Freie Universität Berlin
Institut für Mathematik II
Andreas Paffenholz

Christian Haase

Zusatzblatt

31. Mai 2006

Aufgabe 1.

Ein weiterer Algorithmus zur Umwandlung einer Gröbnerbasis $\mathcal{G}_1$ eines Ideals $\mathcal{I}$ bzgl. einer Termordnung $\geq_1$ in eine Gröbnerbasis $\mathcal{G}_2$ bzgl. einer weiteren Termordnung $\geq_2$ ist der umseitig abgedruckte FGLM-Algorithmus. Er kann nur auf nulldimensionale Ideale angewendet werden.

(1) Beweise, daß der Algorithmus terminiert. Begründe, warum er für Ideale höherer Dimension im Allgemeinen nicht terminieren wird.
(2) Zeige, daß alle Elemente in der Menge $\mathcal{G}_2$ im Ideal liegen.
(3) Zeige, daß die Monome in $\mathsf{InTerms}$ das Initialideal zu $\geq_2$ aufspannen: Wähle dafür ein Polynom h in $\mathcal{I}$. Wir können annehmen, daß h bzgl. $\mathcal{G}_2$ vollständig reduziert ist.
   (a) Angenommen, es gibt ein Monom m in $\mathsf{InTerms}$, daß bzgl. $\geq_2$ größer als $\mathrm{lt}(h)$ ist. Zeige, daß dann $\mathrm{lt}(h)$ in $\mathsf{InTerms}$ liegen muß.
   (b) Zeige, daß, wenn $\mathrm{lt}(h)$ bzgl. $\geq_2$ größer als ein Monom in $\mathsf{InTerms}$ ist, $\mathrm{lt}(h)$ von schon einem Monom aus $\mathsf{InTerms}$ geteilt wird.

Algorithm 1: Der FGLM-Algorithmus für die Umwandlung einer Gröbnerbasis eines nulldimensionales Ideals in eine Gröbnerbasis bzgl. einer anderen Termordnung (FGLM steht für die Anfangsbuchstaben der Autoren des Algorithmus: Faugère, Gianni, Lazard und Mora)

Input: Ideal $\mathcal{I}$ in $\mathcal{S}$, Gröbnerbasis $\mathcal{G}_1$ bzgl. $\geq_1$ von $\mathcal{I}$, Zieltermordnung $\geq_2$.

Output: Gröbnerbasis $\mathcal{G}_2$ von $\mathcal{I}$ bzgl. $\geq_2$.

Functions: `NF(`f`)` berechnet die Normalform eines Polynoms $f \in \mathcal{S}$ bzgl. $\mathcal{G}_1$.
`Extend(L,m)` fügt der Liste L alle Produkte $\mathsf{m}x_i$ für alle Variablen x_i des Polynomringes $\mathcal{S}$ hinzu, entfernt Duplikate und sortiert die Liste aufsteigend bzgl. $\geq_2$.
`pop(`L`)` löscht das erste Element der Liste und gibt es zurück.

$\mathcal{G}_2 := \emptyset$;
$\mathsf{L} := \emptyset$; `// Liste von Paaren` $\mathsf{p} = (Monom, Polynom)$
$\mathsf{InTerms} := \emptyset$;
$\mathsf{Extensions} := \{1\}$;
while $\mathsf{Extensions}\ != \emptyset$ **do**
  $\mathsf{m} :=$ `pop(`$\mathsf{Extensions}$`)`;
  if m *wird von keinem Monom in* $\mathsf{InTerms}$ *geteilt* **then**
    $\mathsf{v} :=$ `NF(`m`)`;
    if $\exists$ $\Bbbk$-*Lineardarstellung* $\mathsf{v} = \sum_{\mathsf{p} \in \mathsf{L}} \mu_{\mathsf{p}}\, \mathsf{p}_2$ **then**
      $f := \mathsf{m} - \sum_{p \in \mathsf{L}} \mu_{\mathsf{p}}\, \mathsf{p}_1$;
      $\mathcal{G}_2 := \mathcal{G}_2 \cup \{f\}$;
      $\mathsf{InTerms} := \mathsf{InTerms} \cup \{\mathsf{m}\}$;
    else
      $\mathsf{L} := \mathsf{L} \cup \{(\mathsf{m}, \mathsf{v})\}$;
      `Extend(`$\mathsf{Extensions}, \mathsf{m}$`)`;