[1] [2] [3]

A property of the solvable radical in finitely decidable varieties

Paweł Idziak Matthew Valeriote

April, 2001

Abstract

It is shown that in a finitely decidable equational class, the solvable radical of any finite subdirectly irreducible member is comparable to all congruences of the irreducible if the type of the monolith is **2**. In the type **1** case we establish that the centralizer of the monolith is strongly solvable.

An equationally defined class of algebras $\mathcal{V}$ is said to be *finitely decidable* if the first order theory of the class of finite members of $\mathcal{V}$ is recursive (or decidable). An advance in the study of finitely generated finitely decidable equational classes was obtained by the first author and can be found in [4]. In that paper a list of conditions is produced which is shown to be both necessary and sufficient for a finitely generated congruence modular equational class to be finitely decidable. One of the conditions in the list is:

> The centralizer of the monolith of any finite subdirectly irreducible algebra in the equational class is comparable to every congruence of the algebra. (†)

In this paper we establish the necessity of this condition under the assumption of finite decidability in a congruence modular setting. Note that if $\mathcal{V}$ is a

[*] 2000 *Mathematical Subject Classification*, Primary 03B25; Secondary 08B99.

[†] *Keywords:* decidability, variety, universal algebra

[‡] The first author was supported by a research grant from KBN of Poland and the second author was supported by a research grant from the NSERC of Canada

congruence modular equational class then the only types (in the sense of tame congruence theory) which can appear in the finite algebras in $\mathcal{V}$ are **2**, **3** and **4**.

If $\mathbf{A}$ is a finite irreducible algebra whose monolith μ has type **3**, **4**, or **5** then the centralizer of μ is 0_A and so the condition (†) automatically holds. Thus, the only interesting cases are when the type of $\langle 0_A, \mu\rangle$ is **1** or **2**. We suspect, but have no proof, that (†) holds even when the type of the monolith is **1**. In this paper we offer a proof of the type **2** case. We also show that an important feature of the type **2** case holds in the type **1** case as well.

In [5] it is shown that if the monolith of a finite irreducible algebra is of type **2** and the algebra generates an equational class which is not hereditarily undecidable then the centralizer of the monolith is equal to the solvable radical of the algebra. Note that the solvable radical of a finite algebra is the largest solvable congruence of the algebra. We establish that in the type **1** case that the centralizer of the monolith is a (strongly) solvable congruence.

For the basic facts of general algebraic structures which we assume in this paper, please consult [2]. For detailed information on tame congruence theory and on decidability, the books [3, 1, 7] are recommended.

We would like to list some terminology and notation which we use throughout this paper and which may not be familiar to the reader. If $\mathbf{D}$ is a subalgebra of $\mathbf{A}^X$ (for some X) which contains all of the constant elements $\hat{a}$, for $a \in A$, then we call $\mathbf{D}$ a **diagonal subalgebra of** $\mathbf{A}^X$ ($\hat{a}$ is the element of A^X which takes on the value a at all coordinates $x \in X$). If $p(\bar{x})$ is a polynomial operation of the algebra $\mathbf{A}$, then the operation on D which acts coordinatewise like the operation p is a polynomial operation of $\mathbf{D}$. When the context is clear, we will also denote this operation by $p(\bar{x})$. If $\mathbf{D}$ is a diagonal subalgebra of $\mathbf{A}^X$ and U is a subset of A then $D(U)$ will denote the set $D \cap U^X$.

The transfer principles are tame congruence theoretic conditions on a finite algebra which have proven to be quite useful in the study of decidability.

Definition 1 *Let* $\mathbf{A}$ *be a finite algebra and let* $\mathbf{i}$, $\mathbf{j}$ *be two distinct integers between 1 and 5. We say that* $\mathbf{A}$ *satisfies the* $(\mathbf{i}, \mathbf{j})$ *transfer principle if whenever* α, β *and* γ *are congruences of* $\mathbf{A}$ *with* $\alpha \prec \beta \prec \gamma$ *and* $\operatorname{typ}(\alpha, \beta) = \mathbf{i}$ *and* $\operatorname{typ}(\beta, \gamma) = \mathbf{j}$*, then there is some congruence* δ *lying below* γ *and covering* α *with* $\operatorname{typ}(\alpha, \delta) = \mathbf{j}$.

The question of which transfer principles must hold in a finitely decidable equational class is greatly simplified by the fact that in such a class, types

4 and **5** cannot occur (see [3]). There are examples of finite algebras which generate finitely decidable equational classes and for which the $(\mathbf{1},\mathbf{3})$ and $(\mathbf{2},\mathbf{3})$ transfer principles fail. All other relevant transfer principles must hold in a finite algebra which generates an equational class which is finitely decidable.

THEOREM 2 ([9, 8]) *Let* $\mathbf{B}$ *be a finite algebra with* $\mathsf{V}_{\text{fin}}(\mathbf{B})$ *not hereditarily undecidable. Then the minimal sets of* $\mathbf{B}$ *of type* $\mathbf{2}$ *and* $\mathbf{3}$ *have empty tails, and the* $(\mathbf{1},\mathbf{2})$, $(\mathbf{2},\mathbf{1})$, $(\mathbf{3},\mathbf{1})$ *and* $(\mathbf{3},\mathbf{2})$ *transfer principles hold in* $\mathbf{B}$.

THEOREM 3 *Let* $\mathbf{A}$ *be a finite irreducible algebra with monolith* μ *of type* $\mathbf{2}$. *If* $\mathsf{SP}_{\text{fin}}(\mathbf{A})$ *is not hereditarily undecidable then the centralizer of* μ *is comparable to all congruences of* $\mathbf{A}$.

PROOF. As noted earlier, since $\mathbf{A}$ lies in a finitely decidable equational class then the only types which can appear as labels in Con $\mathbf{A}$ are **1**, **2**, and **3**. If the centralizer of μ fails to be comparable to all congruences of $\mathbf{A}$, then by the result of Jeong mentioned earlier, we know that the solvable radical of $\mathbf{A}$ has this same defect.

It follows that there is some prime quotient $\langle\alpha,\beta\rangle$ of $\mathbf{A}$ of type **3** with α solvable and with β incomparable to the solvable radical of $\mathbf{A}$. Choose such a prime quotient with α as small as possible in Con $\mathbf{A}$. Since α is solvable and β isn't comparable with the solvable radical then there is some solvable cover γ of α. Since the $(\mathbf{2},\mathbf{1})$ transfer principle holds in $\mathbf{A}$ and the monolith of $\mathbf{A}$ is of type **2** then $\operatorname{typ}(\alpha,\gamma) = 2$.

Let $B = \{0,1\}$ be an $\langle\alpha,\beta\rangle$-minimal set, U an $\langle\alpha,\gamma\rangle$-minimal set and V a $\langle 0,\mu\rangle$-minimal set. According to Lemma 4.30 from [3], it is not possible that U or V contain any type **3** minimal set. In fact neither of these sets can properly contain the range of a nonconstant idempotent polynomial, so, in particular, $\beta|_U \subseteq \alpha$. Of course, it is possible that the $\langle\alpha,\beta\rangle$ and the $\langle 0,\mu\rangle$-minimal sets coincide, and in that case we choose U and V to be equal.

Since μ is the monolith of $\mathbf{A}$, then for any pair $\langle c,d\rangle \in \mu|_V$ and for any distinct elements a and b from A, there is a polynomial p with $p(a) = c$ and $p(b) = d$. We are using the fact that $\mathbf{A}|_V$ is a Malcev algebra, which follows because the tail of V is empty. For a similar reason, $\mathbf{A}|_U$ is also Malcev. Also, the congruence generated by $\langle 0,1\rangle$ is equal to β, due to the minimality of the type **3** prime quotient $\langle\alpha,\beta\rangle$. From this it follows that for any two α-related elements, a and b, from either U or V, there is a unary polynomial p with $p(0) = a$ and $p(1) = b$.

