JOURNAL OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 00, Number 0, Pages 000–000
S 0894-0347(XX)0000-0

THE STRUCTURE OF LOCALLY FINITE VARIETIES WITH POLYNOMIALLY MANY MODELS

PAWEŁ IDZIAK, RALPH MCKENZIE, AND MATTHEW VALERIOTE

1. Introduction

In this paper, *variety* means a class of similar algebras—i.e., models of one first-order language without relation symbols—which is defined by the satisfaction of some fixed set of equations. A variety is locally finite if all of its finitely generated members are finite. Following J. Berman and P. Idziak [2], the *G-spectrum*, or *generative complexity*, of a locally finite variety $\mathcal{C}$, is the function $G_{\mathcal{C}}$ defined on positive integers so that $G_{\mathcal{C}}(k)$ is the number of non-isomorphic (at most) k-generated members of $\mathcal{C}$.

The G-spectrum of $\mathcal{C}$ is a non-decreasing function from and to positive integers. The interest in this function as an invariant of a locally finite variety is tied to the fact, exhaustively demonstrated in J. Berman and P. Idziak [2], that the rate of growth of $G_{\mathcal{V}}$ is closely related to numerous structural and algebraic properties of the members of $\mathcal{V}$. Among other results, [2] contains a characterization of the finitely generated varieties $\mathcal{V}$ which omit type **1** and possess a G-spectrum $G_{\mathcal{V}}(k)$ bounded by a singly exponential function $2^{p(k)}$ for some polynomial $p(k)$.

In this paper, we characterize the locally finite varieties which possess a G-spectrum bounded by a polynomial function. The literature contains two other papers dealing with these varieties. M. Bilski [4], characterizes the finitely generated varieties of semigroups with polynomially bounded G-spectrum. P. Idziak and R. McKenzie [6] prove that if a locally finite variety $\mathcal{V}$ omits type **1** then $G_{\mathcal{V}}(k) \leq k^C$ for some $C > 0$ and for all integers $k > 1$ iff $\mathcal{V}$ is polynomially equivalent to the variety of all unitary left $\mathbf{R}$-modules for some finite ring $\mathbf{R}$ of finite representation type.

This paper is a continuation of P. Idziak, R. McKenzie [6]. Here we extend the result to arbitrary locally finite varieties; and we prove that such a variety has polynomially bounded G-spectrum if and only if it decomposes into a varietal product $\mathcal{A} \otimes \mathcal{S}_1 \otimes \cdots \otimes \mathcal{S}_r$ where $\mathcal{A}$ is polynomially equivalent to the variety of unitary left $\mathbf{R}$-modules over a finite ring $\mathbf{R}$ of finite representation type, and for $1 \leq i \leq r$, $\mathcal{S}_i$ is equivalent to a matrix power of the variety of H_i-sets with some constants, where H_i is a finite group.

The arguments in this paper show that if a locally finite variety $\mathcal{V}$ fails to decompose as $\mathcal{V} = \mathcal{A} \otimes \mathcal{S}$ with $\mathcal{A}$ affine and $\mathcal{S}$ strongly Abelian, then $G_{\mathcal{V}}(k) \geq 2^{k^C}$, for some positive C and for all $k > 1$. We do not know if this statement remains true when 2^{k^C} is replaced by $2^{C\sqrt{k}}$. Our arguments also demonstrate that if $\mathcal{S}$ is

2000 *Mathematics Subject Classification.* Primary 08A05; Secondary 03C45.

strongly Abelian and locally finite and fails to decompose into a finite product of varieties equivalent to varieties of H-sets with constants, for finite groups H, then $G_{\mathcal{S}} \geq 2^{C\sqrt{k}}$ for some positive C and all $k > 1$.

We do not know if there exists a locally finite variety $\mathcal{D}$ such that $G_{\mathcal{D}}$ grows faster than k^C and slower than 2^{k^C} for all positive constants C. Our arguments imply that such a variety exists if and only if for some finite ring $\mathbf{R}$ with unit, the variety of unitary left $\mathbf{R}$-modules has this property.

By combining the results of [2] and [6] and specializing them to groups and rings, we get the following:

- every finitely generated variety of groups has at most doubly exponential G-spectrum,
- a finitely generated variety of groups has singly exponentially bounded G-spectrum if and only if it is nilpotent,
- a locally finite variety of groups has polynomially bounded G-spectrum if and only if it is Abelian,
- every finitely generated variety of rings has at most doubly exponential G-spectrum,
- a finitely generated variety of commutative rings with unit has singly exponentially bounded G-spectrum iff the Jacobson radical in the generating ring squares to 0,
- no non-trivial variety of rings with unit has polynomially bounded G-spectrum.

The chief result of this paper solves Problems 1, 4, 5 and 6, and part of Problem 11 in J. Berman, P. Idziak [2].

2. Basic concepts and pre-requisites

The concepts and results of tame congruence theory underlie nearly all of our work in this paper. The reader will need to be well-acquainted with this theory. We will make frequent reference to D. Hobby, R. McKenzie [5], which is the basic source for this theory and, as well, contains a brief introduction to the basic concepts and terminology of universal algebra that we employ. The following remarks are intended merely to give the reader who is unfamiliar with these subjects a clearer idea of what this paper accomplishes.

Among other things, tame congruence theory provides a classification of the local behavior of finite algebras, relativized to congruence classes, into one of five possible types: (**1**) Unary, (**2**) Vector Space, (**3**) Boolean, (**4**) Lattice, and (**5**) Semilattice. More precisely, if β is a congruence of a finite algebra $\mathbf{A}$ (i.e., an equivalence relation over the universe of $\mathbf{A}$ which is compatible with the operations of $\mathbf{A}$) then modulo any congruence α of $\mathbf{A}$ that β covers in the lattice of congruences of $\mathbf{A}$, the local structure that $\mathbf{A}$ induces on each non-trivial β class is equivalent to one of the five listed types. This allows one to label the congruence lattice of a finite algebra using the type labels **1** through **5**, and to speak of a finite algebra, or class of algebras omitting or admitting certain local types. As Hobby and McKenzie demonstrate, the labelled congruence lattice of a finite algebra determines very deep aspects of the structure of that algebra.

A *variety* is a class of similar algebras—i.e., models of one first-order language without relation symbols—which is identical to the class of all models of this language which satisfy some fixed but arbitrary set of equations. By G. Birkhoff's HSP-theorem, a variety is the same thing as a non-void class of similar algebras closed under the formation of direct products, subalgebras, and homomorphic images. An algebra is *locally finite* if all of its finitely generated subalgebras are finite; and a variety is locally finite if all of its finitely generated members are finite. A variety is non-trivial if it has an algebra of more than one element. The *typeset* of a variety is the set of all tame congruence theoretic types that are admitted by some finite algebra in the variety.

A variety $\mathcal{V}$ is the varietal product of its subvarieties $\mathcal{V}_0$ and $\mathcal{V}_1$, written $\mathcal{V} = \mathcal{V}_0 \otimes \mathcal{V}_1$, if and only if $\mathcal{V} = HSP(\mathcal{V}_0 \cup \mathcal{V}_1)$ and there is a binary term $t(x, y)$ in the language of $\mathcal{V}$ such that $\mathcal{V}_i$ is the class of models of the equation $t(x_0, x_1) = x_i$ in $\mathcal{V}$, for $i \in \{0, 1\}$. If $\mathcal{V} = \mathcal{V}_0 \otimes \mathcal{V}_1$, then every algebra in $\mathcal{V}$ is canonically a direct product, $\mathbf{A} \cong \mathbf{A}_0 \times \mathbf{A}_1$, of algebras $\mathbf{A}_i \in \mathcal{V}_i$. In particular, the free algebra $\mathbf{F}_{\mathcal{V}}(2)$ is isomorphic to $\mathbf{F}_{\mathcal{V}_0}(2) \times \mathbf{F}_{\mathcal{V}_1}(2)$. This has the consequence that if $\mathcal{V}$ is any non-trivial locally finite variety, then there is a finite sequence of non-trivial varieties $\mathcal{V}_0, \ldots, \mathcal{V}_{n-1}$, each indecomposable under the varietal product, such that $\mathcal{V} = \mathcal{V}_0 \otimes \mathcal{V}_1 \otimes \cdots \otimes \mathcal{V}_{n-1}$. The collection $\{\mathcal{V}_0, \ldots, \mathcal{V}_{n-1}\}$ of indecomposable (non-trivial) subvarieties of which $\mathcal{V}$ is the product, is unique.

To characterize the locally finite varieties with polynomially many models (i.e., with polynomially bounded G-spectrum) amounts to characterizing the indecomposable locally finite varieties with polynomially many models, since if $\mathcal{V} = \mathcal{V}_0 \otimes \mathcal{V}_1 \otimes \cdots \otimes \mathcal{V}_{n-1}$ then for all k, $G_{\mathcal{V}}(k) = G_{\mathcal{V}_0}(k) G_{\mathcal{V}_1}(k) \cdots G_{\mathcal{V}_{n-1}}(k)$. Our chief result amounts to the assertion that the only indecomposable locally finite varieties with polynomially many models are the varieties of G-sets over finite groups, varieties of modules over finite rings of finite representation type, and the varieties that can be obtained from these two types by inessential modifications of their unary functions and by forming matrix powers.

Our result implies that each locally finite variety with polynomially many models consists of *Abelian* algebras. A variety of H-sets consists of *strongly Abelian* algebras. The major part of this paper is taken up by a very long proof that every locally finite variety with polynomially many models is Abelian. These are technical but very natural concepts for general algebras, which we will now explain.

Two polynomial functions f_0, f_1 of an algebra $\mathbf{A}$ are called *twins* if, for some m, there is a term $t(x, y_0, \ldots, y_{m-1})$ of the language of $\mathbf{A}$ and m-tuples $\bar{a}_0$, $\bar{a}_1$ of members of $\mathbf{A}$ such that $f_i(x) = t(x, \bar{a}_i)$ $(i \in \{0, 1\})$ holds for all x in $\mathbf{A}$. An algebra $\mathbf{A}$ is said to be *Abelian* iff every pair of twin polynomial functions of $\mathbf{A}$ which agree at one point in $\mathbf{A}$ agree everywhere. An algebra $\mathbf{A}$ is said to be *strongly Abelian* (or *combinatorial*) iff every pair of twin polynomial functions of $\mathbf{A}$ are either equal, or have disjoint ranges.

One further concept we feel compelled to introduce here is that of a *locally solvable* algebra. Let θ be a congruence of an algebra $\mathbf{A}$. Polynomial functions f_0, f_1 of $\mathbf{A}$ are said to be θ-*twins* iff there is a term $t(x, \bar{y})$ and tuples $\bar{a}_i$ such that $\bar{a}_{0j} \equiv \bar{a}_{1j} \pmod{\theta}$ for all j and $f_i(x) = t(x, \bar{a}_i)$. The congruence θ is said to be Abelian iff for every block B of θ and for every pair of θ-twin polynomial functions f, g, if $f(x) = g(x)$ for one $x \in B$ then $f(x) = g(x)$ for all $x \in B$.

Finally, an algebra $\mathbf{A}$ is said to be *locally solvable* iff for every congruence θ of $\mathbf{A}$, every minimal (non-identity) congruence of the quotient algebra $\mathbf{A}/\theta$ is Abelian. It is proved in D. Hobby, R. McKenzie [5] (Chapter 7) that a locally finite algebra $\mathbf{A}$ is locally solvable iff it does not have a binary polynomial operation $x \wedge y$ and two distinct elements a, b such that $a \wedge a = a \wedge b = b \wedge a = a$ and $b \wedge b = b$.

3. Preview

Throughout this manuscript, we assume that $\mathcal{V}$ is a locally finite variety and C is a positive integer such that for all $n \geq 2$, we have $G_{\mathcal{V}}(n) \leq n^C$. Our aim is to prove that $\mathcal{V}$ has a decomposition as claimed in the abstract.

First, it will be shown that the algebras in $\mathcal{V}$ are locally solvable. In tame congruence theoretic terms, this is equivalent to showing that the typeset of $\mathcal{V}$ is contained in $\{\mathbf{1}, \mathbf{2}\}$. Next, we shall show that $\mathcal{V}$ is Abelian. This fact is non-trivial, and our proof of it occupies many pages; the next five sections of this manuscript contain our proof that all algebras in $\mathcal{V}$ are Abelian. Then, we prove in Section 8 that $\mathcal{V}$ has the $(\mathbf{1}, \mathbf{2})$- and the $(\mathbf{2}, \mathbf{1})$-transfer principles. With these results in hand, we can apply a result of K. Kearnes to conclude that $\mathcal{V}$ decomposes as the varietal product of a strongly Abelian and an affine variety.

Finally, we show in Section 9 that the conditions stated in the abstract are the necessary and sufficient conditions on a locally finite affine variety $\mathcal{A}$ and a locally finite strongly Abelian variety $\mathcal{S}$ in order that $G_{\mathcal{A}\otimes\mathcal{S}}$ be bounded by a polynomial function. The result for affine varieties is borrowed from P. Idziak, R. McKenzie [6]. The result for strongly Abelian varieties is obtained by making minor modifications to some of the arguments appearing in R. McKenzie, M. Valeriote [15].

Notation: The following concepts and notation will be used throughout this paper. For any sets $B \subseteq X$, and elements a, b in an algebra $\mathbf{A}$, we define a member of $\mathbf{A}^X$: $[a, b]_B$ denotes the function $f \in A^X$ such that $f(x) = b$ for $x \in B$ and $f(x) = a$ for $x \in X \setminus B$. Then for $x \in X$, we use $[a, b]_x$ to denote $[a, b]_B$ with $B = \{x\}$. For any set $C \subseteq A$ and algebra $\mathbf{D} \subseteq \mathbf{A}^X$, we write $D(C)$ for the set $D \cap C^X$. If $\emptyset \neq C \subseteq A$ and $\mathbf{A}$ is locally finite, we define $\Pi_{\mathbf{A}}(C)$ to be the group of all permutations σ of C such that for some polynomial $p(x)$ of $\mathbf{A}$, $p|_C = \sigma$. We use $\mathrm{Tw}_{\mathbf{A}}(C)$ to denote the group of all $\sigma \in \Pi_{\mathbf{A}}(C)$ such that for some polynomial $p(x, \bar{y})$ of $\mathbf{A}$, there are $\bar{c}$, $\bar{d}$ such that for all $x \in C$, $p(x, \bar{c}) = \sigma(x)$ and $p(x, \bar{d}) = x$ (the group of "twins of the identity" on C).

4. $\mathcal{V}$ is quasi-Hamiltonian

A locally finite variety is called *quasi-Hamiltonian* by K. Kearnes [10] iff every maximal subuniverse of a finite algebra $\mathbf{A}$ in the variety is a congruence block of $\mathbf{A}$. In [10], it is shown that this property is equivalent to several others, among them the property that if e_1 and e_2 are twin idempotent unary polynomials of an algebra $\mathbf{A}$, then $e_1 e_2 e_1(A) = e_1(A)$. Using the arguments of [10], it is easy to show that this is equivalent to: for every term $t(x, \bar{y})$, the implication

$$\{t(x_1, \bar{y}_1) = t(x_1, \bar{y}_2) = t(x_2, \bar{y}_1) = x_1 \text{ and } t(x_2, \bar{y}_2) = x_2\} \Rightarrow x_1 = x_2$$

is valid in the variety.

