...,g_s\}$ baza ideala I prstena više promenljivih $\mathbf{K}[x_1,...,x_n]$. Uslov da za svako $f\in K[x_1,...,x_n]$ važi ekvivalencija $f\in I\Leftrightarrow rem(f,(g_1,...,g_s))=0$ je ekvivalentan sa uslovom da je G Grebnerova baza ideala I.

Teoreme 7.10 Svaka Grebnerova baza $G=\{g_1,...,g_s\}$, u prstenu više promenljivih $\mathbf{K}[x_1,...,x_n]$ jeste jedna baza za ideal I.

Teorema 7.11 Neka su $G=\{g_1,...,g_s\}$ i $G'=\{g'_1,...,g'_k\}$ dve Grebnerove baze ideala $I\subseteq K[x_1,...,x_n]$ u odnosu na isti monomijalni poredak $\succ$. Tada za svako $f\in K[x_1,...,x_n]$ važi $rem(f,(g_1,...,g_s))=rem(f,(g'_1,...,g'_k))$

Teorema 7.12 Sledeći uslovi su međusobno ekvivalentni:

a) Skup G je grebnerova baza za ideal $I\subseteq K[x_1,...,x_n]$
b) Svako $f\in I$ možemo zapisati u obliku $f=a_1\cdot g_1+...+a_s\cdot g_s$ za neke $a_1,...,a_s\in K[x_1,...,x_n]$ pri čemu $(\forall i\in\{1,...,s\})lt(f)\succeq lt(a_i g_i)$
c) Svako $f\in I$ se u potpunosti redukuje na 0 po modulu skupa G

Teorema 7.13 Neka je $G=\{g_1,...,g_s\}$ Grebnerova baza ideala I prstena više promenljivih $\mathbf{K}[x_1,...,x_n]$. Smatramo da je G redukovana Grebnerova baza ako su ispunjeni sledeći uslovi:

a) Skup $\{lt(g_1),...,lt(g_s)\}$ određuje minimalni generatorski skup za $\langle lt(I)\rangle$
b) Vodeći termovi $lt(g_i)$ su monomični monomi, tj. $lc(g_i)=1$, za svako $i \in \{1,...,s\}$
c) Nijedan monom $lm(g_i)$ nije deljiv ma kojim monomom koji se javlja kao sabirak u generatoru $g_j = lm(g_j) + c_{j_1} m_{j_1} + ... + + c_{j_k} m_{j_k} \in G$ za $i \neq j (i, j \in \{1,...,s\})$

Teorema 7.14 Svaki nenula ideal I prstena više promenljivih $\mathbf{K}[x_1,...,x_n]$ ima jedinstveno određenu redukovanu Grebnerovu bazu.

8. Sizidži niza polinoma i S-polinomi

Definicija 8.1 Neka je data k-torka polinoma $F=(f_1,...,f_k)$ nad prstenom polinoma više promenljivih $\mathbf{K}[x_1,...,x_n]$, tada k-torka polinoma $S=(a_1,...,a_k)$ polinoma nad prstenom polinoma više promenljivih $\mathbf{K}[x_1,...,x_n]$ naziva se Sizidži k-torke polinoma F ako važi $a_1 \cdot f_1 + ... + a_k \cdot f_k = 0$

Teorema 8.2 Neka je $m_1,...,m_k$ niz monoma u prstenu polinoma više promenljivih $\mathbf{K}[x_1,...,x_n]$. Ako je $S = syz(m_1,...,m_k)$, tada je S linearna kombinacija sizudžia oblika $s_{ij} = \frac{nzs(m_i,m_j)}{m_i}\vec{e}_i - \frac{nzs(m_j,m_i)}{m_j}\vec{e}_j$ za $1 \le i < j \le k$

Definicija 8.3 [11](Cox,Little,O'Shea,1997) Neka su $f,g \in K[x_1,...,x_n]$ dva polinoma, S-polinom za polinome f i g određen je sa $S(f,g) = \frac{nzs(lm(f),lm(g))}{lt(f)} \cdot f - \frac{nzs(lm(f),lm(g))}{lt(g)} \cdot g$