Under the assumption that the theorem is false, we will be able to semantically embed the class of finite graphs into $\mathsf{SP}_{\text{fin}}(\mathbf{A})$. Fix a pair of elements $(a, b) \in \gamma|_U \setminus \alpha$ and let (c, d) be a pair of elements from $\mu|_V \setminus 0_A$. Let $p(x)$ be some unary polynomial of $\mathbf{A}$ with range contained in V and such that $p(a) = c$ and $p(b) = d$.

Let $\mathbf{G} = \langle G, E\rangle$ be a finite graph and let $X = G \cup E \cup \{\infty\}$. Here, E consists of a set of 2-element subsets of G. We may assume that this union is a disjoint one. Let $\mathbf{D}$ be the diagonal subalgebra of $\mathbf{A}^X$ generated by the sets $\{0, 1\}^X$ and $\{f_v : v \in G\}$, where for $v \in G$, f_v is the function from X to $\{a, b\}$ defined by:

$$f_v(x) = \begin{cases} b & \text{if } x = v \\ b & \text{if } v \in x \in E \\ a & \text{otherwise} \end{cases}.$$

Since there is a polynomial of $\mathbf{A}$ which maps 0 to c and 1 to d, and since $\{0, 1\}^X \subseteq D$, then $\{c, d\}^X \subseteq D$ too and this polynomial can be used to define, in a first order way, a boolean algebra on $\mathbf{D}(\{c, d\})$.

Even though not all of the generators of $\mathbf{D}$ are constant modulo γ, it follows that all of the elements in $\mathbf{D}(U)$ have this property.

Claim 3.1 *Let $f \in \mathbf{D}(U)$. Then f is constant modulo γ.*

Since $f \in \mathbf{D}(U)$, then there is some polynomial $t(\bar{x}, \bar{y})$ of $\mathbf{A}$ with range contained in U, some $\{0, 1\}$-valued functions b_i and some $v_j \in G$, such that

$$f = t(f_{v_1}, \dots, f_{v_n}, b_1, \dots, b_m).$$

(We are applying the polynomial t of $\mathbf{A}$ componentwise in the above display. This operation is a polynomial of $\mathbf{D}$ since $\mathbf{D}$ is a diagonal subalgebra of $\mathbf{A}$. We will continue this practice throughout the proof.) Since $\beta|_U \subseteq \alpha$, then componentwise f is α-related to $t(f_{v_1}, \dots, f_{v_n}, \hat{0}, \dots, \hat{0})$, an element of $\mathbf{D}(U)$ which is γ-constant. Since $\alpha \subseteq \gamma$ then f is also γ-constant.

We now set out to show that we can define, in a first order way, the elements of $\mathbf{D}(U)$ which are two-valued, modulo μ. Once this has been accomplished, it will be a fairly straightforward exercise to specify the semantic embedding.

Claim 3.2 *Let S be a subset of U or V that is contained in some α-class. Then the set $\mathbf{D}(S)$ is definable by some first order formula.*

Let $S = \{s_0, s_1, \ldots, s_k\}$ and let $d(x, y, z)$ be a Malcev polynomial for U or V, depending on whether S is a subset of U or V. Let $x + y$ be the polynomial $d(x, s_0, y)$. Then $f \in \mathbf{D}(S)$ if and only if there are some unary polynomials of $\mathbf{A}$, g_1, ..., g_k and some elements b_1, ..., b_k from $\mathbf{D}(\{0, 1\})$ such that

- $g_i(0) = s_0$ and $g_i(1) = s_i$, for all $i \leq k$;
- $b_i \wedge b_j = \hat{0}$ for all $i < j \leq k$ ($\wedge$ is the meet operation of the boolean algebra on $\mathbf{D}(\{0, 1\})$); and
- $f = g_1(b_1) + g_2(b_2) + \cdots + g_k(b_k)$ (associating to the left).

We leave the detailed verification of this to the reader. Since $\mathbf{A}$ has only a finite number of unary polynomials and $\mathbf{D}(\{0, 1\})$ is definable as the range of a certain unary polynomial of $\mathbf{A}$ then the above condition is clearly first order definable.

An immediate consequence of the above claim is that the α-constant elements in $\mathbf{D}(U)$ or $\mathbf{D}(V)$ are definable by first order formulas $\mathbf{CON}^U_\alpha(x)$ and $\mathbf{CON}^V_\alpha(x)$ since both $\mathbf{D}(U)$ and $\mathbf{D}(V)$ are first order definable.

Claim 3.3 *There is a first order formula $\mathbf{TWO}(x)$ that defines a subset of the elements of $\mathbf{D}(U)$ which are 2-valued modulo μ and which contains the generators f_v for all $v \in G$.*

It is not hard to see that the elements $f = f_v$ for some $v \in G$ satisfy the following first order properties:

- $\neg\mathbf{CON}^U_\alpha(f)$ and $f \in \mathbf{D}(U)$,
- $p(f) \in \mathbf{D}(\{c, d\})$ and $p(f)$ is not constant,
- for each polynomial g of $\mathbf{A}$ with range contained in V, if $\mathbf{CON}^V_\alpha(g(f))$ then $g(f) \in \mathbf{D}(\{u, v\})$ for some $(u, v) \in \alpha|_V$,
- for each pair of polynomials $g(x)$ and $h(x)$ of $\mathbf{A}$, if $g(f)$ and $h(f)$ are $\{c, d\}$-valued and are both nonconstant, then either $g(f) = h(f)$ or $g(f) = h(f)'$, where x' is the boolean complement of the $\{c, d\}$-valued function x in the boolean algebra definable on $\{c, d\}^X$.

It is also true that if an element of $\mathbf{D}$ satisfies all of the above conditions then there are two $(\gamma \setminus \alpha)$-related elements x and y from U such that $\{x, y\} \subseteq \mathsf{range}(f) \subseteq (x/\mu) \cup (y/\mu)$. To see this, let f be an element of D which satisfies the above conditions. Since $\neg\mathbf{CON}^U_\alpha(f)$ holds then modulo μ, f takes on at least 2 values.

To reach a contradiction, suppose that the elements u, v, and w are contained in the range of f and that pairwise none of these elements are μ-related. By an earlier observation, there is a polynomial $g(x)$ of $\mathbf{A}$ such that g has range contained in V and $g(u) = c$ and $g(v) = d$. Since c and d are μ-related and u and v aren't then it follows that $g(\gamma|_U) \subseteq \alpha$. By Claim 3.1 we conclude that $g(f)$ is constant modulo α, i.e., $\mathbf{CON}^V_\alpha(g(f))$ holds. Then, $g(f)$ must be $\{c, d\}$-valued.

There are two cases to consider, and both can be handled similarly. Either $g(w) = g(v) = d$ or $g(w) = g(u) = c$. In the former case, choose some polynomial $h(x)$ of $\mathbf{A}$ with range contained in V and with $h(w) = c$ and $h(v) = d$. By applying the argument from the previous paragraph, we see that $h(f)$ is $\{c, d\}$-valued. By construction though, it turns out that $g(f)$ is not equal to either $h(f)$ or $h(f)'$, a contradiction.

Therefore the conjunction of the above properties defines the sought after formula.

An immediate consequence of the previous claim is that if μ is trivial on the set U, then the formula $\mathbf{TWO}$ defines a collection of 2-valued functions in $\mathbf{D}(U)$ which contains the generators f_v, $v \in G$. In the event that $\mu|_U \neq 0_U$, then $U = V$ (by our assumptions) and so the polynomial p collapses $\mu|_U$ into 0. So, in both cases, if $\mathbf{D} \models \mathbf{TWO}(f)$, then the functions f modulo μ and $p(f)$ have the same "shape".