Theorem 4.1. *$\mathcal{V}$ is quasi-Hamiltonian.*

Proof. Assuming that this fails, we have a finite algebra $\mathbf{A} \in \mathcal{V}$ and a term and elements for which

$$t(a, \bar{c}) = t(a, \bar{d}) = t(b, \bar{c}) = a \neq b = t(b, \bar{d})\,.$$

For $n > 0$, let X be a set of cardinality 2^n and let $\{X_{i,j} : 0 \leq i < n, 0 \leq j \leq 1\}$ be a system of $2n$ subsets of X so that for all $x \in X$ there is a function $p : \{0, 1, \ldots, n-1\} \to \{0, 1\}$ such that

$$\{x\} = \bigcap_{i<n} X_{i,p(i)}\,.$$

For example, we can take $X_{i,0}$ and $X_{i,1}$ to be B_i and its complement, where $B_0, \ldots, B_{n-1}$ is a set of generators of the Boolean algebra of all subsets of X.

Now where $\bar{c} = \langle c_0, \ldots, c_{k-1}\rangle$ and $\bar{d} = \langle d_0, \ldots, d_{k-1}\rangle$, for

$$(i, j) \in \{0, \ldots, n-1\} \times \{0, 1\} \quad \text{and} \quad 0 \leq \ell < k\,,$$

take $g^\ell_{i,j} = [c_\ell, d_\ell]_{X_{i,j}}$. Let $\mathbf{K}$ be the subalgebra of $\mathbf{A}^X$ generated by the set of all such functions $g^\ell_{i,j}$ and the constant function $\langle b\rangle$. Thus $\mathbf{K}$ is a $2kn+1$-generated algebra in $\mathcal{V}$. We claim that $\mathbf{K}$ has at least $2^n + 1$ non-isomorphic homomorphic images, all of which, of course, are $2kn+1$-generated algebras in $\mathcal{V}$. This will contradict our assumption that $G_\mathcal{V}(2kn+1) \leq (2kn+1)^C$, and so prove the theorem.

The first step toward proving the claim is to observe that for all $x \in X$, the function $[a, b]_x$ belongs to $\mathbf{K}$. Indeed, suppose that

$$\{x\} = \bigcap_{i<n} X_{i,p(i)}\,.$$

Let $\bar{g}_{i,j} = \langle g^0_{i,j}, \ldots, g^{k-1}_{i,j}\rangle$. Then note that

$$[a, b]_x = t(t(\cdots t(\langle b\rangle, \bar{g}_{0,p(0)}), \bar{g}_{1,p(1)}), \ldots \bar{g}_{n-1,p(n-1)})\,.$$

This proof shows that also $\langle a\rangle \in K$.

Now enumerate X as $x_0, \ldots, x_{m-1}$, $m = 2^n$. Then for $0 \leq u \leq 2^n$, let $X_u = \{x_0, \ldots, x_{u-1}\}$ and let $\mathbf{K}_u$ be the projection of $\mathbf{K}$ into the algebra $\mathbf{A}^{X_u}$. Now for $u < 2^n$, the projection onto $\mathbf{K}_u$ maps $\langle a\rangle$ and $[a, b]_{x_u}$ to the same element, whereas the projection onto $\mathbf{K}_{u+1}$ does not. Hence we have

$$|\mathbf{K}_0| < |\mathbf{K}_1| < |\mathbf{K}_2| < \cdots < |\mathbf{K}_m|\,,$$

proving the claim. □

Corollary 4.2. *$\mathcal{V}$ is locally solvable.*

Proof. Suppose not. Then $\mathcal{V}$ has a finite algebra $\mathbf{A}$ with elements a and b and a polynomial $x \wedge y$ such that

$$a \wedge a = a \wedge b = b \wedge a = a \neq b = b \wedge b\,.$$

This contradicts Theorem 4.1. □

5. $\mathcal{V}$ is Abelian: outline of the proof

Should $\mathcal{V}$ possess a non-Abelian algebra, it would have a finite such algebra of minimum cardinality. Assume that $\mathbf{S}$ is such an algebra. Then, as is easy to see, $\mathbf{S}$ is subdirectly irreducible and for every congruence $\theta > 0_S$ of $\mathbf{S}$, the quotient algebra $\mathbf{S}/\theta$ is Abelian.

Let μ denote the monolith of $\mathbf{S}$ (i.e., the smallest nonzero congruence of $\mathbf{S}$). Then μ is Abelian (a consequence of Corollary 4.2), $\mathbf{S}/\mu$ is Abelian, and $\mathbf{S}$ is not Abelian. We must somehow use our assumption that $G_{\mathcal{V}}$ is polynomially bounded to show that no algebra with these properties can belong to $\mathcal{V}$. The Abelian congruence μ would be either of type **1** or type **2** (see D. Hobby, R. McKenzie [5]). Our arguments to rule out each of the two cases will be quite different. They are given in the next three sections. The type **1** case proves to be much the more difficult. For the type **2** case, we are able to employ a modification of the argument we used in P. Idziak, R. McKenzie [6].

In both cases, we will be employing various constructions that convert equivalence relations to algebras in such a fashion that the equivalence relation can be recovered from the resulting algebra considered abstractly. More precisely, we will have, for every structure (X, E) consisting of an equivalence relation E over a finite set X, a corresponding algebra $\mathbf{R}(X, E) \in \mathcal{V}$. It is desired that for any two of these structures (X, E), (X', E'), it is the case that $\mathbf{R}(X, E) \cong \mathbf{R}(X', E')$ iff $(X, E) \cong (X', E')$. We also require that $\mathbf{R}(X, E)$ be generated by $p(|X|)$ many elements where $p(x)$ is a polynomial determined independently of X.

The utility of this lies in the fact that the number of non-isomorphic equivalence relation structures on an n-element universe X is the same as the number of partitions of n, i.e., $\pi(n)$, and it is known (see G. E. Andrews [1], p. 70) that $\pi(n)$ is asymptotic to

$$\frac{1}{4n\sqrt{3}} e^{\left(\pi\sqrt{\frac{2n}{3}}\right)};$$

hence $\pi(n)$ is not bounded by any polynomial function.

Let X be finite and E be an equivalence relation over X. Let $B_1, \ldots, B_k$ be the distinct blocks of E. Then the sequence $(|B_1|, \ldots, |B_k|)$ is a full invariant of the structure (X, E). That is, if (X, E) and (Y, F) are finite equivalence relation structures, and if $(b_1, \ldots, b_k)$ and $(c_1, \ldots, c_\ell)$ are their corresponding lists of block sizes, then $(X, E) \cong (Y, F)$ iff $(b_1, \ldots, b_k) \sim (c_1, \ldots, c_\ell)$, i.e., iff $k = \ell$ and there is a permutation σ of $\{1, 2, \ldots, k\}$ so that for all $1 \leq i \leq k$, $b_i = c_{\sigma(i)}$. The sequence $(b_1, \ldots, b_k)$ of block sizes of E on X, or rather the $\sim$-equivalence class of this sequence, is the partition of $n = |X|$ correlated with (X, E). For our needs, it will be convenient to extend the relation $\sim$ to the domain of finite "multi-sets", by which we mean a function with finite domain and taking only positive integers as values. If m_1 and m_2 are two multi-sets with domains D_1 and D_2, respectively, then by $m_1 \sim m_2$, we mean to assert the existence of a bijection π from D_1 onto D_2 so that for all $x \in D_1$, $m_2(\pi(x)) = m_1(x)$.

Our goal, under several different sets of hypotheses, will be to construct the algebras $\mathbf{R}(X, E)$ in such a way that there is a uniform procedure that recovers from $\mathbf{R}(X, E)$ a multi-set which is $\sim$-equivalent to the sequence of block sizes of E on X. Several times, we will also use these observations: Let $(X, E) = (Y, F) \times (Z, G)$, the direct product of equivalence relation structures. Let $\bar{a}$, $\bar{b}$, $\bar{c}$ be multi-sets $\sim$-equivalent to the sequences of block sizes of (X, E), (Y, F), (Z, G) respectively.

Then $\bar{a} \sim \bar{b} \cdot \bar{c}$ where

$$\bar{b} \cdot \bar{c} = \left(\bar{b}(x) \cdot \bar{c}(y) : (x, y) \in \mathrm{dom}(\bar{b}) \times \mathrm{dom}(\bar{c})\right) .$$

Suppose that $\bar{c}'$ is another multi-set and suppose that $\bar{b} \cdot \bar{c} \sim \bar{b} \cdot \bar{c}'$. Our second observation is that under this assumption, it follows that $\bar{c} \sim \bar{c}'$. One way to see this is to use a result contained in L. Lovasz [14]. There is an equivalence relation structure (Z', G') whose partition of $|Z'|$ is represented by $\bar{c}'$. Now $(Y, F) \times (Z, G)$ and $(Y, F) \times (Z', G')$ have the same invariants modulo $\sim$, hence $(Y, F) \times (Z', G) \cong (Y, F) \times (Z', G')$. Now Lovasz' result is that this forces $(Z, G) \cong (Z', G')$. Consequently, we have that $\bar{c} \sim \bar{c}'$.

6. Type **2** monolith

We remark that Corollary 4.2 implies that the minimal sets for any type **2** congruence quotient in $\mathcal{V}$ are without tails. (See D. Hobby, R. McKenzie [5], Lemma 4.27 (4)(ii); also see K. Kearnes and E. Kiss, [11].)

Beginning with the next lemma, we employ the centralizer notation for congruences, $C(\alpha, \beta; \gamma)$, explained in D. Hobby, R. McKenzie [5], (Chp. 3). The lemma is a corollary to Lemma 3.2 in K. Kearnes [8].

Lemma 6.1. *Let* $\mathbf{A}$ *be a finite subdirectly irreducible algebra in* $\mathcal{V}$ *with monolith* μ *of type* **2**. *Then* $C(1, \mu; 0)$ *and* $C(\mu, 1; 0)$.

Proof. It is not hard to show that the failure of either of these conclusions leads to a failure of the quasi-Hamiltonian property. □

Given an algebra $\mathbf{A}$ and set X, we define $\mathbf{Q}_X(\mathbf{A})$ to be the subalgebra of $\mathbf{A}^X$ generated by the set of all functions $[a, b]_x$ with $x \in X$ and $a, b \in A$.

Lemma 6.2. *For* $n \geq 1$, *let* $f_{\mathbf{A}}(n) = |\mathbf{Q}_X(\mathbf{A})|$ *where* $|X| = n$. *Then if* $\mathbf{A}$ *is finite and* $|\mathbf{A}| > 1$, *the function* $f_{\mathbf{A}}$ *is strictly increasing.*

Proof. Straightforward, and left to the reader. □

Here is the principal result of this section. Our proof is, in essence, the proof of Theorem 4 in P. Idziak, R. McKenzie [6]; but since we have to manage without the modular commutator, the argument is more difficult in its details.

Theorem 6.3. *Let* $\mathbf{A}$ *be a finite subdirectly algebra in* $\mathcal{V}$ *with monolith* μ *of type* **2** *and assume that* $\mathbf{A}/\mu$ *is Abelian. Then* $\mathbf{A}$ *is Abelian.*

Proof. Let U be a $(0_A, \mu)$-minimal set, and let $e(x)$ be an idempotent polynomial of $\mathbf{A}$ with $e(A) = U$. Let N be a $(0_A, \mu)$-trace in U and choose an element $0 \in N$.

Let λ be the center (central congruence) of $\mathbf{A}$, so that $\lambda \geq \mu$ by Lemma 6.1. We shall argue by contradiction to establish this theorem. So we now assume that $\mathbf{A}$ is not Abelian, which in this context, is equivalent to: $\lambda < 1_A$.

Let E be any equivalence relation on a finite set X. Let $\mathbf{D} = \mathbf{Q}_X(\mathbf{A})$, as defined above. We use the notation $D(N) = D \cap N^X$, $D(U) = D \cap U^X$. Since $\mathbf{A}|_N$ is polynomially equivalent to a vector space $\mathbf{V}$ with zero element 0, and since D includes all the elements $[0, u]_x$ ($x \in X$ and $u \in N$), then $D(N) = N^X$ and $\mathbf{D}|_{D(N)}$

includes among its polynomial operations the polynomial operations of the vector space $\mathbf{V}^X$. We now put

$$M_E = \{f \in N^X : \textstyle\sum_{x\in B} f(x) = 0 \text{ for all blocks } B \text{ of } E\},$$

where these sums are computed in the vector space $\mathbf{V}$. Notice that M_E is a subspace of $\mathbf{V}^X$. We define Θ to be the congruence of $\mathbf{D}$ generated by all pairs $(\langle 0\rangle, f)$ where $f \in M_E$ (and $\langle 0\rangle$ denotes the constant function of value 0). We define α_E to be the set of all pairs $(f, g) \in D^2$ such that for all polynomials p of $\mathbf{D}$, $(ep(f), ep(g)) \in \Theta$. This is the same as the largest congruence χ of $\mathbf{D}$ such that $\chi|_{D(U)} \leq \Theta$. Finally, we put $\mathbf{R} = \mathbf{D}/\alpha_E$.

We are going to prove that from $\mathbf{R}$ we can recover the structure (X, E) up to isomorphism.

Claim 0: $\alpha_E|_{D(N)} = \Theta|_{D(N)}$; and this relation is precisely the set of all pairs $(f, g) \in N^X \times N^X$ such that $f - g \in M_E$.

It is clear that $\alpha_E|_{D(U)} = \Theta|_{D(U)}$, and consequently, $\alpha_E|_{D(N)} = \Theta|_{D(N)}$. Now if $\{f, g\} \subseteq N^X$ and $f-g \in M_E$, then by definition of Θ, we have that $(\langle 0\rangle, f-g) \in \Theta$, implying that $(f, g) \in \Theta$ (or $g = g + \langle 0\rangle \equiv g + (f - g) \pmod{\Theta}$). To show that conversely, $(f, g) \in \Theta|_{D(N)}$ implies $f - g \in M_E$, it suffices to prove that $\langle 0\rangle/\Theta|_{D(N)} = M_E$; and to do this, it suffices to prove that if $t(u, \bar{w})$ is a term (in the first order language of $\mathbf{A}$), if $\{f, g\} \subseteq M_E$ and $\bar{h} \in D^n$, then $et(f, \bar{h}) \in M_E$ iff $et(g, \bar{h}) \in M_E$. Here we use the fact that μ is contained in the center of $\mathbf{A}$.

So assume that $\{f, g, et(f, \bar{h})\} \subseteq M_E$. To see that $et(g, \bar{h}) \in M_E$, let B be any block of E. We have that $et(f(x), \bar{h}(x)) \in N$ for all $x \in X$, and consequently $et(u, \bar{h}(x)) \in N$ for all $u \in N$ and $x \in X$, since $N = 0/\mu|_U$. We also have that $\sum_{x\in B} et(f(x), \bar{h}(x)) = 0$. Choose any $x_0 \in B$. Since $\mathbf{A}|_N$ is polynomially equivalent to $\mathbf{V}$, then there is a scalar λ and some $c \in N$ so that

$$et(u, \bar{h}(x_0)) = \lambda u + c \text{ for all } u \in N,$$

calculated in $\mathbf{V}$. Moreover, for any $x \in B$, in the true equation

$$et(0, \bar{h}(x)) - et(0, \bar{h}(x)) = et(0, \bar{h}(x_0)) - et(0, \bar{h}(x_0))$$

we can replace the first 0 on both sides of the equality by any $u \in N$ (using that $C(\mu, 1_A; 0)$) to obtain

$$et(u, \bar{h}(x)) - et(0, \bar{h}(x)) = et(u, \bar{h}(x_0)) - et(0, \bar{h}(x_0)).$$

This means that

$$et(u, \bar{h}(x)) = et(u, \bar{h}(x_0)) - et(0, \bar{h}(x_0)) + et(0, \bar{h}(x)) = \lambda u + et(0, \bar{h}(x)).$$

Finally, we calculate:

$$\begin{aligned}\sum_{x\in B} et(g(x),\bar{h}(x)) &= \sum_{x\in B}\{\lambda g(x) + et(0,\bar{h}(x))\}\\ &= \lambda\{\sum_{x\in B} g(x)\} + \sum_{x\in B} et(0,\bar{h}(x))\\ &= \lambda\{\sum_{x\in B} f(x)\} + \sum_{x\in B} et(0,\bar{h}(x))\\ &= \sum_{x\in B} et(f(x),\bar{h}(x))\\ &= 0\,.\end{aligned}$$

Thus $et(g,\bar{h}) \in M_E$ as claimed.

