A Bound that Reduces Differential Nullstellensatz to the Algebraic One

Oleg Golubitsky

Postdoctoral Fellow

Ontario Research Centre for Computer Algebra

University of Western Ontario

Joint work with:

Marina Kondratieva	(Moscow State University)
Alexey Ovchinnikov	(University of Illinois at Chicago)
Agnes Szanto	(North Carolina State University)

The Problem of Consistency

Given a system of **polynomial PDE**, e.g.:

$$\begin{cases} u_x + v_y = 0 \\ u_y - v_x = 0 \\ (u_{xx} + u_{yy})^2 + (v_{xx} + v_{yy})^2 = 0 \end{cases}$$

Question: Is it consistent, i.e., does it have solutions?

(We look for solutions in differential extensions of the coefficient field ...)

The Problem of Consistency

Given a system of **polynomial PDE**, e.g.:

$$\begin{cases} u_x + v_y = 0 \\ u_y - v_x = 0 \\ (u_{xx} + u_{yy})^2 + (v_{xx} + v_{yy})^2 = 0 \end{cases}$$

<u>Question</u>: Is it consistent, i.e., does it have solutions?

(We look for solutions in differential extensions of the coefficient field ...)

<u>Answer</u>: YES

The Problem of Consistency

Given a system of **polynomial PDE**, e.g.:

$$\begin{cases} u_x + v_y = 0 \\ u_y - v_x = 0 \\ (u_{xx} + u_{yy})^2 + (v_{xx} + v_{yy})^2 = 1 \end{cases}$$

Question: Is it consistent, i.e., does it have solutions?

(We look for solutions in differential extensions of the coefficient field ...)

Answer: NO

Corresponding algebraic system

$$\begin{cases} u_x + v_y = 0 \\ u_y - v_x = 0 \\ (u_{xx} + u_{yy})^2 + (v_{xx} + v_{yy})^2 = 0 \end{cases} \longleftrightarrow \begin{cases} z_1 + z_2 = 0 \\ z_3 - z_4 = 0 \\ (z_5 + z_6)^2 + (z_7 + z_8)^2 = 0 \end{cases}$$

PDE system is consistent $\Longrightarrow$ Algebraic system is consistent

Corresponding algebraic system

$$\begin{cases} u_x + v_y = 0 \\ u_y - v_x = 0 \\ (u_{xx} + u_{yy})^2 + (v_{xx} + v_{yy})^2 = 1 \end{cases} \longleftrightarrow \begin{cases} z_1 + z_2 = 0 \\ z_3 - z_4 = 0 \\ (z_5 + z_6)^2 + (z_7 + z_8)^2 = 1 \end{cases}$$

PDE system is *in*consistent

Algebraic system is consistent

The converse is not always true.

Differential Nullstellensatz

Notation $F^{(\leq k)}$

set of all partial derivatives of elements of F of order $\leq k$

Theorem Polynomial PDE system $F = 0$ has **no solutions**

$$\Updownarrow$$

$$\exists \;\; k \geq 0 \quad \text{such that} \quad 1 \in \langle F^{(\leq k)} \rangle.$$

Example

$$\begin{cases} u_x + v_y = 0 \\ u_y - v_x = 0 \\ (u_{xx} + u_{yy})^2 + (v_{xx} + v_{yy})^2 = 1 \end{cases} \qquad k = 1$$

The Problem

Given non-negative integers m, n, h, d.

Find $k(m, n, h, d)$ such that:

Polynomial PDE system $F = 0$
in m independent variables,
n dependent variables
of order h
and degree d
has no solutions

$$\Updownarrow$$

$$1 \in \left\langle F^{\left(\leq k(m,n,h,d)\right)} \right\rangle$$

Main Result

[Seidenberg, 1956] Proposed to analyse the differential elimination algorithm to obtain the bound.

Theorem [GKOS '08]

$$k(m, n, h, d) = A(2m + 2n + 4, \max(3, h, d) + 1).$$

Here $A(m, n)$ is the Ackermann function.

Ackermann Function

Definition

$$\begin{aligned} A(0,n) &= n+1 \\ A(m+1,0) &= A(m,1) \\ A(m+1,n+1) &= A(m,A(m+1,n)). \end{aligned}$$

First few values [Wikipedia]:

	0	1	2	3	4	n
0	1	2	3	4	5	$n+1$
1	2	3	4	5	6	$n+2$
2	3	5	7	9	11	$2n+3$
3	5	13	29	61	125	$2^{n+3}-3$
4	13	65533	$2^{65536}-3$	$2^{2^{65536}}-3$	$A(3,A(4,3))$	$\underbrace{2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}}_{n+3 \text{ twos}}$
5	65533	$\underbrace{2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}}_{65535 \text{ twos}}$	$A(4,A(5,1))$	$A(4,A(5,2))$	$A(4,A(5,3))$	$A(4,A(5,n-1))$
m						

Why Ackermann Function?

Definition. A sequence of non-negative integer n-tuples $\tau_1, \tau_2, \ldots$ is called **dicksonian**, if for all $i < j$, $\tau_j - \tau_i$ has at least one negative coordinate.

Alternative definition: a sequence of monomials $u_1, u_2, \ldots$ such that $u_i \nmid u_j$ for $i < j$.

Lemma [Dickson] Every dicksonian sequence terminates.

Lemma [G. Socias, 1991] Every dicksonian sequence of n-tuples, in which the maximal coordinate at each step increases by 1, has length at most

$$A(n, m-1) - 1,$$

where m is the maximal coordinate of the first tuple.

Why Dicksonian Sequences?

