

## RESEARCH STATEMENT

WILLIAM D. SIMMONS

My research applies mathematical logic to algebra and computation. One major project extracts effective bounds from “nonconstructive” proofs. Another concerns completeness in the young field of differential algebraic geometry. My most recent initiatives involve formalized mathematics and computer science. All address problems with a significant algorithmic component and use tools from logic to give new insights into classical questions.

### 1. CONSTRUCTIVE CONTENT: FINDING THE CONCRETE IN THE ABSTRACT

Surprisingly, proofs that employ ultraproducts or other abstract methods often have a “hidden combinatorial core” [20]. The effective content frequently comes in the form of uniform bounds on the processes in question.

Putting a family of techniques under a single name, *functional interpretations* are syntactic transformations of logical formulas from one language to another, often involving higher-order types [2]. The study of proof interpretations began with Herbrand’s theorem and has grown to include many variants [20]. As a simple example, a formula  $\forall x \exists y \varphi(x, y)$ —read as “for all  $x$ , there exists  $y$  such that property  $\varphi$  holds of  $x$  and  $y$ ”—can be rewritten  $\exists F \forall x \varphi(x, F(x))$ . This claims there is a function (computable, if we are working in an adequate theory) that, given an input, produces a witness to the original claim. Carried out on entire arguments, these “proof mining” methods can actually identify non-obvious structure and proof strategies [3, 38].

In [31], Towsner and I use the functional interpretation to systematically extract uniform bounds from ultraproduct proofs in [18]. In that paper, Harrison-Trainor, Klys, and Moosa adapt the techniques of van den Dries and Schmidt [39] to the more complicated case of differential polynomial rings. Differential fields enrich the ring structure by adding derivations (additive endomorphisms obeying the usual product rule for derivatives). This framework allows applications like deciding the consistency of systems of polynomial differential equations.

Our work in [31] culminates in several bounds that are new to the literature. In [11], Freitag, Li, and Scanlon remark that “producing explicit equations for differential Chow varieties in specific cases would require effectivizing Theorem 6.1” of [18], which is precisely the content of our Corollary 5.49. We also give an explicit bound on a weakened version of the primality problem for differential ideals: let  $\Lambda$  be a finite set of differential polynomials generating a proper differential ideal  $J$ . There exists a bound  $M$  on order and degree such that if  $fg \in J$  implies either  $f \in J$  or  $g \in J$  for all  $f$  bounded by  $M$ , then  $J$  is prime. (The full problem is open and equivalent to the *Ritt problem* [13].) We recursively define a function whose values give an upper bound on  $M$ , and then we analyze the definition to compare the growth rate to a well-known benchmark. Finally, we state and prove a finitary version of the Ritt-Raudenbush basis theorem [22].

A significant meta-mathematical question arising from our work concerns finiteness principles like Dickson’s Lemma and Hilbert’s Basis Theorem. Recently there has been considerable interest in analyzing the complexity of the differential Nullstellensatz [7, 14, 16, 23]. However, all current proofs invoke the aforementioned results or something logically equivalent. Results of Simpson [34] and Socías [35] show that such lemmas introduce non-primitive-recursive bounds. If these principles are *necessary* to prove the differential Nullstellensatz, then the known Ackermannian bounds are probably close to optimal. If not, there may be much smaller bounds but fundamentally new arguments will be needed to prove them. Either way, the complexity of algebraic algorithms (and hence their feasibility for applications) is intimately tied to axiomatic issues that I study.

In [30], Towsner and I extend our methods to the special ultraproducts used by Schmidt in [28]. There Schmidt proves nonconstructively the *existence* of polynomial-growth bounds on deciding (in the algebraic, not differential, case) if a given ideal is prime. Starting from this ultraproduct proof and applying methods from computational algebra (specifically, Gröbner bases), we obtain an upper bound on the complexity of the prime ideal problem as a polynomial function of the degree of the generators (Theorem 4.35 in [30]). To our knowledge, this is the first such bound in the literature. We also find similar bounds on deciding if an ideal is maximal (Theorem 5.4). This makes effective an ultraproduct argument of Schoutens (Lemma 4.1.4 in [29]).