This concludes our proof of Claim 0. To continue, for any congruence ψ of $\mathbf{A}$, and $x \in X$, let ψ_x denote $\pi_x^{-1}(\psi)$ where π_x is the projection of $\mathbf{D}$ onto $\mathbf{A}$ at x. Define $\psi_X = \bigcap_{x\in X} \psi_x$.

Claim 1: We have $\alpha_E \leq \lambda_X$ and λ_X/α_E is the center of $\mathbf{R}$.

To prove this, suppose first that $(f,g) \in D^2$ is not in λ_X. We shall show that $(f,g) \notin \alpha_E$ and that f/α_E and g/α_E are not related by the center of $\mathbf{R}$. This will prove that $\alpha_E \leq \lambda_X$ and λ_X/α_E contains the center of $\mathbf{R}$.

There exists $x_0 \in X$ such that $(f(x_0), g(x_0)) \notin \lambda$. Then by definition of λ, there is a term t and elements $\bar{h}(x_0), \bar{k}(x_0)$ of $\mathbf{A}$ such that

$$t(f(x_0),\bar{h}(x_0)) = t(f(x_0),\bar{k}(x_0)) \leftrightarrow t(g(x_0),\bar{h}(x_0)) \neq t(g(x_0),\bar{k}(x_0))\,.$$

(Note that we are here using the phrase "element of $\mathbf{A}$" in a broad sense: $\bar{h}(x_0)$ is actually a k-tuple of elements of $\mathbf{A}$ for the value of k appropriate to the term $t(x,\bar{y})$.) There are elements $\bar{h},\bar{k}$ in $\mathbf{D}$ such that $\bar{h}$ at x_0 is $\bar{h}(x_0)$ and $\bar{k}$ at x_0 is $\bar{k}(x_0)$, and such that $\bar{h}(x) = \bar{k}(x)$ for all $x \neq x_0$. (This is a consequence of the fact that $\mathbf{D} = \mathbf{Q}_X(\mathbf{A})$.) Then

$$t(f,\bar{h}) = t(f,\bar{k}) \leftrightarrow t(g,\bar{h}) \neq t(g,\bar{k})\,;$$

moreover, assuming (as we may) that $t(g,\bar{h}) \neq t(g,\bar{k})$, then $[\![t(g,\bar{h}) \neq t(g,\bar{k})]\!] = \{x_0\}$. Since $\mathbf{A}/\mu$ is Abelian, it follows that $(t(g,\bar{h}), t(g,\bar{k})) \in \mu_X$. Since μ is the monolith and is of type **2**, and U has empty tail with respect to $(0_A,\mu)$ so that $\mathbf{A}|_U$ is Maltsev, then there is a polynomial $q(x)$ of $\mathbf{D}$ with range $\subseteq D(U)$ such that $q(t(g,\bar{h})) = \langle 0\rangle \neq q(t(g,\bar{k}))$. Since this pair of functions belongs to μ_X, then $q(t(g,\bar{k})) \in D(N)$. It is clear from the fact that $[\![q(t(g,\bar{h})) \neq q(t(g,\bar{k}))]\!] = \{x_0\}$, and from our characterization of $\alpha_E|_{D(N)}$, that these two functions are not α_E-related. This shows both that $(f,g) \notin \alpha_E$ and that $(f/\alpha_E, g/\alpha_E)$ is not in the center of $\mathbf{R}$.

To finish the proof of Claim 1, let $(f/\alpha_E, g/\alpha_E)$ fail to belong to the center of $\mathbf{R}$. Thus there exists a term t and elements $\bar{h},\bar{k}$ in $\mathbf{D}$ such that

$$t(f,\bar{h})\,\alpha_E\,t(f,\bar{k}) \;\text{ say, and }\; t(g,\bar{h})\,\not\alpha_E\,t(g,\bar{k})\,.$$

This means that there exists a polynomial p of $\mathbf{D}$ such that

$$ep(t(f,\bar{h}))\,\Theta\,ep(t(f,\bar{k})) \;\text{ and }\; ep(t(g,\bar{h}))\,\not\Theta\,ep(t(g,\bar{k}))\,.$$

Let $d(x,y,z)$ be a Maltsev polynomial of $\mathbf{A}|_U$ which is invertible at each of its variables (for example, the pseudo-Maltsev polynomial of D. Hobby, R. McKenzie [5], Lemma 4.20). Then form the polynomial of $\mathbf{D}$

$$F(x,\bar{y}) = d\left(ep(t(f,\bar{y})), ep(t(x,\bar{y})), ep(t(g,\bar{k}))\right) .$$

We have that $F(f,\bar{y}) = ep(t(g,\bar{k}))$ for all $\bar{y}$, in particular, $F(f,\bar{h}) = F(f,\bar{k})$. But also,

$$F(g,\bar{k}) = ep(t(f,\bar{k})) = d\left(ep(t(f,\bar{k})), ep(t(g,\bar{k})), ep(t(g,\bar{k}))\right) \quad \text{and}$$

$$F(g,\bar{h})\,\Theta\, d\left(ep(t(f,\bar{k})), ep(t(g,\bar{h})), ep(t(g,\bar{k}))\right) .$$

Since $d(x,y,z)$ is invertible at y, it follows that $F(g,\bar{h})\not\Theta F(g,\bar{k})$, and thus a fortiori, $F(g,\bar{h}) \neq F(g,\bar{k})$. This shows that $(f,g) \notin \lambda_X$, as desired.

Definition of α_B, λ_B, $\lambda_B{}'$: We choose an element $1 \in N \setminus \{0\}$. For any $B \in X/E$, we put $\alpha_B = \alpha_E \vee \mathrm{Cg}_{\mathbf{D}}(\langle 0\rangle, 1^x)$ where $x \in B$ and $1^x = [0,1]_x$. (Since $1^x\,\alpha_E\,1^y$ whenever $(x,y) \in E$, this definition does not depend upon the choice of $x \in B$.)

It is easily seen that α_B/α_E is an atom of $\mathrm{Con}\,\mathbf{R}$. Moreover $\alpha_B|_{D(N)}$ is the set of pairs $(f,g) \in D(N)^2$ such that for all blocks $B' \neq B$ of E, $\sum_{x\in B'}(f(x)-g(x)) = 0$. Thus, if B_1 and B_2 are distinct blocks of E, then $\alpha_{B_1}/\alpha_E \neq \alpha_{B_2}/\alpha_E$.

For B a block of E, let $\lambda_B{}' = \bigcap_{x\in X\setminus B}\lambda_x$ and $\lambda_B = \bigcap_{x\in B}\lambda_x$.

Definition of $\mathrm{Cat}(\psi)$: For ψ any congruence of $\mathbf{R}$, let $C(\psi)$ be the set of pairs (u,v) in $\mathbf{R}^2$ such that for some term t and pair $(x,y) \in \psi$ and elements $\bar{z}^1, \bar{z}^2 \in \mathbf{R}$, we have $t(x,\bar{z}^1) = t(x,\bar{z}^2)$ and $(u,v) = (t(y,\bar{z}^1), t(y,\bar{z}^2))$. Note that $C(\psi) \subseteq \psi$. Then let $\mathrm{Cat}(\psi)$ be the set of atoms β in $\mathrm{Con}\,\mathbf{R}$ such that $\beta \leq \mathrm{Cg}_{\mathbf{R}}C(\psi)$.

Claim 2: A congruence ψ of $\mathbf{R}$ has the property that $\mathrm{Cat}(\psi) = \{\beta\}$ for some β iff there is a block B of E such that $\psi \leq \lambda_B{}'/\alpha_E$ and $\psi \not\leq \lambda_X/\alpha_E$. In this case, $\beta = \alpha_B/\alpha_E$.

To prove the claim, let $\psi = \tau/\alpha_E$ and suppose first that $\tau \not\leq \lambda_B{}'$ for any block B. Then there are x_0, x_1 such that $\tau \not\leq \lambda_{x_i}$, $i \in \{0,1\}$ and $(x_0,x_1) \notin E$, say x_i belongs to block B_i. Our proof of Claim 1 then shows that α_{B_i}/α_E, $i \in \{0,1\}$ belong to $\mathrm{Cat}(\psi)$ and are different atoms of $\mathrm{Con}\,\mathbf{R}$.

To finish the proof of the claim, suppose now that $\alpha_E < \tau \leq \lambda_B{}'$, $\tau \not\leq \lambda_X$. Of course, we have that $\alpha_B/\alpha_E \in \mathrm{Cat}(\tau/\alpha_E)$ by the argument for Claim 1. Letting $\beta \in \mathrm{Cat}(\tau/\alpha_E)$, we have to show that $\beta = \alpha_B/\alpha_E$. We have that $\beta = \gamma/\alpha_E$, where γ is a congruence of $\mathbf{D}$ that covers α_E.

By definition of α_E, γ contains a pair $(u,v) \in D(U)^2 \setminus \Theta$. Then

$$(u/\alpha_E, v/\alpha_E) \in \mathrm{Cg}_{\mathbf{R}}(C(\tau/\alpha_E))$$

implies that (reducing to a Maltsev chain in $D(U)$, and using the fact that $\mathbf{D}|_{D(U)}$ is Maltsev) there are $u'\Theta u$, $v'\Theta v$, $u', v' \in D(U)$, such that

$$u' = ep(t_0(y_0,\bar{z}_0^1), \ldots, t_n(y_n,\bar{z}_n^1)) ,$$

$$v' = ep(t_0(y_0,\bar{z}_0^2), \ldots, t_n(y_n,\bar{z}_n^2)) ,$$

for some polynomial p of $\mathbf{D}$, terms t_i, and elements $\bar{z}_i^j$ $(j \in \{1,2\}, i \in \{0,\ldots,n\})$ such that for some $x_i\tau y_i$ $(i \in \{0,\ldots,n\})$, we have $t_i(x_i,\bar{z}_i^1)\alpha_E t_i(x_i,\bar{z}_i^2)$ $(i \in \{0,\ldots,n\})$. The pair (u',v') lies in $\gamma \setminus \Theta$.

Now we define a polynomial in the variables $s_0, \dots, s_n, \bar{r}_0, \dots, \bar{r}_n$, using the constants $\bar{x} = (x_0, \dots, x_n)$, $\bar{y} = (y_0, \dots, y_n)$, and $\bar{z}_i^j$ occurring in the formulas above. First, put $P(\bar{s}, \bar{r}_0, \dots, \bar{r}_n) = ep(t_0(s_0, \bar{r}_0), \dots, t_n(s_n, \bar{r}_n))$. Next, put

$$Q(\bar{s}, \bar{r}_0, \dots, \bar{r}_n) =$$

$$d(P(\bar{y}, \bar{r}_0, \dots, \bar{r}_n), P(\bar{s}, \bar{r}_0, \dots, \bar{r}_n), P(\bar{x}, \bar{z}_0^2, \dots, \bar{z}_n^2))\,.$$

Now notice that $Q(\bar{y}, \bar{z}_0^1, \dots, \bar{z}_n^1) = Q(\bar{y}, \bar{z}_0^2, \dots, \bar{z}_n^2)$, while

$$Q(\bar{x}, \bar{z}_0^2, \dots, \bar{z}_n^2) = v' \quad \text{and}$$

$$Q(\bar{x}, \bar{z}_0^1, \dots, \bar{z}_n^1) = u'' \alpha_E u'\,.$$

The pair (u'', v') belongs to $\gamma|_{D(U)} \setminus \Theta$. Also, since $\mathbf{A}/\mu$ is Abelian, the pair (u'', v') belongs to μ_X, and since $\tau \subseteq {\lambda_B}'$, the functions u'' and v' agree at each $x \in X \setminus B$.

Letting $w = d(u'', v', \langle 0 \rangle)$, we have that

$$(\langle 0 \rangle, w) \in \gamma \setminus \Theta$$

and $w \in N^X$ and $w = \langle 0 \rangle$ on $X \setminus B$. This gives that $\gamma \wedge \alpha_B \not\leq \alpha_E$, which forces $\gamma = \alpha_B$ since both of these congruences cover α_E. We conclude that $\beta = \alpha_B/\alpha_E$, as desired.

From Claim 2, we see that the set $\{\alpha_B/\alpha_E : B \text{ a block of } E\}$ is a definable set of congruences of $\mathbf{R}$.

Claim 3: For B a block of E, and for ψ a congruence of $\mathbf{R}$, we have $\alpha_B/\alpha_E \notin \mathrm{Cat}(\psi)$ iff $\psi \leq \lambda_B/\alpha_E$.

Our proof of Claim 1 yields that if $\psi \not\leq \lambda_B/\alpha_E$, then $\alpha_B/\alpha_E \in \mathrm{Cat}(\psi)$. For the converse, it suffices, choosing $x_0 \in B$, to assume that

$$(\langle 0 \rangle/\alpha_E, 1^{x_0}/\alpha_E) \in \mathrm{Cg}_{\mathbf{R}}(C(\lambda_B/\alpha_E))\,,$$

and show that this assumption leads to a contradiction. We follow the argument used in the proof of Claim 2. Since $\mathbf{D}|_{D(U)}$ is Maltsev, there exist $u, v \in D(U)$ such that $u\,\alpha_E\,\langle 0 \rangle$, $v\,\alpha_E\,1^{x_0}$, and we can write

$$u = ep(t_0(y_0, \bar{w}_0^1), \dots, t_n(y_n, \bar{w}_n^1))\,,$$

$$v = ep(t_0(y_0, \bar{w}_0^2), \dots, t_n(y_n, \bar{w}_n^2))\,,$$

for some polynomial p of $\mathbf{D}$, terms t_i and elements $\bar{w}_i^j$ such that for some $z_i\,\lambda_B\,y_i$ $(i \in \{0, \dots, n\})$, we have $t_i(z_i, \bar{w}_i^1)\alpha_E t_i(z_i, \bar{w}_i^2)$ $(i \in \{0, \dots, n\})$. Let us again write $P(\bar{s}, \bar{\bar{r}})$ for the polynomial $ep(t_0(s_0, \bar{r}_0), \dots, t_n(s_n, \bar{r}_n))$ where $\bar{s}, \bar{\bar{r}}$ are variables.