Let $\mathbf{GEN}(f)$ be a first order formula which is equivalent to the following conditions:

- $\mathbf{TWO}(f)$,
- the meet of $p(f)$ and χ_G is an atom in the Boolean algebra on $\mathbf{D}(\{c, d\})$,
- the meet of $p(f)$ and χ_∞ equals $\hat{c}$ in the Boolean algebra on $\mathbf{D}(\{c, d\})$

where χ_G is the $\{c, d\}$-valued element of $\mathbf{D}$ that takes on the value d on the set G and c elsewhere and χ_∞ is c-valued except at ∞, where it takes on the value d.

Claim 3.4 $\mathbf{D} \models \mathbf{GEN}(f_v)$ *for all* $v \in G$*, and for all* $h \in D$*, if* $\mathbf{D} \models \mathbf{GEN}(h)$ *then* $p(h) = p(f_v)$ *for some* $v \in G$*.*

By construction, one part of this claim is easy to establish, and for the other, assume that $\mathbf{D} \models \mathbf{GEN}(h)$. Then there is some polynomial t of $\mathbf{A}$ with range contained in U, elements b_i from $\mathbf{D}(\{0,1\})$ and distinct $v_j \in G$ such that

$$h = t(f_{v_1}, \ldots, f_{v_n}, b_1, \ldots, b_m).$$

As in the proof of Claim 3.1 we see that h is componentwise α-related to $t'(f_{v_1}, \ldots, f_{v_n})$, where $t'(\bar{x}) = t(\bar{x}, 0, 0, \ldots, 0)$. Moreover, from Claim 3.1 we know that h is constant modulo γ. Since **TWO** holds for h then there must be two elements x and y of U which are $\gamma \setminus \alpha$-related and such that $\{x, y\} \subseteq \mathsf{range}(h) \subseteq x/\mu \cup y/\mu$. Without loss of generality we may assume that $h(\infty) = x$, and so $p(x) = c$.

Since $p(h) \wedge \chi_G$ is an atom, then there is exactly one $v \in G$ with $p(h)(v) = d$. It follows that $(h(v), x) \notin \mu$, since $p(x) = c$, and so $h(v)$ is μ-related to y. Without loss of generality, we may assume that $h(v) = y$. Using a similar argument, it can be shown that for every $w \neq v$, $h(w)$ is μ-related to x.

We now show that the vertex v must be equal to one of the vertices v_1, …, v_n that are used to produce h. If this is not the case, then evaluating h at v we find that

$$\begin{array}{rcl} y = h(v) & \alpha & t'(f_{v_1}(v), \ldots, f_{v_n}(v)) \\ & = & t'(a, a, \ldots, a) \\ & = & t'(f_{v_1}(\infty), \ldots, f_{v_n}(\infty)) \\ & \alpha & h(\infty) = x, \end{array}$$

a contradiction. By rearranging the variables of t we may assume that $v = v_1$.

We have now established the following facts:

$$y = h(v) \ \alpha \ t'(b, a, \ldots, a),$$

$$x \ \alpha \ h(v_i) \alpha t'(a, a, \ldots, a, b, a, \ldots, a),$$

for $i > 1$, and

$$x = h(\infty) \ \alpha \ t'(a, a, \ldots, a).$$

Using the fact that γ is Abelian over α, the above can be used to show that

$$t'(b, a, \ldots, a, b, a, \ldots, a) \ \alpha \ t'(b, a, \ldots, a, a, a, \ldots, a)$$

and

$$t'(a,\ldots,a,b,a,\ldots,a,b,a,\ldots,a)\ \alpha\ t'(a,\ldots,a,b,a,\ldots,a,a,a,\ldots,a).$$

To complete the proof of this claim we must show that for any edge $e \in E$, $p(h)(e) = d$ if and only if $v \in e$. Assume that $e = \{v, w\}$ belongs to E. Then

$$h(e)\alpha t'(b,a,\ldots,a,z,a,\ldots,a)\alpha t'(b,a,\ldots,a)\alpha y,$$

where z is either b or a depending on whether $w = v_i$ for some i or not. Thus, $p(h)(e) = d$. On the other hand, if the edge e does not contain v, then arguing in a similar fashion, we conclude that $h(e)\alpha x$ and so $p(h)(e) = c$.

We conclude that $p(h) = p(f_v)$ as required.

The vertices of the graph $\mathbf{G}$ can be represented by the elements of $\mathbf{D}(\{c, d\})$ which satisfy the following formula $\mathbf{VER}(f)$:

$$\exists h(\mathbf{GEN}(h) \wedge f \approx p(h))$$

and the edge relation of $\mathbf{G}$ can be recovered from $\mathbf{D}$ by the formula $\mathbf{EDGE}(f, g)$:

$$\mathbf{VER}(f) \wedge \mathbf{VER}(g) \wedge f \not\approx g \wedge [f \wedge g \neq \hat{c}].$$

Thus, up to isomorphism, we can recover the graph $\mathbf{G}$ from $\mathbf{D}$ using the formulas $\mathbf{VER}$ and $\mathbf{EDGE}$ and so $\mathsf{SP}_{\text{fin}}(\mathbf{A})$ is hereditarily undecidable. This contradicts our hypothesis, and so we conclude that the centralizer of μ must be comparable to all congruences of $\mathbf{A}$. ▮

As noted earlier, Jeong has shown that if $\mathbf{A}$ is a finite irreducible with monolith μ of type $\mathbf{2}$ then the centralizer of μ is equal to the solvable radical of $\mathbf{A}$ if the equational class generated by $\mathbf{A}$ is finitely decidable. Here we establish a weaker result in the type $\mathbf{1}$ case.

THEOREM 4 *Let* $\mathbf{A}$ *be a finite irreducible algebra with strongly abelian monolith* μ *and with* $\mathsf{V}_{\text{fin}}(\mathbf{A})$ *not hereditarily undecidable. Then the centralizer of* μ *is a strongly solvable congruence.*

This theorem will follow from a sequence of lemmas which we now present. In order to set them up, let $\mathbf{A}$ be a finite (not necessarily irreducible) algebra with congruences

$$0_A \prec \mu \subseteq \alpha \prec \beta$$

such that α is strongly solvable, $\mathrm{typ}(\alpha, \beta) = \mathbf{3}$, and $\{0, 1\}$ is an $\langle \alpha, \beta \rangle$-minimal set with $\beta = \mathrm{Cg}_{\mathbf{A}}(0, 1)$, for some elements 0 and 1 from A.

We will show that if M is any $\langle 0_A, \mu \rangle$-trace and if $\{0, 1\}^2$ centralizes M^2 over 0_A (or $C(\{0, 1\}^2, M^2; 0_A)$) then $\mathbf{A}$ generates an hereditarily undecidable equational class.

Kearnes and Kiss [6] show that besides the usual notion of centrality, there are others which play a significant role in the study of general algebra. One of them is the rectangulation relation, $R(L, R; \delta)$, and is defined for symmetric binary relations L and R and a congruence δ on an algebra $\mathbf{A}$ as follows:

> For all polynomials $t(x_1, \ldots, x_n, y_1, \ldots, y_m)$ of $\mathbf{A}$ and all $(a_i, b_i) \in L$ and $(c_j, d_j) \in R$ for $i \leq n$ and $j \leq m$, if $(t(\bar{a}, \bar{c}), t(\bar{b}, \bar{d})) \in \delta$ then $(t(\bar{a}, \bar{c}), t(\bar{a}, \bar{d})) \in \delta$.

