Introduction to Differential Grobner Basis

Nazeran Idrees

Government College University Faisalabad

Derivation

Let R be a ring. A function $\delta : R \rightarrow R$ is called a derivation on R if and only if

$\delta(r+r') = \delta(r) + \delta(r')$

$\delta(rr') = \delta(r)\, r' + r\delta(r')$ $\quad \forall\, r, r' \in R$

Commuting derivations

Let R be a ring and Δ a set of derivations on R. We refer to the derivations as being

commutative

if and only if

$$\delta_1(\delta_2(r)) = \delta_2(\delta_1(r)) \qquad \forall\, r \in R \qquad \forall\, \delta_1, \delta_2 \in \Delta$$

Differential polynomial ring

Let I be a finite set, $(y_{i,\theta})_{i\in I,\,\theta\in D}$ be algebraically independent over the field F of characteristic zero, and let Δ be a finite set of commuting derivations on$F[(y_{i,\theta})_{i\in I,\,\theta\in D}]$, using D as abbreviation for ComMonoid (Δ).

We call $F[(y_{i,\theta})_{i\in I,\,\theta\in D}]$, together with Δ, the differential polynomial ring over F in $(y_{i,\theta})_{i\in I,\,\theta\in D}$ and Δ, if and only if

$\delta|_F$ is a derivation on F and

$$\delta(y_{i,\theta}) = y_{i,\delta\theta} \qquad \forall\, \delta \in \Delta$$

It is denoted by $F\{Y\}$.

Differential closure of a set

Let $P \subseteq F\{Y\}$, we define differential closure of P as

$$\bar{P}^D = \{q \in F\{Y\} | \, q = \theta(p) \; for\ some\ p \in P\ and\ \theta \in D\}$$

Differential ideal

An ideal $J \subseteq F\{Y\}$ is called differential ideal iff $J = \bar{J}^D$.

Generated differential ideal

Let P be a subset of $F\{Y\}$. We denote by $[P]$ the smallest subset of $F\{Y\}$ containing P, while being closed under applying derivations and multiplication by elements of $F\{Y\}$ as well as addition.

$[P]$ is a differential ideal called the differential ideal generated by P.

Remarks

- There is no differential equivalent of Hilbert's basis theorem.
- Finite bases need not exist for arbitrary differential ideals .
- Finite basis exist for radical differential ideals (Ritt-Raudenbush Theorem).

Example:

Let $F\{y\}$ be the ordinary ring of differential polynomials. Then, the sequence of differential ideals

$[y^2] \subseteq [y^2, y_1^2] \subseteq \cdots \subseteq [y^2, \ldots, y_n^2] \subseteq \cdots F\{y\}$ (Here $y_i = \delta^i$(y))

is an infinite strictly increasing sequence.

Differentially admissible ordering

We call a total order < on

$T \coloneqq ComMonoid\,((y_{i,\theta})_{i\in I,\,\theta\in D})$ (set of differential monomials)

differentially admissible order on $(y_{i,\theta})_{i\in I,\,\theta\in D}$ if $\forall\, t, s, u \in T$

- $1 < t$
- $t < s \implies ut < us$
- $y_{i,\theta} < y_{i,\varphi\theta}$
- $y_{i,\theta} < y_{i',\theta'} \implies y_{i,\varphi\theta} < y_{i',\varphi\theta'} \quad \forall\, \varphi \in D\backslash\{1\}$ (ranking of derivatives)

Notations

Let $p \in F\{Y\}$ $and >$ be a differentially admissible ordering on $(y_{i,\theta})_{i \in I,\ \theta \in D}$,

Let $p = \sum_{z \in T'} c_z z$, $\quad T' \subseteq T$. We use

- $ld(p) := \max\{z \in T'\}$, $\quad$ here $c_z \in F \setminus \{0\}$.
- $lc(p) := c_z \quad if \;\; z = ld(p)$
- $lt(p) := lc(p)ld(p)$
- $Terms(p) \coloneqq T'$
- For $P \subseteq F\{Y\}$, we define , $L(P) := \{ld(p) | p \in P\}$.

Lexicographic ordering

Let $d_\alpha^i,\ d_\beta^j \in T := ComMonoid((y_{i,\theta})_{i\in I,\,\theta\in D}$. The lexicographic ordering on terms of differential polynomial is given as

$$d_\alpha^i \quad \geq \; d_\beta^j \qquad\qquad \text{if} \qquad i > j$$

Else $i = j$ and first non-zero difference $\alpha_1 \; - \beta_1, \alpha_2 \; - \beta_2 \;, \; \dots.., \alpha_n \; - \beta_n$ is positive.

Total degree ordering

The total degree ordering on the derivative terms is given by

$d_{\alpha}^{i} \geq d_{\beta}^{j}$ if $i > j$

Else $i = j$ and $|\alpha| > |\beta|$

Else $i = j$ and $|\alpha| = |\beta|$

and first non-zero difference $\alpha_1 - \beta_1, \alpha_2 - \beta_2, \ldots, \alpha_n - \beta_n$ is positive.

Example

In the differential polynomial

$f = (u_x^2 - 1)u_{xxy} + u_{zz}^3 - (v_{yy} - v_z)u_{xyy}.$

Let $u > v > x > y > z$, u, v are unknown functions of x, y, z.

