Mining effective information from nonconstructive proofs in differential algebra

William Simmons
(joint with Henry Towsner)

AMS Spring Eastern Sectional Meeting
Hunter College, City University of New York
May 6, 2017

Bounds from an algorithmic perspective

Which of the following, if either, is a prime ideal in $\mathbb{Q}[x, y, z]$?

- $(x^2 + yz, x^2z^3 - y^4, 3xyz - y^2 - 2)$
- $(x^2 + yz, x^2z^3 - y^4, zy^3 - y^2 - 1)$

Bounds from an algorithmic perspective

Which of the following, if either, is a prime ideal in $\mathbb{Q}[x, y, z]$?

- $(x^2 + yz, x^2z^3 - y^4, 3xyz - y^2 - 2)$ ✗
- $(x^2 + yz, x^2z^3 - y^4, zy^3 - y^2 - 1)$ ✓

Bounds from an algorithmic perspective

Which of the following, if either, is a prime ideal in $\mathbb{Q}[x, y, z]$?

- $(x^2 + yz, x^2z^3 - y^4, 3xyz - y^2 - 2)$ ✗
- $(x^2 + yz, x^2z^3 - y^4, zy^3 - y^2 - 1)$ ✓

Theorem (∼ Hermann, 1926)

There is an algorithm for deciding primality of ideals in polynomial rings over fields. There is a bound that is:

1. Uniform,
2. Doubly exponential in the number of variables, and
3. Polynomial in the degree of the generators.

Bounds from an algorithmic perspective

Which of the following, if either, is a prime ideal in $\mathbb{Q}[x, y, z]$?

- $(x^2 + yz, x^2z^3 - y^4, 3xyz - y^2 - 2)$ ✗
- $(x^2 + yz, x^2z^3 - y^4, zy^3 - y^2 - 1)$ ✓

Theorem (∼ Hermann, 1926)

There is an algorithm for deciding primality of ideals in polynomial rings over fields. There is a bound that is:

1. Uniform,
2. Doubly exponential in the number of variables, and
3. Polynomial in the degree of the generators.

In other words, there is $c \in \mathbb{N}$ such that for all ideals $I \subseteq K[X_1, ..., X_n]$ having generators of degree at most b, if $fg \in I$ implies $f \in I$ or $g \in I$ for all f, g of degree $\leq (b^c)^{2^n}$, then I is prime.

Bounds from a nonconstructive perspective

Theorem (van den Dries and Schmidt, 1984)

There *exists* a uniform bound for detecting prime ideals in polynomial rings over fields.

Bounds from a nonconstructive perspective

Theorem (van den Dries and Schmidt, 1984)

There *exists* a uniform bound for detecting prime ideals in polynomial rings over fields.

- Pro: "... by concentrating on existence proofs for bounds, rather than on their construction, it is possible to gain a lot in efficiency of exposition."
- Con: No numerical value

Bounds in differential polynomial rings

- We work with a differential field K of characteristic zero having commuting derivations $\Delta = \{\delta_1, \ldots, \delta_m\}$.

Bounds in differential polynomial rings

- We work with a differential field K of characteristic zero having commuting derivations $\Delta = \{\delta_1, \ldots, \delta_m\}$.
- Given $A \subseteq K\{X_1, \ldots, X_n\}$, we write (A) for the ideal generated by A and $[A]$ for the differential ideal generated by A.

Bounds in differential polynomial rings

- We work with a differential field K of characteristic zero having commuting derivations $\Delta = \{\delta_1, \ldots, \delta_m\}$.
- Given $A \subseteq K\{X_1, \ldots, X_n\}$, we write (A) for the ideal generated by A and $[A]$ for the differential ideal generated by A.

Open question

Is there a uniform bound, depending only on the number of variables and derivations and on the degree and order of the generators, for detecting prime differential ideals?

Bounds in differential polynomial rings

- We work with a differential field K of characteristic zero having commuting derivations $\Delta = \{\delta_1, \ldots, \delta_m\}$.
- Given $A \subseteq K\{X_1, \ldots, X_n\}$, we write (A) for the ideal generated by A and $[A]$ for the differential ideal generated by A.

Open question

Is there a uniform bound, depending only on the number of variables and derivations and on the degree and order of the generators, for detecting prime differential ideals?

This is equivalent to the long-standing *Ritt problem*, one version of which which asks for an algorithm to decompose a radical differential ideal as an intersection of minimal prime differential ideals.

A partial primality bound

Theorem (Harrison-Trainor, Klys, and Moosa, 2012)

There *exists* a uniform bound $M(b, m, n)$ such that a proper differential ideal $[\Lambda] \subseteq K\{X_1, \ldots, X_n\}$ with m derivations and generators of degree and order at most b is prime if $fg \in [\Lambda]$ implies either $f \in [\Lambda]$ or $g \in [\Lambda]$ for all f of order and degree $\leq M(b, m, n)$.

