

THREE LECTURES ON THE RS PROBLEM

ROSS WILLARD

University of Waterloo

Department of Pure Mathematics

Waterloo, ON, Canada N2L 3G1

Abstract. In these lectures we return to the RS Problem discussed in E. Kiss's article (this volume). We discuss the current status of the problem and describe some results which arose from the study of the problem, including the solution to Tarski's finite basis problem. A subtitle for these lectures might be "Some recent results in general algebra, mostly due to R. McKenzie."

1. First lecture: The residual character of an equational class

These three lectures are about a cluster of problems concerning equational classes of algebras, that is, classes of models (in a language having no relation symbols) which can be axiomatized by a set of universally quantified equations. (Such classes are known to general algebraists as *varieties*). These lectures are particularly concerned with the smallest equational class containing a given algebra \mathbf{A} ; this class is denoted by $\text{HSP}(\mathbf{A})$, because it coincides with the closure of $\{\mathbf{A}\}$ first under arbitrary Cartesian powers, then under substructures, finally under homomorphic images. $\text{HSP}(\mathbf{A})$ is called the equational class (or variety) *generated by* \mathbf{A} , and it is this object, when \mathbf{A} is finite, that will be the center of our attention in these lectures.

Readers of Emil Kiss's article in this volume will have noticed a certain obsession with special algebras called *subdirectly irreducible*. In the first lecture I will again explain what these are, then try to give an impression of the questions that are posed of these algebras, and the answers that we hope to find. In the second lecture I will give a partial explanation of R. McKenzie's counterexamples to longstanding conjectures concerning these algebras. In the third lecture I will give a relatively nontechnical

explanation of some surprising spinoffs of these counterexamples, including McKenzie's celebrated solution to Tarski's finite basis problem.

I wish to thank George McNulty for a helpful discussion which saved me from making an embarrassing mistake in Section 3.1.

1.1. WHAT THE HECK ARE SI ALGEBRAS?

Subdirectly irreducible (SI) algebras were defined in Kiss's lectures (see this volume) as those algebras which have no nontrivial subdirect decompositions. Another description is the following: take any algebra \mathbf{A} ; pick two distinct elements $a, b \in A$; then let \equiv be any congruence relation of \mathbf{A} which is maximal with respect to *not* relating a to b . The quotient algebra \mathbf{A}/\equiv is a typical SI algebra.

There is yet another characterization of SI algebras, which I will first illustrate in a familiar setting. If R is a ring and $a, b \in R$, let (b) denote the principal ideal of R generated by b , and define $a \preceq b$ to mean $a \in (b)$. The relation $x \preceq y$ is a pre-ordering of R which is definable by an infinite disjunction of positive primitive formulas (or by a single positive primitive formula if R is commutative and has an identity). R is SI iff it has a smallest nonzero ideal, and this is equivalent to the existence of $a \neq 0$ such that $a \preceq b$ for all $b \neq 0$.

For an arbitrary algebra \mathbf{A} and $a, b, c, d \in A$, let $\text{Cg}(c, d)$ denote the principal congruence relation of \mathbf{A} generated by identifying c with d , and define $(a, b) \preceq (c, d)$ to mean $a \equiv b \pmod{\text{Cg}(c, d)}$. The relation $(x, y) \preceq (z, w)$ is a pre-ordering of R^2 which is definable by a (usually infinite) disjunction of positive primitive formulas. \mathbf{A} is SI iff \mathbf{A} has a smallest nonzero (i.e., not-equality) congruence relation, and this is equivalent to the existence of $a \neq b$ such that $(a, b) \preceq (c, d)$ for all $c \neq d$.

If \mathcal{V} is an equational class, then I will use \mathcal{V}_{si} to denote the class of all SI members of \mathcal{V} . Frequently, the solution to a problem in general algebra requires understanding some aspect of the structure of the members of \mathcal{V}_{si} for the relevant equational classes \mathcal{V} .

By way of example, let us consider the varieties of rings (with identity) generated by \mathbb{Z}_4 and \mathbb{Z}_8 respectively. First, let $\mathcal{V} = \text{HSP}(\mathbb{Z}_4)$. \mathcal{V} is the equational class of commutative rings axiomatized by $(x^2 - x)(y^2 - y) = 0$; equivalently, \mathcal{V} is the class of all commutative rings R for which the (Jacobson) radical J satisfies $2 \in J$ and $J^2 = (0)$, while R/J is a boolean ring. From this description it can be deduced that $\mathcal{V}_{\text{si}} = \{\mathbb{Z}_4, \mathbb{Z}_2\}$. This and the specific nature of \mathbb{Z}_2 and \mathbb{Z}_4 immediately yield, e.g., a soft proof of the fact that the first-order theory of the finite members of $\text{HSP}(\mathbb{Z}_4)$ is decidable (see Theorem 5.3 and the discussion of its converse in Matthew Valeriote's article, this volume).

Next, let $\mathcal{V} = \text{HSP}(\mathbb{Z}_8)$. This time \mathcal{V} is the equational class of commutative rings axiomatized by $(x^2 - x)(y^2 - y)(z^2 - z) = 0$ and $(x^2 - x)^2 = 2(x^2 - x)$; equivalently, \mathcal{V} is the class of all commutative rings R for which the radical J satisfies $2 \in J$, $J^3 = (0)$ and $x^2 = 2x$, while R/J is a boolean ring. \mathcal{V}_{si} turns out to consist of all $R \in \mathcal{V}$ such that $R/J = \mathbb{Z}_2$ and either $J^2 = (0)$ (in which case R is \mathbb{Z}_2 or \mathbb{Z}_4) or $J^2 = \{0, c\}$, in which case for every $x \in J \setminus \{0, c\}$ there exists $y \in J$ such that $xy = c$. It turns out that there is a proper class of SIs of this second type. Here is an explicit description of some of them. Let $\langle a \rangle$ and $\langle b \rangle$ be cyclic groups of orders 2 and 4 respectively (written additively), and let κ be any cardinal other than an odd positive integer. Choose a vector space A_κ over \mathbb{Z}_2 with basis $(e_i : i < \kappa)$. Then \mathcal{V}_{si} includes \mathbb{Z}_2 and the following:

1. A ring R such that $R/J = \mathbb{Z}_2$ and $J = \langle a \rangle \oplus A_\kappa$ with $2 = a$, $e_i^2 = 0$ for all i , and $e_i e_j = a$ for all $i \neq j$.
2. A ring R such that $R/J = \mathbb{Z}_2$ and $J = \langle b \rangle \oplus A_\kappa$ with $2 = b$, $e_i^2 = 0$ for all i , and $e_i e_j = 2b$ for all $i \neq j$.
3. A ring R such that $R/J = \mathbb{Z}_2$ and $J = \langle b \rangle \oplus \langle a \rangle \oplus A_\kappa$ with $2 = a$, $b^2 = 2b$, $b e_i = e_i^2 = 0$ for all i , and $e_i e_j = 2b$ for all $i \neq j$.

Conversely, every countable member of \mathcal{V}_{si} occurs in this list. This is enough information to give, e.g., a soft proof that the theory of $\text{HSP}(\mathbb{Z}_8)$ has a model companion (see [2, Theorem 8.4]).

In general, we do not expect to be able to describe \mathcal{V}_{si} in this much detail for every variety \mathcal{V} . However, there may be some hope if we restrict the class of varieties to be considered (e.g., to locally finite varieties), and restrict the detail in which \mathcal{V}_{si} is to be understood (e.g., whether there is a cardinal upper bound to the sizes of the SIs). In particular, we are optimistic that the following problem will soon be solved:

PROBLEM 1.1 (The RS Problem; cf. Kiss's article, Problem 3.2) *Determine (or characterize) which finitely generated varieties have a cardinal upper bound to the sizes of their SIs (i.e., are residually small).*

We are optimistic for three reasons. First, finitely generated varieties are the simplest examples of locally finite varieties. Second, we can use tame congruence theory. And third, McKenzie has shown us how to proceed.

1.2. A SPECIAL CASE OF THE PROBLEM

In the previous section we saw two finitely generated varieties, $\text{HSP}(\mathbb{Z}_4)$ and $\text{HSP}(\mathbb{Z}_8)$, one of which is residually large while the other is residually small. The difference, it turns out, is the following: \mathbb{Z}_4 satisfies a polynomial identity $(xy = xy^2 + x^2y - x^2y^2)$ which forces the radical in any finite model to be self-annihilating, while \mathbb{Z}_8 already fails to have this property. More

generally, we have the following theorem of Freese and McKenzie (cf. Kiss's article, Theorem 6.2):

THEOREM 1.2 (R. Freese, R. McKenzie [3]) *If:*

- (1) \mathcal{V} is a variety generated by a finite algebra, and
- (2) For every $\mathbf{A} \in \mathcal{V}$, the lattice of congruences of \mathbf{A} is a modular lattice, then \mathcal{V} is residually large iff there exists $\mathbf{A} \in \mathcal{V}_{\text{si}}$ with least nonzero congruence μ and having another congruence $\alpha \geq \mu$, such that α centralizes μ (i.e., $[\alpha, \mu] = 0$) but α does not centralize itself (i.e., $[\alpha, \alpha] \neq 0$).

The proof is instructive. First, assume that \mathcal{V} has such an SI algebra \mathbf{A} with congruences μ and α satisfying the above conditions. By local finiteness we can assume that \mathbf{A} is finite. Then use tame congruence theory to obtain a $(0, \mu)$ -trace N (N will be a 1-dimensional vector space contained in some μ -class). Let $+$ denote its addition, 0 its zero, and let c be some nonzero element of N .