Now $P(\bar{z}, \bar{\bar{w}}^1)\,\alpha_E\,P(\bar{z}, \bar{\bar{w}}^2)$ and these elements belong to $D(U)$. Hence

$$d(\langle 0 \rangle, P(\bar{z}, \bar{\bar{w}}^1), P(\bar{z}, \bar{\bar{w}}^2))\,\alpha_E\,\langle 0 \rangle,$$

implying that this element belongs to $D(N)$ and we have

$$\sum_{x \in B} d\left(0, P(\bar{z}(x), \bar{\bar{w}}^1(x)), P(\bar{z}(x), \bar{\bar{w}}^2(x))\right) =$$

$$\sum_{x \in B} d\left(0, P(\bar{z}(x), \bar{\bar{w}}^1(x)), P(\bar{z}(x), \bar{\bar{w}}^1(x))\right) = 0\,.$$

Since $z_i(x)\,\lambda y_i(x)$ for all $x \in B$, it follows that

$$\sum_{x \in B} d\left(0, P(\bar{y}(x), \bar{\bar{w}}^1(x)), P(\bar{y}(x), \bar{\bar{w}}^2(x))\right) =$$

$$\sum_{x\in B} d\left(0, P(\bar{y}(x), \bar{\bar{w}}^1(x)), P(\bar{y}(x), \bar{\bar{w}}^1(x))\right) = 0\,.$$

Since $P(\bar{y}, \bar{\bar{w}}^1) = u \,\Theta\, \langle 0\rangle$ and $P(\bar{y}, \bar{\bar{w}}^2) = v \,\Theta\, 1^{x_0}$, we have

$$1^{x_0} = d(\langle 0\rangle, \langle 0\rangle, 1^{x_0})\, \alpha_E\, d(\langle 0\rangle, u, v)$$

and this element belongs to $D(N)$. Hence

$$1 = \sum_{x\in B} 1^{x_0}(x) = \sum_{x\in B} d(\langle 0\rangle, u, v)(x) = 0$$

as follows from the calculation above. This absurd conclusion finishes our proof of the claim.

Now from Claims 2 and 3, we have that the set of congruences $T = \{\lambda_B/\alpha_E : B \text{ a block of } E\}$ is definable in $\mathbf{R}$. With each $\psi \in T$, we also have the number

$$n(\psi) = |\mathbf{R}/\psi|\,,$$

and it is quite clear that if $\psi = \lambda_B/\alpha_E$ then

$$n(\psi) = |\mathbf{D}/\lambda_B| = |\mathbf{Q}_B(\mathbf{A}/\lambda)| = f_{\mathbf{C}}(|B|)\,,$$

where $\mathbf{C} = \mathbf{A}/\lambda$ and the function $f_{\mathbf{C}}$ is defined in Lemma 6.2. Since $|\mathbf{C}| > 1$, the function $f_{\mathbf{C}}$ is one-to-one, by Lemma 6.2. Now let us choose some arbitrary one-to-one enumeration of T, say $T = \{\psi_1, \ldots, \psi_k\}$. Then we have an enumeration of the blocks of E as $B_1, \ldots, B_k$ with $\psi_i = \lambda_{B_i}/\alpha_E$. Here, $|B_i| = f_{\mathbf{C}}^{-1}(|\mathbf{R}/\psi_i|)$. Thus we have recovered the partition of $|X|$ corresponding to E from the abstract algebra $\mathbf{R}$.

Let us label the algebra $\mathbf{R}$ constructed from (X, E) in this proof by $\mathbf{R}(X, E)$. Now it follows immediately from our work that for any two finite equivalence relation structures (X, E) and (Y, F) we have $\mathbf{R}(X, E) \cong \mathbf{R}(Y, F)$ iff $(X, E) \cong (Y, F)$. We can observe that our canonical generating set for the algebra $\mathbf{Q}_X(\mathbf{A})$ has cardinality bounded by $a^2 n$ ($a = |\mathbf{A}|$, $n = |X|$). (For $n \geq 3$, the generating set has exactly $a^2 n - a(n-1)$ elements.) Thus $\mathbf{R}(X, E)$ is an $a^2|X|$ generated algebra.

Since $\mathcal{V}$ has at most $a^{2C} n^C$ non-isomorphic $a^2 n$ generated algebras, while the number of non-isomorphic structures (X, E) with $|X| = n$ is equal to $\pi(n)$, we get a contradiction by taking n sufficiently large. □

7. Type **1** monolith, Part I

Before stating the result to be proved in this section and the next, we prove several lemmas. Recall that for a locally finite algebra $\mathbf{B}$ and its subset C, if $\mathbf{D} \subseteq \mathbf{B}^X$ where X is some set, then $D(C)$ denotes the set $D \cap C^X$. For non-void $C \subseteq B$, we defined at the end of Section 2 two groups of permutations on C, $\Pi_{\mathbf{B}}(C)$ and $\mathrm{Tw}_{\mathbf{B}}(C)$ (the group of "twins of the identity" on C).

The first lemma is a variation of Lemma 2.4 in K. A. Kearnes, E. Kiss [12].

Lemma 7.1. *Suppose that $\mathbf{B}$ is a locally finite algebra, X is a finite set, $C \subseteq B$, and $\mathbf{D}$ is a subalgebra of $\mathbf{B}^X$ containing all the functions $[u, v]_x$ where $\{u, v\} \subseteq B$, $x \in X$. Then the natural embedding of $Tw_{\mathbf{D}}(D(C))$ into $Tw_{\mathbf{B}}(C)^X$ is surjective.*

Proof. We know that $\mathrm{Tw}_{\mathbf{D}}(D(C))$ is a group including all the functions $f = [\mathrm{id}, \delta]_x$ ($x \in X$, $\delta \in \mathrm{Tw}_{\mathbf{B}}(C)$) with $f(z)(y) = z(y)$ for $y \neq x$ and $f(z)(x) = \delta(z(x))$. (This is because $\mathbf{D}$ includes all the functions $[u, v]_x$.) Clearly these permutations generate the group consisting of the natural actions of $\mathrm{Tw}(C)^X$ on $D(C)$. □

Statement (1) in the next lemma is due to M. Maroti. Statement (2) is a special case of Theorem 4.5 in K. Kearnes [8].

Lemma 7.2. *Suppose that δ is a minimal congruence in a finite algebra $\mathbf{F}$, β is a congruence of $\mathbf{F}$, $\delta \leq \beta$, and V is a $(0_F, \delta)$-minimal set.*

1. *Assume that δ is strongly Abelian and $C(\beta, \delta|_V; 0_F)$. Let $p(x_0, \ldots, x_{k-1})$ be a polynomial mapping of a finite product set $B = B_0 \times \cdots \times B_{k-1}$ into V where B_i are β-equivalence classes. Then there is $i_0 < k$ such that we have $p(\bar{c}) = p(\bar{d})$ whenever $\bar{c}, \bar{d} \in B$, $c_{i_0} = d_{i_0}$ and for all $j \neq i_0$, $(c_j, d_j) \in \delta$.*
2. *If $C(\delta, \beta; 0_F)$ and $C(\beta, \delta|_V; 0_F)$, then $C(\beta, \delta; 0_F)$.*

Proof. To prove (1), let $p : B \to V$ be such a polynomial mapping. Suppose that there are $i \neq j$, $i < k$, $j < k$, and $\bar{c}, \bar{d}, \bar{e}, \bar{f} \in B$ such that $c_r = d_r$ for $r \neq i$, $e_r = f_r$ for $r \neq j$, $(c_i, d_i), (e_j, f_j) \in \delta$ and $p(\bar{c}) \neq p(\bar{d})$, $p(\bar{e}) \neq p(\bar{f})$. We can assume that $\{c_i, d_i\} \subseteq M_i$, $\{e_j, f_j\} \subseteq M_j$, M_i, M_j are $(0, \delta)$-traces. Letting N be the trace in V that contains $p(\bar{c})$, there is a polynomial $f(x)$ and elements $c_i', d_i' \in N$ with $f(c_i') = c_i$, $f(d_i') = d_i$. Likewise, there is a polynomial $g(x)$ with $g(e_j') = e_j$, $g(f_j') = f_j$ for some $e_j', f_j' \in N$. Now for $x, y \in N$ put $h(x, y) = p(\bar{u}^{x,y})$ where $u_r^{x,y} = c_r$ for $r \notin \{i, j\}$, $u_i^{x,y} = f(x)$, $u_j^{x,y} = g(y)$. Since $C(\beta, \delta_V; 0)$, we have

$$h(d_i', e_j') \neq h(c_i', e_j') \neq h(c_i', f_j') \,.$$

This is a contradiction since the assumption that δ is strongly Abelian implies that every polynomial mapping of $N \times N$ into V depends on at most one variable. The assertion (1) is easily seen to be equivalent to what we have proved.

We shall only need to apply (2) when δ is strongly Abelian, so we supply the proof only under that assumption. Assume that (2) fails and δ is strongly Abelian. Define the distance $d(x, y)$ where $x \delta y$, to be 0 if $x = y$ and else, the least n such that there are $(0, \delta)$-traces $N_0, \ldots, N_{n-1}$ such that $x \in N_0$, $y \in N_{n-1}$ and $N_i \cap N_{i+1} \neq \emptyset$ for $i < n - 1$.

By (1), we can choose $(a, b) \in \beta$, $(u, v) \in \delta$ and a polynomial $p(x, y)$ and an idempotent polynomial $e(x)$ such that $e(F) = V$ and $ep(a, u) = ep(a, v)$ while $ep(b, u) \neq ep(b, v)$. We can assume that $d(u, v) = k$ is minimal for such an example. We have that $k > 1$ since $C(\beta, \delta|_V; 0_F)$ implies that $C(\beta, N^2; 0_F)$ for any $(0, \delta)$-trace N. We have traces $N_0, \ldots, N_{k-1}$ such that $u = u_0 \in N_0$, $v = u_k \in N_{k-1}$, $N_i \cap N_{i+1} \neq \emptyset$ for $i < k - 1$.

We have $ep(a, u_0) = ep(a, u_k)$, $ep(b, u_0) \neq ep(b, u_k)$. Choose $u_1 \in N_0 \cap N_1$ and $u_{k-1} \in N_{k-2} \cap N_{k-1}$. Either both $ep(a, u_0) = ep(a, u_1)$ and $ep(b, u_0) = ep(b, u_1)$, or else neither pair are equal, since β centralizes traces. If both are equal, replacing (u, v) by (u_1, v), we get a contradiction to the minimality of k. Thus for $w \in \{a, b\}$, $ep(w, u_0) \neq ep(w, u_1)$. Likewise, $ep(w, u_{k-1}) \neq ep(w, u_k)$.

Thus, employing the polynomial equivalence of $(0_F, \delta)$-minimal sets, and changing V to a minimal set including N_0, we can assume that $ep(b, x) = x$ for $x \in V$

and $N_0 \subseteq V$; and also that the function $ep(a, x)$ gives a permutation of V, and $ep(a, N_{k-1})$, $ep(a, N_0)$, $ep(b, N_{k-1})$ are traces in V.

Now $N_0 \times N_{k-1} \subseteq \delta$ implies that $ep(b, N_{k-1}) = ep(b, N_0) = N_0$, as well as $ep(a, N_{k-1}) = ep(a, N_0)$.

Notice that $ep(a, ep(b, u_0)) = ep(b, ep(a, u_0))$, yielding, since $C(\delta, \beta; 0)$, that $ep(a, ep(b, v)) = ep(b, ep(a, v))$. Since $ep(b, x) = x$ for $x \in V$, this is the same as

$$ep(a, u) = ep(a, v) = ep(a, ep(b, v)) .$$

Since $(u, ep(b, v)) \in \delta_V$, and $ep(a, x)$ restricted to V is a permutation, then $ep(b, u) = u = ep(b, v)$. This contradiction proves (2). □

Here is the chief result of this section.

Theorem 7.3. *Let* $\mathbf{A}$ *be a finite subdirectly algebra in* $\mathcal{V}$ *with monolith* μ *of type* **1** *and assume that* $\mathbf{A}/\mu$ *is Abelian. Then* $\mathbf{A}$ *is Abelian.*

The entire remainder of this section, and the next section, are devoted to a proof of this theorem. Again, we shall argue by contradiction to establish the theorem. So we hold to the following assumptions from here to the end of Section 8. $\mathbf{A}$ is a finite subdirectly irreducible algebra in $\mathcal{V}$ with monolith μ of type **1**. $\mathbf{A}$ is not Abelian, but $\mathbf{A}/\mu$ is Abelian. U is a fixed $(0_A, \mu)$-minimal set.

Statement (1) in the next lemma will be proved here, but it is a special case of another property shown by Kearnes to be equivalent to the quasi-Hamiltonian property (see K.A. Kearnes [10], Lemma 3.4 and our Theorem 4.1).

Lemma 7.4. (1) $C(1_A, \mu|_U; 0_A)$.

(2) *If* $\tau \in Tw_{\mathbf{A}}(U)$ *and for some* $x \in U$, $\tau(x) \equiv x$ *(mod* μ*), then for all* $x \in U$, $\tau(x) \equiv x$ *(mod* μ*).*

Proof. Suppose that (1) fails, so that we have a polynomial p satisfying $p(c, \bar{a}) = p(c, \bar{b})$, $p(d, \bar{a}) \neq p(d, \bar{b})$ for some $c, d \in A$ and $\bar{a}, \bar{b} \in U^k$ with $(a_i, b_i) \in \mu$ for $i < k$. We can assume that $p(A \times A^k) \subseteq U$ and that where N is the $(0, \mu)$ trace in U to which $p(c, \bar{a})$ and $p(c, \bar{b})$ belong, we have $\bar{a}, \bar{b} \in N^k$. Since the type of μ is **1**, then there are $i, j < k$ and functions $f, g : N \to U$ such that $p(c, \bar{x}) = f(x_i)$ and $p(d, \bar{x}) = g(x_j)$ for all $\bar{x} \in N^k$. Put $h(x, y) = p(x, \bar{a}^y)$ for $x \in A, y \in U$, where $\bar{a}^y_r = a_r$ for $r \neq j$ and $\bar{a}^y_j = y$. Then $h(d, y) = g(y)$ for $y \in N$, so that $h(d, a_j) \neq h(d, b_j)$. This implies that $h(d, y)$ restricted to U is a permutation, belonging to $\Pi_{\mathbf{A}}(U)$. Further, $h(c, a_j) = h(c, b_j)$ as can be checked by considering the two cases, where $i = j$, or $i \neq j$.

Now iterate the polynomial $h(x, y)$ as a function of its second variable to obtain $g(x, y)$ such that $g(c, y)$ and $g(d, y)$ are idempotent functions of y on U. We have $g(d, y) = y$ for $y \in U$ and $g(c, a_j) = g(c, b_j)$ so that we can choose $b \in U$ with $g(c, b) = a = g(c, a) \neq b$ for some $a \in U$. Of course we have $g(d, a) = a$, $g(d, b) = b$. We have demonstrated a failure of the quasi-Hamiltonian property, contradicting Theorem 4.1.