Let T be the tolerance of $\mathbf{A}$ generated by $(0, 1)$. Our proof of Theorem 4 is divided into three pieces, with the main division being whether or not $R(T, M^2; 0_A)$ holds. Under our centrality assumption, this condition is equivalent to the following holding for all a, $b \in M$:

> For all polynomials $t(x, y)$ of $\mathbf{A}$, if $t(a, 0) = t(b, 1)$ then $t(a, 0) = t(b, 0)$.

LEMMA 5 *If $R(T, M^2; 0_A)$ holds then $T \cap \mu = 0_A$.*

Proof. If $T \cap \mu \neq 0_A$ then there is a polynomial $p(x)$ of $\mathbf{A}$ with $p(0) = a \neq b = p(1)$ and with a, $b \in M$. By modifying an argument due to Jeong ([5], lemma 9), we can show that the class of finite boolean triples can be semantically embedded into $\mathsf{V}_{\text{fin}}(\mathbf{A})$, contradicting our assumption.

Let $\mathbf{F}$ be the subalgebra of $\mathbf{A}^3$ generated by the diagonal and $\{0, 1\}^3$ and let $c_0 = (0, 0, 0)$, $c_1 = (1, 0, 0)$, $c_2 = (0, 1, 0)$ and $c_3 = (0, 0, 1)$. For $i \leq 3$, let $d_i = p(c_i)$.

Claim 5.1 *For $i = 1, 2, 3$, the set $N_i = \{c_0, c_i\}$ is a type $\mathbf{3}$ minimal set of $\mathbf{F}$.*

Since F contains all of $\{0, 1\}^3$ and the diagonal, and since $\{0, 1\}$ supports all of the boolean operations as restrictions of polynomials of $\mathbf{A}$, it follows that the induced algebra of $\mathbf{F}$ on N_i is polynomially equivalent to a boolean algebra.

Furthermore, since $\{0,1\}$ is the range of some idempotent polynomial of $\mathbf{A}$, we can easily construct an idempotent polynomial of $\mathbf{F}$ with range N_i. If we let β_i be the congruence of $\mathbf{F}$ generated by N_i and α_i some subcover of β_i then it follows that N_i is a minimal set with respect to the pair $\langle \alpha_i, \beta_i \rangle$.

Let Γ be the congruence of $\mathbf{F}$ generated by $\{d_1, d_2, d_3\}^2$.

Claim 5.2 *The Γ-class of d_0 is a singleton, and so $(d_0, d_i) \notin \Gamma$ for $i = 1, 2, 3$.*

It suffices to show that if $s(x)$ is a polynomial of $\mathbf{F}$ such that $s(d_i) = d_0$ then $s(d_j) = d_0$ for all i, j between 1 and 3. For example, suppose that $s(d_1) = d_0$ and consider $s(d_2)$. Since s is a polynomial of $\mathbf{F}$ then there is a polynomial $r(x, \bar{y})$ of $\mathbf{A}$ and elements σ_i from $\{0,1\}^3$ such that $s(x) = r(x, \bar{\sigma})$ for all $x \in F$.

From the equality $s(d_1) = d_0$ we gather that

$$r(b, \bar{\gamma}_0) = r(a, \bar{\gamma}_1) = r(a, \bar{\gamma}_2) = a,$$

where, for $i < 3$, $\bar{\gamma}_i$ is the sequence of 0's and 1's determined by the ith component of the tuple $\bar{\sigma}$.

Using the rectangularity condition, combined with the fact that $\{0,1\}$ supports a polynomial complementation operation, it follows that $r(a, \bar{\gamma}_0) = r(b, \bar{\gamma}_0) = a$. Now employing our centrality assumption, we conclude that $r(a, \bar{\gamma}_i) = r(b, \bar{\gamma}_i) = a$ for all $i < 3$. The claim follows from these equalities.

Let $\mathbf{F}' = \mathbf{F}/\Gamma$ and set $\theta_0 = \alpha^3/\Gamma$, $\theta_1 = (\beta \times \alpha \times \alpha)/\Gamma$, $\theta_2 = (\beta \times \beta \times \alpha)/\Gamma$, and $\theta_3 = (\beta \times \alpha \times \beta)/\Gamma$. By the previous claim we know that the element d_0/Γ is distinct from the element $d_1/\Gamma = d_2/\Gamma = d_3/\Gamma$.

Using $\mathbf{F}'$ and the congruences just defined, we can semantically embed the class of finite boolean triples into the class of all finite powers of $\mathbf{F}'$. The details of how to accomplish this are identical with those presented by Jeong in [5] and so will not presented here. ▮

LEMMA 6 *If $R(T, M^2; 0_A)$ fails then $\mathsf{SP}_{\mathrm{fin}}\mathsf{HS}(\mathbf{A}^2)$ is hereditarily undecidable.*

Proof. Let U be a $\langle 0_A, \mu \rangle$-minimal set which contains the trace M. Since the type of $\langle 0_A, \mu \rangle$ is $\mathbf{1}$ then the failure of $R(T, M^2; 0_A)$ can be witnessed by a binary polynomial $t(x, y)$ and elements a, $b \in M$ such that:

- $t(a,0) = t(b,1)$ and $t(a,0) \neq t(b,0)$,
- t has range contained in U,
- $t(x,0) = x$ for all $x \in U$,
- $t(x,1)|_U$ is a permutation of U which is not the identity map.

It would be nice to know that additionally, $t(a,1) = a$ and $t(b,1) \neq b$, but this may not be the case. In order to arrange this, we consider a particular quotient of a subalgebra of $\mathbf{A}^2$.

Let $\mathbf{B}$ be the diagonal subalgebra of $\mathbf{A}^2$ generated by the singleton $\{(a,b)\}$ and let δ be the congruence of $\mathbf{B}$ generated by $\{((u,u),(v,v)) : u,\, v \in M\}$. Let $\mathbf{C}$ be the quotient of $\mathbf{B}$ by δ and let c and d denote the elements $(a,a)/\delta$ and $(a,b)/\delta$ respectively. We will use 0 and 1 to denote the elements $(0,0)/\delta$ and $(1,1)/\delta$ of C respectively and will use $t(x,y)$ to denote the polynomial of $\mathbf{C}$ determined by the original t.

Let $\bar{U}$ denote $\{(u,v)/\delta : (u,v) \in U^2 \cap B\}$ and let $e(x)$ be an idempotent polynomial of $\mathbf{C}$ whose range is $\bar{U}$. The following observations follow directly from the construction of $\mathbf{C}$.

Claim 6.1

1. *The set $\{0,1\}$ is the range of an idempotent polynomial of $\mathbf{C}$ and the induced algebra on this set is polynomially equivalent to a boolean algebra.*
2. *$(u,v) \in U^2 \cap B$ if and only if $u = p(a)$ and $v = p(b)$ for some polynomial p of $\mathbf{A}$ with range contained in U.*
3. *For (u,v), $(x,y) \in U^2 \cap B$, $((u,v),(x,y)) \in \delta$ if and only if $(u,v) = (x,y)$ or $u = v\mu x = y$.*
4. *$t(x,0) = x$ for all $x \in \bar{U}$, $t(c,1) = c$ and $t(d,1) \neq d$.*
5. *$C(\{0,1\}^2, \{c,d\}^2; 0|_{\bar{U}})$ holds, i.e., if $s(x,\bar{y})$ is a polynomial of $\mathbf{C}$ whose range is contained in $\bar{U}$ and $\bar{u}$ and $\bar{v}$ are $\{c,d\}$-sequences then $s(0,\bar{u}) = s(0,\bar{v})$ if and only if $s(1,\bar{u}) = s(1,\bar{v})$.*
6. *If $s(\bar{x})$ is a polynomial of $\mathbf{C}$ whose range is contained in $\bar{U}$ then $s|_{\{c,d\}}$ depends on at most 1 variable. If this restriction is essentially unary, then it is a permutation of $\bar{U}$.*

We will interpret the class of finite graphs in the class $\mathsf{SP}_{\text{fin}}(\mathbf{C})$. Let $\mathbf{G} = \langle V, E\rangle$ be a finite graph and set $X = V \times 2$. For $v \in V$, let $f_v \in C^X$ be defined by:

$$f_v((w,i)) = \begin{cases} 1 & \text{if } v = w \\ 0 & \text{if } v \neq w \end{cases}$$

and for $e \in E$ let $f_e \in C^X$ be defined by:

$$f_e((w,i)) = \begin{cases} d & \text{if } w \in e \text{ and } i = 1 \\ c & \text{otherwise} \end{cases}$$

Let $\mathbf{D}$ be the diagonal subalgebra of $\mathbf{C}^X$ generated by the f_v's and the f_e's. Note that since $\{0,1\}$ supports the boolean operations then D contains all of the componentwise joins of sets of f_v's. In fact, all $\{0,1\}$-valued elements of $\mathbf{D}$ can be expressed in this way. Furthermore, the set of vertices of $\mathbf{G}$ are in bijective correspondence with the atoms of the boolean algebra of $\{0,1\}$-valued elements of D.