$\mathbf{A}, \alpha, 0, c$ can be used to build a proper class of SIs in \mathcal{V} in a "canonical" way, as follows. Let $(I, <)$ be a dense linearly ordered set without endpoints and containing designated elements $0 < 1$. For each $(a, b) \in A^2$ and $i \in I$, define $f_i^{ab} : I \rightarrow A$ by

$$f_i^{ab}(j) = \begin{cases} b & \text{if } j = i \\ a & \text{else.} \end{cases}$$

For each $a \in A$ let \hat{a} be the constant a -valued function from I to A . Let \mathbf{B} be the subalgebra of \mathbf{A}^I whose universe consists of all $f \in A^I$ such that for some $a \in A$, $f \stackrel{\text{ae}}{=} \hat{a}$ and the range of f is contained entirely within the α -class of a . Next we define some congruences on \mathbf{B} . Let β be the smallest congruence which collapses the set $\{f_i^{0c} : i \in I\}$ to a single point; and for each pair $(i, j) \in I^2$ with $i < j$, define δ_{ij} to be the least congruence which identifies f_i^{ab} with f_j^{ab} whenever a is related to b by α .

Let $W = \{f \in \mathbf{B} : \text{range}(f) \subseteq N \text{ and } f \stackrel{\text{ae}}{=} \hat{0}\}$. W is a large-dimensional vector space under coordinatewise addition and scalar multiplication. Let $W_0 = \{f \in W : \sum_{i \in I} f(i) = 0\}$, a subspace of codimension 1. Since $[\alpha, \mu] = 0$ in \mathbf{A} , and using tame congruence theory and the definition of β , it can be shown that the classes of β restricted to W are the cosets of some subspace of W_0 . In particular, $\hat{0} \not\equiv f_0^{0c} \pmod{\beta}$ since $\hat{0}$ and f_0^{0c} belong to different cosets of W_0 . On the other hand, since $[\alpha, \alpha] \neq 0$ and in fact $0 \equiv c \pmod{[\alpha, \alpha]}$, it can be shown that $\hat{0} \equiv f_0^{0c} \pmod{\delta_{01}}$ and hence $\hat{0} \equiv f_i^{0c} \equiv f_0^{0c} \pmod{\beta \vee \delta_{ij}}$ for all $i < j$, by the homogeneous nature of \mathbf{B} relative to $(I, <)$.

Now let θ be a congruence of \mathbf{B} extending β and maximal with respect to not identifying $\hat{0}$ with f_0^{0c} . \mathbf{B}/θ is an SI member of \mathcal{V} . Moreover, $\delta_{ij} \not\subseteq \theta$

for all $i < j$, which means that for all $i < j$ there exists a pair (a, b) related by α such that $f_i^{ab} \not\equiv f_j^{ab} \pmod{\theta}$. As there are only finitely many possible pairs (a, b) , we get a finite coloring of $I^{(2)}$. By the Erdős-Rado theorem, if κ is an infinite cardinal and $|I| = (2^\kappa)^+$, there will exist $(a, b) \in \alpha$ and $J \subseteq I$ with $|J| = \kappa^+$ such that the elements f_i^{ab} ($i \in J$) are pairwise noncongruent mod θ . Hence $|\mathbf{B}/\theta| \geq \kappa^+$. Since κ is arbitrary, \mathcal{V} is residually large.

Next, assume that \mathcal{V} does *not* have any SI algebra \mathbf{A} as in the statement of the theorem. Let n be the size of some finite generating algebra of \mathcal{V} . Assume $\mathbf{A} \in \mathcal{V}_{\text{si}}$ and let μ be its least nonzero congruence (a.k.a. “the monolith”). If μ is nonabelian (doesn’t centralize itself), then $|A| \leq n$ automatically (using the commutator and the fact that \mathcal{V} has modular congruence lattices – see Kiss’s article, Section 6). If instead μ is abelian, then again using the commutator one can show that \mathbf{A} has a congruence α which centralizes μ and has at most n classes. By the assumption, α centralizes itself. Once again with the help of commutator theory, this implies that each of the congruence classes C_1, \dots, C_m of α can be endowed with the structure $\mathbf{C}_i = (C_i, +, -, 0)$ of an abelian group, so that the operations of \mathbf{A} are “compatible” with the relations $(x - y + z = w)^{\mathbf{C}_i}$ in the following sense: if F is a k -ary fundamental operation of \mathbf{A} and if i_1, \dots, i_k are arbitrary indices from $\{1, \dots, m\}$, then there exists $l \in \{1, \dots, m\}$ such that

- (*) $F(C_{i_1} \times \dots \times C_{i_k}) \subseteq C_l$, and
- (**) $F(a_1 - b_1 + c_1, \dots, a_k - b_k + c_k) = F(\bar{a}) - F(\bar{b}) + F(\bar{c})$ whenever $a_j, b_j, c_j \in C_{i_j}$, $j = 1, \dots, k$. Here each occurrence of $+$ or $-$ is to be interpreted in the appropriate group.

This, plus local finiteness, is already enough to prove that $|A| \leq 2^\omega$. To see this, pick a pair $a, b \in A$ of distinct elements which are μ -related. a, b belong to the same α -class, say to C_l . Let C_k be any class having more than one element in it; our task is to prove that C_k is small. Let $<$ be a linear ordering of C_k . We have $(a, b) \preceq (c, d)$ for all $c < d$ in C_k ; thus for each pair $c < d$ there is a certain kind of positive primitive formula $\pi_{cd}(x, y, z, w)$ witnessing this. π_{cd} has the form $\exists u_1 \dots \exists u_t \phi_{cd}(x, y, z, w, \bar{u})$ where ϕ_{cd} is quantifier-free; choose $\bar{e} \in A^t$ witnessing $\phi_{cd}(a, b, c, d, \bar{e})$ and let σ_{cd} be the finite sequence of indices (i_1, \dots, i_t) defined so that $e_j \in C_{i_j}$ for $j = 1, \dots, t$.

Conditions (*) and (**) imply that for each pair $c < d$ in C_k there exists $h \in \text{Hom}(\mathbf{C}_k, \mathbf{C}_l)$ such that for all $x < y$ in C_k , if $\pi_{xy} = \pi_{cd}$ and $\sigma_{xy} = \sigma_{cd}$, then $b - a = h(y - x)$. Now suppose that there exist $c < d < e$ in C_k such that $\pi_{cd} = \pi_{ce} = \pi_{de}$ and $\sigma_{cd} = \sigma_{ce} = \sigma_{de}$. Pick $h \in \text{Hom}(\mathbf{C}_k, \mathbf{C}_l)$ for c, d as described above. Then $b - a = h(d) - h(c) = h(e) - h(c) = h(e) - h(d)$. Subtracting the third item from the sum of the second and fourth (in \mathbf{C}_l) yields $b - a = 0$, a contradiction. So there cannot exist $c < d < e$ in C_k such

that all 3 pairs $(x, y) = (c, d), (c, e), (d, e)$ have the same positive primitive formula and the same sequence of indices witnessing $(a, b) \preceq (x, y)$.

On the other hand, \mathcal{V} is locally finite and so there are only countably many positive primitive formulas (up to equivalence in \mathcal{V}), hence only countably many possible pairs (π_{cd}, σ_{cd}) . Thus we have a countable coloring of $C_k^{(2)}$. By the Erdős-Rado theorem and the comments in the previous paragraph, $|C_k| \leq 2^\omega$ as desired. This proves that every member of \mathcal{V}_{si} has cardinality at most 2^ω , hence \mathcal{V} is residually small.¹ ■

Theorem 1.2 solves the restriction of the RS Problem to congruence modular varieties. The proof outlined above contains all of the main themes of current work on the unrestricted problem. We expect the full problem will be solved by identifying a number of “bad configurations” (such as an SI having a congruence which centralizes the monolith but doesn’t centralize itself), whose presence in a variety “generates residual largeness” via a canonical construction of large SIs. The absence of all the bad configurations will imply a certain structuredness of the SIs which will restrict the complexity of their term operations and thereby prevent the SIs from having cardinality greater than 2^ω . In general the analysis will require the consideration of several cases (e.g., on the structured side the “nonabelian monolith” case will no longer come for free).

1.3. A MODEST CONJECTURE

A few other special cases of the RS Problem have been solved. In every case known to me, the proof of residual largeness (on the unstructured side) is cast, or can be recast, using the same canonical construction presented in the proof of Theorem 1.2. First some notation: if R is a reflexive relation on a set A and $2 \leq n < \omega$, then $R^{(n)}$ denotes the set

$$R^{(n)} = \{(a_0, \dots, a_{n-1}) \in A^n : a_i R a_j \text{ whenever } 0 \leq i < j < n\}.$$

Typically, a “bad configuration” leads to certain data:

- an algebra \mathbf{A} in \mathcal{V}
- a reflexive subuniverse ρ of \mathbf{A}^2
- two elements $\mathbf{d}, \mathbf{e} \in \rho^{(3)}$
- a binary relation S on $\rho^{(5)}$.

¹In fact, using the theory of the commutator again, one can show that only finitely many positive primitive formulas are needed in the above argument. This gives a finite upper bound to the size of the SI members of \mathcal{V} , though quite a bit worse than the one obtained by Freese and McKenzie.

