

Canonical Representation of Radical Differential Ideals

Oleg Golubitsky

`oleg.golubitsky@gmail.com`

Ontario Research Centre for Computer Algebra
University of Western Ontario
London, Canada

in collaboration with Marina Kondratieva and William Sit

Motivation: Gröbner Bases

In a polynomial ring $K[x_1, \dots, x_n]$:

- fix a term order, then

ideal $I \longleftrightarrow$ Reduced Gröbner Basis (I)

Motivation: Gröbner Bases

In a polynomial ring $K[x_1, \dots, x_n]$:

- fix a term order, then

ideal $I \longleftrightarrow$ Reduced Gröbner Basis (I)

- independently of term order:

$I \longleftrightarrow$ Universal Gröbner Basis (I)

Motivation: Gröbner Bases

In a polynomial ring $K[x_1, \dots, x_n]$:

- fix a term order, then

ideal $I \longleftrightarrow$ Reduced Gröbner Basis (I)

- independently of term order:

$I \longleftrightarrow$ Universal Gröbner Basis (I)

- yields canonical representation of I

Motivation: Gröbner Bases

In a polynomial ring $K[x_1, \dots, x_n]$:

- fix a term order, then

ideal $I \longleftrightarrow$ Reduced Gröbner Basis (I)

- independently of term order:

$I \longleftrightarrow$ Universal Gröbner Basis (I)

- yields canonical representation of I
- allows to compute:

$$f \in I, \quad I \subseteq J, \quad I \cap J, \quad I : f^\infty, \quad \sqrt{I}, \quad I = P_1 \cap \dots \cap P_k, \dots$$

Motivation: Differential Ideals

In a differential polynomial ring $K\{y_1, \dots, y_n\}$, $\text{char } K = 0$, with derivations $\Delta = \{\delta_1, \dots, \delta_m\}$:

- differential ideals may be infinitely generated:

$$I = [y^2, y'^2, y''^2, \dots]$$

Motivation: Differential Ideals

In a differential polynomial ring $K\{y_1, \dots, y_n\}$, $\text{char } K = 0$, with derivations $\Delta = \{\delta_1, \dots, \delta_m\}$:

- differential ideals may be infinitely generated:

$$I = [y^2, y'^2, y''^2, \dots]$$

- for finitely generated differential ideals, their differential Gröbner basis may be infinite

Motivation: Radical Differential Ideals

- admit a finite system of generators [Ritt]:

$$I = \sqrt{[F]} = \{F\}$$

Motivation: Radical Differential Ideals

- admit a finite system of generators [Ritt]:

$$I = \sqrt{[F]} = \{F\}$$

- admit a unique finite decomposition into minimal differential prime components [Ritt]:

$$I = P_1 \cap \dots \cap P_k$$

Motivation: Radical Differential Ideals

- admit a finite system of generators [Ritt]:

$$I = \sqrt{[F]} = \{F\}$$

- admit a unique finite decomposition into minimal differential prime components [Ritt]:

$$I = P_1 \cap \dots \cap P_k$$

- prime differential ideals can be represented by their characteristic sets as saturated differential ideals:

$$P = [\mathbb{C}] : H_{\mathbb{C}}^{\infty}$$

(here $H_{\mathbb{C}}$ is the **product** of the initials and separants of the elements of \mathbb{C} ; $H_{\mathbb{C}}$ depends on the ranking)

Motivation: Radical Differential Ideals

- admit a finite system of generators [Ritt]:

$$I = \sqrt{[F]} = \{F\}$$

- admit a unique finite decomposition into minimal differential prime components [Ritt]:

$$I = P_1 \cap \dots \cap P_k$$

- prime differential ideals can be represented by their characteristic sets as saturated differential ideals:

$$P = [\mathbb{C}] : H_{\mathbb{C}}^{\infty}$$

(here $H_{\mathbb{C}}$ is the **product** of the initials and separants of the elements of \mathbb{C} ; $H_{\mathbb{C}}$ depends on the ranking)