Primer računanja S-polinoma

$f = (x^2 + yz^2 - 2z)$

$g = 3xz^2 + y^3 - yz$

$\mathrm{nzs(f,g)} = \mathrm{nzs(lm(f),lm(g))} = nzs(x^2, xz^2) = x^2z^2$

$S(f,g) = \frac{nzs(lm(f),lm(g))}{lt(f)} \cdot f - \frac{nzs(lm(f),lm(g))}{lt(g)} \cdot g$

$S(f,g) = \frac{x^2z^2}{x^2} \cdot (x^2 + yz^2 - 2z) - \frac{x^2z^2}{3xz^2} \cdot (3xz^2 + y^3 - yz)$

$S(f,g) = z^2 \cdot (x^2 + yz^2 - 2z) - \frac{x}{3} \cdot (3xz^2 + y^3 - yz)$

$S(f,g) = x^2z^2 + yz^4 - 2z^3 - x^2z^2 - \frac{xy^3}{3} + \frac{xyz}{3}$

$S(f,g) = -\frac{xy^3}{3} + \frac{xyz}{3} + yz^4 - 2z^3$

Lema 8.4 Za polinome $f, g \in K[x_1,...,x_n]$ važi $lt(f \cdot g) = lt(f) \cdot lt(g)$

Lema 8.5 Za polinome $f_1, f_2, g_1, g_2 \in K[x_1,...,x_n]$ neka važe uslovi $lt(f_1 g_1) + lt(f_{21} g_2) = 0$ i $nzs(lm(g_1), lm(g_2)) \mid nzs(lm(f_1), lm(f_2))$. Neka je $\gamma = md(lt(f_1 g_1)) = md(lt(f_2 g_2))$ i $\delta = md(nzs(lm(g_1), lm(g_2)))$. Tada važo $lt(f_1) g_1 + lt(f_2) g_2 = c_1 x^{\gamma_1} \cdot S(g_1, g_2)$ za neki koeficijent $c_1 \in K \setminus \{0\}$ i multistepen $\gamma_1 = \gamma - \delta \in N_0^n$.

Lema 8.6 Za svaka dva polinoma $f, g \in K[x_1,...,x_n]$ važi $nzs(lm(f), lm(g)) \succ lt(S(f, g))$

Teorema 8.7 Neka je da skup $G = \{g_1,..., g_s\}$ koji generiše ideal $I \subseteq K[x_1,...,x_n]$. Ako za svako $g_i, g_j \in G$ S-polinomi $S(g_i, g_j)$ ispunjavaju uslove $S(g_i, g_j) = a_1 g_1 + ... + a_s g_s$ i $(\forall k \in \{1,...,s\}) lt(S(g_i g_j)) \succeq lt(a_k g_k)$ za neke polinome $a_1,..., a_s \in K[x_1,..., x_n]$ tada skup G određuje Grebnerovu bazu.

Teorema 8.8 Skup $G = \{g_1,..., g_s\}$ određuje jednu Grebnerovu bazu ideala $I = \langle \{g_1,..., g_s\} \rangle$ u prstenu polinoma više promenljivih **K**[$x_1,..., x_n$] ako i samo ako važi $(\forall g_i, g_j \in G) S(g_i, g_j) \in I$

9. Buchbergerov algoritam

Buchbergerov algoritam	
Input:	Skup polinom $F = (f_1,..., f_k)$ koji generiše ideal I
Output:	Skup $G = (g_1,..., g_s)$ Grebnerova baza ideala I
	$G := F$ $M := \{(f_i, f_j) \mid f_i, f_j \in G \wedge f_i = f_j\}$ *while*$(M \neq 0)$*do* *(p,q):=a neki uređeni par iz M* $M := M \setminus \{(p.q)\}$ $S := S(p, q)$ $h := normalf(S, G)$ *if* $(h \neq 0)$*then* $M := M \cup \{(g, h) \mid g \in G\}$ $G := G \cup \{h\}$ *endWhile*

Teorema 9.1 [11](Cox,Little,O'Shea,1997) Neka je dat skup polinoma $F = (f_1,...,f_k)$ gde su polinomi $f_i \in K[x_1,...,x_n]$ svaki za sebe sređeni u istom monomijalnom poretku $\succ (i = 1,...,k)$. Tada primenom Buchbergerovog algoritma od svako skupa polinoma $F = (f_1,...,f_k)$ dobijamo $G = (g_1,...,g_s)$ koji određuje jednu Grebnerovu bazu ideala *I*.