A partial primality bound

Theorem (Harrison-Trainor, Klys, and Moosa, 2012)

There *exists* a uniform bound $M(b, m, n)$ such that a proper differential ideal $[\Lambda] \subseteq K\{X_1, \ldots, X_n\}$ with m derivations and generators of degree and order at most b is prime if $fg \in [\Lambda]$ implies either $f \in [\Lambda]$ or $g \in [\Lambda]$ for all f of order and degree $\leq M(b, m, n)$.

The proof involves *ultraproducts*; this statement of the theorem is the finitary version of the nonstandard result that HTKM actually prove.

The strategy is to examine how notions like primality transfer back and forth from ultraproducts.

Functional interpretations

Functional interpretations translate proofs in one formal system into constructive proofs in another system.

Functional interpretations

Functional interpretations translate proofs in one formal system into constructive proofs in another system.

Idea: Define a syntactic transformation that gives a constructive reading of the connectives and quantifiers.

Functional interpretations

Functional interpretations translate proofs in one formal system into constructive proofs in another system.

Idea: Define a syntactic transformation that gives a constructive reading of the connectives and quantifiers.

The original system is a classical system of arithmetic like PA (Peano Arithmetic).The new system (which we denote by T) is quantifier-free and works with computable functionals such as primitive recursive functions and others like Ackermann's function.

Functional interpretations

Functional interpretations translate proofs in one formal system into constructive proofs in another system.

Idea: Define a syntactic transformation that gives a constructive reading of the connectives and quantifiers.

The original system is a classical system of arithmetic like PA (Peano Arithmetic).The new system (which we denote by T) is quantifier-free and works with computable functionals such as primitive recursive functions and others like Ackermann's function.

Theorem (Gödel, 1958)

Let ψ be a formula in the language of arithmetic and $\psi_{FI}(x, y)$ the functional interpretation of ψ.

If $PA \vdash \psi$, then there exists a tuple of terms t such that $T \vdash \psi_{FI}(t, y)$, where t witnesses the existential claims of ψ and freeness of y witnesses the universal claims.

Example: Noetherian versus "local" Noetherian

In an appropriate language, being *Noetherian* is an $\forall\exists\forall$ or Π_3-statement:

Example: Noetherian versus “local” Noetherian

In an appropriate language, being *Noetherian* is an $\forall\exists\forall$ or Π_3-statement:

For all ascending sequences of ideals (I_j), there exists $m \in \mathbb{N}$ such that for all $n \geq m$, $I_n = I_m$.

Example: Noetherian versus "local" Noetherian

In an appropriate language, being *Noetherian* is an $\forall\exists\forall$ or Π_3-statement: For all ascending sequences of ideals (I_j), there exists $m \in \mathbb{N}$ such that for all $n \geq m$, $I_n = I_m$.

$$\Downarrow$$

The functional interpretation weakens this to a $\forall\exists/\Pi_2$-statement:

Example: Noetherian versus "local" Noetherian

In an appropriate language, being *Noetherian* is an $\forall\exists\forall$ or Π_3-statement:

For all ascending sequences of ideals (I_j), there exists $m \in \mathbb{N}$ such that for all $n \geq m$, $I_n = I_m$.

$$\Downarrow$$

The functional interpretation weakens this to a $\forall\exists/\Pi_2$-statement:

For all monotonically increasing functions $\mathbf{D} : \mathbb{N} \to \mathbb{N}$ and ascending sequences of ideals (I_j) such that the generators of I_j have degrees bounded by $\mathbf{D}(j)$, there exists $m \in \mathbb{N}$ such that $I_j = I_{j+1}$ for some $j < m$.

Some consequences and caveats

- The functional interpretation leaves Π_2 statements unchanged, so if ψ was originally equivalent to a Π_2 statement, we get a constructive proof of ψ.

Some consequences and caveats

- The functional interpretation leaves Π_2 statements unchanged, so if ψ was originally equivalent to a Π_2 statement, we get a constructive proof of ψ.
- So to prove Π_2-statements (like HTKM's partial primality result) the functional interpretation implies that it is never *necessary* to use nonconstructive axioms.

Some consequences and caveats

- The functional interpretation leaves Π_2 statements unchanged, so if ψ was originally equivalent to a Π_2 statement, we get a constructive proof of ψ.
- So to prove Π_2-statements (like HTKM's partial primality result) the functional interpretation implies that it is never *necessary* to use nonconstructive axioms.
- In practice, you can informally use the functional interpretation to write constructive proofs in ordinary mathematical language.

Some consequences and caveats

- The functional interpretation leaves Π_2 statements unchanged, so if ψ was originally equivalent to a Π_2 statement, we get a constructive proof of ψ.
- So to prove Π_2-statements (like HTKM's partial primality result) the functional interpretation implies that it is never *necessary* to use nonconstructive axioms.
- In practice, you can informally use the functional interpretation to write constructive proofs in ordinary mathematical language.
- There is a close relationship between the functional interpretation, properties preserved under ultraproducts, and the existence of uniform bounds.