My ongoing research encompasses more general rings and classes of ideals. Combining theorems from [1] and [30], I have found an explicit bound on prime ideals in polynomial rings over  $\mathbb{Z}$ . I have also obtained bounds in the field case on the degree of generators for the radical of a given ideal. (Proofs available upon request for current results.)

## 2. DIFFERENTIAL ALGEBRAIC GEOMETRY, MODEL THEORY, AND COMPLETE DIFFERENTIAL VARIETIES

Compactness is a critical “finiteness property” of a topological space. One characterization of compactness that captures the intended meaning for algebraic varieties is that of completeness: an algebraic variety  $V$  is *complete* if for every variety  $W$  the projection map  $\pi : V \times W \rightarrow W$  takes Zariski-closed sets to Zariski-closed sets.

The fundamental theorem of elimination theory states that projective algebraic varieties over an algebraically closed field  $K$  are complete. Using the same definition (only replacing the Zariski topology with the finer Kolchin topology in which closed sets are zero loci of differential polynomials), one obtains the notion of a *complete differential variety*. Kolchin studied complete differential varieties in [21], proving that the projective closure of the constants (i.e., elements whose derivatives are all zero) is differentially complete while projective  $n$ -space  $\mathbb{P}^n$  is not. Later researchers such as Pong, Freitag, León Sánchez, and I investigated differential completeness for its own sake as well as for mathematical applications [10, 12, 27, 33].

In [32, 33] I adapt the methods of [27] to pursue the question of which projective differential varieties are complete. This involves retooling Pong’s valuative criterion in order to apply it directly to projective differential varieties as well as remove reference to nonconstructive objects like maximal differential rings. I obtain versions of the valuative criterion that emphasize different perspectives (see Theorems 3.1,

3.3, and 3.4 in [33]): a valuative criterion for projective differential varieties that mirrors the affine case, a more geometric version using only the Kolchin closure of the image under projection of subvarieties of a special form, and a more “syntactic” version concerning the form of polynomials that show up in differential elimination ideals.

Throughout the project I have frequently used computer algebra to formulate examples and test conjectures. The projective valuative criterion and explicit elimination algorithms enabled me to find new examples of complete  $\delta$ -subvarieties of  $\mathbb{P}^1$  [32,33]. I also identified the following family of counterexamples (the only incomplete, finite-rank projective differential varieties known at present): the projective closure of  $x'' = x^n$  is not  $\delta$ -complete for  $n \geq 2$ .

In [12], Freitag, León Sánchez, and I present a simplification of the differential completeness recognition problem, albeit one that assumes a weak form of the *catenary conjecture* [6] from differential algebra. We show that if the weak catenary conjecture (Conjecture 5.2 in [12]) is true, then a  $\Delta$ -closed subset  $V \subseteq \mathbb{P}^n$  is differentially complete if and only if  $\pi : V \times W \rightarrow W$  is a  $\Delta$ -closed map for every quasiprojective zero-dimensional differential variety  $W$ . This result, while conditional, may make it easier to classify complete differential varieties.

There are many open questions surrounding differential completeness, and making progress will likely pay dividends to differential algebra beyond the specific problems. Of particular interest to me is determining whether differential completeness is a decidable property. The projective valuative criterion gives conditions for completeness to hold, but in the absence of bounds on checking the conditions we do not know if this can be done algorithmically. My proof-theoretic work on bounds in polynomial rings and my model-theoretic work on valuative criteria complement each other well here.

### 3. FORMAL METHODS FOR MATHEMATICS AND COMPUTER SCIENCE

The background for proof mining includes type theory and higher-order logic. These concepts are also important for my most recent projects, which revolve around tools from computer science.

Elimination theory for differential equations holds promise for analyzing dynamics in biology, chemistry, and hybrid systems [5,25,26]. However, little has been done so far to implement theories of polynomial rings with additional operators in provers such as Coq and Isabelle. I am constructing such a theory in Coq with input from members of the theorem-proving community (code available upon request). Recent papers on multivariate polynomials and formalization [4,17,37] also give guidance for design choices. The SSReflect proof language [15] provides tools for efficient theory development and I am seeking to build on the algebraic hierarchy from the Mathematical Components library [24].