We shall try to construct arbitrarily large SIs in $\text{HSP}(\mathbf{A})$ in a canonical way using the above data. Let $(I, <)$ be a dense linearly ordered set without endpoints and containing designated elements $0 < 1$. For each $\mathbf{a} = (a_0, a_1, a_2) \in \rho^{(3)}$ and $i \in I$ define $f_i^{\mathbf{a}} : I \rightarrow A$ by

$$f_i^{\mathbf{a}}(j) = \begin{cases} a_0 & \text{if } j < i \\ a_1 & \text{if } j = i \\ a_2 & \text{if } j > i. \end{cases}$$

For each $\mathbf{b} = (b_0, \dots, b_4) \in \rho^{(5)}$ and $i < j$ in I define $h_{ij}^{\mathbf{b}} : I \rightarrow A$ by

$$h_{ij}^{\mathbf{b}}(k) = \begin{cases} b_0 & \text{if } k < i \\ b_1 & \text{if } k = i \\ b_2 & \text{if } i < k < j \\ b_3 & \text{if } k = j \\ b_4 & \text{if } k > j. \end{cases}$$

Let $\rho^{(I)}$ be the set of all functions $f : I \rightarrow A$ which satisfy $f(i)\rho f(j)$ whenever $i < j$. Then let \mathbf{B} be the subalgebra of \mathbf{A}^I whose universe consists of all functions $f \in \rho^{(I)}$ whose preimages partition I into finitely many intervals. Next we define some congruences on \mathbf{B} . Let β be the smallest congruence of \mathbf{B} which collapses the set $\{f_i^{\mathbf{d}} : i \in I\}$ to a single point and collapses the set $\{f_i^{\mathbf{e}} : i \in I\}$ to a single point. Let γ be the smallest congruence of \mathbf{B} which identifies $h_{ij}^{\mathbf{b}}$ with $h_{ij}^{\mathbf{c}}$ whenever $i < j$ and $\mathbf{b}S\mathbf{c}$. Finally, for each $i < j$ define δ_{ij} to be the least congruence which identifies $f_i^{\mathbf{a}}$ with $f_j^{\mathbf{a}}$ for all $\mathbf{a} \in \rho^{(3)}$. If $f_0^{\mathbf{d}} \not\equiv f_0^{\mathbf{e}} \pmod{\beta \vee \gamma}$ but $f_0^{\mathbf{d}} \equiv f_0^{\mathbf{e}} \pmod{\delta_{01} \vee \gamma}$, then the construction is successful and we get arbitrarily large SIs in $\text{HSP}(\mathbf{A})$.²

(The construction in the previous section can be recast in this format by setting $\rho = \alpha$, $\mathbf{d} = (0, 0, 0)$, $\mathbf{e} = (0, c, 0)$, and $S = \emptyset$.)

Let us say that the 5-tuple $(\mathbf{A}, \rho, \mathbf{d}, \mathbf{e}, S)$ forces residual largeness if the above construction is successful. A reasonable working conjecture is:

Conjecture 1.3 *If a finitely generated variety is residually large, then it contains a 5-tuple $(\mathbf{A}, \rho, \mathbf{d}, \mathbf{e}, S)$ which forces residual largeness in the above sense.*

I should remark that there exist nonfinitely generated varieties which are residually large but have no such 5-tuple forcing residual largeness in this sense. Any residually large congruence distributive variety is an example.

²This is true even if \mathbf{A} is infinite. The proof follows that of Theorem 1.2 in the previous section, assuming in addition that $\kappa \geq \max(|A|, \omega)$.

1.4. FURTHER RESULTS

Several other cases of the RS Problem have been solved. Some of the results are quite technical and are best characterized as partial results or work in progress. Others represent significant milestones. Here is a sampling of the latter.

- D. Hobby and R. McKenzie [5] solved the RS Problem for all finitely generated varieties whose finite members “omit types **1** and **5**” in the sense of tame congruence theory.
- K. Kearnes, E. Kiss and M. Valeriote [7] have solved the RS Problem for all minimal varieties³ generated by a finite simple algebra of type **3** or **4**.

The solutions isolate new bad configurations, and show that the varieties under consideration which omit these configurations must be congruence modular.

- In the summer of 1996, M. Valeriote announced a solution to the RS Problem for finitely generated varieties all of whose members are *abelian* (see Kiss’s article near the end of Section 6 for the definition).

In finitely generated abelian varieties, SIs with type **2** monolith are automatically small by an old argument of McKenzie’s. Valeriote proves that if the bad configuration from [7] is omitted, then the finite SIs with type **1** monolith are also small. The proof uses the new theory of “multi-traces” invented in [6] (also see Kiss’s article, Section 9).

Of particular relevance to these lectures is an unpublished result of McKenzie’s. In 1986 he discovered a configuration which can be found in some nonabelian algebras, and proved that the configuration is bad. Then in the spring of 1993 McKenzie proved that, conversely, if \mathcal{V} is a finitely generated variety which omits this configuration, then every SI in \mathcal{V} *with nonabelian monolith* has a certain structuredness which forces it to have size at most 2^ω .

Here is the structure. Roughly speaking, each SI with nonabelian monolith will be embeddable in an algebra which can be covered by finitely many (possibly overlapping) meet semilattices where the semilattice operations are compatible with the operations of the larger algebra. More precisely, let \mathbf{B} be an algebra. McKenzie calls \mathbf{B} *semilattice-decomposable* if there exist

³A variety is *minimal* if it is nontrivial (i.e., contains more than just the 1-element algebras) and its only proper subvariety is the trivial variety. The RS Problem is uninteresting for minimal varieties generated by a finite simple algebra of type **1** or **2**, as a consequence of results due to Á. Szendrei [15, 16] and, independently, Kearnes, Kiss and Valeriote [6]. Concerning the RS Problem for minimal varieties generated by a finite simple algebra of type **5**, Szendrei has recently announced a solution in the “term-minimal” case.

a partial ordering \leq of B and a finite collection C_1, \dots, C_m of subsets of B such that

- (i) Each fundamental operation of \mathbf{B} is monotone in each variable with respect to the ordering \leq .
- (ii) $C_1 \cup \dots \cup C_m = B$.
- (iii) Each C_i is a meet subsemilattice of (B, \leq) in the following strong sense: if $x, y \in C_i$ then x and y have a greatest lower bound $x \wedge y$ in B , and this element is contained in C_i .
- (iv) If F is a k -ary fundamental operation of \mathbf{B} and if i_1, \dots, i_k are arbitrary indices from $\{1, \dots, m\}$, then there exists $l \in \{1, \dots, m\}$ such that

$$(*) F(C_{i_1} \times \dots \times C_{i_k}) \subseteq C_l, \text{ and}$$

$$(**) F(a_1 \wedge b_1, \dots, a_k \wedge b_k) = F(\bar{a}) \wedge F(\bar{b}) \text{ whenever } a_j, b_j \in C_{i_j}, j = 1, \dots, k.$$

McKenzie [13] proves that (1) in a finitely generated variety which realizes his configuration, there is a 5-tuple which forces residual largeness in the sense of Section 1.3; furthermore, the SIs forced by the 5-tuple have nonabelian monolith; (2) in a finitely generated variety which omits his configuration, any SI with nonabelian monolith can be embedded in a semilattice-decomposable algebra; and (3) any SI which can be embedded in a semilattice-decomposable algebra and whose language is essentially countable must have cardinality at most 2^ω . The proof of (3) is similar in form to the corresponding part of the proof of Theorem 1.2, using the Erdős-Rado theorem.

This result of McKenzie's solves that portion of the RS Problem pertaining to the SIs whose monoliths have type **3**, **4** or **5**. Very recently, Kearnes announced a similar solution for SIs whose monoliths have type **2**. Thus the full RS Problem has been reduced to the consideration of SIs with type **1** monolith.

2. Second lecture: McKenzie's counterexamples

2.1. THE RS CONJECTURE

In 1988 D. Hobby and R. McKenzie stated the following conjecture [5, p. 147]:

Conjecture 2.1 (The RS conjecture) *Let \mathbf{A} be a finite algebra. Either $\text{HSP}(\mathbf{A})$ is residually large, or there is a finite bound to the size of the SIs in $\text{HSP}(\mathbf{A})$.*

This conjecture strengthened an older conjecture⁴ and reflected conventional wisdom as to what the solution to the RS problem would turn out to look like. Another piece of conventional wisdom, though not stated until 1993, was:

Conjecture 2.2 (The effective RS conjecture) *There is an algorithm that, given a finite algebra \mathbf{A} in a finite language, determines which of the two alternatives in the RS conjecture holds.*

By the fall of 1993 McKenzie had refuted both conjectures. His constructions are ingenious, but what is more important is his method. In this lecture I will attempt to explain some aspects of the method. Then in my third lecture I will indicate how the method has been used to prove the undecidability of some seemingly unrelated decision problems concerning finite algebras and the varieties they generate.

2.2. SEMILATTICE-BASED ALGEBRAS

McKenzie's counterexamples arose from his investigation of SIs with nonabelian monolith in finitely generated varieties. Recall that McKenzie had proved that if the variety omits a certain configuration, then these SIs can be embedded in something called a semilattice-decomposable algebra. The universe of such an algebra can be expressed as the union of finitely many semilattices, and the fundamental operations are compatible with the corresponding semilattice operations. Hence semilattices play a significant role.