- this allows to test membership: $f \in P \iff f \xrightarrow{\mathbb{C}} 0$

Motivation: Prime Differential Ideals

Example:

$$P = \{y'^2 + y, 2y'' + 1\} = [y'^2 + y] : y'^{\infty}$$

Motivation: Ritt Problems

- given \mathbb{C} , find F such that

$$P = [\mathbb{C}] : H_{\mathbb{C}}^{\infty} = \{F\}$$

Motivation: Ritt Problems

- given \mathbb{C} , find F such that

$$P = [\mathbb{C}] : H_{\mathbb{C}}^{\infty} = \{F\}$$

- given F , determine whether $\{F\}$ is prime

Motivation: Ritt Problems

- given \mathbb{C} , find F such that

$$P = [\mathbb{C}] : H_{\mathbb{C}}^{\infty} = \{F\}$$

- given F , determine whether $\{F\}$ is prime
- given $\mathbb{C}_1, \mathbb{C}_2$, determine whether

$$P_1 = [\mathbb{C}_1] : H_{\mathbb{C}_1}^{\infty} \subseteq P_2 = [\mathbb{C}_2] : H_{\mathbb{C}_2}^{\infty}$$

Motivation: Ritt Problems

- given \mathbb{C} , find F such that

$$P = [\mathbb{C}] : H_{\mathbb{C}}^{\infty} = \{F\}$$

- given F , determine whether $\{F\}$ is prime
- given $\mathbb{C}_1, \mathbb{C}_2$, determine whether

$$P_1 = [\mathbb{C}_1] : H_{\mathbb{C}_1}^{\infty} \subseteq P_2 = [\mathbb{C}_2] : H_{\mathbb{C}_2}^{\infty}$$

- determine whether 0 is a zero of $P = [\mathbb{C}] : H_{\mathbb{C}}^{\infty}$

Motivation: Ritt Problems (ctd.)

- given F , it is possible to compute $\mathbb{C}_1, \dots, \mathbb{C}_k$ such that $P_i = [\mathbb{C}_i] : H_{\mathbb{C}_i}^\infty$ are prime and

$$\{F\} = P_1 \cap \dots \cap P_k$$

Motivation: Ritt Problems (ctd.)

- given F , it is possible to compute $\mathbb{C}_1, \dots, \mathbb{C}_k$ such that $P_i = [\mathbb{C}_i] : H_{\mathbb{C}_i}^\infty$ are prime and

$$\{F\} = P_1 \cap \dots \cap P_k$$

- however, it may happen that the above decomposition is redundant, i.e., for some $i \neq j$

$$P_i \subset P_j$$

Motivation: Ritt Problems (ctd.)

- given F , it is possible to compute $\mathbb{C}_1, \dots, \mathbb{C}_k$ such that $P_i = [\mathbb{C}_i] : H_{\mathbb{C}_i}^\infty$ are prime and

$$\{F\} = P_1 \cap \dots \cap P_k$$

- however, it may happen that the above decomposition is redundant, i.e., for some $i \neq j$

$$P_i \subset P_j$$

- removing redundant components is equivalent to testing inclusions

$$[\mathbb{C}_i] : H_{\mathbb{C}_i}^\infty \subseteq [\mathbb{C}_j] : H_{\mathbb{C}_j}^\infty$$

Motivation: Ritt Problems (ctd.)

- given the minimal decomposition

$$I = \bigcap_{i=1}^k [\mathbb{C}_i] : H_{\mathbb{C}_i}^{\infty},$$

it is not known how to compute F such that

$$I = \{F\}$$

Motivation: Ritt Problems (ctd.)

- given the minimal decomposition

$$I = \bigcap_{i=1}^k [\mathbb{C}_i] : H_{\mathbb{C}_i}^{\infty},$$

it is not known how to compute F such that

$$I = \{F\}$$

- given F and f , it is not known how to determine whether f is a zero-divisor modulo $\{F\}$.