I have defined a polymorphic inductive type that allows for different coefficient rings, sets of indeterminates, and classes of operators. (For instance, one would like to use the same basic set-up for both differential and difference algebra.) Using Coq’s setoid mechanism [36], I defined an equivalence relation on formal polynomials to enable rewriting. There is much left to do, such as writing and verifying programs for elimination, but I can conduct simple calculations and proofs. I presented my preliminary work during the workshop portion of Formal Methods in Mathematics/Lean Together 2020 at Carnegie Mellon.

In related research, I am working to formalize the Ax-Schanuel theorem from transcendence theory. The proof uses differential algebra as well as objects like Puiseux series. The project will make a valuable contribution to formal mathematics and will require significant engineering insights (for instance, to incorporate de Rauglaudre’s formal proof of Puiseux’s theorem [9] into my setting).

In support of this project, I have attended programs like the Coq Intensive portion of the DeepSpec 2018 Summer School held at Princeton (<https://deepspec.org/event/dsss18/>). Attendees were computer scientists, logicians, and users of formal methods in industry. By interacting with these peers and the organizers in talks and problem sessions, I gained additional experience with the theory and application of theorem proving. As a mathematics postdoc I also participated in the programming languages group at the University of Pennsylvania. Particularly valuable were seminar talks and working discussions on type-theoretic methods for differential privacy with Benjamin Pierce and his colleagues.

#### 4. HAVING IT BOTH WAYS

Both ends of the abstract/concrete spectrum are connected in ways amenable to mathematical logic. Davis and Hersh [8] cite Henrici’s view [19] that “Dialectic [i.e., nonconstructive] mathematics generates insight. Algorithmic mathematics generates results.” My research program is motivated by both traditions, generating insight *and* results throughout algebra and computing.

#### REFERENCES

- [1] Matthias Aschenbrenner. Ideal membership in polynomial rings over the integers. *J. Amer. Math. Soc.*, 17(2):407–441 (electronic), 2004.
- [2] Jeremy Avigad and Solomon Feferman. Gödel’s functional (“Dialectica”) interpretation. In *Handbook of proof theory*, volume 137 of *Stud. Logic Found. Math.*, pages 337–405. North-Holland, Amsterdam, 1998.
- [3] Jeremy Avigad and Henry Towsner. Metastability in the Furstenberg-Zimmer tower. *Fundamenta Mathematicae*, 210(3):243–268, 2010.
- [4] Sophie Bernard, Yves Bertot, Laurence Rideau, and Pierre-Yves Strub. Formal proofs of transcendence for e and pi as an application of multivariate and symmetric polynomials. In *Proceedings of the 5th ACM SIGPLAN Conference on Certified Programs and Proofs*, pages 76–87. ACM, 2016.
- [5] François Boulrier and François Lemaire. Differential algebra and system modeling in cellular biology. *Algebraic Biology*, pages 22–39, 2008.
- [6] Alexander Buium and Phyllis Cassidy. Differential algebraic geometry and differential algebraic groups. *Selected Works of Ellis Kolchin with Commentary*, Bass, Buium, Cassidy, eds., American Mathematical Society, 1999.
- [7] Lisi D’Alfonso, Gabriela Jeronimo, and Pablo Solernó. Effective differential nullstellensatz for ordinary DAE systems with constant coefficients. *Journal of Complexity*, 30(5):588–603, 2014.
- [8] Philip J Davis and Reuben Hersh. *The mathematical experience*. Houghton Mifflin Harcourt, 1998.
- [9] Daniel de Rauglaudre. Formal proof in Coq of Puiseux’s theorem (InriaForge). <https://gforge.inria.fr/projects/puiseuxth>. Accessed: 2020-06-01.
- [10] James Freitag. Completeness in partial differential fields. *Journal of Algebra*, 420:350–372, 2014.
- [11] James Freitag, Wei Li, and Thomas Scanlon. Differential Chow varieties exist. *arXiv preprint arXiv:1504.03755, v1*, 2015.
- [12] James Freitag, Omar León Sánchez, and William Simmons. On linear dependence over complete differential algebraic varieties. *Communications in Algebra*, 44(6):2645–2669, 2016.
- [13] OD Golubitsky, MV Kondratieva, and AI Ovchinnikov. On the generalized Ritt problem as a computational problem. *Journal of Mathematical Sciences*, 163(5):515–522, 2009.