To prove (2), assume that we have a polynomial $p(x, \bar{y})$ and $\bar{c}, \bar{d}$ such that for $x \in U$, $p(x, \bar{c}) = \tau(x)$, $p(x, \bar{d}) = x$ and $\tau \in \mathrm{Tw}_{\mathbf{A}}(U)$. Assume also that for a certain $a \in U$, $\tau(a) \equiv a \pmod{\mu}$. Thus $p(a, \bar{c}) \equiv p(a, \bar{d}) \pmod{\mu}$. Since $\mathbf{A}/\mu$ is Abelian, then for every $x \in A$, $p(x, \bar{c}) \equiv p(x, \bar{d}) \pmod{\mu}$. □

Definition 7.5. *We choose a $k+1$-ary term $s(x,\bar{y})$ such that for all $\bar{c} \in A^k$, $s_{\bar{c}}(x) = s(x,\bar{c})$ is an idempotent function on A, and for some $\bar{a}$, $s_{\bar{a}}(A) = U$. For technical reasons, we arrange (as we may, by adding a dummy variable if necessary) that $k > 0$. The following definitions are made for any algebra $\mathbf{B} \in \mathcal{V}$.*

1. *$P_s(\mathbf{B})$ is the set of all sets $s_{\bar{y}}(B)$, $\bar{y} \in B^k$.*
2. *$P_s^\diamond(\mathbf{B})$ is the set of all polynomial mappings p of $\mathbf{B}$ such that for some $\bar{b} \in B^k$, $p = p \circ s_{\bar{b}}$ (the composition of the functions p and $s_{\bar{b}}$) and there is a polynomial q of $\mathbf{B}$ satisfying $s_{\bar{b}} = q \circ p$.*

Lemma 7.6. *Suppose that $\mathbf{D} \subseteq \mathbf{A}^X$ is a diagonal subdirect power of $\mathbf{A}$ and $\varphi : \mathbf{D} \to \mathbf{B}$ is a surjective homomorphism. For all $V = s_{\bar{c}}^{\mathbf{B}}(B)$, $W = s_{\bar{d}}^{\mathbf{B}}(B)$ in $P_s(\mathbf{B})$ where $\bar{c}, \bar{d} \in B^k$, we have that $s_{\bar{c}}^{\mathbf{B}}$ gives a bijection of W onto V and $s_{\bar{d}}^{\mathbf{B}}$ gives a bijection of V onto W. A subset of $\mathbf{B}$ is polynomially isomorphic to $\varphi(D(U))$ iff it is of the form $\sigma(B)$ for some $\sigma \in P_s^\diamond(\mathbf{B})$.*

Proof. Since $\mathcal{V}$ is quasi-Hamiltonian (Lemma 4.1), for all $\bar{c}, \bar{d} \in A^k$, $(s_{\bar{c}} s_{\bar{d}} s_{\bar{c}})^m = s_{\bar{c}}$, where $m = |A|!$. These equations in $2k+1$ variables hold in all algebras $\mathbf{B} \in HSP(\mathbf{A})$. This lemma is a consequence of that fact. □

Lemma 7.7. *Let $\mathrm{id}|_U \neq \lambda \in Tw_{\mathbf{A}}(U)$. Then for all $x \in U$, $\lambda(x) \neq x$, and for all $(0_A, \mu)$-traces M in U, $\lambda(M) \neq M$. Thus, in particular, the group $Tw_{\mathbf{A}}(U)$ acts regularly on U.*

Corollary 7.8. *We have that $C(\mu, 1_A; 0_A)$ and $C(1_A, \mu; 0_A)$.*

Corollary 7.9. *Let $t(x,\bar{y})$ be a term of $n+1$ variables, and write it as $t_{\bar{y}}(x)$. The following are equivalent.*

1. *For all $\bar{b} \in A^n$ and $\bar{c} \in A^k$, $t_{\bar{b}} \circ s_{\bar{c}} \in P_s^\diamond(\mathbf{A})$.*
2. *For some $\bar{b} \in A^n$ and $\bar{c} \in A^k$, $t_{\bar{b}} \circ s_{\bar{c}} \in P_s^\diamond(\mathbf{A})$.*
3. *For some $\bar{b} \in A^n$ and $\bar{c} \in A^k$, $t_{\bar{b}}$ is one-to-one on $s_{\bar{c}}(A)$.*
4. *There is a term $t'_{\bar{z}}(x)$ of $n+k+1$ variables for which the equation $t'_{\bar{v},\bar{u}} \circ t_{\bar{u}} \circ s_{\bar{v}} = s_{\bar{v}}$ is valid in $\mathbf{A}$.*

Proof of Corollary 7.8. If $C(\mu, 1_A; 0_A)$ fails to hold then we have a polynomial p with $p(A^k, A) \subseteq U$ and $(a,b) \in \mu|_U$ and $\bar{c}, \bar{d} \in A^k$ such that $p(\bar{c}, a) = p(\bar{d}, a)$, $p(\bar{c}, b) \neq p(\bar{d}, b)$. Writing $p_{\bar{y}}(x) = p(\bar{y}, x)$, we have that at least one of $p_{\bar{c}}, p_{\bar{d}}$ is a permutation on U. By Lemma 7.4(1), both $p_{\bar{c}}$ and $p_{\bar{d}}$ belong to $\Pi_{\mathbf{A}}(U)$. They agree at a but not at b. Then $\tau = p_{\bar{c}}^{-1} \circ p_{\bar{d}} \in \mathrm{Tw}_{\mathbf{A}}(U)$ and $\tau(a) = a$ while $\tau(b) \neq b$. But this contradicts Lemma 7.7. Hence $C(\mu, 1_A; 0_A)$ holds.

Now it follows from Lemmas 7.2 and 7.4 that $C(1_A, \mu; 0_A)$ holds as well. □

Proof of Corollary 7.9. Trivially, (4) $\Rightarrow$ (1) $\Rightarrow$ (2) $\Rightarrow$ (3). Now suppose that (3) holds, so that we have $\bar{b} \in A^n$, $\bar{c} \in A^k$, and $t_{\bar{b}}$ is one-to-one on $s_{\bar{c}}(A)$. Since $s_{\bar{c}}(A)$ is a $(0_A, \mu)$-minimal set, it follows from Theorem 2.8 (3) and Theorem 5.7 (1) in D. Hobby, R. McKenzie [5] that there is a polynomial p such that $p \circ t_{\bar{b}}|_{s_{\bar{c}}(A)}$ is the identity function. This implies that $t_{\bar{b}} \circ s_{\bar{c}} \in P_s^\diamond(\mathbf{A})$; i.e., we have (3) $\Rightarrow$ (2). Now suppose that $t_{\bar{b}} \circ s_{\bar{c}} \in P_s^\diamond(\mathbf{A})$. Therefore, for some $\bar{c}' \in A^k$, $t_{\bar{b}} \circ s_{\bar{c}} = t_{\bar{b}} \circ s_{\bar{c}} \circ s_{\bar{c}'}$ and there is a polynomial q so that

$$q \circ t_{\bar{b}} \circ s_{\bar{c}} = s_{\bar{c}'} \,.$$

Let $m > 0$ be such that the m th power of every self-map of A is idempotent. Since $s_{\bar{c}} s_{\bar{c}'} s_{\bar{c}}(A) = s_{\bar{c}}(A)$ (by Theorem 4.1), then $(s_{\bar{c}} s_{\bar{c}'})^m \circ s_{\bar{c}} = s_{\bar{c}}$. Now multiplying the displayed equation on the left by $s_{\bar{c}}$ and on the right by $(s_{\bar{c}'} s_{\bar{c}})^m$, we obtain

$$s_{\bar{c}} q t_{\bar{b}} s_{\bar{c}} = s_{\bar{c}} \,.$$

Write $q(x) = \bar{t}_{\bar{d}}(x)$ for some term $\bar{t}$. Let

$$t'(x, \bar{u}, \bar{v}, \bar{w}) = \left(s_{\bar{v}} \bar{t}_{\bar{w}} t_{\bar{u}}\right)^m (x)$$

and write this as $t'_{\bar{u},\bar{v},\bar{w}}(x)$.

Now choose $(c, d) \in \mu|_{s_{\bar{c}}(A)}$, $c \neq d$. Since $t'_{\bar{b},\bar{c},\bar{d}} s_{\bar{c}} s_{\bar{c}} = s_{\bar{c}}$, we have that

$$t'_{\bar{b},\bar{c},\bar{d}} s_{\bar{c}}(c) \neq t'_{\bar{b},\bar{c},\bar{d}} s_{\bar{c}}(d) \,.$$

Since $C(1_A, \mu; 0_A)$ by the previous corollary, then for all $\bar{b}', \bar{c}', \bar{d}'$

$$t'_{\bar{b}',\bar{c}',\bar{d}'} s_{\bar{c}'}(c) \neq t'_{\bar{b}',\bar{c}',\bar{d}'} s_{\bar{c}'}(d) \,.$$

Now $s_{\bar{c}'}(A)$ is polynomially isomorphic to U, so it is a $(0_A, \mu)$-minimal set, call it V. Then $(s_{\bar{c}'}(c), s_{\bar{c}'}(d)) \in \mu|_V \setminus 0_A$. Since $q'(s_{\bar{c}'}(c)) \neq q'(s_{\bar{c}'}(d))$, where $q' = t'_{\bar{b}',\bar{c}',\bar{d}'}$, and $q' : V \to V$, then $q'|_V \in \Pi_{\mathbf{A}}(V)$. Since also, $q' = q' \circ q'$, then q' is the identity on V. Thus we have established that $\mathbf{A}$ satisfies the equation

$$t'_{\bar{y},\bar{x},\bar{z}} s_{\bar{x}}(z) = s_{\bar{x}}(z) \,.$$

The proof of Corollary 7.9 is readily completed by replacing every variable of the tuple $\bar{z}$ in the above equation by the variable x_1. □

Proof of Lemma 7.7. We have to prove that there is no non-identity member of the twin group having a fixed element or a fixed trace. We assume otherwise, introduce a construction, and eventually use our initial assumption that $G_{\mathcal{V}}$ is polynomially bounded.

Let E be any equivalence relation on a finite set X with $|X/E| > 1$ and such that every E-equivalence class has at least three elements. We take $\mathbf{D}$ to be the subalgebra of $\mathbf{A}^X$ generated by

$$G_0 = \{[a, b]_B : \{a, b\} \subseteq A \text{ and } B \text{ a block of } E \}$$

together with

$$G_1 = \{[a, b]_x : x \in X \text{ and } (a, b) \in \mu|_U, a \neq b\} \,.$$

Note that $\mathbf{D}$ is a diagonal subalgebra of $\mathbf{A}^X$ since $a = b$ is allowed in the definition of G_0. We now fix a $(0_A, \mu)$-trace $N \subseteq U$, and note that $\mathbf{D}$ is also generated by G_0 together with

$$G_1' = \{[a, b]_x : x \in X \text{ and } \{a, b\} \subseteq N, a \neq b\} \,.$$

Claim 1: If $f \in D(U)$, then either f is constant on every block of E, or else there is a block B and $x \in B$ and $(a,b) \in \mu|_U$, $a \neq b$, such that f is constant on each block except B and $f(x) = b$ and $f(y) = a$ for all $y \in B \setminus \{x\}$. Elements of the first kind will be said to comprise the set $G^{(0)}$; those of the second kind comprise the set $G^{(1)}$.

To see this, let $f \in D(U)$, and say f is not constant on the block B of E. Write

$$f = et(g_0^0, \ldots, g_{n-1}^0, g_0^1, \ldots, g_{r-1}^1)$$

where t is a term, $g_i^0 \in G_0$, $g_i^1 \in G_1'$, and e is an idempotent polynomial of $\mathbf{A}$ with $e(A) = U$. By Lemma 7.2(1) and Lemma 7.4(1), $et(\bar{x}, \bar{y})$ restricted to $A^n \times N^r$ depends on at most just one y_{i_0}, $0 \leq i_0 < r$. Since $\bar{g}^0$ is constant on each block and $g_{i_0}^1 = [u,v]_x$, $\{u,v\} \subseteq N$, is constant on all but one block B containing x, then f is constant on each block except B, and there is a polynomial of $\mathbf{A}$ inducing $\sigma : U \to U$, such that $f|_B = \sigma \circ g_{i_0}^1|_B$. Since f is not constant on B, then σ is a permutation of U and $f|_B = [a,b]_x|_B$ for some $(a,b) \in \mu|_U$, $a \neq b$.

We now define a congruence on $\mathbf{D}$. Let μ_X denote the kernel of the natural homomorphism of $\mathbf{D}$ into $(\mathbf{A}/\mu)^X$. Let $\Gamma_0 = (G^{(0)})^2 \cap \mu_X$. Let Γ_1 be the set of all pairs $(f,g) \in (G^{(1)})^2 \cap \mu_X$ such that for some block B and some $x \in B$, and some $a \equiv b \equiv a' \pmod{\mu|_U}$, we have $a \neq b \neq a'$, $f|_B = [a,b]_x|_B$, $g|_B = [a',b]_x|_B$, (and of course, $f|_{B'}$, $g|_{B'}$ are constant for each E-block $B' \neq B$).

We take Θ to be the congruence on $\mathbf{D}$ generated by $\Gamma = \Gamma_0 \cup \Gamma_1$, and we put $\mathbf{R} = \mathbf{R}(X,E) = \mathbf{D}/\Theta$.

Claim 2: $\Theta|_{D(U)} = \Gamma$.

To prove this claim, it suffices to show that Γ is a congruence of $\mathbf{D}|_{D(U)}$. So let $p(x)$ be any polynomial of $\mathbf{D}$ such that $p(D(U)) \subseteq D(U)$ and let $(s_0, s_1) \in \Gamma$. It must be shown that $(p(s_0), p(s_1)) \in \Gamma$. We first consider the case $(s_0, s_1) \in \Gamma_0$.

We can write $p(x) = et(x, \bar{g}^1, \bar{g}^0)$ where t is a term, $\bar{g}^i$ is a list of all the generators of $\mathbf{D}$ in the set G_i. By Lemma 7.2(1), there is one variable in $et(\bar{z})$ such that the polynomial has no dependence on any other variable when it is moved along μ. Suppose first that that variable is not at the place occupied by x. In that case, $p(s_0) = p(s_1)$ since $(s_0, s_1) \in \mu_X$. On the other hand, suppose that it is x. Then for calculating $p(s_i)$, the parameters $\bar{g}^1$ can be replaced by a set of constant functions, yielding that $p(s_0)$, $p(s_1)$ are constant on each E-block. Since they are μ-related, it follows that they are equivalent modulo Γ.

Now consider the case $(s_0, s_1) \in \Gamma_1$, say there is a block B and $x \in B$ so that $s_i|_B = [a_i, b]_x|_B$ for some $a_0 \equiv b \equiv a_1 \pmod{\mu|_U}$, $a_0 \neq b \neq a_1$, and also s_i are constant on each block different from B. Returning to the previous argument, we get the same conclusion unless $et(\bar{z})$ depends at most on its first variable when varied along μ. In this case, it is clear that $p(s_0), p(s_1)$ are constant on each block different from B, and that there is a polynomial $q(x)$ of $\mathbf{A}$ such that $p(s_i)|_B = eq \circ s_i|_B$. If $eq|_U \notin \Pi_{\mathbf{A}}(U)$, then $(p(s_0), p(s_1)) \in \Gamma_0$. If $eq|_U \in \Pi_{\mathbf{A}}(U)$, then clearly $p(s_i)|_B = [eq(a_i), eq(b)]_x|_B$ and $(p(s_0), p(s_1)) \in \Gamma_1$.

Claim 3: The polynomial isomorphism class of the set $D(U)/\Theta$ is a definable set of subsets of $\mathbf{R}$.

This is a consequence of Definition 7.5 and Lemma 7.6. The full polynomial isomorphism class of $D(U)/\Theta$ is equal to the set of ranges of functions belonging to $P_s^\diamond(\mathbf{R})$, but we are most interested in its definable sub-family $P_s(\mathbf{R})$.

Now for $V \in P_s(\mathbf{R})$, we consider the group $\mathrm{Tw}_{\mathbf{R}}(V)$ of twins of the identity on V. For $\pi \in \mathrm{Tw}_{\mathbf{R}}(V)$, $\mathrm{Fix}(\pi)$ denotes the set of $v \in V$ with $\pi(v) = v$, and we put $\mathrm{Mov}(\pi) = V \setminus \mathrm{Fix}(\pi)$. Let $M(V)$ be the set of all non-identity members χ of $\mathrm{Tw}_{\mathbf{R}}(V)$ such that for all $\tau \in \mathrm{Tw}_{\mathbf{R}}(V)$,

$$V \neq \mathrm{Fix}(\tau) \supseteq \mathrm{Fix}(\chi) \Rightarrow \mathrm{Fix}(\tau) = \mathrm{Fix}(\chi)\,.$$

In other terms, $M(V)$ is the set of all members of $\mathrm{Tw}_{\mathbf{R}}(V)$ of maximal proper fixed set.