Uniqueness of Representation

- None of the following representations is unique for the corresponding ideal:
 - $I = \{F\}$
 - $I = P_1 \cap \dots \cap P_k$
 - $P = [\mathbb{C}] : H_{\mathbb{C}}^{\infty}$

Uniqueness of Representation

- None of the following representations is unique for the corresponding ideal:
 - $I = \{F\}$
 - $I = P_1 \cap \dots \cap P_k$
 - $P = [\mathbb{C}] : H_{\mathbb{C}}^{\infty}$
- Goal: impose some restrictions to make them unique.

Uniqueness of Representation

- None of the following representations is unique for the corresponding ideal:
 - $I = \{F\}$
 - $I = P_1 \cap \dots \cap P_k$
 - $P = [\mathbb{C}] : H_{\mathbb{C}}^{\infty}$
- Goal: impose some restrictions to make them unique.
- Hope: uniqueness may clarify relationship between these representations.

Canonical characteristic set

Assume that a ranking is fixed.

[Boulier, Lemaire; Hubert; G., Kondratieva, Ovchinnikov]:

Then a prime differential ideal has a unique characteristic set C such that for all $C \in \mathbb{C}$

- initial of C does not depend on leading derivatives of \mathbb{C}

Canonical characteristic set

Assume that a ranking is fixed.

[Boulier, Lemaire; Hubert; G., Kondratieva, Ovchinnikov]:

Then a prime differential ideal has a unique characteristic set C such that for all $C \in \mathbb{C}$

- initial of C does not depend on leading derivatives of \mathbb{C}
- C has no factors of the same rank, except for C itself

Canonical characteristic set

Assume that a ranking is fixed.

[Boulier, Lemaire; Hubert; G., Kondratieva, Ovchinnikov]:

Then a prime differential ideal has a unique characteristic set \mathbb{C} such that for all $C \in \mathbb{C}$

- initial of C does not depend on leading derivatives of \mathbb{C}
- C has no factors of the same rank, except for C itself
- the leading coefficient of C is 1

Computing unique prime decomp.

- Given F , we can compute *some* prime decomposition

$$I = \{F\} = \bigcap_{i=1}^k [\mathbb{C}_i] : H_{\mathbb{C}_i}^{\infty}$$

where the \mathbb{C}_i are canonical characteristic sets.

Computing unique prime decomp.

- Given F , we can compute *some* prime decomposition

$$I = \{F\} = \bigcap_{i=1}^k [\mathbb{C}_i] : H_{\mathbb{C}_i}^\infty$$

where the \mathbb{C}_i are canonical characteristic sets.

- **Lemma.** Let \mathbb{C} be the characteristic set of the highest rank among $\mathbb{C}_1, \dots, \mathbb{C}_k$. Then $P = [\mathbb{C}] : H_{\mathbb{C}}^\infty$ is the minimal prime component of I of the highest rank, among all minimal prime components of I .

Computing unique prime decomp.

- Given F , we can compute *some* prime decomposition

$$I = \{F\} = \bigcap_{i=1}^k [\mathbb{C}_i] : H_{\mathbb{C}_i}^\infty$$

where the \mathbb{C}_i are canonical characteristic sets.

- **Lemma.** Let \mathbb{C} be the characteristic set of the highest rank among $\mathbb{C}_1, \dots, \mathbb{C}_k$. Then $P = [\mathbb{C}] : H_{\mathbb{C}}^\infty$ is the minimal prime component of I of the highest rank, among all minimal prime components of I .
- **Proposition.** Let $\mathbb{C} = \{C_1, \dots, C_l\}$ be as above. Then

$$I = [\mathbb{C}] : H_{\mathbb{C}}^\infty \cap I : C_1 \cap \dots \cap I : C_l \cap \{F \cup H_{\mathbb{C}}\}$$

Computing unique prime decomp.