Some consequences and caveats

- The functional interpretation leaves Π_2 statements unchanged, so if ψ was originally equivalent to a Π_2 statement, we get a constructive proof of ψ.
- So to prove Π_2-statements (like HTKM's partial primality result) the functional interpretation implies that it is never *necessary* to use nonconstructive axioms.
- In practice, you can informally use the functional interpretation to write constructive proofs in ordinary mathematical language.
- There is a close relationship between the functional interpretation, properties preserved under ultraproducts, and the existence of uniform bounds.
- The functional interpretation does not optimize bounds for you.

Mining the partial primality proof

Theorem (S. and Towsner, 2016)

Let $\Lambda \subseteq K\{X_1, \ldots, X_n\}_{\leq b}$ be given with $1 \notin [\Lambda]$. If either $f \in [\Lambda]$ or $g \in [\Lambda]$ for all $f, g \in K\{X_1, \ldots, X_n\}$ with $fg \in [\Lambda]$ and $f \in K\{X_1, \ldots, X_n\}_{\leq M(b,m,n)}$, then $[\Lambda]$ is prime.

- Subscripts denote a bound on the order and degree.
- $M(b, m, n)$ is now an explicit recursively-defined function described below.

Mining the partial primality proof

Theorem (S. and Towsner, 2016)

Let $\Lambda \subseteq K\{X_1, \ldots, X_n\}_{\leq b}$ be given with $1 \notin [\Lambda]$. If either $f \in [\Lambda]$ or $g \in [\Lambda]$ for all $f, g \in K\{X_1, \ldots, X_n\}$ with $fg \in [\Lambda]$ and $f \in K\{X_1, \ldots, X_n\}_{\leq M(b,m,n)}$, then $[\Lambda]$ is prime.

- Subscripts denote a bound on the order and degree.
- $M(b, m, n)$ is now an explicit recursively-defined function described below.

Strategy:

1. Apply the functional interpretation to each contributing lemma. We know we will get uniform bounds because these lemmas involve properties preserved under ultraproducts.

Mining the partial primality proof

2. Eventually we get back to the core ingredients: flat extensions of (algebraic) polynomial rings and (local) finiteness of descending chains of autoreduced sets.

3. Compute bounds on the basic steps.

Mining the partial primality proof

2. Eventually we get back to the core ingredients: flat extensions of (algebraic) polynomial rings and (local) finiteness of descending chains of autoreduced sets.
3. Compute bounds on the basic steps.
4. Go forward packaging the bounds on the basic steps and the intermediate lemmas. Arrive systematically at the final bound $M(b, m, n)$.
5. Analyze $M(b, m, n)$'s recursive definition.

Conclusions

- Recall the *fast growing hierarchy*, defined inductively by:
  - $f_0(n) = n + 1$,
  - $f_{\alpha+1}(n) = f_\alpha^n(n)$, and
  - $f_\alpha(n) = f_{\beta_n}(n)$ for a certain increasing sequence $\{\beta_n\}$ converging to α.

  Functions can be compared to the benchmarks f_α on the basis of eventual dominance by a some finite power of f_α.

Conclusions

- Recall the *fast growing hierarchy*, defined inductively by:
  - $f_0(n) = n + 1$,
  - $f_{\alpha+1}(n) = f_\alpha^n(n)$, and
  - $f_\alpha(n) = f_{\beta_n}(n)$ for a certain increasing sequence $\{\beta_n\}$ converging to α.

  Functions can be compared to the benchmarks f_α on the basis of eventual dominance by a some finite power of f_α.

- With m, n fixed, $M(b, m, n)$ grows as an iterated Ackermannian function of b. It grows roughly as fast as f_{ω^m}.

- By comparison, the usual Ackermann function appears at stage ω of the hierarchy.

Questions remain

Results of Moreno Socías and Simpson in essence show that if you need (local) Noetherianity in your proof, the bounds must be non-primitive recursive.

Question: Is local Noetherianity *necessary* to prove theorems such as the partial primality bound?

References I

Kurt Gödel.
Über eine bisher noch nicht benützte Erweiterung des finiten Standpunktes.
Dialectica, 12:280–287, 1958.

Matthew Harrison-Trainor, Jack Klys, and Rahim Moosa.
Nonstandard methods for bounds in differential polynomial rings.
J. Algebra, 360:71–86, 2012.

Grete Hermann.
Die Frage der endlich vielen Schritte in der Theorie der Polynomideale.
Math. Ann., 95(1):736–788, 1926.

William Simmons and Henry Towsner.
Proof mining and effective bounds in differential polynomial rings.
arXiv preprint arXiv:1609.07509, 2016.

References II

L. van den Dries and K. Schmidt.
Bounds in the theory of polynomial rings over fields. A nonstandard approach.
Invent. Math., 76(1):77–91, 1984.