Primer funkcionisanja Buchbergerovog algoritma

Ulazni polinomi: $f_1 = -4x^2 - 9y^2 + z$

$f_2 = 4x^2 - 2x + 9y^2 - 3y$

$M := \{(f_1, f_2)\}$

Korak 1:

$p = f_1$

$q = f_2$

$M = M/\{(f_1, f_2)\}$

$s = S(f_1, f_2)$

$$s = \frac{x^2}{-4x^2} \cdot -4x^2 - 9y^2 + z - \frac{x^2}{4x^2} \cdot 4x^2 - 2x + 9y^2 - 3y$$

$s = x/2 + 3y/4 - z/4$

$h = normalf(s, G)$

$x/2 + 3y/4 - z/4 : (-4x^2 - 9y^2 + z,\ 4x^2 - 2x + 9y^2 - 3y) = (0,0)$

$rem = x/2 + 3y/4 - z/4$

$h = x/2 + 3y/4 - z/4$

$h \neq 0$

$f_3 = h$

$G = G \cup \{f_3\}$

$M = M \cup \{(f_1, f_3), (f_2, f_3)\}$

Korak 2:

$p = f_1$

$q = f_3$

$M = M/\{(f_1, f_3)\}$

$s = S(f_1, f_3)$

$s = 3xy/2 - xz/2 - 9y^2/4 + z/4$

$h = normalf(s, G)$

$h = -9y^2/2 + 3yz/2 - z^2/4 + z/4$

$h \neq 0$

$f_4 = h$

$G = G \cup \{f_4\}$

$M = M \cup \{(f_1, f_4), (f_2, f_4), (f_3, f_4)\}$

Korak 3:

$p = f_2$
$q = f_3$
$M = M/\{(f_2, f_3)\}$

$s = S(f_2, f_3)$
$s = 3xy/2 - xz/2 + x/2 - 9y^2/4 + 3y/4$

$h = normalf(s, G)$
$h = 0$

Korak 4:

$p = f_1$
$q = f_4$
$M = M/\{(f_1, f_4)\}$

$s = S(f_1, f_4)$
$s = -x^2yz/3 + x^2z^2/18 - x^2z/18 - 9y^4/4 + y^2z/4$

$h = normalf(s, G)$
$h = 0$

Korak 5:

$p = f_2$
$q = f_4$
$M = M/\{(f_2, f_4)\}$
$s = S(f_2, f_4)$
$s = - x\text{^}2yz/3 + x^2z^2/18 - x^2z/18 + xy^2/2 - 9y^4/4 + 3y^3/4$

$h = normalf(s, G)$
$h = 0$

Korak 6:

$p = f_3$
$q = f_4$
$M = M/\{(f_3, f_4)\}$

$s = S(f_3, f_4)$
$s = -xyz/3 + xz^2/18 - xz/18 - 3y^3/2 + y^2z/2$
$h = normalf(s, G)$
$h = 0$

Grebnerova baza: $f_1 = -4x^2 - 9y^2 + z$
$f_2 = 4x^2 - 2x + 9y^2 - 3y$
$f_3 = x/2 + 3y/4 - z/4$
$f_4 = -9y^2/2 + 3yz/2 - z^2/4 + z/4$

10. Algoritam redukcije baze

Teorema 10.1 Neka je G jedna Grebnerova baza ideala $I \subseteq K[x_1,...,x_n]$. Ako postoji element $p \in G$ takav da $lt(p) \in \langle lt(G \setminus \{p\}) \rangle$ tada je $G \setminus \{p\}$ generatorski skup i Grebnerova baza.