If in the decomposition

$$I = \{F\} = \bigcap_{i=1}^k [\mathbb{C}_i] : H_{\mathbb{C}_i}^\infty$$

there are several characteristic sets of the highest rank, say, $\mathbb{C}_1, \dots, \mathbb{C}_m$, then

$$\begin{aligned} I &= [\mathbb{C}_1] : H_{\mathbb{C}_1}^\infty \cap I : C_{1,1} \cap \dots \cap I : C_{1,l} \cap \{F \cup H_{\mathbb{C}_1}\} \cap \\ &\dots \\ &[\mathbb{C}_m] : H_{\mathbb{C}_m}^\infty \cap I : C_{m,1} \cap \dots \cap I : C_{m,l} \cap \{F \cup H_{\mathbb{C}_m}\} \end{aligned}$$

Computing unique prime decomp.

Observe:

- \mathbb{C} , and hence all ideals in

$$I = [\mathbb{C}] : H_{\mathbb{C}}^{\infty} \cap I : C_1 \cap \dots \cap I : C_l \cap \{F \cup H_{\mathbb{C}}\}$$

are uniquely determined by I (i.e., they do not depend on the choice of the set of generators F)

Computing unique prime decomp.

Observe:

- \mathbb{C} , and hence all ideals in

$$I = [\mathbb{C}] : H_{\mathbb{C}}^{\infty} \cap I : C_1 \cap \dots \cap I : C_l \cap \{F \cup H_{\mathbb{C}}\}$$

are uniquely determined by I (i.e., they do not depend on the choice of the set of generators F)

- Ideals $I : C_j$ and $\{F \cup H_{\mathbb{C}}\}$ strictly contain I

Computing unique prime decomp.

Observe:

- \mathbb{C} , and hence all ideals in

$$I = [\mathbb{C}] : H_{\mathbb{C}}^{\infty} \cap I : C_1 \cap \dots \cap I : C_l \cap \{F \cup H_{\mathbb{C}}\}$$

are uniquely determined by I (i.e., they do not depend on the choice of the set of generators F)

- Ideals $I : C_j$ and $\{F \cup H_{\mathbb{C}}\}$ strictly contain I
- The problem reduces to the computation of unique prime decomposition for these ideals.

Computing unique prime decomp.

Observe:

- \mathbb{C} , and hence all ideals in

$$I = [\mathbb{C}] : H_{\mathbb{C}}^{\infty} \cap I : C_1 \cap \dots \cap I : C_l \cap \{F \cup H_{\mathbb{C}}\}$$

are uniquely determined by I (i.e., they do not depend on the choice of the set of generators F)

- Ideals $I : C_j$ and $\{F \cup H_{\mathbb{C}}\}$ strictly contain I
- The problem reduces to the computation of unique prime decomposition for these ideals.
- There exist no infinitely growing chains of radical differential ideals [Ritt].

Computing unique generators

- Given the unique prime decomposition of $I = \{F\}$:

$$I = \bigcap_{i=1}^k [\mathbb{C}_i] : H_{\mathbb{C}_i}^{\infty} \quad (*)$$

Computing unique generators

- Given the unique prime decomposition of $I = \{F\}$:

$$I = \bigcap_{i=1}^k [\mathbb{C}_i] : H_{\mathbb{C}_i}^{\infty} \quad (*)$$

- Define d -prolongation of \mathbb{C}

$$\mathbb{C}^{(\leq d)} = \{C^{(j)} \mid C \in \mathbb{C}, 0 \leq j \leq d\}$$

Computing unique generators

- Given the unique prime decomposition of $I = \{F\}$:

$$I = \bigcap_{i=1}^k [\mathbb{C}_i] : H_{\mathbb{C}_i}^{\infty} \quad (*)$$

- Define d -prolongation of \mathbb{C}

$$\mathbb{C}^{(\leq d)} = \{C^{(j)} \mid C \in \mathbb{C}, 0 \leq j \leq d\}$$

- We have:

$$[\mathbb{C}] : H_{\mathbb{C}}^{\infty} = \bigcup_{d=0}^{\infty} (\mathbb{C}^{(\leq d)}) : H_{\mathbb{C}}^{\infty}.$$

Computing unique generators (ctd.)