- [14] Oleg Golubitsky, Marina Kondratieva, Alexey Ovchinnikov, and Agnes Szanto. A bound for orders in differential Nullstellensatz. *J. Algebra*, 322(11):3852–3877, 2009.
- [15] Georges Gonthier, Assia Mahboubi, and Enrico Tassi. The SSReflect proof language (Coq Reference Manual). <https://coq.inria.fr/refman/proof-engine/ssreflect-proof-language.html>. Accessed: 2019-09-14.
- [16] Richard Gustavson and Omar León Sánchez. Effective bounds for the consistency of differential equations. *Journal of Symbolic Computation*, 89:41–72, 2018.
- [17] Florian Haftmann, Andreas Lochbihler, and Wolfgang Schreiner. Towards abstract and executable multivariate polynomials in Isabelle. In *Isabelle Workshop*, volume 201, 2014.
- [18] Matthew Harrison-Trainor, Jack Klys, and Rahim Moosa. Nonstandard methods for bounds in differential polynomial rings. *J. Algebra*, 360:71–86, 2012.
- [19] Peter Henrici. Computational complex analysis. In *The Influence of Computing on Mathematical Research and Education*, volume 20 of *Proc. of Symposia in Applied Math.*, pages 79–86. American Mathematical Soc., 1974.
- [20] U. Kohlenbach. *Applied proof theory: proof interpretations and their use in mathematics*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2008.
- [21] E. R. Kolchin. Differential equations in a projective space and linear dependence over a projective variety. *Contributions to analysis (A collection of papers dedicated to Lipman Bers)*, pages 195–214, 1974.
- [22] E. R. Kolchin. *Differential Algebra and Algebraic Groups*. Academic Press, New York, 1976.
- [23] Omar León Sánchez and Alexey Ovchinnikov. On bounds for the effective differential Nullstellensatz. *J. Algebra*, 449:1–21, 2016.
- [24] Assia Mahboubi and Enrico Tassi (with contributions by Yves Bertot and Georges Gonthier). *Mathematical Components*. <https://math-comp.github.io/mcb/>. Updated 2018-08-11; accessed 2019-09-14.
- [25] Alexey Ovchinnikov, Gleb Pogudin, and N Thieu Vo. Effective differential elimination and Nullstellensatz. *arXiv preprint arXiv:1610.04022*, 2016.
- [26] André Platzer. *Logical analysis of hybrid systems: proving theorems for complex dynamics*. Springer Science & Business Media, 2010.
- [27] Wai Yan Pong. Complete sets in differentially closed fields. *Journal of Algebra*, 224:454–466, 2000.
- [28] Karsten Schmidt-Götttsch. Polynomial bounds in polynomial rings over fields. *Journal of Algebra*, 125(1):164–180, 1989.
- [29] Hans Schoutens. *The use of ultraproducts in commutative algebra*, volume 1999. Springer Science & Business Media, 2010.
- [30] William Simmons and Henry Towsner. Explicit polynomial bounds on prime ideals in polynomial rings over fields. *arXiv:1808.04805*, 2019. Accepted for publication in *Pacific J. of Mathematics*.
- [31] William Simmons and Henry Towsner. Proof mining and effective bounds in differential polynomial rings. *Advances in Mathematics*, 343:567–623, 2019.
- [32] William D. Simmons. *Completeness of finite-rank differential varieties*. PhD thesis, University of Illinois at Chicago, 2013.
- [33] William D Simmons. New examples (and counterexamples) of complete finite-rank differential varieties. *Communications in Algebra*, 45(7):3137–3149, 2017.
- [34] Stephen G. Simpson. Ordinal numbers and the Hilbert basis theorem. *J. Symbolic Logic*, 53(3):961–974, 1988.
- [35] Guillermo Moreno Socías. Length of polynomial ascending chains and primitive recursiveness. *Mathematica Scandinavica*, pages 181–205, 1992.
- [36] Matthieu Sozeau. Generalized rewriting (Coq Reference Manual). <https://coq.inria.fr/refman/addendum/generalized-rewriting.html>. Accessed: 2019-09-15.
- [37] Christian Sternagel and René Thiemann. Executable multivariate polynomials. archive of formal proofs, 2010.
- [38] Henry Towsner. A worked example of the functional interpretation. *arXiv preprint arXiv:1503.05572*, 2015.
- [39] 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.