$ld(f) = u_x^2 u_{xxy}$ w.r.t lex. ordering

$ld(f) = v_{yy}\, u_{xyy}$ w.r.t total degree ordering

Differential Gröbner basis

Let J be a differential ideal in $F\{Y\}$ and $G \subseteq F\{Y\}$, G is called differential Gröbner basis of J iff

- $0 \notin G \subseteq J$
- $< L(J) > = < L(\bar{G}^D) >$

Remark

Differential Gröbner basis may not be finite.

If we know finite DGB of a differential ideal I, we can algorithmically test the membership to this ideal:

Example. Any linear ideal in one variable has a finite differential Gröbner basis.

Unfortunately, differential Gröbner bases are often infinite:

Example. The ideal $[y^n], \quad n \geq 2$, does not have finite DGB w.r.t. lex.

Differentially reduced polynomial

Let $P \subseteq F\{Y\}$ and $p, q \in F\{Y\}$, we say that p is differentially reduced with respect to q iff

$$ld\big(\theta(q)\big) \nmid terms(p) \qquad\qquad \forall\theta \in D$$

We say that p is differentially reduced with respect to set P if p is differentially reduced with respect to all polynomials of P.

Differentially reduced set

Let $P \subseteq F\{Y\}$, then P is called differentially reduced if and only if p is differentially reduced w.r.t q for all $p, q \in P$.

Moreover, leading coefficients of all polynomials must be 1.

S-Polynomial

Let $p, q \in F\{Y\}$ be non-zero differential polynomials, then S-polynomial of p, q, denoted by $S(p, q)$, is defined as

$$S(p,q) = \frac{1}{lc(p)}\ tp - \frac{1}{lc(q)}\ sq$$

where $t, s \in D$, such that

$lcm\big(ld(p), ld(q)\big) = t\ ld(p) = sld(q)$.

$S(p,q) = 0$ if either of p or q is zero.

Normal form is a remainder of a polynomial after division by a set of given polynomials.

Normal form of a polynomial

Let R be a ring, $f \in R$ and $G = \{g_1, g_2, \dots, g_s\}$ is a finite list of polynomials in R, then normal form of f w.r.t G, denoted by $NF(f|G)$, is a polynomial in R such that

- $NF(0|G) = 0$
- $NF(f|G) \neq 0 \quad \Longrightarrow \quad ld\big(NF(f|G)\big) \notin L(G)$
- $f - NF(f|G) = \sum_{i=1}^{s} a_i\, g_i$ where $a_i \in R$, such that

  $ld(\sum_{i=1}^{s} a_i\, g_i) \geq ld(a_i\, g_i)$ for all i such that $a_i\, g_i \neq 0$.

Algorithm: Normal form(NF(f|G))

Input: $f \in K[x]$ and a finite set of polynomials G.

Output: h:= normal form of f w.r.t G

```
- $h := f;$
- While ($h \neq 0 \; and \; G_h := \{g \in G | LM(g) \; divides \; LM(h)\} \neq \emptyset$)
        choose any $g \in G_h$
        $h := h - \frac{lc(h)}{lc(g)} \frac{ld(h)}{ld(g)} g$      (S-polynomial($h, g$))
- Return $h$ ;
```

Algorithm: Reduced Normal form (redNF(f|G))

Input: $f \in K[x]$ and a finite set of polynomials G.

Output: h:= a reduced normal form of f w.r.t G

```
• $h \coloneqq 0$ ;    $g \coloneqq f$;
• While ($g \neq 0$ )
          $g = NF(g|G)$
          If $g \neq 0$
           $h \coloneqq h + lt(g)$;
           $g \coloneqq tail(g)$;
• Return ${}^{h}/_{lc(h)}$;
```

Theorem

Let J be a differential ideal in $F\{Y\}$, and $P \subseteq J\backslash\{0\}$. Then the following statements are equivalent

- P is a Gröbner basis of J.
- $< L(J) > = < L(\bar{P}^D) >$
- $f \in J \quad iff \quad NF(f|P) = 0$
- $J \subseteq [P] \qquad and \qquad for\ any\ p, q \in \bar{P}^D: \quad NF(S(p, q)|P) = 0$

Differential Gröbner basis algorithm

Input: a monomial ordering >, a set $G \subseteq F\{Y\}$, normal form algorithm

Output: A differential Gröbner basis S such that $J =< S >$

```
• $S := G$;
• $P := \{(f,g) \mid f,g \in S, f \neq g\}$;
• While ($P \neq \emptyset$)
        choose $(f,g) \in P$
        $P := P \setminus \{(f,g)\}$;
        $h := NF(spoly(f,g) | \bar{S}^D)$;
        if $(h \neq 0)$
            $P := P \cup \{(h,f) | f \in S\}$;
            $S := S \cup \{h\}$ ;
• return $S$;
```

Theorem

Every differential ideal J in differential polynomial ring $F\{Y\}$ has a unique differentially reduced differential Gröbner basis for J.

Remark:

We can make an arbitrary Gröbner basis G reduced by applying reduced normal form to $(f, G \setminus \{f\})$ for all $f \in G$.

The End

Any Questions????