Prezapisivanje termova i Grebnerove baze

Danijela Petrović

November 24, 2010

Sadržaj

Termi

- Termi se grade od konstanti, promenljivih i funkcionalnih simbola na sledeći način:

  i) konstante su termi
  ii) promenljive su termi
  iii) ako je f n-aran funkcionalan simbol i $t_1, \ldots, t_n$ termi onda je i $f(t_1, \ldots, t_n)$ term

- Primer: $x + s(y)$

Sistem za prezapisivanje termova

- Pravila oblika $a \to b$, pri čemu su a i b termovi i a nije promenljiva i $Var(b) \subseteq Var(a)$ nazivaju se pravila za prezapisivanje termova
- Primer: $x + 0 \to x$
- Skup ovakvih pravila naziva se sistem za prezapisivanje termova
- Za sistem za prezapisivanje termova važno je da bude: **terminirajuć** i **konfluentan**

Terminirajuć sistem

- Da li uvek važi da posle primene **konačno** mnogo pravila dobijamo izraz na koji se ni jedno pravilo ne može primeniti?
- Izraz na koji se ni jedno pravilo ne može primeniti naziva se normalna forma
- Primer neterminirajućeg pravila: $u + v \to v + u$
- Sistem za prezapisivanje termova R je terminirajući akko postoji poredak $\prec$ tako da za svako $l \to r \in R$ važi $r \prec l$

Konfluentan sistem

- Neka je dat sistem za prezapisivanje termova R i term t
- Neka različitom primenom pravila iz R na t možemo dobiti terme t_1 i t_2
- Da li postoji term s takav da ga možemo dobiti i primenom pravila iz R na t_1 i primenom pravila iz R na t_2?
- Tj. ako $t_1 \overset{*}{\leftarrow} t \overset{*}{\rightarrow} t_2$ da li uvek postoji s takvo da $t_1 \overset{*}{\rightarrow} s \overset{*}{\leftarrow} t_2$

Problem pripadnosti idealu

- $K[X_1, \ldots, X_n]$ - označavamo **prsten polinoma** sa n promenljivih, pri čemu su promenljive polinoma $X_1, \ldots, X_n$, a koeficijenti polinoma su u K
- **Ideal** nad prstenom $K[X_1, \ldots, X_n]$ je neprazan skup $J \subseteq K[X_1, \ldots, X_n]$ takav da važi:

  i) ako $f, g \in J$ onda $f + g \in J$

  ii) ako $f \in J$ i $g \in K[X_1, \ldots, X_n]$ onda $f \cdot g \in J$
- **Ideal generisan** sa $f_1, \ldots, f_k \in K[X_1, \ldots, X_n]$ je skup

$$< f_1, \ldots, f_n >= \{f_1 \cdot g_1 + \ldots + f_k \cdot g_k | g_1, \ldots, g_k \in K[X_1, \ldots, X_n]\}$$

Problem pripadnosti idealu

Problem

Ako važi $f, f_1, \ldots, f_k \in K[X_1, \ldots, X_n]$
Treba proveriti da li važi: $f \in < f_1, \ldots, f_k >$

- Problem pripadnosti idealu $J =< f_1, \ldots, f_n >$ je odlučiv ako i samo ako je kongruencija nad idealom J - $\equiv_J$ odlučiva

Uređenje nad polinomima

- Potrebno je uvesti uređenje
- Totalno uređenje: Neka su m_1, m_2, m monomi. Uvodimo uređenje $\prec$ za koje važi

  i) $m_1 | m_2$ povlači $m_1 \preceq m_2$

  ii) $m_1 \prec m_2$ povlači $m \cdot m_1 \preceq m \cdot m_2$
- Ovo uređenje je dobro definisano

Relacija redukcije nad polinomima

- Neka je $f \in K[X_1, \ldots, X_n]$
- Najveći monom u f (prema uređenju $\prec$) označimo sa $H(f)$

f indukuje relaciju redukcije nad polinomima: $g \to_f g'$ akko

i) g sadrži monom m sa koeficijentom $a \neq 0$

ii) postoji monom m' takav da $m = H(f) \cdot m'$

iii) $g' = g - am' \cdot f$

Primer

- $f = x_1^2 x_2 - x_1^2$

Primer

- $f = x_1^2 x_2 - x_1^2$
- $H(f) = x_1^2 x_2$

Primer

- $f = x_1^2 x_2 - x_1^2$
- $H(f) = x_1^2 x_2$
- $g = x_1^2 x_2^2$

Primer

- $f = x_1^2 x_2 - x_1^2$
- $H(f) = x_1^2 x_2$
- $g = x_1^2 x_2^2$
- $g \to_f g'$: $g' = g - x_2 \cdot f = x_1^2 x_2^2 - x_1^2 x_2^2 - x_2 x_1^2 = -x_2 x_1^2$