In this lecture, I shall always assume that the finite generating algebras \mathbf{A} under consideration have a binary term defining a meet semilattice operation \wedge throughout A . Among other things, this forces all SIs in $\mathbf{HSP}(\mathbf{A})$ to have nonabelian monolith. Let \leq be the partial ordering of A induced by \wedge . Until further notice, I shall also assume that:

- (*) The poset (A, \leq) has height 1 with least element named 0; and each fundamental operation yields 0 whenever one or more of its variable inputs is 0.

The assumption (*) forces each fundamental operation F of \mathbf{A} to be monotone with respect to \leq , but not necessarily compatible with \wedge . Moreover, it makes the compatibility of F with \wedge , i.e., the condition $F(\bar{x} \wedge \bar{y}) = F(\bar{x}) \wedge F(\bar{y})$, equivalent to the "unique factorization" condition $F(\bar{x}) = F(\bar{y}) \neq 0 \Rightarrow \bar{x} = \bar{y}$. If all the fundamental operations of \mathbf{A} satisfy this condition, then every SI in $\mathbf{HSP}(\mathbf{A})$ has cardinality less than $|A|^{|A|}$. So we

⁴The so-called 'Quackenbush conjecture,' which asserted that if \mathbf{A} is finite and $\mathbf{HSP}(\mathbf{A})$ has arbitrarily large finite SIs, then it has at least one infinite SI.

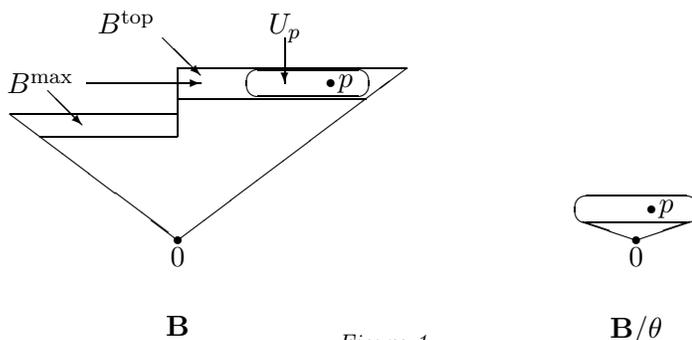


Figure 1.

shall consider finite algebras \mathbf{A} which satisfy $(*)$ but whose fundamental operations are not generally compatible with \wedge .

It is easy to describe the SIs in such a variety. First, each member of $\text{HSP}(\mathbf{A})$ is isomorphic to a quotient \mathbf{B}/θ of a subalgebra \mathbf{B} of some power of \mathbf{A} , say $\mathbf{B} \leq \mathbf{A}^I$. \mathbf{B} is itself a meet semilattice; let B^{\max} denote the set of maximal elements of \mathbf{B} with respect to its semilattice ordering. Regarding the elements of \mathbf{B} as functions, define $B^{\text{top}} = \{f \in B : 0 \notin \text{range}(f)\}$ and observe that $B^{\text{top}} \subseteq B^{\max}$. For each $p \in B^{\text{top}}$ define

$$U_p = \{f \in B^{\text{top}} : \lambda(f) = p \text{ for some unary polynomial operation } \lambda \text{ defined by a nonconstant term using parameters from } B^{\text{top}}\}.$$

If \mathbf{B}/θ is SI then there must exist elements p, q of B such that θ is maximal with respect to not identifying p with q . The next lemma is our description of the SIs in $\text{HSP}(\mathbf{A})$.

LEMMA 2.3 *Suppose \mathbf{A} is a finite semilattice-based algebra satisfying $(*)$, and \mathbf{S} is an SI in $\text{HSP}(\mathbf{A})$. Then \mathbf{B}, θ, p, q can be chosen as above so that:*

- (1) $p \in B^{\text{top}}$ and $q = 0$.
- (2) The θ -classes are precisely $B \setminus U_p$ and the singletons $\{f\}$, $f \in U_p$.
- (3) Hence \mathbf{B}/θ is a height-1 meet semilattice whose universe is essentially $U_p \cup \{0\}$ (see Figure 1).
- (4) Conversely, any $\mathbf{B} \leq \mathbf{A}^I$ and $p \in B^{\text{top}}$ are associated to some SI in $\text{HSP}(\mathbf{A})$ in this way.

The point is that the SIs in $\text{HSP}(\mathbf{A})$ can be completely understood by analyzing the sets U_p which arise in the top part of subalgebras of powers of \mathbf{A} .

Let me apply this lemma to an example essentially due to McKenzie. The universe is $\{C, D, 1, H, 2, 0\}$; the operations are 0 (constant) and \wedge and

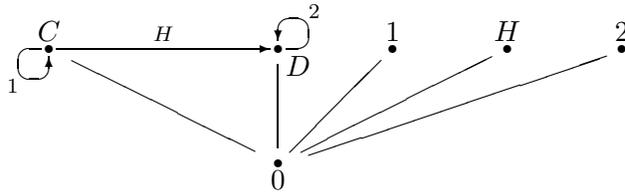


Figure 2. The algebra \mathbf{M}

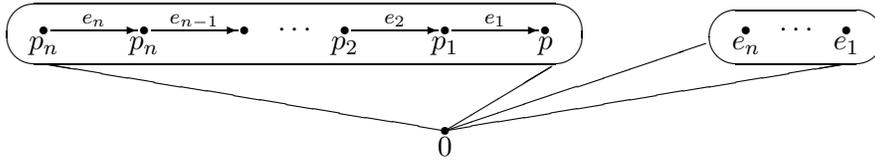


Figure 3. The "chain" SI \mathbf{B}_n/θ in $\text{HSP}(\mathbf{M})$

\cdot (both binary) where

$$\begin{aligned}
 x \wedge y &= \begin{cases} x & \text{if } x = y \\ 0 & \text{otherwise} \end{cases} \\
 1 \cdot C &= C, \quad H \cdot C = D, \quad 2 \cdot D = D, \\
 x \cdot y &= 0 \text{ otherwise.}
 \end{aligned}$$

Call this algebra \mathbf{M} . The operation \cdot defines a directed looped graph structure on the set $\{C, D\}$; the elements $1, H, 2$ function as the individual edges of the graph (see Figure 2).⁵ Now we shall construct some medium-size SIs in $\text{HSP}(\mathbf{M})$. Fix $n \geq 2$ and define the following elements in M^n :

$$\begin{aligned}
 p_0 &= DDD \cdots D \\
 p_1 &= CDD \cdots D & e_1 &= H22 \cdots 2 \\
 p_2 &= CCD \cdots D & e_2 &= 1H2 \cdots 2 \\
 &\vdots & & \\
 p_n &= CCC \cdots C & e_n &= 111 \cdots H
 \end{aligned}$$

Let $X = \{p_i : i \leq n\} \cup \{e_i : 1 \leq i \leq n\}$. These elements have been designed so that, computing in \mathbf{M}^n , we have $e_i \cdot p_i = p_{i-1}$ and $0 \in \text{range}(x \cdot y)$ for all other $x, y \in X$. Now construct the subalgebra \mathbf{B}_n of \mathbf{M}^n generated by the set X . It is easy to see that for each $f \in X$ there exists a unary

⁵Note that $H \cdot C = 2 \cdot D \neq 0$, so unique factorization fails in \mathbf{M} .

polynomial λ of \mathbf{B}_n , built using parameters in X only, which sends f to p_0 . For example, if $f = e_3$ then use $\lambda(x) = e_1 \cdot (e_2 \cdot (x \cdot p_3))$. Thus if we set $p = p_0$ then U_p will be precisely X . Hence $\text{HSP}(\mathbf{M})$ contains the SI algebra pictured in Figure 3: a height-1 semilattice whose nonzero elements encode the vertices and edges of a directed chain of length $n + 1$ terminating at p . By this same technique we can produce an SI whose nonzero elements encode the vertices and edges of an infinite chain order-isomorphic to ω^* .

$\text{HSP}(\mathbf{M})$ contains many other SIs; for example, all height-1 semilattices whose nonzero elements encode the vertices and edges of a tree rooted at p . What separates the chain SIs from all others is that they are the ones which satisfy the conditions:

1. No loops (i.e., edges of the form $v \xrightarrow{e} v$).
2. If $u \xrightarrow{e} v$ and $u' \xrightarrow{e'} v$, then $u = u'$ and $e = e'$.

Translated back to the language of $\text{HSP}(\mathbf{M})$, these conditions are just:

- 1'. $\neg \exists xy(x \cdot y = y \neq 0)$
- 2'. Unique factorization: $\forall \bar{x}\bar{y}[(x_1 \cdot x_2 = y_1 \cdot y_2 \neq 0) \Rightarrow \bar{x} = \bar{y}]$.

Note that (1') and (2') are universal sentences. What McKenzie's method will allow us to do is to modify a finite semilattice-based algebra such as \mathbf{M} so that desirable universal conditions such as (1') and (2') will be forced upon almost all SIs in the generated variety, even if they do not hold in the generating algebra itself.

2.3. THE DEVIOUS TRICK

In this section \mathbf{A} is a finite but otherwise arbitrary semilattice-based algebra. To avoid the conclusion of Lemma 2.3(4), I no longer assume that \mathbf{A} satisfies (*). The nature of the SIs in $\text{HSP}(\mathbf{A})$ is not as simple as in Lemma 2.3, but still something can be said. Each SI in $\text{HSP}(\mathbf{A})$ can be embedded in an ultraproduct of finite SIs in $\text{HSP}(\mathbf{A})$, so I will focus on the latter. Fix \mathbf{S} , a finite SI in $\text{HSP}(\mathbf{A})$. For any $\mathbf{B} \leq \mathbf{A}^I$ define $B^{\text{top}} = \{f \in B : 0 \notin \text{range}(f)\}$.