Claim 6.2 *Each element $f \in D(\bar{U})$ is of one of the following two disjoint sorts:*

1. *$s(f_{v_1}, \ldots, f_{v_m})$ for some polynomial s of $\mathbf{C}$ with range contained in $\bar{U}$ and some vertices $v_1, \ldots, v_m$ in V.*

2. *$s(f_e, f_{v_1}, \ldots, f_{v_m})$ for some polynomial s of $\mathbf{C}$ with range contained in $\bar{U}$ such that $s(x, 0, \ldots, 0)|_{\bar{U}}$ is a permutation, some $e \in E$ and some vertices $v_1, \ldots, v_m$ in V.*

Any element $f \in D(\bar{U})$ is of the form $s(f_{e_1}, \ldots, f_{e_n}, f_{v_1}, \ldots, f_{v_m})$ for some polynomial s of $\mathbf{C}$ with range contained in $\bar{U}$ and some edges and vertices e_i and v_j. By the previous claim we have that $s(x_1, \ldots, x_n, 0, \ldots, 0)|_{\{c,d\}}$ is either constant or is essentially unary. In the former case it follows that $s(\bar{x}, \bar{\sigma})|_{\{c,d\}}$ is constant for any sequence $\bar{\sigma}$ of 0's and 1's. So, in this case we can express f in the form $s'(f_{v_1}, \ldots, f_{v_m})$, for a suitable polynomial s' of $\mathbf{C}$. We'll say that such an element is of vertex sort.

In the latter case, suppose that $s(x_1, \ldots, x_n, 0, \ldots, 0)|_{\{c,d\}}$ depends just on its first variable. Then for any sequence $\bar{\sigma}$ of 0's and 1's the polynomial $s(x_1, \ldots, x_n, \bar{\sigma})|_{\{c,d\}}$ also depends only on the first variable. So, we can write f as $s'(f_{e_1}, f_{v_1}, \ldots, f_{v_m})$ for some suitably chosen polynomial s' with

$s'(x, 0, \ldots, 0)|_{\bar{U}}$ a permutation. Such an element will be said to be of edge sort.

To show that each element in $D(\bar{U})$ is assigned a unique sort, it suffices to find a property which differentiates the two sorts.

Let $\mathcal{P}$ denote the set of all polynomials p of $\mathbf{C}$ whose range is $\bar{U}$ and such that $p(x, 0, \ldots, 0)|_{\bar{U}}$ is a permutation of $\bar{U}$. Note that because of our centrality assumption, it follows that if $p \in \mathcal{P}$ then $p(x, \bar{\sigma})|_{\bar{U}}$ is a permutation of $\bar{U}$ for any sequence $\bar{\sigma}$ of 0's and 1's.

Note that if f can be expressed as $s'(f_{v_1}, \ldots, f_{v_m})$ then $f((w, 0)) = f((w, 1))$ for all $w \in V$, while if it can be written in the form $s'(f_e, f_{v_1}, \ldots, f_{v_m})$ with $s' \in \mathcal{P}$ then $f((w, 0)) \neq f((w, 1))$ if and only if $w \in e$. This demonstrates that the two sorts of elements in $D(\bar{U})$ provide a partition of this set into two classes. It also demonstrates that in the latter case, the edge e is uniquely determined by f.

Claim 6.3 *The set of elements of vertex sort and the set of elements of edge sort are first order definable.*

It suffices to show that the set of elements of vertex sort is definable, since the set of elements of edge sort is complementary to this set within $D(\bar{U})$. Choose finitely many polynomials s_1, s_2, ..., s_k of $\mathbf{C}$ such that each polynomial s of $\mathbf{C}$ has the same range as one of the s_i's on the set $\{0, 1\}$.

Since $\mathbf{D}$ contains a large variety of $\{0, 1\}$-valued functions then it is the case that an element f is of vertex sort if and only if

$$f \in D(\bar{U}) \text{ and } f = s_i(\bar{g}) \text{ for some } i \leq k \text{ and some } g_j \in D(\{0, 1\}).$$

Let **EDGE** be a first order formula which defines the set of elements of edge sort. Note that $\mathbf{D} \models \mathbf{EDGE}(f_e)$ for any $e \in E$. We know that each element of edge sort determines a unique edge from the graph $\mathbf{G}$, but this association may be many to one, and so in general the set of elements of edge sort is not in one to one correspondence with E. To remedy this, we next define an equivalence relation $\sim$ on the set of elements of edge sort such that each $\sim$ class contains exactly one generator f_e.

Consider the following set of permutations of $\bar{U}$:

$$\begin{aligned} N = \{\lambda \ : \ & \lambda(x) = p(x, \bar{\sigma})|_{\bar{U}} \text{ for some polynomial } p(x, \bar{y}) \text{ of } \mathbf{C} \text{ with} \\ & \text{range contained in } \bar{U} \text{ and some sequence } \bar{\sigma} \text{ of 0's and 1's} \\ & \text{with } p(x, 0, \ldots, 0) = x \text{ for all } x \in \bar{U} \ \}. \end{aligned}$$

Our centrality condition ensures that $p(x, \bar{\sigma})$ is a permutation of $\bar{U}$ if $p(x, 0, \ldots, 0)$ is. Note that this set of permutations is actually a finite subgroup of the group of symmetries of $\bar{U}$ and that, by suitably composing polynomials, we can produce a single polynomial $s(x, \bar{y})$ with range contained in $\bar{U}$, with $s(x, 0, \ldots, 0) = x$ for all $x \in \bar{U}$ and with

$$N = \{s(x, \bar{\sigma})|_{\bar{U}} : \bar{\sigma} \text{ some sequence of 0's and 1's}\}.$$

Define the relation $\sim$ on the set of elements of edge sort as follows: $f \sim g$ if and only if

> $\mathbf{EDGE}(f)$, $\mathbf{EDGE}(g)$ and there is some polynomial p of $\mathbf{C}$ with $p(\bar{U}) = \bar{U}$ and some sequence $\bar{\sigma}$ from $D(\{0,1\})$ with $f = p(s(g, \bar{\sigma}))$.