Suppose that $|M(V)| = \alpha$ and $M(V) = \{\chi_0, \ldots, \chi_{\alpha-1}\}$ and let $(n_0, \ldots, n_{\alpha-1})$ be the system of numbers $n_i = |\mathrm{Mov}(\chi_i)|$. Clearly, the system $\bar{n} = (n_0, \ldots, n_{\alpha-1})$, taken up to permutation of the list, is an invariant of $\mathbf{R}$, the same for all $V \in P_s(\mathbf{R})$.

We shall now calculate this invariant $\bar{n}$. It suffices to take $V = D(U)/\Theta$, and we do so. Let $e(x) = s(x, \bar{a})$ be the idempotent polynomial of $\mathbf{A}$ with $e(A) = U$ (chosen in Definition 7.5).

We define $M'(U)$ as the set of non-identity elements σ of $\mathrm{Tw}_{\mathbf{A}}(U)$ with maximal fixed set and having the property that $\sigma(x)\,\mu\,x$ for all $x \in U$. This set is non-empty: If no non-identity member of $\mathrm{Tw}_{\mathbf{A}}(U)$ has a fixed point, then $M'(U)$ is just the set of those $\sigma \in \mathrm{Tw}_{\mathbf{A}}(U)$ such that $\sigma \neq \mathrm{id}_U$ and $\sigma(x)\,\mu\,x$ holds which, by our starting assumption and Lemma 7.4(2), is a non-empty set. On the other hand, if there is a non-identity member of $\mathrm{Tw}_{\mathbf{A}}(U)$ having a fixed point, then $M'(U)$ is identical with the set of non-identity members of $\mathrm{Tw}_{\mathbf{A}}(U)$ having maximal fixed set (again by Lemma 7.4(2)).

For $\lambda \in \mathrm{Tw}_{\mathbf{A}}(U)$ and $B \in X/E$ we define $\tau(B, \lambda)$ to be the permutation of $D(U)$ such that for all $f \in D(U)$, $\tau(B, \lambda)(f) = g$ agrees with f at all $x \in X \setminus B$ while $g(x) = \lambda(f(x))$ for $x \in B$. Let $\sigma(B, \lambda)$, be defined by $\sigma(B, \lambda)(f/\Theta) = \tau(B, \lambda)(f)/\Theta$ for $f \in D(U)$. Clearly, $\tau(B, \lambda) \in \mathrm{Tw}_{\mathbf{D}}(D(U))$, since $\mathbf{D}$ includes the set G_0. Hence $\sigma(B, \lambda) \in \mathrm{Tw}_{\mathbf{R}}(V)$.

Claim 4: We have

(1) $\sigma(B, \lambda) \in M(V)$ iff $\lambda \in M'(U)$.
(2) $M(V)$ is identical with the set of functions $\sigma(B, \lambda)$, where $B \in X/E, \lambda \in M'(U)$.
(3) The function $(B, \lambda) \mapsto \sigma(B, \lambda)$ is a bijection between $(X/E) \times M'(U)$ and $M(V)$.

To prove this, we begin by examining an arbitrary $\sigma \in \mathrm{Tw}_{\mathbf{R}}(V)$. There is a term t and $\bar{h}, \bar{k} \in D^n$ for some n, such that for $f \in D(U)$,

$$\sigma(f/\theta) = et(f, \bar{h})/\Theta \;\text{ while }\; f \equiv et(f, \bar{k}) \pmod{\Theta}\,.$$

We claim that these relations imply that for all $x \in X$, $et_{\bar{h}(x)}|_U \in \mathrm{Tw}_{\mathbf{A}}(U)$ and in fact, $et_{\bar{k}(x)}|_U = \mathrm{id}|_U$. Indeed, let $x \in X$ and $(a, b) \in \mu_U$, $a \neq b$, and put $f = [a, b]_x$. Since $f \equiv et(f, \bar{k}) \pmod{\Theta}$, it follows from Claim 2 that $et(b, \bar{k}(x)) = b$. Since b is really any member of the body of U, then $et_{\bar{k}(x)}$ is the identity on the body of U. Then for u in the tail of U, $et(u, \bar{k}(x)) \equiv u \pmod{\mu}$ implies $et(u, \bar{k}(x)) = u$. It follows that $et_{\bar{k}(x)}|_U = \mathrm{id}|_U$ for all x. Now an easy application of Lemma 7.4(1)

yields that, for each $x \in X$, $et(c, \bar{h}(x)) = et(d, \bar{h}(x))$ and $(c, d) \in \mu|_U$ imply $c = d$; and from this, tame congruence theory gives that $et_{\bar{h}(x)}|_U$ is a permutation of U. Thus, $et_{\bar{h}(x)}|_U \in \mathrm{Tw}_{\mathbf{A}}(U)$ for all x.

We now show that whenever $(x_0, x_1) \in E$, then $et_{\bar{h}(x_0)}|_U$ and $et_{\bar{h}(x_1)}|_U$ are the same function. Let $B \in X/E$ and $\{x_0, x_1\} \subseteq B$. All generators of $\mathbf{D}$ take μ-congruent values at x_0 and x_1, hence $\bar{h}(x_0)\, \mu\, \bar{h}(x_1)$. For any $(0_A, \mu)$-trace $M \subseteq U$, et restricted to $M \times \bar{h}(x_0)/\mu$ is essentially unary, since the type of $(0_A, \mu)$ is $\mathbf{1}$. This function must depend on the variable ranging over M, because $z \mapsto et(z, \bar{h}(x_0))$ gives a permutation of U. Thus et restricted to $M \times \bar{h}(x_0)/\mu$ depends only on the variable ranging over M—i.e., $et_{\bar{h}(x_0)}|_M = et_{\bar{h}(x_1)}|_M$. Thus the two functions agree on the body of U. Then by Lemma 7.4(2), the permutation $(et_{\bar{h}(x_0)})^{-1} \circ et_{\bar{h}(x_1)} \in \mathrm{Tw}_{\mathbf{A}}(U)$ is the identity function. So we do have $et_{\bar{h}(x_0)}|_U = et_{\bar{h}(x_1)}|_U$.

Now assume that σ belongs to $M(V)$. We keep the notation developed in the previous two paragraphs. It should be clear that there are non-identity members of $\mathrm{Tw}_{\mathbf{R}}(V)$ with non-empty set of fixed points. Just choose $\lambda \in \mathrm{Tw}_{\mathbf{A}}(U)$, $\lambda \neq \mathrm{id}$, such that $\lambda(x) \equiv x \pmod{\mu}$ for all $x \in U$. There is $\gamma \in \mathrm{Tw}_{\mathbf{R}}(V)$ satisfying $\gamma(f/\Theta) = \lambda \circ f/\Theta$ for $f \in D(U)$. Then γ has as fixed points all members of $G^{(0)}/\Theta$. Since $\lambda(b) \neq b$ holds for some element b in the body of U, we have by Claim 2 that $\gamma(f/\Theta) \neq f/\Theta$ if $f = [a, b]_x \in G_1$ for some $x \in X$.

From what we just proved, since $\sigma \in M(V)$, it follows that σ has fixed points. Then since $\Theta \leq \mu_X$, Lemma 7.4(2), implies that that for all $f \in D(U)$, $et(f, \bar{h})\mu_X f$. Thus, for all $x \in X$, the map $et_{\bar{h}(x)}$ leaves all traces invariant. Finally, since $et_{\bar{h}(x)} = et_{\bar{h}(x')}$ when $(x, x') \in E$, we find that $\mathrm{Mov}(\sigma) \subseteq G^{(1)}/\Theta$. In fact, the reader can now easily verify, using Claims 1 and 2, that for $f \in D(U)$, $f/\Theta \in \mathrm{Mov}(\sigma)$ iff $f \in G^{(1)}$ and where B and $x \in B$ and $b \in U$ are the unique block, point, and element such that $f|_B = [a, b]_x|_B$ for some $a \neq b$, we have that $et(b, \bar{h}(x)) \neq b$.

There must be $x_0 \in X$ such that $et_{\bar{h}(x_0)}|_U$ is not the identity. Letting $\lambda = et_{\bar{h}(x_0)}|_U$ and letting B be the block of E containing x_0, we put $\gamma = \sigma(B, \lambda)$. From the above analysis, $V \neq \mathrm{Fix}(\gamma) \supseteq \mathrm{Fix}(\sigma)$. Thus $\mathrm{Fix}(\gamma) = \mathrm{Fix}(\sigma)$. Our analysis also shows that from this equation, we can conclude that $\sigma = \sigma(B, \lambda)$.

It should be clear by now that all three statements in Claim 4 are true. We leave it to the reader to arrange the remaining details in the proof of the claim.

Let $\sigma = \sigma(B, \lambda) \in \mathrm{Tw}_{\mathbf{R}}(V)$. We need to count the set $\mathrm{Mov}(\sigma)$. To begin, for $x \in B$ and c in the body of U, we define $P(x, c)$ to be the set of all $f \in G^{(1)}$ such that $f|_B = [a, c]_x|_B$ for some $a \in U$ where $(a, c) \in \mu|_U$, $a \neq c$.

Claim 5: Let $B \in X/E$, $\lambda \in M'(U)$. Then $\mathrm{Mov}(\sigma(B, \lambda))$ is the disjoint union of the sets $P(x, c)/\Theta$ for $(x, c) \in B \times \mathrm{Mov}(\lambda)$. Moreover, $\Theta|_{P(x,c)} = \mu_X|_{P(x,c)}$, so

$$|\mathrm{Mov}(\sigma(B, \lambda))| = \sum_{(x,c) \in B \times \mathrm{Mov}(\lambda)} |P(x, c)/\mu_X| \,.$$

This claim follows easily from our analysis for Claim 4 together with the fact that for $f \in P(x, c)$, $f' \in P(x', c')$, we have $(f, f') \in \Theta$ iff $(x, c) = (x', c')$ and $(f, f') \in \mu_X$.

The last non-trivial fact we need is that for all $x, x' \in X$ and for all u, u' in the body of U, $|P(x,u)/\mu_X| = |P(x',u')/\mu_X|$. Before proving this, we need some more definitions.

Let $T = \{t_0, \dots, t_{m-1}\}$ be the set (up to equality over $\mathcal{V}$) of all terms of $n+1$ variables, where $n = |G_0|$, with the property that for all (or any) $\bar{c}$, $et_{\bar{c}}|_U$ is a permutation. (The fact that if $et_{\bar{c}}|_U$ is a permutation for one $\bar{c}$ in $\mathbf{A}$, then $et_{\bar{c}}|_U$ is a permutation for all $\bar{c}$ in $\mathbf{A}$ follows from Lemma 7.4(1) and the fact from tame congruence theory that a polynomial mapping of U into itself is a permutation iff it fails to be constant on some trace.) Let $\bar{g}_0 \in D^n$ be a tuple listing all the elements of G_0.

Finally, put

$$Q = \{et(\langle a \rangle, \bar{g}_0) : t \in T \quad \text{and } a \text{ is in the body of } U\} \ ,$$

and for any $x \in X$ and for any trace $M \subseteq U$, put

$$Q(x, M) = \{q \in Q : q(x) \in M\} \ .$$

Claim 6: Let $x \in X$ and u belong to the body of U, and put $M = u/\mu|_U$.

(1) $P(x,u)$ is identical with the set of all elements $f = et([a,b]_x, \bar{g}_0)$ where $t \in T$, $(a,b) \in \mu|_U$, $a \neq b$, and $et(b, \bar{g}_0(x)) = u$.
(2) Where $f = et([a,b]_x, \bar{g}_0) \in P(x,u)$, we have that f is μ_X equivalent to $g = et(\langle a \rangle, \bar{g}_0) \in Q(x,M)$ and both f and g take all their values in the body of U (since $et_{\bar{g}_0(y)}|_U$ is a permutation for all $y \in X$).
(3) For each $q \in Q(x,M)$ there is $f \in P(x,u)$ such that $(f,q) \in \mu_X$.
(4) $|P(x,u)/\mu_X| = |Q(x,M)/\mu_X|$.

Assertions (1) and (2) can easily be proved by an extension of our argument for Claim 1. We prove (3). Statement (4) follows from (2) and (3).

To prove (3), let $q \in Q(x,M)$. Write $q = et(\langle a \rangle, \bar{g}_0)$, $t \in T$, a in the body of U. Write M' for the trace containing a in U. Tame congruence theory tells us that $et_{\bar{g}_0(x)}|_{M'}$ is a bijection between M' and M. Choose $a', b' \in M'$ so that $et(b', \bar{g}_0(x)) = u$ and $a' \neq b'$. Write $f = et([a',b']_x, \bar{g}_0)$. Now clearly, $f \in P(x,u)$ and $(f,q) \in \mu_X$.

Claim 7: For all $x, x' \in X$ and for all b, b' in the body of U, $|P(x,b)/\mu_X| = |P(x',b')/\mu_X|$.

To prove this claim, let $x, x' \in X$, let b and b' be two elements of the body of U, and put $M = b/\mu|_U$, $M' = b'/\mu|_U$. Since μ is a minimal congruence, there is some $p \in \Pi_{\mathbf{A}}(U)$ with $p(M) = M'$. p gives rise to $p_X \in \Pi_{\mathbf{D}}(D(U))$. Obviously, p_X maps $Q(x,M)$ bijectively onto $Q(x,M')$, and this mapping preserves μ_X and its complement. Hence $|Q(x,M)/\mu_X| = |Q(x,M')/\mu_X|$.

Let $M_0, \dots, M_{\ell-1}$ be a one-to-one list of all the traces in U. Then Q/μ_X is partitioned as the disjoint union of the sets $Q(x,M_i)/\mu_X$ $(i < \ell)$ (for a fixed $x \in X$). Since all these sets are of equal cardinality, then for each x and for each trace M and each $u \in M$,

$$|P(x,u)/\mu_X| = |Q(x,M)/\mu_X| = |Q/\mu_X|/\ell \, .$$

This establishes Claim 7.

Now combining the above equalities with the formula of Claim 5, we obtain

Claim 8: For $B \in X/E$ and $\lambda \in M'(U)$, we have

$$|\mathrm{Mov}(\sigma(B,\lambda))| = |B| \cdot |\mathrm{Mov}(\lambda)| \cdot |Q/\mu_X|/\ell\,,$$

where ℓ is the number of $(0_A, \mu)$-traces included in U.

We can now conclude the proof of this lemma. Suppose that $|X/E| = H$ and let $\bar{e} = (e_0, \ldots, e_{H-1})$ be the sequence of block sizes of E. As before, let

$$\{\chi_0, \ldots, \chi_{\alpha-1}\} = M(V), \quad |M(V)| = \alpha\,,$$

and now put put $\bar{n}' = (\ell n_0, \ldots, \ell n_{\alpha-1})$ where $n_i = |\mathrm{Mov}(\chi_i)|$ and ℓ is from Claim 8. Put

$$\{\lambda_0, \ldots, \lambda_{\delta-1}\} = M'(U), \quad |M'(U)| = \delta\,,$$

and put $\bar{m} = (m_0, \ldots, m_{\delta-1})$ and $\bar{m}' = (qm_0, \ldots, qm_{\delta-1})$ where $m_i = |\mathrm{Mov}(\lambda_i)|$ and $q = |Q/\mu_X|$.