FACT 1. $\mathbf{B} \leq \mathbf{A}^I$, $\theta \in \text{Con } \mathbf{B}$, and $p, q \in B$ can be chosen so that $\mathbf{S} \cong \mathbf{B}/\theta$ and:

1. θ is maximal with respect to not relating p to q .
2. $p \in B^{\text{top}}$ and $q < p$.
3. p is the minimum element of its θ -class. Hence $\{x \in B : x \geq p\}$ is a union of θ -classes. All θ -classes are determined as follows: $f \not\equiv g \pmod{\theta}$ iff there exists a unary polynomial operation λ of \mathbf{B} such that $\lambda(f) = p$ while $\lambda(g) < p$, or vice versa.

4. q/θ is the unique lower cover of p/θ in $(B/\theta, \leq)$. That is,

$$\mathbf{B}/\theta \models \forall x(x < p/\theta \Leftrightarrow x \leq q/\theta).$$

5. For each $i \in I$ there exists $p_i \in B$ such that $p_i(j) = p(j)$ for all $j \neq i$, while $p_i(i) < p(i)$.

PROOF. Choose $\mathbf{B} \leq \mathbf{A}^I$ and $\theta \in \text{Con } \mathbf{B}$ so that $\mathbf{S} \cong \mathbf{B}/\theta$ with $|I|$ minimal. Then choose $q/\theta < p/\theta$ in \mathbf{B}/θ satisfying item 1 and so that p/θ is minimal (with respect to the semilattice ordering of \mathbf{B}/θ) among all possible choices. This makes item 4 true. Now replace p by the minimum element of p/θ ; this makes items 3 and 5 true (the latter by the minimality of I), hence proving $p \in B^{\text{top}}$ as well. Finally, replace q if necessary by $q \wedge p$; this makes item 2 true. \blacksquare

Note in particular that if \mathbf{A} has height 1, then the situation becomes slightly simpler: $\{p\}$ is itself a θ -class, and the elements p_i referred to in item 5 are uniquely specified by $p_i(i) = 0$.

For the remainder of this section, fix $\mathbf{B} \leq \mathbf{A}^I$ and θ, p, q as in Fact 1.

FACT 2. If $h_1, \dots, h_m \in B$ with $h_i < p$ ($i = 1, \dots, m$), and if λ is an m -ary polynomial operation of \mathbf{B} , then $\lambda(\bar{h}) \geq p$ iff $\lambda(h_1 \wedge q, \dots, h_m \wedge q) \geq p$.

PROOF. $h_i < p$ implies $h_i/\theta < p/\theta$, hence $h_i/\theta \leq q/\theta$, i.e., $h_i \equiv h_i \wedge q \pmod{\theta}$. So $\lambda(\bar{h}) \equiv \lambda(h_1 \wedge q, \dots, h_m \wedge q) \pmod{\theta}$. Since $\{x \in B : x \geq p\}$ is a union of θ -classes, the claim follows. \blacksquare

Some notation: if $\Phi(\bar{x})$ is an n -ary predicate on the set A and $f_i \in A^I$ for $i = 1, \dots, n$, then $\llbracket \Phi(\bar{f}) \rrbracket$ denotes the set $\{i \in I : \Phi(f_1(i), \dots, f_n(i)) \text{ holds}\}$. For example, Fact 1 implies $\llbracket q < p \rrbracket = \llbracket q \neq p \rrbracket \neq \emptyset$; and if \mathbf{A} has height 1, then $\llbracket q < p \rrbracket = \llbracket q = 0 \rrbracket$. As a special case of Fact 2 we have:

FACT 3. Let $\Phi(\bar{u}, x, \bar{y})$ be an $n + 1 + m$ -ary predicate on A which is “monotone in \bar{y} on the half-open interval $[0, x)$,” i.e., if $\Phi(\bar{u}, x, \bar{a})$ holds and $a_i \leq b_i < x$ for all $i = 1, \dots, m$, then $\Phi(\bar{u}, x, \bar{b})$ also holds. Suppose that among the term operations of \mathbf{A} is the $n + 1 + m$ -ary operation t_Φ defined by

$$t_\Phi(\bar{u}, x, \bar{y}) = \begin{cases} x & \text{if } \Phi(\bar{u}, x, \bar{y}) \\ 0 & \text{otherwise.} \end{cases}$$

Then for all $\bar{f} \in B^n$ and $\bar{h} \in B^m$ with $h_i < p$ ($i = 1, \dots, m$), and putting $\bar{q} = (q, q, \dots, q) \in B^m$, the following implication holds:

$$\text{If } \llbracket \Phi(\bar{f}, p, \bar{h}) \rrbracket = I, \text{ then } \llbracket q < p \rrbracket \subseteq \llbracket \Phi(\bar{f}, p, \bar{q}) \rrbracket.$$

Thus an operation of the form t_Φ can allow the nature of \bar{f}, p, q at the coordinates $\llbracket q < p \rrbracket$ to have some influence on the nature of \bar{f}, p outside

of $\llbracket q < p \rrbracket$. This influence is mediated by the parameters \bar{h} . By item 5 of Fact 1, there exist sufficient parameters so that all coordinates in I can participate.

For example, suppose $H(\bar{u}, x)$, $K(\bar{u}, x)$ and $C(\bar{u}, x)$ are $n + 1$ -ary predicates on A . Let $\Phi(\bar{u}, x, y_1, y_2)$ be the following predicate:

$$\Phi(\bar{u}, x, y_1, y_2) \quad \leftrightarrow \quad H(\bar{u}, x) \text{ and } \begin{cases} y_1 = y_2 = x, \text{ or} \\ K(\bar{u}, x) \text{ and } x \in \{y_1, y_2\}, \text{ or} \\ C(\bar{u}, x) \text{ and } y_1, y_2 < x \end{cases}$$

and let $\Phi^*(\bar{u}, x)$ be $\Phi(\bar{u}, x, y, y)$.

FACT 4.

1. If t_Φ is among the term operations of \mathbf{A} , then for all \bar{f} in B :
If $\llbracket H(\bar{f}, p) \rrbracket = I$ and $\llbracket K(\bar{f}, p) \rrbracket \geq 2$, then $\llbracket q < p \rrbracket \subseteq \llbracket C(\bar{f}, p) \rrbracket$.
2. If t_{Φ^*} is among the term operations of \mathbf{A} , then for all \bar{f} in B :
If $\llbracket H(\bar{f}, p) \rrbracket = I$ and $\llbracket C(\bar{f}, p) \rrbracket \neq \emptyset$, then $\llbracket q < p \rrbracket \subseteq \llbracket C(\bar{f}, p) \rrbracket$.

As a special case of item 1,

3. If $K = \text{True}$ while $C = \text{False}$, and t_Φ is among the term operations of \mathbf{A} , then for all \bar{f} in B , $|I| \geq 2 \Rightarrow \llbracket H(\bar{f}, p) \rrbracket \neq I$.

In item 2 I shall denote t_{Φ^*} by $J_{H,C}$; in item 3 I shall denote t_Φ by S_H . Note that if both $J_{H,C}$ and $J_{H,-C}$ are present (as term operations of \mathbf{A}), then $\llbracket H(\bar{f}, p) \rrbracket = I$ implies $\llbracket C(\bar{f}, p) \rrbracket = \emptyset$ or I . If S_{-C} is also present, then $\llbracket H(\bar{f}, p) \rrbracket = I$ forces $\llbracket C(\bar{f}, p) \rrbracket = I$, provided $|I| \geq 2$. This is a universal implication of sorts, imposed on the elements of \mathbf{B} even if it fails to hold in \mathbf{A} . These remarks are true for any \mathbf{B}, p corresponding to any finite SI in $\text{HSP}(\mathbf{A})$ in accordance with Fact 1.

This is the germ of McKenzie's method. One builds a semilattice-based algebra satisfying (or nearly satisfying) the condition (*), and whose generated variety contains certain desired SIs. Then one adds operations of the form $J_{H,C}$ and S_H , or more generally t_Φ , to the algebra in order to banish the remaining undesirable SIs. The extra operations must be sufficiently innocuous so that (i) the desired SIs remain present (as reducts of SIs in the new variety), and (ii) no (or not too many) new undesired SIs are inadvertently created.

A strategy for accomplishing this is to pray that the SIs in the new variety arise more or less in the way described in Lemma 2.3, that is, from quotients of the form \mathbf{B}/θ where \mathbf{B} is a subalgebra of a power of the new generating algebra, and θ is a congruence which collapses all but a portion of the top of \mathbf{B} to 0. Then all of the structure of \mathbf{B}/θ will live in the top of \mathbf{B} , while the garbage created in \mathbf{B} by the new operations will lie strictly

below the top, and hence will be collapsed by θ to 0. McKenzie showed that this strategy (perhaps without the praying) can succeed.

2.4. AN EXAMPLE

In this last section I will give some hints on how one can use the ideas from the previous section to enlarge the example \mathbf{M} from Section 2.2 to get a finite algebra \mathbf{A} so that the SIs in $\text{HSP}(\mathbf{A})$ are just the chain SIs plus a finite number of inconsequential (finite) SIs.