Primer

- $f = x_1^2 x_2 - x_1^2$
- $H(f) = x_1^2 x_2$
- $g = x_1^2 x_2^2$
- $g \to_f g'$: $g' = g - x_2 \cdot f = x_1^2 x_2^2 - x_1^2 x_2^2 - x_2 x_1^2 = -x_2 x_1^2$
- $g' \to_f g''$: $g'' = g' + f = -x_2 x_1^2 + x_1^2 x_2 - x_1^2 = -x_1^2$

Veza između relacije redukcije i kongruencije nad idealnom

- $F = \{f_1, \ldots, f_n\}$

$$\rightarrow_F = \bigcup_{i=1}^{k} \rightarrow_{f_i}$$

Ako je $F = \{f_1, \ldots, f_n\}$ konačan skup polinoma i $J =< f_1, \ldots, f_n >$, onda

$$\equiv_J = \overset{*}{\leftrightarrow}_F$$

Veza relacije redukcije i problema pripadnosti idealu

- Podsetnik: Problem pripadnosti idealu $J =< f_1, \ldots, f_n >$ je odlučiv ako i samo ako je kongruencija nad idealom J - $\equiv_J$ odlučiva

Ako je $F = \{f_1, \ldots, f_n\}$ konačan skup polinoma i $J =< f_1, \ldots, f_n >$.
Ako je $\rightarrow_F$ konfluentno i terminirajuće onda je $\equiv_J$ odlučivo.

- Ako je F konačan skup polinoma onda je $\rightarrow_F$ terminirajuća redukciona relacija
- Treba ispitati da li je $\rightarrow_F$ konfluentno

Grebnerova baza

Neka je $G = \{f_1, \ldots, f_k\}$ konačan skup polinoma. G je Grebnerova baza ideala $J =< f_1, \ldots, f_k >$ ako i samo ako je $\rightarrow_G$ konfluentno.

- Neka je $G = \{f_1, \ldots, f_k\}$ Grebnerova baza ideala $J =< f_1, \ldots, f_k >$
- Problem da li $f \in J$ se svodi na ispitivanje da li $f \overset{*}{\rightarrow}_F 0$

S-polinom

- Neka je dat konačan skup polinoma $G = \{f_1, \ldots, f_m\}$.
- Kako od njega konstruisati Grebnerovu bazu?

S-polinom

- Neka je dat konačan skup polinoma $G = \{f_1, \ldots, f_m\}$.
- Kako od njega konstruisati Grebnerovu bazu?
- Koristićemo S-polinome

S-polinom

S-polinom nad polinomima f_i i f_j, u oznaci $S(f_i, f_j)$ konstruišemo na sledeći način:

i) neka je $m = NZS(H(f_i), H(f_j))$

ii) $m = m_i \cdot H(f_i)$

iii) $m = m_j \cdot H(f_j)$

iv) $S(f_i, f_j) = m_i \cdot f_i - m_j \cdot f_j$

Primer

- $f = x_1x_2^2 - x_1$
- $g = x_1 - x_2$
- $S(f,g) = f - x_2^2 \cdot g = x_1x_2^2 - x_1 - x_2^2x_1 - x_2^3 = -x_1 - x_2^3$

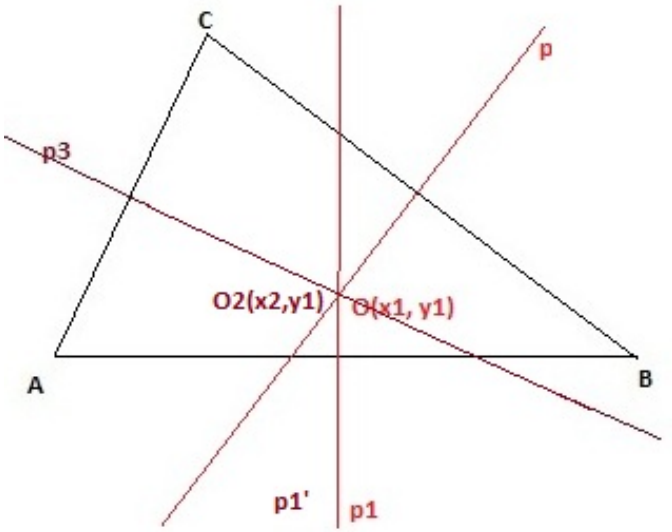
Primer

- $f = x_1 x_2^2 - x_1$
- $g = x_1 - x_2$
- $S(f, g) = f - x_2^2 \cdot g = x_1 x_2^2 - x_1 - x_2^2 x_1 - x_2^3 = -x_1 - x_2^3$
- Ukoliko su vodeći monomi dva polinoma uzajamno prosta tada za dobijeni S-polinom važi $S \xrightarrow{*}_{\{f_i, f_j\}} 0$

