The reverse mathematics of some finiteness theorems in algebra

Stephen G. Simpson
Pennsylvania State University
http://www.math.psu.edu/simpson/
simpson@math.psu.edu

New Challenges in Reverse Mathematics
Institute of Mathematical Sciences
National University of Singapore

January 3–16, 2016

Basis theorems in algebra.

Definition. A ring satisfies the ACC (ascending chain condition) if every increasing sequence of ideals is finite. Equivalently, every ideal is finitely generated.

Theorem (Hilbert 1890)**.** Let K be a field. For all positive integers d, the polynomial ring $K[x_1, \ldots, x_d]$ satisfies the ACC.

This is the Hilbert Basis Theorem.

The Hilbert Basis Theorem is very important in invariant theory and in algebraic geometry.

It is not to be confused with "basis theorems" in recursion theory!

Basis theorems in algebra (continued).

There are also the following basis theorems.

Theorem (Hilbert)**.** Let K be a field. For all positive integers d, the formal power series ring $K[[x_1, \ldots, x_d]]$ satisfies the ACC.

Theorem (Formanek/Lawrence 1976)**.** Let K be a field of characteristic 0. Let S be *infinite symmetric group*, i.e., the group of finitely supported permutations of $\mathbb{N}$.
Then, the group ring $K[S]$ satisfies the ACC for 2-sided ideals.

Does this hold for other locally finite groups beside S?
In particular, does it hold for the Hall group?

Theorem (Robson 1978)**.** Let K be a field.
For all d the polynomial ring $K\langle x_1, \ldots, x_d\rangle$
in d noncommuting indeterminates
satisfies the ACC for insertive ideals.

An insertive ideal is closed under multiplication on the left, multiplication on the right, and multiplication in the middle.

Some related finiteness theorems:

Theorem (Hatzikiriakou/Simpson 2015). $K[S]$ satisfies the antichain condition, i.e., there is no infinite set of 2-sided ideals which are pairwise incomparable under inclusion.

Theorem (Maclagan 2000). For all positive integers d, the polymonial ring $K[x_1,\ldots,x_d]$ and the power series ring $K[[x_1,\ldots,x_d]]$ satisfy the antichain condition for monomial ideals, i.e., ideals generated by monomials.

Questions for algebraists:
Is the antichain condition of interest to algebraists?
What does the antichain condition mean for algebraic geometry, etc.?

Some reverse mathematics.

Working in RCA_0, we restrict ourselves to countable fields.

Theorem (Simpson 1988). Over RCA_0,

1. Hilbert Basis Theorem $\iff \mathsf{WO}(\omega^\omega)$.
2. Robson's Theorem $\iff \mathsf{WO}(\omega^{\omega^\omega})$.

Theorem (Hatzikiriakou 1994). Over RCA_0, the Hilbert Basis Theorem for power series rings is equivalent to $\mathsf{WO}(\omega^\omega)$.

Theorem (Hatzikiriakou/Simpson 2015). Over RCA_0, the Formanek/Lawrence Theorem is equivalent to $\mathsf{WO}(\omega^\omega)$, and Maclagan's Theorem is equivalent to $\mathsf{WO}(\omega^{\omega^\omega})$.

Note: The Hilbert Basis Theorem refers to an infinite sequence of rings, $K[x_1,\ldots,x_d]$, $d \in \mathbb{N}$, while Formanek/Lawrence refers to only one ring, $K[S]$.

We also show that, in all of these reverse-mathematical results, the base theory RCA_0 can be weakened to RCA_0^*.

Foundational significance:

The foundational significance of these results is as follows:

> None of these basis theorems is finitistically reducible in the sense of Hilbert's Program in the foundations of mathematics.)

In particular, our results support Gordan's famous remark concerning the Hilbert Basis Theorem:

> **"That is not mathematics. That is theology!"**

The point is that finitistic reducibility is equivalent to Π^0_2-conservativity over PRA (primitive recursive arithmetic). And $\mathsf{RCA}_0 + \mathsf{WO}(\omega^\omega)$ is not even Π^0_1-conservative over PRA, because it proves consistency of PRA and totality of the Ackermann function.

I will say more about Hilbert's Program in my Public Lecture, Wednesday January 6, 18:30–19:30.

References:

Edward Formanek and John Lawrence, The group algebra of the infinite symmetric group, Israel Journal of Mathematics, 23, 1976, 325–331.

J. C. Robson, Well quasi-ordered sets and ideals in free semigroups and algebras, Journal of Algebra, 55, 1978, 521–535.

Stephen G. Simpson, Ordinal numbers and the Hilbert Basis Theorem, Journal of Symbolic Logic, 53, 1988, 961–974.

Kostas Hatzikiriakou, A note on ordinal numbers and rings of formal power series, Archive for Mathematical Logic, 33, 1994, 261–263.

Kostas Hatzikiriakou and Stephen G. Simpson,
Reverse mathematics, Young diagrams, and the ascending chain condition,
2015, 14 pages, submitted for publication.