Let \mathbf{M}_1 be the algebra in the same language as \mathbf{M} and with universe $M \cup \{a, b\}$, defined so that \mathbf{M}_1 has height 1, extends \mathbf{M} , and satisfies $a \cdot x = x \cdot a = b \cdot x = x \cdot b = 0$. a and b will function as “flags” for other operations. \mathbf{M}_2 will be an expansion of \mathbf{M}_1 . Define the relations $H(u, x)$ and $C(u, x)$ on M_1 by

$$\begin{aligned} H(u, x) &\leftrightarrow u \in \{a, b\} \\ C(u, x) &\leftrightarrow u = a. \end{aligned}$$

\mathbf{M}_2 will include the operations $J_{H,C}$, $J_{H,-C}$ and S_{-C} . These will force the condition

$$f \in \{a, b\}^I \text{ implies } f = \hat{a}$$

in all $\mathbf{B} \leq \mathbf{M}_2^I$ corresponding to finite SIs assuming $|I| \geq 2$ (as explained in the previous section). Next define a 4-ary operation T on M_1 by

$$T(x, y, z, w) = \begin{cases} a & \text{if } x \cdot y = z \cdot w \neq 0 \text{ and } x = z \text{ and } y = w \\ b & \text{if } x \cdot y = z \cdot w \neq 0 \text{ and } \neg(x = z \text{ and } y = w) \\ 0 & \text{otherwise.} \end{cases}$$

T will do the following: if $v, v' \in \{C, D\}^I$ and $e, e' \in \{1, H, 2\}^I$ and $e \cdot v = e' \cdot v' \in \{C, D\}^I$ but $e \neq e'$ or $v \neq v'$, then $T(e, v, e', v')$ will be an element of $\{a, b\}^I$ different from \hat{a} . Since this has been forbidden by the previous operations, the “unique factorization law” for \cdot (item 2' from Section 2.2) will be enforced whenever $|I| \geq 2$. Now define the relation $K(u, x)$ by

$$K(u, x) \leftrightarrow u \in \{1, 2\}$$

and introduce S_K . In SIs for which $|I| \geq 2$, the presence of S_K ensures that if $e \in \{1, H, 2\}^I$, i.e., if e potentially represents an edge, then $H \in \text{range}(e)$. This will enforce item 1' in Section 2.2 (disallowing loops).

We let $\mathbf{M}_2 = (\mathbf{M}_1, J_{H,C}, J_{H,-C}, S_{-C}, T, S_K)$, hold our collective breath, and hope that everything works: that (1) the intended SIs (the chain SIs from Section 2.2) remain in $\text{HSP}(\mathbf{M}_2)$ (not literally, but as reducts), and (2) no new unintended SIs are created by the introduction of the new elements

and operations; then \mathbf{M}_2 will be a counterexample to the RS conjecture. In fact, (1) is achieved, but (2) fails miserably: $\text{HSP}(\mathbf{M}_2)$ is residually large. The extra SIs arise from the fact that, using the language of Section 2.2, and in particular Lemma 2.3, the directed graphs which are encoded by the sets U_p no longer need to be rooted. Indeed, if $p = \hat{a}$ and $v \xrightarrow{e} v'$ is any edge in B^{top} (for some $\mathbf{B} \leq \mathbf{M}_2^f$), then $T(e, v, e, v) = \hat{a}$ and hence $\{e, v\} \subseteq U_{\hat{a}}$.

McKenzie was more clever. Among other things, instead of adding flags as new elements, he incorporated them into the existing elements by “doubling” C and D . The role of \hat{a} in the above argument is then taken over by every vertex in the directed graph. See his paper [8] for the details.

In the end, McKenzie succeeded in building an 8-element semilattice-based algebra \mathbf{A} such that the SIs in $\text{HSP}(\mathbf{A})$ are essentially just the chain SIs defined in the previous section, plus a few extra SIs for which $|I| = 1$. This example refutes the RS conjecture.

McKenzie also used the method to construct a finite algebra \mathbf{B} such that $\text{HSP}(\mathbf{B})$ has an SI of cardinality 2^ω , but no SI of larger cardinality; and a finite algebra \mathbf{C} in an infinite language such that $\text{HSP}(\mathbf{C})$ has arbitrarily large finite SIs but no infinite SI. In my final lecture, I will outline McKenzie’s idea of using the method to capture Turing machine computations in the structure of the SIs.

3. Third lecture: Tarski’s finite basis problem and other undecidable problems

In light of McKenzie’s refutation of the RS conjecture, the so-called effective RS conjecture (Conjecture 2.2 from the second lecture) must be revised. Let me pose the revision as a pair of problems.

PROBLEM 3.1 *Is there an algorithm which, given a finite algebra \mathbf{A} in a finite language, determines whether $\text{HSP}(\mathbf{A})$ is residually small?*

PROBLEM 3.2 *Is there an algorithm which, given a finite algebra \mathbf{A} in a finite language, determines whether there is a finite bound to the sizes of the SIs in $\text{HSP}(\mathbf{A})$?*

A famous but (apparently) unrelated problem in general algebra is “Tarski’s finite basis problem,” posed by A. Tarski in the mid-1960s:

PROBLEM 3.3 *Is there an algorithm which, given a finite algebra \mathbf{A} in a finite language, determines whether the first-order theory of $\text{HSP}(\mathbf{A})$ is finitely axiomatizable?*

Almost immediately after discovering his counterexamples to the RS conjecture, McKenzie realized that he had at hand the tools to solve Problems 3.2 and 3.3 negatively. McKenzie (mainly) and others have used these

methods to prove the undecidability of other decision problems involving the equational classes generated by finite algebras, including Problem 3.1. In this lecture I will try to sketch some of the main ideas of these results.

3.1. ENCODING THE HALTING PROBLEM

Recall the discussion of the semilattice-based algebra \mathbf{M} from Section 2.2. The finite chain SIs in $\text{HSP}(\mathbf{M})$ arise as quotients of algebras $\mathbf{B}_n \leq \mathbf{M}^n$; the nonzero elements of the SI correspond to certain elements at the top of \mathbf{B}_n , which fall into two classes: *vertices*, which are elements (n -tuples from \mathbf{M}) of the form $v_i = C \cdots CCDD \cdots D$, and *edges*, which are elements of the form $e_i = 1 \cdots 1H22 \cdots 2$. The multiplication operation of \mathbf{M} acts coordinatewise in \mathbf{B}_n so that $e_i \cdot v_i = v_{i-1}$, and we interpreted this as a directed edge $v_i \xrightarrow{e_i} v_{i-1}$.

McKenzie saw that the vertices $C \cdots CCDD \cdots D$ in \mathbf{B}_n could be construed as finite fragments of blank Turing machine tapes (the interface between the Cs and Ds representing the current position of the machine's read/write head). If \mathcal{T}_0 is the Turing machine which always moves left and always writes blanks, then the directed edge relation of \mathbf{B}_n would represent some of the steps in a (rather uninteresting) computation of \mathcal{T}_0 .

Suppose now that \mathcal{T} is a less trivial Turing machine. Imagine that, by changing \mathbf{M} somehow, we can modify the algebras \mathbf{B}_n so that:

1. In place of the "blank" tape fragments $C \cdots CCDD \cdots D$ we can encode fragments of *arbitrary* Turing machine tapes or, more precisely, *configurations* (i.e., tapes plus the current location of the read/write head and the current state of the machine). These are to be encoded as n -tuples over some fixed finite set in some standard way.
2. In place of the directed edge relation encoded by multiplication, we can encode the transition relation of \mathcal{T} restricted to the above configuration fragments. This relation will be encoded by various operations corresponding to the individual instructions of \mathcal{T} . With a little care, these operations can be defined so that they operate coordinatewise on the configuration fragments.

Adding a 0 element to the finite set of elements used so far, we should get a finite semilattice-based algebra \mathbf{A} in a finite language such that $\text{HSP}(\mathbf{A})$ contains SIs which encode fragments of the computations done by \mathcal{T} .

More precisely, Turing machine tapes shall be sequences of symbols indexed by \mathbb{Z} . Fix an interval $I \subseteq \mathbb{Z}$ and let $\text{Config}_I(\mathcal{T})$ be the set of all configurations for \mathcal{T} restricted to I . The action of \mathcal{T} determines a directed edge relation $\vdash_{\mathcal{T}}$ (the forward transition function) on $\text{Config}_I(\mathcal{T})$. Thus if $q, q' \in \text{Config}_I(\mathcal{T})$ and Q, Q' are their expansions to elements of $\text{Config}_{\mathbb{Z}}(\mathcal{T})$ obtained by adding blanks outside of I , then the following are equivalent:

1. (q, q') is in the transitive closure of $\vdash_{\mathcal{T}}$.
2. The computation of \mathcal{T} starting from Q eventually reaches Q' , and the read/write head never leaves the interval I during this portion of the computation.

If the interval I is finite, then there is a finite upper bound (depending on \mathcal{T}) to the sizes of the connected components of the directed graph $\langle \text{Config}_I(\mathcal{T}), \vdash_{\mathcal{T}} \rangle$. On the other hand, I assume with no loss of generality that for every Turing machine \mathcal{T} under consideration, $\text{Config}_{\mathbb{Z}}(\mathcal{T})$ has at least one infinite connected component in which no configuration is in the halting state.