Claim 6.4 *$f \sim g$ if and only if there are polynomials t_1 and t_2 in $\mathcal{P}$, an edge $e \in E$, and vertices v_i and $w_j \in V$ with $f = t_1(f_e, f_{v_1}, \ldots, f_{v_n})$ and $g = t_2(f_e, f_{w_1}, \ldots, f_{w_m})$.*

Assume that $f \sim g$. Then there is a polynomial r of $\mathcal{P}$, an edge e of E and vertices w_j of V with $g = r(f_e, f_{w_1}, \ldots, f_{w_m})$. $f \sim g$ implies that $f = p(s(g, \bar{\sigma}))$ for suitable p and $\bar{\sigma}$. Since the $\{0,1\}$-valued functions in $\mathbf{D}$ can be expressed as boolean combinations of the f_v's then we may replace $\bar{\sigma}$ by a sequence of these elements if we first modify the polynomial s. So, we can find an element s' of $\mathcal{P}$ and some vertices v_i with $f = p(s'(g, f_{v_1}, \ldots, f_{v_k}))$ and thus

$$f = p(s'(r(f_e, f_{w_1}, \ldots, f_{w_m}), f_{v_1}, \ldots, f_{v_k})),$$

as required.

Conversely, suppose that $f = t_1(f_e, f_{v_1}, \ldots, f_{v_n})$ and $g = t_2(f_e, f_{w_1}, \ldots, f_{w_m})$. Since $t_2(x, \bar{\sigma})|_{\bar{U}}$ is a bijection for all $\{0,1\}$-sequences $\bar{\sigma}$ then there is a polynomial t' in $\mathcal{P}$ with $t'(x, \bar{\sigma})|_{\bar{U}}$ the inverse to $t_2(x, \bar{\sigma})|_{\bar{U}}$ for all $\bar{\sigma}$. Thus $f_e = t'(g, f_{w_1}, \ldots, f_{w_m})$ and hence $f = t_1(t'(g, f_{w_1}, \ldots, f_{w_m}), f_{v_1}, \ldots, f_{v_k})$.

Let $p(x) = t_1(t'(x, 0, \ldots, 0), 0, \ldots, 0)$ and let $p'(x)$ be a polynomial of $\mathbf{C}$ with $p'(p(x)) = x$ for all $x \in \bar{U}$. Then, for any sequences $\bar{\sigma}$ and $\bar{\sigma}'$ of 0's and 1's, the function $p'(t_1(t'(x, \bar{\sigma}), \bar{\sigma}'))|_{\bar{U}}$ is in N. Thus we can find some sequence $\bar{\sigma} \in D(\{0,1\})$ with $p'(t_1(t'(g, f_{w_1}, \ldots, f_{w_m}), f_{v_1}, \ldots, f_{v_k}) = s(g, \bar{\sigma})$. Finally, we have that $f = p(s(g, \bar{\sigma}))$ as required.

It easily follows from this claim that $\sim$ is an equivalence relation on the set of elements of edge sort and that each $\sim$ class contains a unique generator

f_e. Thus, the set of edges of $\mathbf{G}$ is in bijective correspondence with the set of $\sim$ classes.

To finish the proof we need only recover the edge relation amongst the vertices of $\mathbf{G}$. Recall that we have identified the vertices of $\mathbf{G}$ with the atoms in the boolean algebra $D(\{0,1\})$. Define $\mathcal{D}$ to be the set

$$\{\lambda \in \operatorname{Pol}\mathbf{C}|_{\bar{U}} \,:\, \lambda(\bar{U}) = \bar{U} \text{ and either } t(\lambda(c),1) \neq \lambda(c) \text{ or } t(\lambda(d),1) \neq \lambda(d)\}$$

and let κ be the cardinality of $\mathcal{D}$. Note that both $\mathcal{D}$ and κ are independent of the graph $\mathbf{G}$.

For $v \in V$ and f an element of $\mathbf{D}$ with $\mathbf{D} \models \mathbf{EDGE}(f)$, define $\Gamma(f, f_v)$ to be the set

$$\{\pi \in \operatorname{Pol}\mathbf{C}|_{\bar{U}} \,:\, \pi(\bar{U}) = \bar{U} \text{ and } t(\pi(f), f_v) \neq \pi(f)\}.$$

Claim 6.5 *If $f \sim g$ and $v \in V$ then $\Gamma(f, f_v)$ and $\Gamma(g, f_v)$ have the same size and no more than κ elements.*

If $f \sim g$ then $f = p(s(g,\bar{\sigma}))$ for some sequence $\bar{\sigma} \in D(\{0,1\})$ and some polynomial $p(x)$ of $\mathbf{C}$ with $p(\bar{U}) = \bar{U}$. Let $\bar{\tau}$ be the sequence of 0's and 1's of the same length as $\bar{\sigma}$ defined by: $\tau_i = \sigma_i((v,0))$. We claim that the map which sends λ in $\Gamma(f, f_v)$ to $\lambda(p(s(x,\bar{\tau}))|_{\bar{U}})$ is an injection into $\Gamma(g, f_v)$.

Since $p(s(x,\bar{\tau}))|_{\bar{U}}$ is a permutation of $\bar{U}$, then certainly our map is an injection. We need only check that its range is indeed in $\Gamma(g, f_v)$. To do this, we need to determine if

$$t(\beta(g), f_v) \neq \beta(g),$$

where $\beta = \lambda(p(s(x,\bar{\tau}))|_{\bar{U}})$. Since $t(x,0) = x$ for all $x \in \bar{U}$ and $t(\lambda(f), f_v) \neq \lambda(f)$, then $t(\lambda(f), f_v)((v,i)) \neq \lambda(f)((v,i))$ for some $i = 0$ or 1. But then

$$\begin{aligned}
t(\beta(g), f_v)((v,i)) &= t(\beta(g((v,i))), 1) \\
&= t(\lambda(p(s(g((v,i)),\bar{\tau}))), 1) \\
&= t(\lambda(p(s(g,\bar{\sigma}))), f_v)((v,i)) \\
&= t(\lambda(f), f_v)((v,i)) \\
&\neq \lambda(f)((v,i)) \\
&= \beta(g)((v,i)).
\end{aligned}$$

Thus our map is an injection from $\Gamma(f, f_v)$ into $\Gamma(g, f_v)$ and so, by symmetry, these two sets have the same size.

As there is a unique $e \in E$ with $f \sim f_e$ then to finish the proof of this claim it will suffice to show that $\Gamma(f_e, f_v) \subseteq \mathcal{D}$. This follows from the fact that f_e is a $\{c, d\}$-valued function.

Claim 6.6 *For $w \in V$ and $e \in E$, the set $\Gamma(f_e, f_w)$ has size κ if and only if $w \in e$.*

Let $e = \{u, v\}$ and assume that $w = u$. We will show that $\mathcal{D} \subseteq \Gamma(f_e, f_w)$ in this case. If $\lambda \in \mathcal{D}$ then $t(\lambda(c), 1) \neq \lambda(c)$ or $t(\lambda(d), 1) \neq \lambda(d)$. Since $\{f_e((w, 0)), f_e((w, 1))\} = \{c, d\}$ then $t(\lambda(f_e), f_w)$ and $\lambda(f_e)$ differ at either $(w, 0)$ or $(w, 1)$, demonstrating that $\lambda \in \Gamma(f_e, f_w)$.

Conversely, suppose that $w \notin e$. We need only find some element of $\mathcal{D}$ which is not in $\Gamma(f_e, f_w)$. Since $t(c, 0) = t(c, 1) = c$ and $t(x, 0) = x$ for all $x \in \bar{U}$ then it is not hard to see that $t(f_e, f_w) = f_e$, demonstrating that the identity map is not a member of $\Gamma(f_e, f_w)$. As the identity map on $\bar{U}$ is in $\mathcal{D}$ then we have shown that $\Gamma(f_e, f_w)$ has fewer than κ elements.

To finish the proof, we need to find a first order formula which describes the edge relation on $\mathbf{G}$. Let $\mathbf{E}(x, y)$ be any first order formula which expresses that

- x and y are distinct atoms in the boolean algebra $D(\{0, 1\})$, and
- there exists some h with $\mathbf{EDGE}(h)$ and with $\Gamma(h, x)$ and $\Gamma(h, y)$ both having κ elements.