The equation of Claim 8 is equivalent to

$$\bar{n}' \sim \bar{e} \cdot \bar{m}'\,;$$

i.e., $\bar{n}'$ is the product of the multi-sets $\bar{e}$ and $\bar{m}'$, as defined at the end of Section 4. The sequence $\bar{n}'$ is an invariant of $\mathbf{R}$. The sequence $\bar{m}$ is an invariant of $\mathbf{A}$, i.e., is independent of (X, E); and so the displayed formula shows that the number $H = \alpha/\delta$ is an invariant of $\mathbf{R}$. The number q will be shown in Claim 9 below to be a function of $\mathbf{A}$ and H, yielding that also the sequence $\bar{m}'$ is an invariant of $\mathbf{R}$. As we remarked at the end of Section 4, the Lovász cancellation theorem, applied to finite equivalence relation structures, yields that $\bar{e}_1 \cdot \bar{m}' \sim \bar{e}_2 \cdot \bar{m}'$ implies $\bar{e}_1 \sim \bar{e}_2$, where $\sim$ here means equal after permutation of the list. Thus, finally, the sequence $\bar{e}$ can be recovered from the abstract structure of $\mathbf{R}$ (and of $\mathbf{A}$). It is the unique solution of the displayed equation, up to $\sim$-equivalence.

The number of generators of $\mathbf{R}$ is bounded by $|G_0 \cup G_1|$ which is dominated by $2|X||\mathbf{A}|^2$. If $|X| = 3n+1$, $n \geq 3$, then the number of non-isomorphic equivalence relation structures (X, E) satisfying our initial conditions is greater than the number $\pi(n)$ of partitions of n. Thus we find that

$$\pi(n) \leq G_{\mathcal{V}}(2a^2(3n+1)) \leq (2a)^{2C}\,(3n+1)^C\,,$$

where $a = |\mathbf{A}|$. For large n, this is impossible.

Claim 9: The number $q = |Q/\mu_X|$ is a function of $H = |X/E|$.

To see this, choose a transversal $Y \subseteq X$ where $|Y \cap B| = 1$ for all $B \in X/E$. Let $\mathbf{D}_0$ be the subalgebra of $\mathbf{D}$ generated by G_0. The restriction map $\eta : f \mapsto f|_Y$ yields an isomorphism of $\mathbf{D}_0$ with $\mathbf{Q}_Y(\mathbf{A})$. We have $Q \subseteq D_0$ and the subset $\eta(Q)$ of $\mathbf{Q}_Y(\mathbf{A})$ is easily characterized. It is the set Q_Δ of all elements f which can be expressed as $et(\langle a \rangle, \bar{h})$ for some term t and tuple $\bar{h}$ of elements of $\mathbf{Q}_Y(\mathbf{A})$ where t has the property that for all $\bar{c}$, $et_{\bar{c}}|_U$ is a permutation. Thus $|Q/\mu_X| = |Q_\Delta/\mu_X|$. $\square$

8. Type **1** monolith, Part II

We are now ready to begin the (rather complicated) construction which will finish the proof of Theorem 7.3.

We continue to use the notation P_s from Definition 7.5, recalling that $s_{\bar{a}}(A) = U$ and $s_{\bar{y}}$ is idempotent for all $\bar{y} \in A^k$.

For any $n+1$-ary polynomial $p(x, \bar{y})$ and $\bar{c}, \bar{d} \in A^n$, we define

$$E(p, \bar{c}, \bar{d}) = \{x \in A : p(x, \bar{c}) = p(x, \bar{d})\}.$$

Using the assumption that $\mathbf{A}$ is non-Abelian, we now choose an $m+1$-ary term t_0 such that

$$\emptyset \neq E(s_{\bar{a}} t_0, \bar{c}, \bar{d}) \neq A\,, \quad \text{for some } \bar{c}, \bar{d} \in A^m\,.$$

Before proceeding further, we define some constants. We put

(0) $M_0 = 2|A|^{k+2m}$, where k and m are determined in the paragraph above.
(1) $M_1 = 2|U|^2$.
(2) $M_2 = 4(M_1)^3 + 12$.
(3) M_3 is the least positive integer such that $M_3 > \max(M_2, |U|^{2M_1+3})$ and whenever the set of two-element subsets of a set of size M_3 is colored in two colors, there exists a subset of size $2M_1$ such that all of its two-element subsets have the same color. (This is a Ramsey number.)

Now let (X, E) be any finite equivalence relation structure such that

(E1) There is a unique singleton equivalence class for E, and each non-singleton class has more than M_0 elements.
(E2) $|X| \geq 2M_3 + 1$.

Definition of $\mathbf{D}(X)$: We define $G(X)$ to be the set of all $f \in A^X$ such that for some $a \in A$,

$$|[\![f \neq a]\!]| \leq M_2\,.$$

We define $\mathbf{D} = \mathbf{D}(X)$ as the subalgebra of $\mathbf{A}^X$ generated by $G(X)$.

Definition of $\mathbf{R}(X, E)$: Let

$$\Gamma = \{([a,b]_x, [a,b]_y) : (a,b) \in \mu|_U, a \neq b, (x,y) \in E\}\ .$$

We define Θ as the congruence of $\mathbf{D}$ generated by Γ, and we put $\mathbf{R} = \mathbf{R}(X, E) = \mathbf{D}/\Theta$.

We now begin the rather extended analysis that will eventually allow us to prove that (X, E) is recoverable, up to isomorphism, from $\mathbf{R}(X, E)$.

Claim 1: For $f, g \in D(U)$ we have that $(f, g) \in \Theta$ iff either $f = g$ or there exists $\tau \in \Pi_{\mathbf{D}}(D(U))$ (a polynomially defined permutation of $D(U)$) such that $(\tau(f), \tau(g)) \in \Gamma$. In fact, for any $f \in D(U)$, if $f/\Theta|_{D(U)} \neq \{f\}$ then there is $\tau \in \Pi_{\mathbf{D}}(D(U))$, a block B of E, and $(a,b) \in \mu|_U$ $(a \neq b)$ such that

$$f/\Theta|_{D(U)} = \tau^{-1}(\{[a,b]_x : x \in B\})\,.$$

As a consequence, if $f \neq g$, $(f, g) \in \Theta$ and $\{f, g\} \subseteq D(U)$, then

$$[\![f \neq g]\!] = \{x, y\}, \quad \text{where} \quad x \neq y \quad \text{and} \quad (x, y) \in E\,.$$

Moreover, for $(a,b) \in \mu|_U$, $a \neq b$, and for any block B of E and $x \in B$,

$$[a,b]_x/\Theta|_{D(U)} = \{[a,b]_y : y \in B\}.$$

Finally, for $f = \langle a \rangle$, $a \in U$, we have that $f/\Theta|_{D(U)} = \{f\}$.

To prove Claim 1, suppose that $(f,g) \in \Theta|_{D(U)}$, $f \neq g$. Then there is a polynomial p of $\mathbf{D}$ and $(h,k) \in \Gamma$ such that $s_{\bar{a}}p(h) = f \neq s_{\bar{a}}p(k)$. Let us write $h = [a,b]_x$, $k = [a,b]_y$, $(x,y) \in E$. Also, write $p(z) = t(z,\bar{\alpha})$ where $\bar{\alpha} \in \mathbf{D}^n$ for some n, and t is a term. Clearly, $s_{\bar{a}}t(a,\bar{\alpha}(x)) \neq s_{\bar{a}}t(b,\bar{\alpha}(x))$, or the same with x exchanged by y. By Lemma 7.4, the functions $s_{\bar{a}}t(u,\bar{\alpha}(v))|_U$ (functions of u parametrized by $v \in X$) are mutually twin members of $\Pi_{\mathbf{A}}(U)$. By iterating $s_{\bar{a}}p$ we obtain τ which is the inverse of $s_{\bar{a}}p$ on U^X. Of course, we have that $\tau(f) = h = [a,b]_x$. Since $\tau \in \Pi_{\mathbf{D}}(D(U))$, then it carries $f/\Theta|_{D(U)}$ bijectively onto $[a,b]_x/\Theta|_{D(U)}$, and $\tau(g)$ belongs to this set.

Let B be the block of E containing x. We claim that

$$[a,b]_x/\Theta|_{D(U)} = \{[a,b]_w : w \in B\}.$$

To see this, it suffices to show that for any $([c,d]_r, [c,d]_s) \in \Gamma$ and for any polynomial q of $\mathbf{D}$, if

$$s_{\bar{a}}q([c,d]_r) = [a,b]_w \neq s_{\bar{a}}q([c,d]_s)$$

where $w \in B$, then $w = r$ and $s_{\bar{a}}q([c,d]_s) = [a,b]_s$ where of course $s \in B$ since $(r,s) \in E$.

So let $([c,d]_r, [c,d]_s) \in \Gamma$ and $s_{\bar{a}}q([c,d]_r) = [a,b]_w \neq s_{\bar{a}}q([c,d]_s)$. As above, we find that $s_{\bar{a}}q|_{D(U)} \in \Pi_{\mathbf{D}}(D(U))$, and at every coordinate, it is acting as a bijection of $c/\mu|_U$ onto $a/\mu|_U$. Thus by Lemma 7.7, there is some $\lambda \in \Pi_{\mathbf{A}}(U)$ such that this function on $D(U)$ is acting as λ at every coordinate; i.e., for $h \in U^X$, $s_{\bar{a}}q(h) = \lambda \circ h$. We find then that $a = \lambda(c)$ and $b = \lambda(d)$, and $r = w$. It also follows immediately that $s_{\bar{a}}p([c,d]_s) = [a,b]_s$.

Essentially the same argument shows that for $a \in U$, $\langle a \rangle/\Theta|_U = \{\langle a \rangle\}$. That concludes the proof of Claim 1.

Remark 1: The congruence Θ and algebra $\mathbf{R}$ do not really depend on the choice of the minimal set U. Let V be any $(0_A, \mu)$-minimal set. Since V is polynomially isomorphic to U in $\mathbf{A}$, then Θ is generated also by the set

$$\Gamma_V = \{([a,b]_x, [a,b]_y) : (a,b) \in \mu|_V, (x,y) \in E\}.$$

Thus Claim 1 remains true if it is modified by substituting V for U, $D(V)$ for $D(U)$, and Γ_V for Γ.

Lemma 8.1. *Let $\bar{a} \in A^k$.*

1. *Let $t(x,\bar{y})$ be any term (say $n+1$-ary). Then where $\bar{u} \in A^n$, $\bar{v}, \bar{w} \in A^k$, $t_{\bar{u}} \circ s_{\bar{v}} \in P_s^\diamond(\mathbf{A})$ iff $t_{\bar{u}} \circ s_{\bar{v}}|_{s_{\bar{w}}(A)}$ is one-to-one. Moreover, this property is independent of the choice of $\bar{u}, \bar{v}, \bar{w}$.*
2. *Let $t(x,\bar{y})$ be any term (say $n+1$-ary). Let $\bar{u} \in A^n$, $\bar{v} \in A^k$, $\bar{e} \in D^n$, $\bar{b} \in D^k$, and put $p(f) = t_{\bar{e}} \circ s_{\bar{b}}(f)$ and $\pi(f/\Theta) = p(f)/\Theta$ for $f \in D$. Then $\pi \in P_s^\diamond(\mathbf{R})$ iff $p \in P_s^\diamond(\mathbf{D})$ iff $t_{\bar{u}} \circ s_{\bar{v}} \in P_s^\diamond(\mathbf{A})$.*
3. *$D(U) \in P_s(\mathbf{D})$, and for all $p \in P_s^\diamond(\mathbf{D})$, we have $p(D(U)) = p(D)$ and there is a polynomial q of $\mathbf{D}$ such that $q(p(D)) = D(U)$ and qp is the identity on $D(U)$ while pq is the identity on $p(D)$.*

(4) *Where $R(U)$ is defined to be $D(U)/\Theta$, we have $R(U) \in P_s(\mathbf{R})$, and for all $\pi \in P_s^\diamond(\mathbf{R})$, we have $\pi(R(U)) = \pi(R)$ and there is a polynomial ν of $\mathbf{R}$ such that $\nu(\pi(R)) = R(U)$, $\nu\pi$ is the identity on $R(U)$ and $\pi\nu$ is the identity on $\pi(R)$.*

Proof. Statements (1), (3) and (4) are consequences of Definition 7.5, Lemma 7.6, and Corollaries 7.8 and 7.9. For the non-obvious part of statement (2), suppose that $t_{\bar{u}} \circ s_{\bar{v}} \notin P_s^\diamond(\mathbf{A})$. Choose any $x_0 \in X$. According to (1), there are $a_0, a_1 \in s_{\bar{b}(x_0)}(A)$, $a_0 \neq a_1$ with $t_{\bar{e}(x_0)} \circ s_{\bar{b}(x_0)}(a_0) = t_{\bar{e}(x_0)} \circ s_{\bar{b}(x_0)}(a_1)$. There are $g_0, g_1 \in D$ with $g_i(x_0) = a_i$ (for $i \in \{0,1\}$) and $g_0(x) = g_1(x)$ for all $x \neq x_0$. Let $f_i = s_{\bar{b}}(g_i)$. Then $f_i(x_0) = a_i$ and $f_0(x) = f_1(x)$ when $x \neq x_0$. Thus $p(f_0) = p(f_1)$. Since $s_{\bar{b}}(D)$ is polynomially isomorphic with $D(U)$, it follows from Claim 1 that $f_0/\Theta \neq f_1/\Theta$. Thus p is not one-to-one on $s_{\bar{b}}(D)$ and π is not one-to-one on $s_{\bar{b}/\Theta}(R)$. For any $\bar{b}' \in D^k$, $s_{\bar{b}}(D)$ and $s_{\bar{b}'}(D)$ are polynomially isomorphic via $s_{\bar{b}'}$ and $s_{\bar{b}}$; thus p fails to be one-to-one on $s_{\bar{b}'}(D)$ and π fails to be one-to-one on $s_{\bar{b}'/\Theta}(R)$. We conclude that $p \notin P_s^\diamond(\mathbf{D})$ and $\pi \notin P_s^\diamond(\mathbf{R})$. □

We remark that we are using, as usual, μ_X to denote the kernel of the homomorphism $\mathbf{D} \to (\mathbf{A}/\mu)^X$, and obviously, we have $\Theta \subseteq \mu_X$.

Claim 2: Let t be any $n+1$-ary term. Let $\bar{f}, \bar{g} \in D^n$ be such that $\emptyset \neq E(t, \bar{f}, \bar{g})$ (calculated in $\mathbf{D}$). Then for all $u \in D$, $(t(u, \bar{f}), t(u, \bar{g})) \in \mu_X$. Let $\bar{v}, \bar{w} \in R^n$ be such that $\emptyset \neq E(t, \bar{v}, \bar{w})$ (calculated in $\mathbf{R}$). Then for all $u \in R$, $(t(u, \bar{v}), t(u, \bar{w})) \in \mu_X/\Theta$.

Both parts of this claim follow from the assumption that $\mathbf{A}/\mu$ is Abelian, and from the fact that $\Theta \subseteq \mu_X$.

The next result simplifies the study of the twin groups in $\mathbf{D}$ and $\mathbf{R}$ in which we shall be interested.

Lemma 8.2. *Suppose that $p \in P_s^\diamond(\mathbf{D})$. Since $p(D)$ is polynomially isomorphic to $D(U)$, there is an idempotent polynomial e' of $\mathbf{D}$ such that $e'(D) = p(D)$. Now let $t(x, \bar{y})$ be a term, say $r+1$-ary, let $\bar{h} \in D^r$, and for $z \in p(D)$ put $f(z) = e't(z, \bar{h})$, and $g(z/\Theta) = f(z)/\Theta$. Then*

(1) *If $g \in \Pi_{\mathbf{R}}(p(D)/\Theta)$, then $f \in \Pi_{\mathbf{D}}(p(D))$.*
(2) *If g is the identity on $p(D)/\Theta$ then f is the identity on $p(D)$.*
(3) *If $g \in Tw_{\mathbf{R}}(p(D)/\Theta)$, then $f \in Tw_{\mathbf{D}}(p(D))$.*

Proof. Let $K : D(U) \to p(D)$ and $L : p(D) \to D(U)$ be mutually inverse bijections obtained as restrictions of polynomials. Choose $(a, b) \in \mu|_U \setminus 0_U$.