- for $d = 0, 1, 2, \dots$ consider the algebraic ideal:

$$J_d = \bigcap_{i=1}^k (\mathbb{C}^{(\leq d)}) : H_{\mathbb{C}}^{\infty}$$

Computing unique generators (ctd.)

- for $d = 0, 1, 2, \dots$ consider the algebraic ideal:

$$J_d = \bigcap_{i=1}^k (\mathbb{C}^{(\leq d)}) : H_{\mathbb{C}}^{\infty}$$

- compute lexicographic reduced Gröbner basis B_d of J_d

Computing unique generators (ctd.)

- for $d = 0, 1, 2, \dots$ consider the algebraic ideal:

$$J_d = \bigcap_{i=1}^k (\mathbb{C}^{(\leq d)}) : H_{\mathbb{C}}^{\infty}$$

- compute lexicographic reduced Gröbner basis B_d of J_d
- compute the unique prime decomposition of $\{B_d\}$

Computing unique generators (ctd.)

- for $d = 0, 1, 2, \dots$ consider the algebraic ideal:

$$J_d = \bigcap_{i=1}^k (\mathbb{C}^{(\leq d)}) : H_{\mathbb{C}}^{\infty}$$

- compute lexicographic reduced Gröbner basis B_d of J_d
- compute the unique prime decomposition of $\{B_d\}$
- if this decomposition coincides with $(*)$, output B_d

Example

- Let $I = \{y'^2 + y^3\}$ (actually, this ideal is prime)

Example

- Let $I = \{y'^2 + y^3\}$ (actually, this ideal is prime)
- Compute some prime decomposition:

$$I = [y'^2 + y^3] : y'^{\infty} \cap [y]$$

Example

- Let $I = \{y'^2 + y^3\}$ (actually, this ideal is prime)
- Compute some prime decomposition:

$$I = [y'^2 + y^3] : y'^{\infty} \cap [y]$$

- Among the two characteristic sets, choose the one with maximal rank:

$$\mathbb{C} = \{y'^2 + y^3\}$$

Example

- Let $I = \{y'^2 + y^3\}$ (actually, this ideal is prime)
- Compute some prime decomposition:

$$I = [y'^2 + y^3] : y'^{\infty} \cap [y]$$

- Among the two characteristic sets, choose the one with maximal rank:

$$\mathbb{C} = \{y'^2 + y^3\}$$

- $I = [y'^2 + y^3] : y'^{\infty} \cap I : (y'^2 + y^3) \cap \{y'^2 + y^3, 2y'\}$

Example

- Let $I = \{y'^2 + y^3\}$ (actually, this ideal is prime)
- Compute some prime decomposition:

$$I = [y'^2 + y^3] : y'^{\infty} \cap [y]$$

- Among the two characteristic sets, choose the one with maximal rank:

$$\mathbb{C} = \{y'^2 + y^3\}$$

- $I = [y'^2 + y^3] : y'^{\infty} \cap I : (y'^2 + y^3) \cap \{y'^2 + y^3, 2y'\}$
- We have: $I : (y'^2 + y^3) = (1)$ and $\{y'^2 + y^3, 2y'\} = [y]$

Example

- Let $I = \{y'^2 + y^3\}$ (actually, this ideal is prime)
- Compute some prime decomposition:

$$I = [y'^2 + y^3] : y'^{\infty} \cap [y]$$

- Among the two characteristic sets, choose the one with maximal rank:

$$\mathbb{C} = \{y'^2 + y^3\}$$

- $I = [y'^2 + y^3] : y'^{\infty} \cap I : (y'^2 + y^3) \cap \{y'^2 + y^3, 2y'\}$
- We have: $I : (y'^2 + y^3) = (1)$ and $\{y'^2 + y^3, 2y'\} = [y]$
- Output: $I = [y'^2 + y^3] : y'^{\infty} \cap [y]$

Example

Recover generators from $I = [y'^2 + y^3] : y'^\infty \cap [y]$.