Stephen G. Simpson and Rick L. Smith, Factorization of polynomials and Σ^0_1 induction, Annals of Pure and Applied Logic, 31, 1986, 289–306.

Diane Maclagan, Antichains of monomial ideals are finite, Proceedings of the American Mathematical Society, 129, 2000, 1609–1615.

I will now give some details about the proof
of both the Formanek/Lawrence Theorem and its reversal.

Partition theory.

As noted by Formanek and Lawrence, 2-sided ideals in $K[S]$ are in 1-to-1 correspondence with certain sets of partitions.

A partition of n is a finite sequence of integers $n_1 \geq \cdots \geq n_k > 0$ such that $n = n_1 + \cdots + n_k$.

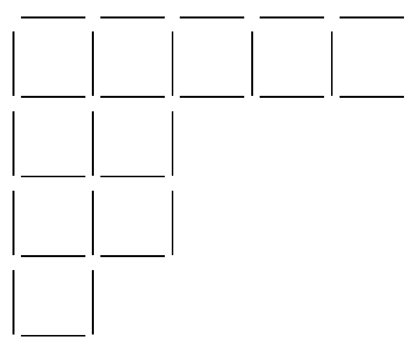
Example: $(5, 2, 2, 1)$ is a partition of 10, because $10 = 5 + 2 + 2 + 1$ and $5 \geq 2 \geq 2 \geq 1 > 0$.

Partitions of n are in 1-to-1 correspondence with conjugacy classes of S_n. Here S_n is the group of permutations of the set $\{1, \ldots, n\}$.

Partition theory is a large branch of mathematics, closely connected to the representation theory of S_n.

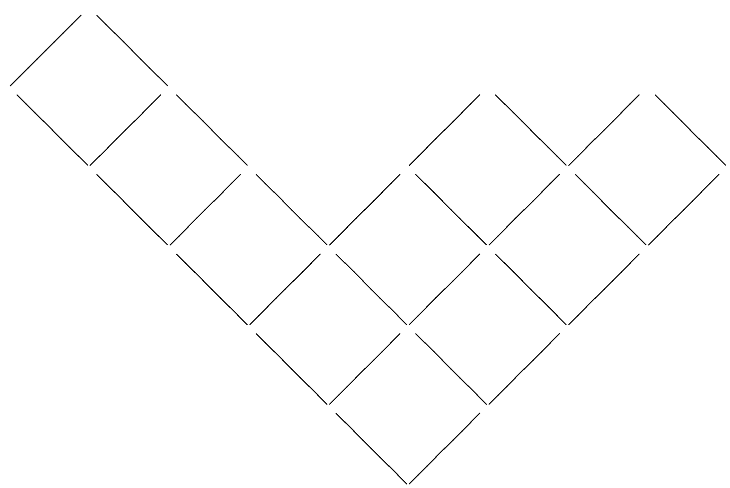
Note: $S = \bigcup_{n=1}^{\infty} S_n$ and $K[S] = \bigcup_{n=1}^{\infty} K[S_n]$.

Partitions are often visualized as Young diagrams. For example, the partition $10 = 5 + 2 + 2 + 1$ corresponds to the Young diagram



consisting of 10 boxes.

Rotated counterclockwise 135 degrees,
this Young diagram becomes a downwardly closed set in $(\mathbb{N}^2, \leq)$,
partially ordered by $(m,n) \leq (p,q) \iff (m \leq p$ and $n \leq q)$.



A <u>diagram</u> is a finite downwardly closed set in $\mathbb{N}^2$.
Let $\mathcal{D}_2$ be the set of diagrams, partially ordered by inclusion.

A poset P is said to be WPO (<u>well partially ordered</u>)
if $(\forall f : \mathbb{N} \to P)\, \exists i\, \exists j\, (i < j$ and $f(i) \leq f(j))$.

In my 1988 paper I show that, over RCA_0,
1. $K[x_1, \ldots, x_d]$ has ACC $\Longleftrightarrow \mathbb{N}^d$ is WPO.
2. $K\langle x_1, \ldots, x_d \rangle$ ACC for insertive ideals $\Longleftrightarrow \{x_1, \ldots, x_d\}^*$ WPO.

Since $\mathbb{N}^2$ is WPO, it follows by Higman's Lemma that $\mathcal{D}_2$ is WPO.

A set $\mathcal{U} \subseteq \mathcal{D}_2$ is said to be <u>closed</u> if
$\forall D\, (D \in \mathcal{U} \Longleftrightarrow \forall E\, (D \subsetneqq E \Rightarrow E \in \mathcal{U}))$.
This implies that $\mathcal{U}$ is upwardly closed, but not conversely!

Formanek and Lawrence exhibit a 1-to-1 correspondence between 2-sided ideals in $K[S]$ and closed sets in $\mathcal{D}_2$. Since $\mathcal{D}_2$ is WPO, it has the ACC on closed sets, hence $K[S]$ has the ACC on 2-sided ideals.