Then for v, $w \in V$, $\{v, w\} \in E$ if and only if $\mathbf{E}(f_v, f_w)$ holds in $\mathbf{D}$. ▮

One final semantic embedding is needed to complete our proof. We state the following lemma in rather general terms since it will have applications beyond the present situation.

LEMMA 7 *Let $\mathbf{B}$ be a finite algebra which contains a minimal set $\{0, 1\}$ with respect to some type $\mathbf{3}$ prime quotient. Suppose that U is a minimal set with respect to a type $\mathbf{1}$ prime quotient $0_B \prec \nu$ and that there is some polynomial $p(x)$ of $\mathbf{B}$ with range contained in U and with $\{p(0), p(1)\}$ intersecting, but not contained in some $\langle 0_B, \nu\rangle$-trace. $\mathsf{V}_{fin}(\mathbf{B})$ is hereditarily undecidable if either one of the following conditions holds:*

1. *The set $\{p(0), p(1)\}$ is polynomially isomorphic to $\{0, 1\}$.*

2. *There is no polynomial q of* $\mathbf{B}$ *with* $(q(0), q(1)) \in \nu \setminus 0_B$ *and for every polynomial h of* $\mathbf{B}$ *with range contained in U if $h(0) \neq h(1)$ then $\{h(0), h(1)\}$ can be mapped onto a 2 element set contained in a proper subset of U which is the range of some idempotent polynomial of* $\mathbf{B}$.

Proof.

If case 1 holds then we may assume that 0 and 1 belong to U and that p is an idempotent map with range U. In either case, let V be some proper subset of U which is the range of some idempotent polynomial e with $q(x)$ some polynomial with range V and which separates $p(0)$ and $p(1)$. Let $a = p(0)$ and $b = p(1)$ and suppose that a belongs to the $\langle 0_A, \nu\rangle$-trace N in U. Choose some other element a' from N.

Let $\mathbf{G} = \langle V, E\rangle$ be a finite graph and let ∞_1 and ∞_2 be two points not in V. Let $X = V \cup \{\infty_1, \infty_2\}$ and for $e \in E$, let f_e be the function from X to $\{a, a', b\}$ defined by

$$f_e(x) = \begin{cases} b & \text{if } x \in e \\ a' & \text{if } x = \infty_2 \\ a & \text{otherwise} \end{cases} .$$

For $v \in V$, let f_v be the $\{0,1\}$-valued function in B^X defined by

$$f_v(x) = \begin{cases} 1 & \text{if } x = v \\ 0 & \text{otherwise} \end{cases} .$$

Let $\mathbf{D}$ be the diagonal subalgebra of $\mathbf{A}^X$ generated by the set of f_e's and f_v's.

As in the proof of Claim 6.2 of Lemma 6 it is the case that every element f of $D(U)$ falls into one of two classes: either it can be expressed, for some $e \in E$ and $v_i \in V$, as

- $t(f_{v_1}, \ldots, f_{v_k})$ for some polynomial t with range contained in U, or
- $t(f_e, f_{v_1}, \ldots, f_{v_k})$ for some polynomial t with range contained in U and with $t(x, 0, \ldots, 0)|_U$ a permutation.

To see why this is so in the present circumstances, let's consider an element $f \in D(U)$. We can write f as $t(f_{e_1}, \ldots, f_{e_m}, f_{v_1}, \ldots, f_{v_k})$ for some polynomial t with range contained in U and for some generators f_{e_i} and f_{v_j}. Now, either $t(x_1, \ldots, x_m, 0, \ldots, 0)|_{\{a,a'\}}$ is constant or essentially unary since ν is strongly abelian. In the former case, it follows that $f = t(p_{e_1}, \ldots, p_{e_m}, f_{v_1}, \ldots, f_{v_k})$ where, for $i \leq m$, p_{e_i} is equal to f_{e_i} at all coordinates except ∞_2, where it takes on the value a. This is because at ∞_2, the generators f_{v_j} all take on the value 0. The elements p_{e_i} are not generators of $\mathbf{D}$, but they are members of this algebra, since they can be obtained by applying the polynomial $p(x)$ to a join of an appropriate pair of $\{0, 1\}$-valued generators. The end result of this is that we can express the element f as a polynomial of $\mathbf{B}$ applied to a number of generators of the form f_v.

The remaining case in this analysis can be handled in a similar manner. Let us call an element permutational if it falls into the second class.

It is not difficult to see that the permutational elements can be characterized as those elements f of $D(U)$ for which $f(\infty_1) \neq f(\infty_2)$. Using an argument similar to the one employed in the proof of Claim 6.3 of Lemma 6 it can be shown that the set of permutational elements can be defined via a first order formula.

We would like to associate a unique element of E to each permutational element but will instead only achieve this for a particular definable collection of permutational elements which resemble the f_e's with respect to the action of unary polynomials of $\mathbf{B}$. Let us define the unary relation $\mathbf{EDGE}(f)$ by:

- f is permutational,
- $q(f)$ is nonconstant, and
- there are distinct vertices v and w so that for all unary polynomials h of $\mathbf{B}$ with range properly contained in U if $h(f)$ is not constant then $h(f) = h(p(f_v \vee f_w))$ (where $\vee$ is a polynomial which acts as the boolean join operation on $\{0, 1\}$).

This relation is first order definable since the f_v's coincide with the atoms in the boolean algebra $D(\{0, 1\})$ which take on the value 0 at ∞_1 and ∞_2.

Claim 7.1 *For f a permutational element, if $\mathbf{D} \models \mathbf{EDGE}(f)$ then $q(f) = q(p(f_v \vee f_w))$ for some unique v, $w \in V$ with $\{v, w\} \in E$. For any $e \in E$, $\mathbf{D} \models \mathbf{EDGE}(f_e)$.*

By design, if $e \in E$ then $\mathbf{D} \models \mathbf{EDGE}(f_e)$. On the other hand, suppose that f is permutational and satisfies $\mathbf{EDGE}$. Let $t(x, \bar{y})$ be some polynomial of $\mathbf{B}$ with range contained in U and with $t(x, 0, \ldots, 0)|_U$ a permutation and let $e \in E$ and $\bar{v} \in V$ with $f = t(f_e, f_{v_1}, \ldots, f_{v_k})$. Since **EDGE** holds for f then there are v, $w \in V$ which witness this. We will show that $e = \{v, w\}$.

Suppose not, say $u \in e \setminus \{v, w\}$. Let $c = f(\infty_1)$, $c' = f(\infty_2)$ and $d = f(u)$. Since f is permutational, then $c = t(a, 0, \ldots, 0) \neq t(a', 0, \ldots, 0) = c'$ and by suitably rearranging the variables of t we may assume that $d = t(b, 0, \ldots, 0, 1, \ldots, 1)$. In case 1 (where $0 = a$ and $1 = b$) it follows that $\{c, d\}$ is polynomially isomorphic to $\{0, 1\}$ and so there is a polynomial h of $\mathbf{B}$ with range equal to $\{0, 1\}$ and with $h(c) = 0$ and $h(d) = 1$. Thus $h(f)$ is nonconstant and so $h(f) = h(p(f_v \vee f_w))$. But

$$h(f)(\infty_1) = h(c) = 0 \neq 1 = h(d) = h(f)(u)$$

and $f_v \vee f_w(\infty_1) = f_v \vee f_w(u)$ leads to a contradiction.

In case 2, the fact that $c = t(a, 0, \ldots, 0)$ and $d = t(b, 0, \ldots, 0, 1 \ldots, 1)$ along with the fact that p maps 0 to a and 1 to b leads to a polynomial h with range contained in U and with $h(0) = c$ and $h(1) = d$. By assumption $\{c, d\}$ can be mapped onto a two element subset of U via some polynomial $r(x)$ with range properly contained in U. Then since **EDGE** holds for f it follows that $r(f) = r(p(f_v \vee f_w))$. As in the previous case, this leads to a contradiction, since $r(f)$ takes on different values at ∞_1 and u while $r(p(f_v \vee f_w))$ doesn't.