In the algebra \mathbf{A} that we are imagining, the members of $\text{Config}_I(\mathcal{T})$ can be coded as elements of A^I . I further assume that \mathbf{A} includes operations which ensure that if $q, q' \in \text{Config}_I(\mathcal{T})$ and $q \vdash_{\mathcal{T}} q'$, then some polynomial operation of \mathbf{A}^I maps q to q' . To simplify the discussion that follows, I shall also assume that \mathbf{A} includes “reversing” operations so that another polynomial operation maps q' back to q . Then the intended SIs in $\text{HSP}(\mathbf{A})$ will be all SIs whose nonzero elements encode, for some I , a connected component of $\text{Config}_I(\mathcal{T})$.

By adding further operations to enforce various universal implications, as explained in the second lecture, it will be possible to obtain a finite algebra \mathbf{A}' such that the SIs in $\text{HSP}(\mathbf{A}')$ are essentially the desired SIs described above and little else. Thus, the SIs in $\text{HSP}(\mathbf{A}')$ will encode in a transparent way the connected components of $\text{Config}_I(\mathcal{T})$ for all intervals $I \subseteq \mathbb{Z}$.

To encode the halting problem in Problem 3.2, McKenzie made two further changes to \mathbf{A}' . To explain these changes, I must again direct your attention to Lemma 2.3. Though our algebra \mathbf{A}' will not satisfy the hypotheses of this lemma, we expect the SIs in $\text{HSP}(\mathbf{A}')$ to more or less satisfy the description provided by the conclusion. Thus a typical SI will have the form \mathbf{B}/θ where $\mathbf{B} \leq (\mathbf{A}')^I$ and θ has the form given in Lemma 2.3(2); in particular, there will exist $p \in B^{\text{top}}$ such that the nonzero elements of \mathbf{B}/θ may be identified with the elements of a certain subset $U_p \subseteq B^{\text{top}}$. This set U_p consists of those elements in B^{top} which can be mapped to p by certain polynomial operations of \mathbf{B} . Assuming I is an interval in \mathbb{Z} and p is a configuration fragment in $\text{Config}_I(\mathcal{T})$, the set U_p will turn out to be precisely the connected component of $\text{Config}_I(\mathcal{T})$ containing p .⁶

An important detail is that when $\mathbf{B} \leq (\mathbf{A}')^I$, $\theta \in \text{Con } \mathbf{B}$ and $p \in B^{\text{top}}$ correspond to an SI in this way, there is nothing to prevent B^{top} from containing configuration fragments beyond those in U_p , or even from containing garbage (tuples from A' which do not encode configuration fragments).

⁶I am lying. The set U_p will also contain certain “helper” elements, similar to the edge elements $e_i = 1 \cdots 1H22 \cdots 2$ from Section 2.2.

These elements in $B^{\text{top}} \setminus U_p$ add nothing to the structure of \mathbf{B}/θ , since they are all collapsed by θ to 0. In any event, the operations of \mathbf{A}' ensure that $B^{\text{top}} \cap \text{Config}_I(\mathcal{T})$ is a union of connected components of $\text{Config}_I(\mathcal{T})$, one of which is U_p .

Here are the two changes McKenzie made to \mathbf{A}' :

1. Add a new operation whose role is to put, in any \mathbf{B} corresponding to an SI of configuration fragments from $\text{Config}_I(\mathcal{T})$, an element which encodes an *initial* configuration fragment (blank tape, initial state) with the read/write head positioned in the middle of I . This element is put into B^{top} but not necessarily into U_p .
2. Add an enforcing operation S_H (of the kind described in Section 2.3) which prohibits the presence in B^{top} of an element encoding a configuration fragment which is in the halting (accepting) state.

Call the modified algebra \mathbf{A}^* .

Now suppose that \mathcal{T} eventually halts when its computation starts on a blank tape in the initial state. Let \mathbf{B} correspond to an SI in $\text{HSP}(\mathbf{A}^*)$, via the set $U_p \subseteq B^{\text{top}}$ encoding a connected component of $\text{Config}_I(\mathcal{T})$. B^{top} also contains an initial configuration fragment q_0 with its read/write head positioned in the middle of I . By the above remarks, the entire connected component of $\text{Config}_I(\mathcal{T})$ containing q_0 must also be present in B^{top} . If I is sufficiently large, this latter component will contain a configuration fragment in the halting state. As this is forbidden by the presence of the operation S_H , I must be small. Hence the connected component U_p is also small. Since the cardinality of \mathbf{B}/θ is $|U_p| + 1$, there is a finite bound to the sizes of the SIs in $\text{HSP}(\mathbf{A}^*)$.

On the other hand, if \mathcal{T} does not halt when started on the initial configuration, then it will be possible to define an algebra $\mathbf{B} \leq (\mathbf{A}^*)^{\mathbb{Z}}$ whose top elements include an infinite component of $\text{Config}_{\mathbb{Z}}(\mathcal{T})$ while including no configurations in the halting state. The infinite connected component yields a countably infinite SI in $\text{HSP}(\mathbf{A}^*)$. In approximately this way, McKenzie proved:

THEOREM 3.4 (McKenzie [9]) *There is an effective procedure which associates to each Turing machine \mathcal{T} a finite algebra $\mathbf{A}(\mathcal{T})$ in a finite language, so that the following are equivalent:*

1. *there is a finite bound to the sizes of the SIs in $\text{HSP}(\mathbf{A}(\mathcal{T}))$.*
2. *\mathcal{T} halts.*

Hence there is no algorithm which, given an arbitrary finite algebra \mathbf{A} in a finite language, decides whether there is a finite bound to the sizes of the SIs in $\text{HSP}(\mathbf{A})$.

3.2. TARSKI'S FINITE BASIS PROBLEM

McKenzie's $\mathbf{A}(\mathcal{T})$ used in proving Theorem 3.4 is slightly richer than the algebra \mathbf{A}^* I have described. In particular, $\text{HSP}(\mathbf{A}(\mathcal{T}))$ contains not only the configuration SIs described previously, but also some of the chain SIs from Section 2.2. If \mathcal{T} halts, then the chain SIs in $\text{HSP}(\mathbf{A}(\mathcal{T}))$ are of bounded finite size, but if \mathcal{T} does not halt, then $\text{HSP}(\mathbf{A}(\mathcal{T}))$ contains all the chain SIs. The latter fact yields a more or less immediate proof that the first-order theory of $\text{HSP}(\mathbf{A}(\mathcal{T}))$ is not finitely axiomatizable when \mathcal{T} does not halt (see [8, Lemmas 6.1 and 6.2] or [1, Theorem 1.1]).

McKenzie investigated the first-order theory of $\text{HSP}(\mathbf{A}(\mathcal{T}))$ when \mathcal{T} halts. Since the theory is axiomatized by its equations, it suffices to study the equational theory of $\text{HSP}(\mathbf{A}(\mathcal{T}))$ (or equivalently, of $\mathbf{A}(\mathcal{T})$). It turns out that the equational theory is syntactically very complicated. In order to make the equations more tractable, McKenzie replaced the algebra $\mathbf{A}(\mathcal{T})$ with a different algebra $\mathbf{F}(\mathcal{T})$. This latter algebra is still finite with a finite language, is constructed effectively from \mathcal{T} , and resembles $\mathbf{A}(\mathcal{T})$ in many ways. The equational class it generates still includes all the chain SIs when \mathcal{T} does not halt. Beyond this, the extra operations included in the definition of $\mathbf{F}(\mathcal{T})$ do not aim to force the remaining SIs in $\text{HSP}(\mathbf{F}(\mathcal{T}))$ to have a particular form, but rather aim to force the equations of $\mathbf{F}(\mathcal{T})$ to have tractable properties. In particular, if \mathcal{T} halts then a specific composition of the fundamental operations representing the halting computation can be used to transform arbitrary terms to certain normal forms; this allowed McKenzie to conclude that the equational theory is finitely axiomatizable.

In my opinion, the intuition underlying the construction of $\mathbf{F}(\mathcal{T})$ is far more devious, and more ad hoc, than that of $\mathbf{A}(\mathcal{T})$. Moreover, it is a rare moment when I believe that I have a full grasp of this intuition. Therefore I will not try to explain it, but simply state the amazing result:

THEOREM 3.5 (McKenzie [10]) *There is an effective procedure which associates to each Turing machine \mathcal{T} a finite algebra $\mathbf{F}(\mathcal{T})$ in a finite language, so that the following are equivalent:*

1. *The first-order theory of $\text{HSP}(\mathbf{F}(\mathcal{T}))$ is finitely axiomatizable.*
2. *\mathcal{T} halts.*

Hence there is no algorithm which, given an arbitrary finite algebra \mathbf{A} in a finite language, decides whether the first-order theory of $\text{HSP}(\mathbf{A})$ is finitely axiomatizable.

One year after McKenzie settled Tarski's problem, I discovered an essentially algebraic proof that the theory of $\text{HSP}(\mathbf{A}(\mathcal{T}))$ is finitely axiomatizable when \mathcal{T} halts [17]. This yields another proof of Theorem 3.5. For an excellent exposition of this proof as well as the proof of Theorem 3.4, see [14].

3.3. MODEL COMPANIONS

Consider 2-sorted structures $\langle G, A, * \rangle$ where $G = (G, E)$ is a directed acyclic graph, $A = (A, +, 0)$ is a vector space over \mathbb{Z}_2 , and $*$ is an action of A on G (which I will write as left multiplication). Say $\langle G, A, * \rangle$ is *strongly regular* if for all $v \in G$ and $a \in A$, if v and av belong to the same connected component of G , then $a = 0$. Say $\langle G, A, * \rangle$ is *weakly transitive* if for all $v, w \in G$ there exists $a \in A$ such that av and w belong to the same connected component of G .