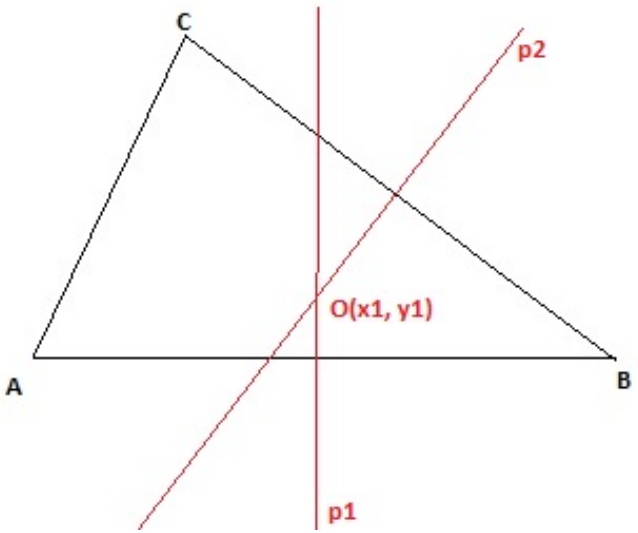
Konstrukcija Grebnerove baze nad datim skupom polinoma - Buhbergerov algoritam

- Neka je dat konačan skup polinoma $G = \{f_1, \ldots, f_m\}$
- Za svaka dva polinoma iz G ciji vodeći monomi nisu uzajamno prosti odredimo S-polinom
- Ove S polinome dodamo u G
- Postupak ponovimo za novododate polinome u G
- Postupak se završava kada ne postoje novi polinomi koje možemo dodati

Primer

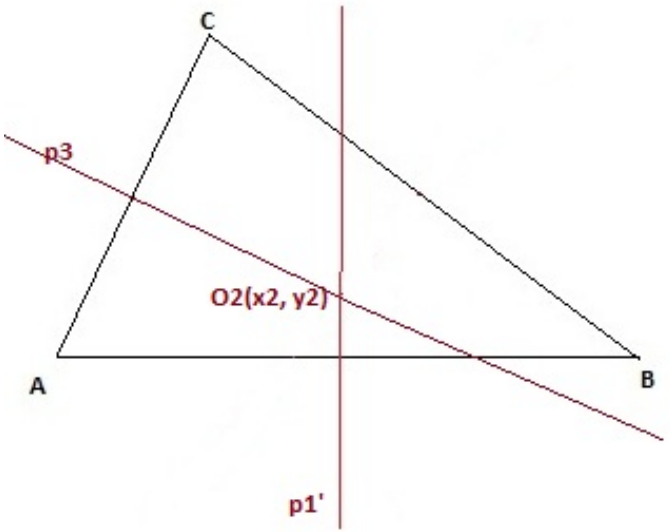


Primer



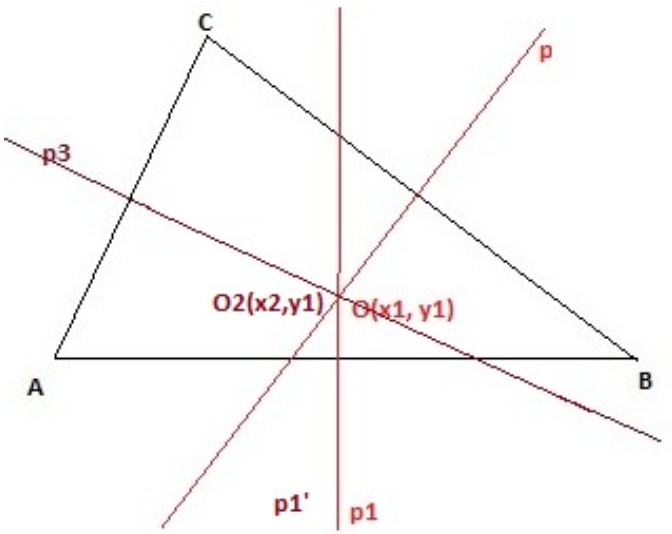
- A(0, 0), B(0, c), C(a, b)
- $O_1(x_1, y_1) = p_1 \cap p_2$
- $p_1 = x_1 - \frac{c}{2}$
- $p_2 = \frac{c-a}{b}x_1 - y_1 + \frac{b^2-c^2+a^2}{2b}$