Definicija 10.2 Grebnerova baza ideala $I \subseteq K[x_1,...,x_n]$ jeste minimalna Grebnerova baza ideala I ako važi:

a) $(\forall p \in G) lc(p) = 1$

b) $(\forall p \in G) lt(p) \notin \langle lt(G \setminus \{p\}) \rangle$

Teorema 10.3 Grebnerova baza G ideala $I \subseteq K[x_1,...,x_n]$ jeste minimalna Grebnerova baza ako i samo ako važi:

a) $(\forall p \in G) lc(p) = 1$

b) $\langle lt(G) \rangle$ jeste minimalna baza monomijalnog ideala $\langle lt(I) \rangle$

Definicija 10.4 [11](Cox,Little,O'Shea,1997) Grebnerova baza G ideala $I \subseteq K[x_1,...,x_n]$ jeste redukovana Grebnerova baza ako važi:

a) $(\forall p \in G) lc(p) = 1$

b) Za svako $p \in G$ ne postoji monom x^α polinoma p tako da $x^\alpha \in \langle lt(G \setminus \{p\}) \rangle$

Algoritam redukcije Grebnerove baze

Input: $G = \{g_1,..., g_s\}$ - Grebnerova baza

Output: $\hat{G} = \{\hat{g}_1,..., \hat{g}_k\}$ - Redukovana Grebnerova baza

$\hat{G} := G$
for all $g \in \hat{G}$ *do*
  if $(\exists \mu \in \hat{G} \mid \mu \neq g) lt(\mu) \mid lt(g)$ *then*
    $\hat{G} := \hat{G} \setminus \{g\}$
  else
    $g := rem(g, \hat{G} \setminus \{g\})$
for all $g \in \hat{G}$ *do*
  $g := \frac{g}{lc(g)}$

Teorema 10.5 Neka je data Grebnerova baza ideala $I \subseteq K[x_1,...,x_n]$ u odnosu na fiksirani monomijalni poredak $\succ$. Primenom algoritma redukcije baze od svake Grebnerove baze dobijamo redukovanu Grebnerovu bazu.

Teorema 10.6 Redukovana Grebnerova baza je jedinstvena i predstavlja specijalan slučaj minimalne Grebnerove baze nenula ideala *I.*

Primer funkcionisanja algoritma redukcije Grebnerove baze
Grebnerova baza: $f_1=-4x^2 -9y^2 +z$ $f_2=4x^2 -2x +9y^2 -3y$ $f_3=x/2 +3y/4 -z/4$ $f_4=-9y^2/2 +3yz/2 -z^2/4 +z/4$
Korak 1: $p=f_1=-4x^2 -9y^2 +z$ $lt(p)=-4x^2$ $\{ 4x^2, x/2 \}\|lt(p)$ $\hat{G} := G \setminus \{f_1\}$
Korak 2: $p=f_2=4x^2 -2x +9y^2 -3y$ $lt(p)=4x^2$ $\{ x/2 \}\|lt(p)$ $\hat{G} := G \setminus \{f_2\}$
Korak 3: $p=f_3=x/2 +3y/4 -z/4$ $lt(p)=x/2$ $\{ \}\|lt(p)$ $p=rem(p,G)$ $p=x/2 +3y/4 -z/4$
Korak 4: $p=f_4=-9y^2/2 +3yz/2 -z^2/4 +z/4$ $lt(p)=x/2$ $\{ \}\|lt(p)$ $p=rem(p,G)$ $p=-9y^2/2 +3yz/2 -z^2/4 +z/4$
Redukovana Grebnerova baza: $f_1=x/2 +3y/4 -z/4$ $f_2=-9y^2/2 +3yz/2 -z^2/4 +z/4$

11. Algoritam za pronalaženje planarnih preseka polinoma

Definicija 11.1 [5.](Malešević,Obradović ,2009) Ukoliko je dat sistem dve nelinearne polinomijalne jednačine $f_1(x,y,z)=0 \wedge f_2(x,y,z)=0$, sistem ima planarno rešenje ako postoji linearan polinom $g=g(x,y,z)=Ax+By+Cz+D$ takvo da svako rešenje sistema je takođe rešenje linearne jednačine $g(x,y,z)=0$ za neke realne promenljive *A,B,C* i *D*.