Let \mathcal{K} denote the class of all strongly regular, weakly transitive structures $\langle G, A, * \rangle$ such that each connected component of G is a chain (finite or infinite). For each $n \geq 1$ let

$$\mathcal{K}_n = \{ \langle G, A, * \rangle : \text{the chains in } G \text{ all have length at most } n \}.$$

It is a simple exercise to prove that the $\forall\exists$ -theory of \mathcal{K}_n has a model companion for each n , but the $\forall\exists$ -theory of \mathcal{K} does not have a model companion.

Recall that $\text{HSP}(\mathbf{A}(\mathcal{T}))$ contains all the chain SIs when \mathcal{T} does not halt, but contains chain SIs only of bounded length when \mathcal{T} halts. By modifying the construction of $\mathbf{A}(\mathcal{T})$, I can build a finite algebra $\mathbf{M}(\mathcal{T})$ such that $\text{HSP}(\mathbf{M}(\mathcal{T}))$ contains SIs encoding all the members of \mathcal{K} when \mathcal{T} does not halt, but only those of \mathcal{K}_n for some fixed n when \mathcal{T} halts (plus configuration SIs). This is the idea behind the proof of:

THEOREM 3.6 (Willard [18]) *There is an effective procedure which associates to each Turing machine \mathcal{T} a finite algebra $\mathbf{M}(\mathcal{T})$ in a finite language, so that the following are equivalent:*

1. *The first-order theory of $\text{HSP}(\mathbf{M}(\mathcal{T}))$ has a model companion.*
2. *\mathcal{T} halts.*

Hence there is no algorithm which, given an arbitrary finite algebra \mathbf{A} in a finite language, decides whether the first-order theory of $\text{HSP}(\mathbf{A})$ has a model companion.

3.4. OTHER RESULTS

A basic problem from tame congruence theory is to determine, given a finite algebra \mathbf{A} in a finite language, the set of types $\mathbf{i} \in \{\mathbf{1}, \mathbf{2}, \mathbf{3}, \mathbf{4}, \mathbf{5}\}$ which occur⁷ in $\text{HSP}(\mathbf{A})$ (see Section 7 of Kiss's article). D. Hobby [4] proved that determining whether $\mathbf{3}$ belongs to the type set of $\text{HSP}(\mathbf{A})$ is PSPACE-hard. McKenzie saw that he could use his method to prove that it is undecidable.

⁷As the type of a covering pair of congruences in a finite algebra.

THEOREM 3.7 (McKenzie [11]) *There is an effective procedure which associates to each Turing machine \mathcal{T} a finite algebra $\mathbf{C}(\mathcal{T})$ in a finite language, so that the following are equivalent:*

1. $\mathbf{3}$ belongs to the type set of $\text{HSP}(\mathbf{C}(\mathcal{T}))$.
2. \mathcal{T} halts.

Hence there is no algorithm which, given an arbitrary finite algebra \mathbf{A} in a finite language, determines the type set of $\text{HSP}(\mathbf{A})$.

As these lecture notes go to press (November 1996), Japheth Wood of Vanderbilt University has announced a proof of the analogous result for type $\mathbf{4}$. The idea behind both proofs begins with the algebra \mathbf{A}' discussed in Section 3.1. A new set P is adjoined to the universe of \mathbf{A}' ; configuration fragments originally encoded as I -tuples $q \in (A')^I$ will now be encoded as $I \cup \{\infty\}$ -tuples $q \hat{\ } a \in (A' \cup P)^{I \cup \{\infty\}}$, where a can be any element in P . Now if $\mathbf{3}$ (or $\mathbf{4}$) is to belong to the type set of the variety being constructed, then it will have to occur as the type of the monolith of some finite SI in the variety. The algebra $\mathbf{C}(\mathcal{T})$ is built so that if \mathbf{B} corresponds to a finite SI in $\text{HSP}(\mathbf{C}(\mathcal{T}))$ whose monolith has the desired type, then one of the traces of the corresponding pair of congruences in \mathbf{B} must be a set of the form $\{q \hat{\ } a, q \hat{\ } b\}$ for some $q \in \text{Config}_I(\mathcal{T})$ and some distinct $a, b \in P$. However, the operations of $\mathbf{C}(\mathcal{T})$ are designed in such a way that the required polynomial structure on this pair arises only if q belongs to a connected component of $\text{Config}_I(\mathcal{T})$ containing both an initial configuration *and* a halting configuration. Thus if \mathcal{T} halts and I is sufficiently large, then some subalgebra $\mathbf{B} \leq \mathbf{C}(\mathcal{T})^{I \cup \{\infty\}}$ will have an SI quotient whose monolith has the desired type ($\mathbf{3}$ or $\mathbf{4}$); while if \mathcal{T} does not halt then the type in question does not appear anywhere in $\text{HSP}(\mathbf{C}(\mathcal{T}))$.

By a similar construction, McKenzie designed a finite algebra $\mathbf{B}_0(\mathcal{T})$ which encodes configurations by elements of the form $q \hat{\ } a$ as before. This time, the operations are designed so that if $\mathbf{B} \leq \mathbf{B}_0(\mathcal{T})^{I \cup \{\infty\}}$ corresponds to an SI encoding a connected component of $\text{Config}_I(\mathcal{T})$, and if this component includes both an initial configuration q and a halting configuration p , then the polynomial operations of \mathbf{B} enable the set $\{q \hat{\ } 0, q \hat{\ } a, p \hat{\ } a\}$ to support McKenzie's "bad configuration" of Section 1.4, forcing the variety to be residually large. Thus if \mathcal{T} halts, then $\text{HSP}(\mathbf{B}_0(\mathcal{T}))$ is residually large. On the other hand, if \mathcal{T} does not halt, then it turns out that the bad configuration never occurs; since $\text{HSP}(\mathbf{B}_0(\mathcal{T}))$ has no SIs with abelian monolith, it is residually small (see the next-to-last paragraph of Section 1.4). This answers Problem 3.1 negatively.

By combining the features of this last construction with those of $\mathbf{A}(\mathcal{T})$, McKenzie proved:

THEOREM 3.8 (McKenzie [12]) *There is an effective procedure which associates, to each Turing machine \mathcal{T} having two designated halting states s_1 and s_2 , a finite algebra $\mathbf{B}(\mathcal{T})$ in a finite language, so that:*

1. *If \mathcal{T} halts in state s_1 , then there is a finite bound to the sizes of the SIs in $\text{HSP}(\mathbf{B}(\mathcal{T}))$.*
2. *If \mathcal{T} halts in state s_2 , then $\text{HSP}(\mathbf{B}(\mathcal{T}))$ is residually large.*

Hence if finite algebras in finite languages are coded by positive integers in some effective way, then the set of codes of algebras \mathbf{A} for which there is a finite bound to the sizes of the SIs in $\text{HSP}(\mathbf{A})$, and the set of codes of algebras \mathbf{A} for which $\text{HSP}(\mathbf{A})$ is residually large, are recursively inseparable.

References

1. K. Baker, G. McNulty and H. Werner, *Shift-automorphism methods for inherently nonfinitely based varieties of algebras*, Czechoslovak Math. J. **39** (1989), 53–69.
2. S. Burris and H. Werner, *Sheaf constructions and their elementary properties*, Trans. Amer. Math. Soc. **248** (1979), 269–309.
3. R. Freese and R. McKenzie, *Commutator Theory for Congruence Modular Varieties*, London Mathematical Society Lecture Note Series, 125, Cambridge University Press, Cambridge–New York, 1987.
4. D. Hobby, *Finding type sets is NP-hard*. Internat. J. Algebra Comput. **1** (1991), 437–444.
5. D. Hobby and R. McKenzie, *The Structure of Finite Algebras*, Contemporary Mathematics, 76, American Mathematical Society, Providence, RI, 1988.
6. K. Kearnes, E. Kiss and M. Valeriote, *Minimal sets and varieties*, Trans. Amer. Math. Soc., to appear.
7. K. Kearnes, E. Kiss and M. Valeriote, *A geometric consequence of residual smallness*, manuscript, 1996.
8. R. McKenzie, *The residual bounds of finite algebras*, Internat. J. Algebra Comput. **6** (1996), 1–28.
9. R. McKenzie, *The residual bound of a finite algebra is not computable*, Internat. J. Algebra Comput. **6** (1996), 29–48.
10. R. McKenzie, *Tarski's finite basis problem is undecidable*, Internat. J. Algebra Comput. **6** (1996), 49–104.
11. R. McKenzie, *The type-set of a variety is not computable*, manuscript, 1995.
12. R. McKenzie, *Recursive inseparability for residual bounds of finite algebras*, manuscript, 1995.
13. R. McKenzie, *Residual smallness relativized to congruence types*, manuscript, 1996.
14. G. McNulty, *Residual finiteness and finite equational bases: undecidable properties of finite algebras*, manuscript, 1996.
15. Á. Szendrei, *Maximal non-affine reducts of simple affine algebras*, Algebra Universalis **34** (1995), 144–174.
16. Á. Szendrei, *Strongly abelian minimal varieties*, Acta Sci. Math. (Szeged) **59** (1994), 25–42.
17. R. Willard, *Tarski's finite basis problem via $\mathbf{A}(T)$* , Trans. Amer. Math. Soc., to appear.
18. R. Willard, *Determining whether $\text{HSP}(\mathbf{A})$ has a model companion is undecidable*, manuscript, 1995.