Primer



- A(0, 0), B(0, c), C(a, b)
- $O_2(x_2, y_2) = p_1' \cap p_3$
- $p_1' = x_2 - \frac{c}{2}$
- $p_3 = \frac{a}{b}x_2 + y_2 - \frac{b}{2} - \frac{a^2}{2b}$

Primer



- A(0, 0), B(0, c), C(a, b)
- $O_1(x_1, y_1) = O_2(x_2, y_2)$
- $p_1 = x_1 - \frac{c}{2}$
- $p_2 = \frac{c-a}{b}x_1 - y_1 + \frac{b^2-c^2+a^2}{2b}$
- $p_1' = x_2 - \frac{c}{2}$
- $p_3 = \frac{a}{b}x_2 + y_2 - \frac{b}{2} - \frac{a^2}{2b}$

Primer

- Neka je $G = \{$
- $p_1 = x_1 - \frac{c}{2}$,
- $p_2 = \frac{c-a}{b}x_1 - y_1 + \frac{b^2-c^2+a^2}{2b}$,
- $p_1' = x_2 - \frac{c}{2}$,
- $p_3 = \frac{a}{b}x_2 + y_2 - \frac{b}{2} - \frac{a^2}{2b}\}$

- Problem $O_1(x_1, y_1) = O_2(x_2, y_2)$ se svodi na:

$$\text{i) } g_1 = x_1 - x_2 \xrightarrow{*}_{G'} 0$$
$$\text{ii) } g_2 = y_1 - y_2 \xrightarrow{*}_{G'} 0$$

pri čemu je G' Grebnerova baza nad skupom polinoma G

Primer

- Određujemo S-polinome

Primer

- Određujemo S-polinome
- $S_1 =< p_1, p_2 >= p_2 - \frac{c-a}{b} \cdot p_1 = -y_1 + \frac{b}{2} + \frac{a^2}{2b} - \frac{ac}{2b}$

Primer

- Određujemo S-polinome
- $S_1 =< p_1, p_2 >= p_2 - \frac{c-a}{b} \cdot p_1 = -y_1 + \frac{b}{2} + \frac{a^2}{2b} - \frac{ac}{2b}$
- $S_2 =< p_1', p_3 >= p_3 - \frac{a}{b} \cdot p_1' = y_2 - \frac{b}{2} - \frac{a^2}{2b} + \frac{ac}{2b}$

Primer

- Novodobijeni sistem: $G' = \{p_1, p_2, p_3, p_1', S_1, S_2\} =$
$\{x_1 - \frac{c}{2},$
$\frac{c-a}{b}x_1 - y_1 + \frac{b^2-c^2+a^2}{2b},$
$\frac{a}{b}x_2 + y_2 - \frac{b}{2} - \frac{a^2}{2b},$
$x_2 - \frac{c}{2},$
$-y_1 + \frac{b}{2} + \frac{a^2}{2b} - \frac{ac}{2b},$
$y_2 - \frac{b}{2} - \frac{a^2}{2b} + \frac{ac}{2b}\}$

Primer

- Pokazujemo da $g_1 = x_1 - x_2 \xrightarrow{*}_{G'} 0$
- $g_1 \rightarrow_{p_1} g_1'$
- $g_1' = g_1 - p_1 = -x_2 + \frac{c}{2}$
- $g_1' \rightarrow_{p_1'} g_1''$
- $g_1'' = g_1' + p_1' = -x_2 + \frac{c}{2} + x_2 - \frac{c}{2} = 0$

Primer

- Pokazujemo da $g_2 = y_1 - y_2 \overset{*}{\to}_{G'} 0$
- $g_2 \to_{S_1} g_2'$
- $g_2' = g_2 - S_1 = -y_2 + \frac{b}{2} + \frac{a^2}{2b} - \frac{ac}{2b}$
- $g_2' \to_{S_2} g_2''$
- $g_2'' = g_2' + S_2 = -y_2 + \frac{b}{2} + \frac{a^2}{2b} - \frac{ac}{2b} + y_2 - \frac{b}{2} - \frac{a^2}{2b} - \frac{ac}{2b} = 0$

Zaključci

- Postoji veza između sistema za prezapisivanje i Buhbergerovog algoritma
- Primena Grebnerovih baza:

  i) Algebra (monomi, ideali, polinomi, rešavanje sistema linearnih jednačina)
  ii) Geometrija
  iii) Kriptografija
  iv) Grafovski problemi (bojenje grafova)
  v) Celobrojno programiranje
  vi) ....
- Grebnerove baze mogu se koristiti za probleme kao što je automatko dokazivanje