We are now in a position to finish the proof. As noted earlier, the elements of the graph can be identified with the atoms of the boolean algebra $D(\{0, 1\})$ which take on the value 0 at ∞_1 and ∞_2. From the previous claim, two vertices v and w will be edge related if and only if there is some element f of D for which **EDGE** holds and such that $q(f) = q(p(f_v \vee f_w))$. ▮

The following lemma will provide a reduction to our earlier results under certain circumstances.

LEMMA 8 *Let* $\mathbf{B}$ *be a finite algebra and let* $\mu \prec \nu$ *and* $\gamma \prec \delta$ *be a pair of prime quotients in the congruence lattice of* $\mathbf{B}$ *with* $\operatorname{typ}(\mu, \nu) = \operatorname{typ}(\gamma, \delta) = \mathbf{1}$. *If* U *is a minimal set with respect to both* (μ, ν) *and* (γ, δ) *and* R *is any binary relation on* B *then* $C(R, \nu|_U; \mu)$ *iff* $C(R, \delta|_U; \gamma)$.

Proof. Assume that $C(R, \nu|_U; \mu)$ holds and let $t(x, y_1, \ldots, y_k)$ be a polynomial of $\mathbf{B}$ and $\bar{\tau}$ and $\bar{\sigma}$ are sequences from U with $(\tau_i, \sigma_i) \in \delta$ for $i \leq k$. Suppose that $(0, 1) \in R$ and that $(t(0, \bar{\tau}), t(0, \bar{\sigma})) \notin \gamma$ but $(t(1, \bar{\tau}), t(1, \bar{\sigma})) \in \gamma$. We may assume that t has range contained in U.

Since $\langle \gamma, \delta \rangle$ is of type $\mathbf{1}$ then $t(0, \bar{y})$ depends, modulo γ on at exactly 1 variable when restricted to the product of the $\delta|_U$-classes which contain the τ_i's. Suppose that this polynomial depends on y_1. Then $(\tau_1, \sigma_1) \notin \gamma$ and the map $t(0, y_1, \tau_2, \ldots, \tau_k)|_U$ is a permutation of U since it does not collapse $\delta|_U$ into γ. Thus $t(0, y_1, \tau_2 \ldots, \tau_k)$ does not collapse $\nu|_U$ into μ and by $C(R, \nu|_U; \mu)$ we conclude that $t(1, y_1, \tau_2, \ldots, \tau_k)$ has the same property. This implies that $t(1, y_1, \tau_2, \ldots, \tau_k)$ is a permutation of U and so $t(1, \bar{\tau})$ and $t(1, \bar{\sigma})$ lie in different γ-classes since τ_1 and σ_1 do. This contradicts $(t(1, \bar{\tau}), t(1, \bar{\sigma})) \in \gamma$ and so we are done. ∎

Finally, we may present the proof of Theorem 4.

Proof. By virtue of Theorem 2 we may assume that the $(\mathbf{1}, \mathbf{2})$ transfer principle holds and that all type $\mathbf{3}$ minimal sets have exactly 2 elements. It follows that all solvable congruences of $\mathbf{A}$ are actually strongly solvable. Suppose that the centralizer of μ is not strongly solvable and let M be a $\langle 0_A, \mu \rangle$-trace contained in a $\langle 0_A, \mu \rangle$-minimal set U. Choose β minimal with $\alpha \prec \beta$ a type $\mathbf{3}$ pair of congruences for some α with $C(\beta, M^2; 0_A)$. Let $\{0, 1\}$ be an $\langle \alpha, \beta \rangle$-minimal set and let T be the tolerance of $\mathbf{A}$ generated by $(0, 1)$. By the minimality of β, it follows that $\mathrm{Cg}_{\mathbf{A}}(0, 1) = \beta$, and that α is strongly solvable. By choice, $C(\{0, 1\}^2, M^2; 0_A)$ holds. From Lemmas 5 and 6 we may assume that $R(T, M^2; 0_A)$ holds and that there is no polynomial $p(x)$ with $(p(0), p(1)) \in \mu \setminus 0$ (this is equivalent to $T \cap \mu = 0_A$).

Fix some element a in M. Since the congruence μ of $\mathbf{A}$ is contained in the congruence generated by $\{0, 1\}$ then there must be a polynomial p of $\mathbf{A}$ whose range is contained in U and with $p(0) = a \neq p(1)$. Since $(p(0), p(1)) \notin \mu$ then $\{p(0), p(1)\}$ is not contained in any $\langle 0_A, \mu \rangle$-trace of U.

We will show that condition 2 of Lemma 7 holds in order to finish our proof. Suppose that h is a polynomial of $\mathbf{A}$ with range contained in U and with $h(0) \neq h(1)$. Further, suppose that $\{h(0), h(1)\}$ cannot be mapped onto a 2 element subset of any proper subset of U which is the range of an idempotent polynomial of $\mathbf{A}$.

Let δ be the congruence generated by $h(0)$ and $h(1)$ and let γ be some subcover of δ. Note that $\delta \neq \mu$ and so $\gamma \neq 0_A$. Also, note that $\delta \subseteq \alpha$ or else $\{h(0), h(1)\}$ would be an $\langle \alpha, \beta \rangle$-minimal set, contrary to our assumptions on $\{h(0), h(1)\}$. Thus δ is a strongly solvable congruence. Since $\delta|_U \not\subseteq \gamma|_U$ then it follows that U contains some $\langle \gamma, \delta \rangle$-minimal set V. By our assumption on h, we see that V must be equal to U and so by Lemma 8 it follows that $C(\{0, 1\}^2, \delta|_U; \gamma)$ holds.

By considering the quotient $\mathbf{A}/\gamma$ we see that we are now in a position to apply either Lemma 5 or 6 to show that $\mathbf{A}$ generates an equational class which is not finitely decidable. So, condition 2 of Lemma 7 holds and we conclude that $\mathsf{V}_{fin}(\mathbf{A})$ is hereditarily undecidable. ▮

References

[1] S. Burris and R. McKenzie. *Decidability and Boolean Representations*, volume 246 of *Memoirs of the American Mathematical Society.* American Mathematical Society, 1981.

[2] S. Burris and H.P. Sankappanavar. *A Course in Universal Algebra.* Springer-Verlag, 1981.

[3] D. Hobby and R. McKenzie. *The Structure of Finite Algebras*, volume 76 of *Contemporary Mathematics.* American Mathematical Society, 1988.

[4] P. Idziak. A characterization of finitely decidable congruence modular varieties. *Transactions of the American Mathematical Society*, 349:903–934, 1997.

[5] J. Jeong. Type 2 subdirectly irreducible algebras in finitely decidable varieties. *Journal of Algebra*, 174:772–793, 1995.

[6] K. Kearnes and E. Kiss. Finite algebras of finite complexity. *Discrete Math.*, 207:89–135, 1999.

[7] R. McKenzie and M. Valeriote. *The Structure of Locally Finite Decidable Varieties*, volume 79 of *Progress in Mathematics.* Birkhäuser Boston, 1989.

[8] M. Valeriote. On solvable congruences in finitely decidable varieties. *Mathematical Logic Quarterly*, 40:398–414, 1994.

[9] M. Valeriote and R. Willard. Some properties of finitely decidable varieties. *The International Journal of Algebra and Computation*, 2:89–101, 1992.

Computer Science Department, Jagiellonian University, Kraków, Poland
E-mail address: idziak@ii.uj.edu.pl

Department of Mathematics and Statistics, McMaster University, Hamilton, Ontario, Canada
E-mail address: valeriot@mcmaster.ca