Teorema 11.2 Ukoliko Grebnerova baza sadrži linearan polinom, onda je rešenje sistema planarno.

Teorema 11.3 Sistem ima planarni presek $Ax+By+Cz+D=0$ za neke $A,B,C,D \in R$ i $A \neq 0$. Ukoliko za ideal $I=\langle f_1,f_2 \rangle$ je istinito $y \notin \langle lt(I) \rangle \wedge z \notin \langle lt(I) \rangle$ onda linearni polinom $\hat{g}=\hat{g}(x,y,z)=x+(B/A)y+(C/A)z+(D/A)$ je element redukovane Grebnerove Baze

Teorema 11.4 [5.](Malešević,Jovovoić,Čampara,2010) Ako za ideal $I=\langle f_1,f_2 \rangle$ postoji generator *h* u Buchbergerovom algoritmu koji je linearan, ili primenom algoritma redukcije pronađemo redukovani algoritam h_p koji je linearan, onda sistem ima planaran presek

Napomenat 11.5 Pomenuta tvrđenja su dokazana samo na leksikografskom monomijalnom poretku, a nisu još dokazana na sistemima sa više od tri promenljive i u drugim monomijalnim poretcima

<table>
<tr><th colspan="2">Primer utvrđivanja planarnog preseka</th></tr>
<tr><td colspan="2">Ulazni polinomi : $f_1 = x+yz+y-z^4-4$
$f_2 = y-z^3-1$</td></tr>
<tr><td colspan="2">Korak 1:

$GB = buchberger(f_1,f_2)$
$GB = \{x+yz+y-z^4-4, y-z^3-1\}$
Nijedan polinom u GB nije linearan.
Vrši se redukcija GB</td></tr>
<tr><td colspan="2">Korak 2:
Vrši se redukcija nad polinomom $p=x+yz+y-z^4-4$

<table>
<tr><td>Parcijalna redukcija</td></tr>
<tr><td>$p=x+yz+y-z^4-4$
$f_2=y-z^3-1$
$lt_2=y$</td></tr>
<tr><td>Korak 1:
$t=x$
lt_1 ne deli t</td></tr>
</table>
</td></tr>
</table>

Korak 2:

$t=yz$
$lt_1 \mid t$
$t / lt_1 = z$
$p=p - z*f_2$
$p=(x + yz + y - z^4 - 4) - (yz - z^4 - z) = x + y + z - 4$
p je planaran polinom
$p' = x + y + z - 4$

Otkriven planarni presek p' .
Izvršavanje algoritma se zaustavlja

Literatura

[1.] Profesor Branko Malešević , Materijali za nastavu iz predmeta Simbolička aglebra, Elektrotehnički fakultet u Beogradu

[2.] A. Heck: *Bird's-eye view of Gröbner Bases*, Nuclear Inst. and Methods in Physics Research A 389 (1997), 16-21

[3.] K. Forsman: *Hitchhiker guide to Gröbner bases*, Research Institute for Symbolic Computation, Linz, Technical Report 0374(1992).

[4.] B. Malešević, M. Obradović: *An Application of Groebner Basest to Planarity of Intersection of Surfaces*, Filomat 23:2 (2009), pp. 43-55. (Thompson SCIE list 2009.)

[5.] B. Malešević, I. Jovović, M. Čampara: *Groebner bases in JAVA with applications in computer graphic*s, Proceedings of 2-nd International Conference for Geometry and Engineering Graphics "moNGeometrija 2010", Paper No. 29, pp. 1-10, June 2010, Belgade.

[6.] B. Malešević, I. Jovović, M. Makragić, B. Banjac, V. Katić, A. Jovanović, A. Pejović: *Buchberger-ov algoritam i vizuelizacija monomijalnih ideala,* konferencija „*Matematika i promene*", Prirodno matematički fakultet, maj 2011, Beograd

[7.] D. Cox, J. Little, D. O'Shea : *Ideals,Varieties and Algorithms*, Springer, New York, 1997

[8.] Ralf Frooberg: *An Introduction to Groobner bases*, John Wiley & Sons Ltd., 1997