Reversing Formanek/Lawrence.

Working in RCA_0, we formalize the work of Formanek/Lawrence to prove that $K[S]$ has the ACC if and only if $\mathcal{D}_2$ has the ACC on closed sets. Also working in RCA_0, we use methods of Simpson 1988 to prove that $\mathsf{WO}(\omega^\omega) \iff \mathcal{D}_2$ is WPO.

Still working in RCA_0, it remains to prove:
$\mathcal{D}_2$ is WPO $\iff \mathcal{D}_2$ has the ACC on closed sets.
To prove this, we use a new combinatorial lemma.

Lemma. Let $\mathcal{S}$ be a finite set of diagrams. Then, the closure of $\mathcal{S}$ is equal to the upward closure of $\{D_r \cup E_c \mid D, E \in \mathcal{S}\}$.

Moreover, there are only finitely many diagrams in the closure of $\mathcal{S}$ which are not in the upward closure of $\mathcal{S}$.

D_r and D_c are the results of truncating the first row and first column of D, respectively.

For example, if $D = (5,2,2,1)$ then $D_r = (2,2,2,1)$ and $D_c = (5,2,2)$.

Weakening the base theory.

Recall that $\mathsf{RCA}_0^* =$
RCA_0 minus Σ^0_1 induction plus integer exponentiation.

In our ACC reversals, we wish to replace RCA_0 by RCA_0^*. For this, it suffices to prove in RCA_0^* that if $K[x]$ has ACC then Σ^0_1 induction holds.

Lemma. Over RCA_0^*, if Σ^0_1 induction fails, then there exist an infinite set $I \subseteq \mathbb{N}$ and a function $f : I \to \mathbb{N}$ such that $(\forall i \in I)\,(\forall j \in I)\,(i < j \Rightarrow f(i) > f(j))$.

In this situation, letting $n_i = 2^{f(i)}$, the ideals in $K[x]$ generated by x^{n_i} for each $i \in I$ are a counterexample to the ACC.

Philosophical aspect.

I have suggested that, in contrast to the concept of potential infinity, the concept of actual infinity appears to lack objective justification. Therefore, in order to promote objectivity in mathematics, it seems desirable to limit the use of actual infinity.

I see a close connection to Hilbert's program of finitistic reductionism. Let us say that a system $T \subseteq Z_2$ is finitistically reducible if all Π^0_1 (or possibly even Π^0_2) sentences provable in T are provable in PRA, i.e., Primitive Recursive Arithmetic.

Some important systems *are* finitistically reducible, namely WKL_0, and $\mathsf{WKL}_0 + \Sigma^0_2$ bounding, and some stronger systems. These systems suffice for the formalization of large parts of mathematics.

On the other hand, $\mathsf{RCA}_0 + \mathsf{WO}(\omega^\omega)$ and $\mathsf{RCA}_0 + \Sigma^0_2$ induction *are not* finitistically reducible, because they prove Con(PRA) and totality of the Ackermann function.

Philosophical aspect (continued).

In particular, the Hilbert Basis Theorem
and the Formanek/Lawrence Theorem
are not finitistically reducible.

(However, for each specific positive integer d,
the Hilbert Basis Theorem for $K[x_1, \ldots, x_d]$ *is* finitistically reducible,
because it is provable in RCA_0.)

A remark on RT(2, 2).

Over the past few years, Chong, Slaman, Yang, and Yokoyama
have done some important work on the reverse mathematics of
RT(2, 2), i.e., Ramsey's Theorem for exponent 2.

Very recently, Patey and Yokoyama solved an important problem
by proving that $\mathsf{RCA}_0 + \mathsf{RT}(2,2)$ is finitistically reducible.
In fact, they proved that $\mathsf{RCA}_0 + \mathsf{RT}(2,2)$ is Π^0_3-conservative over RCA_0.

More references:

David Hilbert, Über das Unendliche, Mathematische Annalen, 95, 1926, 161–190.

William W. Tait, Finitism, Journal of Philosophy, 78, 1981, 524–546.

Stephen G. Simpson, Partial realizations of Hilbert's program, Journal of Symbolic Logic, 53, 1988, 349–363.

Stephen G. Simpson, Subsystems of Second Order Arithmetic, Springer-Verlag, 1999, XIV + 445 pages; 2nd edition, Association for Symbolic Logic, 2009, XVI + 444 pages.

Richard Zach, Hilbert's Program, Stanford Encyclopedia of Philosophy, 2003, http://plato.stanford.edu/entries/hilbert-program/.

Stephen G. Simpson, Toward objectivity in mathematics, in: Infinity and Truth, edited by C.-T. Chong, Q. Feng, T. A. Slaman, and W. H. Woodin, World Scientific, 2014, 157–169.

Stephen G. Simpson, An objective justification for actual infinity?, same volume, 2014, 225–228.

Thank you for your attention!