Polynomial *completion* algorithms such as

Algorithm Buchberger (F, $\leq$)
  repeat
    $R :=$ NormalForm(SPoly(F), F, $\leq$) $\setminus \{0\}$
    $F := F \cup R$
  until $R = \varnothing$
  return F
end

produce dicksonian sequences of leading monomials.

Why Dicksonian Sequences?

Differential-algebraic completion algorithms, when applied to polynomial PDE systems, produce sequences of *powers of leading partial derivatives* of the form

$$\left(\frac{\partial^h u_j}{\partial x_1^{i_1} \ldots \partial x_m^{i_m}}\right)^d$$

such that the corresponding $(m+n)$-tuples

$$(i_1, \ldots, i_m, 0, \ldots, d, \ldots, 0)$$

form dicksonian sequences.

How Fast Do Tuples Grow?

Polynomial case: at each iteration, degree doubles (at most).

Differential case: at each iteration,

- order h doubles
- degree d becomes $(4d)^{\binom{2h+m}{m}+1}$ [GKOS '08].

We have a dicksonian sequence of $(m+n)$-tuples, in which the coordinates of the i-th tuple are bounded by a certain function $f(i)$.

How Long Are these Sequences?

Function $f(i)$ is not growing too fast: $\exists\ \delta$ such that $\forall\ i$

$$f(i+1) - f(i) \leq A(\delta, f(i) - 1).$$

Lemma [GKOS'08] Length of such sequence does not exceed

$$\left\lceil f^{-1}(A[m+n+\delta, f(1) - 1]) \right\rceil$$

and the coordinates of the last tuple do not exceed

$$A(m+n+\delta, f(1) - 1).$$

Complexity of Differential Completion

The number of iterations is bounded by:

$$A(m + n + 3, \max(9, 2^h, d) - 1)$$

and the orders and degrees of the output, as well as the number of differentiations required to produce it, by:

$$k_{\text{completion}} = A(m + n + 4, \max(3, h, d) - 1).$$

End of story?

What is the output of differential completion?

Inequations

Differential completion uses *pseudo-reduction*. Therefore, its output is equivalent to the input only *subject to inequations*.

Formally:

$$F = 0 \quad \xrightarrow{\text{completion}} \quad \bar{F} = 0,\ s \neq 0$$

such that

- $F(u) = 0 \;\Rightarrow\; \bar{F}(u) = 0$
- $\bar{F}(u) = 0 \;\; and \;\; s(u) \neq 0 \;\Rightarrow\; F(u) = 0$
- There may be solutions of $F = 0$ on which s vanishes. These solutions cannot be obtained from $\bar{F} = 0$, $s \neq 0$.

Completion of Inconsistent Systems

If $F = 0$ is inconsistent, it is *not* guaranteed that

$$\bar{F} = \{1\},$$

or even that

$$1 \in \langle \bar{F} \rangle,$$

but only that system

$$\bar{F} = 0, \; s \neq 0$$

is inconsistent, i.e.,

$$s \in \sqrt{\langle \bar{F} \rangle},$$

where s is the product of initials and separants of $\bar{F}$.

Splitting

$$F = 0$$

$$\bar{F} = 0,\ s \neq 0 \qquad F_1 = F \cup \{s\} = 0$$

$$\bar{F}_1 = 0,\ s_1 \neq 0 \qquad F_2 = F_1 \cup \{s_1\} = 0$$

$$\ldots \qquad \ldots$$

Height of Splitting Tree

$$F = 0$$

$$\bar{F} = 0,\ s \neq 0 \qquad F_1 = F \cup \{s\} = 0$$

$$\bar{F}_1 = 0,\ s_1 \neq 0 \qquad F_2 = F_1 \cup \{s_1\} = 0$$

$$\ldots \qquad \ldots$$

- Walking down the tree produces a dicksonian sequence
- At each step orders and degrees grow no faster than

$$A(m + n + 4, \max(3, h, d) - 1).$$

- Therefore, the height of the tree is bounded by

$$\log_4(\log_4(\log_4(A(2m + 2n + 4, \max(3, h, d) - 1)))).$$

Obtaining Expression for 1

Let $F = 0$ be an inconsistent system.

$$F = 0$$

$$\bar{F} = 0,\ s \neq 0 \qquad\qquad F_1 = F \cup \{s\} = 0$$

$$\bar{F} \subset \langle F^{(\leq k_{\text{completion}})} \rangle$$
$$s \in \sqrt{\langle \bar{F} \rangle}$$

Suppose that we "recursively" obtained bound k_1 for F_1.
Then $1 \in \langle F^{(\leq k_1)} \rangle + \langle s^{(\leq k_1)} \rangle$.
And sufficiently large powers of derivatives of s can be expressed in terms of derivatives of $\bar{F}$.

Expressing Powers of Derivatives

- $s \in \sqrt{\langle \bar{F} \rangle}$
- [Kollar, 1988] A bound for q such that

$$s^q \in \langle \bar{F} \rangle$$

  in terms of number of variables and degrees of $\bar{F}$.
- [Ritt] If $s^q \in \langle G \rangle$, then

$$\left(\frac{\partial s}{\partial x_i} \right)^{2q-1} \in \langle G^{(\leq q)} \rangle.$$

  Proof for $q = 2$:

$$s^2 \in \langle G \rangle \;\Rightarrow\; ss' \in \langle G, G' \rangle \;\Rightarrow\; (s')^2 + ss'' \in \langle G, G', G'' \rangle \;\Rightarrow\; (s')^3 \in \langle G, G', G'' \rangle.$$