- $d = 0 : (y'^2 + y^3) : y'^\infty \cap (y) = (yy'^2 + y^4)$

Example

Recover generators from $I = [y'^2 + y^3] : y'^\infty \cap [y]$.

- $d = 0 : (y'^2 + y^3) : y'^\infty \cap (y) = (yy'^2 + y^4)$
- Unique prime decomposition of $\{yy'^2 + y^4\}$:

$$[y'^2 + y^3] : y'^\infty \cap [y]$$

Example

Recover generators from $I = [y'^2 + y^3] : y'^\infty \cap [y]$.

- $d = 0 : (y'^2 + y^3) : y'^\infty \cap (y) = (yy'^2 + y^4)$
- Unique prime decomposition of $\{yy'^2 + y^4\}$:

$$[y'^2 + y^3] : y'^\infty \cap [y]$$

- Output the unique generator of I : $yy'^2 + y^4$.

Property of unique prime decomp.

- **Definition** Let $P = [\mathbb{C}] : H_{\mathbb{C}}^{\infty}$. A point $\eta \in L^n$, where L is a differential extension of K , is a **regular zero** of \mathbb{C} , if $\mathbb{C}(\eta) = 0$ and $H_{\mathbb{C}}(\eta) \neq 0$.

Property of unique prime decomp.

- **Definition** Let $P = [\mathbb{C}] : H_{\mathbb{C}}^{\infty}$. A point $\eta \in L^n$, where L is a differential extension of K , is a **regular zero** of \mathbb{C} , if $\mathbb{C}(\eta) = 0$ and $H_{\mathbb{C}}(\eta) \neq 0$.
- **Proposition** Let

$$I = \{F\} = \bigcap_{i=1}^k [\mathbb{C}_i] : H_{\mathbb{C}_i}^{\infty}$$

be the unique prime decomposition of I . Then $F(\eta) = 0$ iff η is a regular zero of some \mathbb{C}_i .

Property of unique prime decomp.

- **Definition** Let $P = [\mathbb{C}] : H_{\mathbb{C}}^{\infty}$. A point $\eta \in L^n$, where L is a differential extension of K , is a **regular zero** of \mathbb{C} , if $\mathbb{C}(\eta) = 0$ and $H_{\mathbb{C}}(\eta) \neq 0$.
- **Proposition** Let

$$I = \{F\} = \bigcap_{i=1}^k [\mathbb{C}_i] : H_{\mathbb{C}_i}^{\infty}$$

be the unique prime decomposition of I . Then $F(\eta) = 0$ iff η is a regular zero of some \mathbb{C}_i .

- **Claim.** All known algorithms compute decompositions satisfying the above property.

Property of unique prime decomp.

- **Definition** Let $P = [\mathbb{C}] : H_{\mathbb{C}}^{\infty}$. A point $\eta \in L^n$, where L is a differential extension of K , is a **regular zero** of \mathbb{C} , if $\mathbb{C}(\eta) = 0$ and $H_{\mathbb{C}}(\eta) \neq 0$.
- **Proposition** Let

$$I = \{F\} = \bigcap_{i=1}^k [\mathbb{C}_i] : H_{\mathbb{C}_i}^{\infty}$$

be the unique prime decomposition of I . Then $F(\eta) = 0$ iff η is a regular zero of some \mathbb{C}_i .

- **Claim.** All known algorithms compute decompositions satisfying the above property.
- **Claim.** Given any prime decomposition satisfying the above property, one can compute generators of I .
(see: W. Sit, *Computations on Quasi Algebraic Set*)