Now suppose first that $f \notin \Pi_{\mathbf{D}}(p(D))$. Then LfK is not a permutation of $D(U)$. By Lemma 7.4, at every coordinate, LfK collapses traces. Then $LfK(\langle a \rangle) = LfK(\langle b \rangle)$. This means that $f(K(\langle a \rangle)) = f(K(\langle b \rangle))$. Since $(\langle a \rangle, \langle b \rangle) \notin \Theta$, by Claim 1, it follows that $g \notin \Pi_{\mathbf{R}}(p(D)/\Theta)$.

Now, assume that g is the identity. This means that for all $z \in D(U)$, $LfK(z)\Theta z$. There cannot be three distinct coordinates at which LfK is not acting as the identity on U, for then there would be $z \in D(U)$ with $LfK(z)$ differing from z at three coordinates, making $LfK(z)\Theta z$ impossible by Claim 1. Thus there is a coordinate at which LfK is acting as the identity. Then it follows that at every

coordinate, the action of LfK belongs to $\mathrm{Tw}_{\mathbf{A}}(U)$ and fixes the element a (since $LfK(\langle a\rangle)\Theta\langle a\rangle$ implies $LfK(\langle a\rangle) = \langle a\rangle$ by Claim 1). Hence it follows with Lemma 7.7 that at every coordinate, LfK is acting as the identity. This means that LfK is the identity permutation of $D(U)$, implying that f is the identity on $p(D)$.

Finally, assume that $g \in \mathrm{Tw}_{\mathbf{R}}(p(D)/\Theta)$, so that $f \in \Pi_{\mathbf{D}}(p(D))$. For some term t', there are tuples $\bar{h}$ and $\bar{k}$ in D so that for $z \in p(D)$, $e't'(z,\bar{h})/\Theta = g(z/\Theta)$ and $e't'(z,\bar{k})\Theta z$. From what we just proved above, $e't'(z,\bar{k}) = z$ for all $z \in p(D)$. Thus by Lemma 7.4 (1), $e't'(z,\bar{h}) = f'(z)$ defines $f' \in \mathrm{Tw}_{\mathbf{D}}(p(D))$. Then $f^{-1}f' \in \Pi_{\mathbf{D}}(p(D))$ and $f^{-1}f'(z)\Theta z$ for all $z \in p(D)$. Thus again, it follows that $f^{-1}f'(z) = z$ for $z \in p(D)$, implying that $f = f' \in \mathrm{Tw}_{\mathbf{D}}(p(D))$. This finishes our proof of the lemma. □

Orbits of a twin group: Let C be a subset of an algebra $\mathbf{B} \in \mathcal{V}$. We shall be writing $u \overset{\mathrm{tw}}{\sim} v$ to mean that elements u and v of C are in the same orbit of $\mathrm{Tw}_{\mathbf{B}}(C)$ acting on C. (When the notation $u \overset{\mathrm{tw}}{\sim} v$ is used, the algebra $\mathbf{B}$ and set C are to be determined from the context.)

Remark 2: Let $p \in P_s^\diamond(\mathbf{D})$ and $\{f,g\} \subseteq p(D)$. As a consequence of Claim 1 and Lemma 8.1, if $(f,g) \in \Theta$ then either $f = g$ or $|[\![f \neq g]\!]| = 2$. Using Lemmas 7.1 and 8.2, we see that if $\{h,k\} \subseteq p(D)$ and $h/\Theta \overset{\mathrm{tw}}{\sim} k/\Theta$ with respect to the twin group induced by $\mathbf{R}$ on $p(D)/\Theta$ then for all but at most two $x \in X$ we must have $h(x) \overset{\mathrm{tw}}{\sim} k(x)$ in the group induced by $\mathbf{A}$ on the x th projection of $p(D)$ (which is a $(0_A,\mu)$- minimal set).

The next three lemmas contain key observations.

Lemma 8.3. *Let $p \in P_s^\diamond(\mathbf{D})$ and $\pi(z/\Theta) = p(z)/\Theta$. Suppose that $y_0 \in X$ and (f_i,g_i), $0 \leq i \leq 2|U|^2$ are pairs of elements of $p(D)$ such that for all i, $f_i\Theta g_i$ and $f_i(y_0) \neq g_i(y_0)$. There exists $i < j \leq 2|U|^2$ such that $f_i/\Theta \overset{tw}{\sim} f_j/\Theta$ (with respect to the twin group that $\mathbf{R}$ induces on the set $\pi(R)$).*

Proof. We can replace $p(D)$, $\pi(R)$ by the polynomially isomorphic $s_{\bar{a}}(D) = D(U)$ and $s_{\bar{a}/\Theta}(R) = R(U)$. Thus we assume that f_i, g_i belong to $D(U)$. Since $f_i\Theta g_i$, by Claim 1, we can find $p_i \in \Pi_{\mathbf{D}}(D(U))$ and $(c_i,d_i) \in \mu|_U$ and $z_i \neq y_0$ such that

$$\{p_i(f_i), p_i(g_i)\} = \{[c_i,d_i]_{y_0}, [c_i,d_i]_{z_i}\}\,.$$

Now $\Pi_{\mathbf{D}}(D(U))$ contains the permutation $\chi = \xi_X$, where $\xi = p_i^{y_0}$ (since $\mathbf{D}$ is a diagonal subalgebra of $\mathbf{A}^X$). By multiplying p_i on the left by χ^{-1}, we can assume that $p_i \in \mathrm{Tw}_{\mathbf{D}}(D(U))$ and at the coordinate y_0, p_i acts as the identity.

Now by cardinality considerations, there exist $i < j$ such that

$$(f_i(y_0), g_i(y_0)) = (f_j(y_0), g_j(y_0))$$

and either $c_i = c_j = f_i(y_0)$, or else $d_i = d_j = f_i(y_0)$. The cases are essentially symmetric. Suppose that $c_i = c_j = f_i(y_0)$, so that $d_i = d_j = g_i(y_0)$. In this case,

$$p_i(g_i) = [c_i,d_i]_{y_0} = [c_j,d_j]_{y_0} = p_j(g_j)\,.$$

Since $p_i, p_j \in \mathrm{Tw}_{\mathbf{D}}(D(U))$, this shows that $g_i \overset{\mathrm{tw}}{\sim} g_j$ and hence that

$$f_i/\Theta = g_i/\Theta \overset{\mathrm{tw}}{\sim} g_j/\Theta = f_j/\Theta\,.$$

Thus ends the proof of this lemma. □

Lemma 8.4.

(1) *Let $\{f, f'\} \subseteq D(U)$ and assume that $\{x_0, x_1\} \subseteq X$, $x_0 \neq x_1$, and $f(x_i) \overset{tw}{\not\sim} f'(x_i)$ with respect to $Tw_{\mathbf{A}}(U)$ for $i = 0$ and $i = 1$. Then $f/\Theta \overset{tw}{\sim} f'/\Theta$ with respect to $Tw_{\mathbf{R}}(R(U))$ iff the following conditions are satisfied (in which $\overset{tw}{\sim}$ is understood to be with respect to $Tw_{\mathbf{A}}(U)$):*
   (i) *For some $e \in \{f(x_0), f(x_1)\}$, for all $x \in X \setminus \{x_0, x_1\}$ we have $f(x) \overset{tw}{\sim} f'(x) \overset{tw}{\sim} e$.*
   (ii) *$f'(x_i) \overset{tw}{\sim} f(x_{1-i})$ for each $i \in \{0, 1\}$.*
   (iii) *$(x_0, x_1) \in E$ and there exist $c \overset{tw}{\sim} f(x_0)$ and $d \overset{tw}{\sim} f(x_1)$ such that $(c, d) \in \mu$.*

(2) *Let $p \in P_s^\diamond(\mathbf{D})$, and for $f \in D$, put $\pi(f/\Theta) = p(f)/\Theta$. Suppose that $\{f, f'\} \subseteq p(D)$, that $\{x_0, x_1\} \subseteq X$, $x_0 \neq x_1$, that $f(x_i) \overset{tw}{\not\sim} f'(x_i)$ with respect to $Tw_{\mathbf{A}}(p_x(A))$ for $i = 0$ and $i = 1$, and that $f/\Theta \overset{tw}{\not\sim} f'/\Theta$ with respect to $Tw_{\mathbf{R}}(\pi(R))$. Then there are $x_2, x_3 \in X$ such that whenever $\{u, u'\} \subseteq p(D)$ and $u(x) = f(x)$ and $u'(x) = f'(x)$ for all $x \in \{x_0, x_1, x_2, x_3\}$ then $u/\Theta \overset{tw}{\not\sim} u'/\Theta$.*

Proof. To prove (1), let $\{f, f'\} \subseteq D(U)$, $\{x_0, x_1\} \subseteq X$ satisfy the conditions stated in the first sentence of (1). Suppose first that $f/\Theta \overset{\mathrm{tw}}{\sim} f'/\Theta$ with respect to $\mathrm{Tw}_{\mathbf{R}}(R(U))$. Then by Lemma 8.2 (3), there is $q \in \mathrm{Tw}_{\mathbf{D}}(D(U))$ so that $q(f)\Theta f'$. Now $q(f)(x) \overset{\mathrm{tw}}{\sim} f(x)$ for all $x \in X$ (with respect to $\mathrm{Tw}_{\mathbf{A}}(U)$), and so $q(f)$ must differ from f' at x_0 and x_1. Since $q(f)\Theta f'$, then by Claim 1, $(x_0, x_1) \in E$ and there is $r \in \Pi_{\mathbf{D}}(D(U))$ and $(c, d) \in \mu|_U$, $c \neq d$, so that $\{r(q(f)), r(f')\} = \{[c, d]_{x_0}, [c, d]_{x_1}\}$. Let for $u \in D(U)$, $r(u) = \langle r_x(u(x)) : x \in X\rangle$; put $t(u) = r_{x_0} \circ u$; and put $r' = t^{-1} \circ r$. Thus $r' \in \mathrm{Tw}_{\mathbf{D}}(D(U))$ and $\{r'(q(f)), r'(f')\} = \{[c', d']_{x_0}, [c', d']_{x_1}\}$ with $(c', d') \in \mu$. Now for all $x \in X$, $f(x) \overset{\mathrm{tw}}{\sim} r'(q(f))(x)$ and $f'(x) \overset{\mathrm{tw}}{\sim} r'(f')(x)$. It should be obvious that this establishes that (i)–(iii) hold.

Conversely, suppose that (i)–(iii) are satisfied. Let $(c, d) \in \mu$ be as in (iii). Thus $f(x_0) \overset{\mathrm{tw}}{\sim} c \overset{\mathrm{tw}}{\sim} f'(x_1)$ and $f'(x_0) \overset{\mathrm{tw}}{\sim} d \overset{\mathrm{tw}}{\sim} f(x_1)$. There are two cases: either we have $f(x) \overset{\mathrm{tw}}{\sim} f'(x) \overset{\mathrm{tw}}{\sim} c$ for all $x \in X \setminus \{x_0, x_1\}$, or we have $f(x) \overset{\mathrm{tw}}{\sim} f'(x) \overset{\mathrm{tw}}{\sim} d$ for all $x \in X \setminus \{x_0, x_1\}$. In the first case, choose for all $x \in X \setminus \{x_0, x_1\}$ some $r_x, t_x \in \mathrm{Tw}_{\mathbf{A}}(U)$ with $r_x(f(x)) = c = t_x(f'(x))$, and choose $r_{x_0}, r_{x_1}, t_{x_0}, t_{x_1} \in \mathrm{Tw}_{\mathbf{A}}(U)$ so that

$$(r_{x_0}(f(x_0)), r_{x_1}(f(x_1))) = (c, d) = (t_{x_1}(f'(x_1)), t_{x_0}(f'(x_0)))\,.$$

By Lemma 7.1, there are $r, t \in \mathrm{Tw}_{\mathbf{D}}(D(U))$ with $r(u) = \langle r_x(u(x)) : x \in X\rangle$, $t(u) = \langle t_x(u(x)) : x \in X\rangle$, for all $u \in D(U)$. Clearly, $r(f) = [c, d]_{x_1}$ and $t(f') = [c, d]_{x_0}$. Here, $r(f)\Theta t(f')$. Thus $t^{-1}r(f)\Theta f'$ and $t^{-1}r \in \mathrm{Tw}_{\mathbf{D}}(D(U))$, which shows that $f/\Theta \overset{\mathrm{tw}}{\sim} f'/\Theta$ with respect to the group $\mathrm{Tw}_{\mathbf{R}}(R(U))$, as required. The proof in the second case is essentially the same.

To prove (2), note that since $p(D)$ is polynomially isomorphic in $\mathbf{D}$ to $D(U)$, then we lose no generality by assuming that $p(D) = D(U)$. Then by statement (1), some one of (i), (ii), (iii) fails. If (ii) or (iii) fails, then statement (1) implies that we get the desired result by taking $x_2 = x_3 = x_0$. If (i) fails then there are x_2, x_3

in $X \setminus \{x_0, x_1\}$ so that $\neg(f(x_2) \overset{\text{tw}}{\sim} f'(x_2) \overset{\text{tw}}{\sim} f(x_0))$ and $\neg(f(x_3) \overset{\text{tw}}{\sim} f'(x_3) \overset{\text{tw}}{\sim} f(x_1))$. Then for u, u' in $D(U)$ agreeing with f, f' respectively at x_0, x_1, x_2, x_3, statement (1) implies that $u \overset{\text{tw}}{\not\sim} u'$ relative to $\mathrm{Tw}_{\mathbf{D}}(D(U))$, as desired. □

Lemma 8.5. *Let $\{f, f'\} \subseteq D(U)$ and assume that $\{x_0, x_1\} \subseteq X$, $x_0 \neq x_1$, and $[\![f \neq g]\!] = \{x_0, x_1\}$.*

(1) *$(f, f') \in \Theta$ iff the following conditions are satisfied.*
   (i) *$(x_0, x_1) \in E$ and $(f(x_0), f'(x_0)) \in \mu$.*
   (ii) *There is $\sigma \in Tw_{\mathbf{A}}(U)$ with $(\sigma(f(x_1)), \sigma(f'(x_1))) = (f'(x_0), f(x_0))$.*
   (iii) *For some $e \in \{f(x_0), f'(x_0)\}$, for all $x \in X \setminus \{x_0, x_1\}$ we have $f(x) \overset{tw}{\sim} e$ with respect to the group $Tw_{\mathbf{A}}(U)$.*

(2) *If $(f, f') \notin \Theta$ then there are $x_2, x_3 \in X$ such that whenever $\{u, u'\} \subseteq D(U)$ and $(u(x), u'(x)) = (f(x), f'(x))$ for all $x \in \{x_0, x_1, x_2, x_3\}$ then $(u, u') \notin \Theta$.*

Proof. We use Claim 1. Suppose that $(f, f') \in \Theta$ and choose $\tau \in \Pi_{\mathbf{D}}(D(U))$ such that $\{\tau(f), \tau(f')\} = \{[c, d]_{x_0}, [c, d]_{x_1}\}$ with $(c, d) \in \mu$ and $(x_0, x_1) \in E$. For $u \in D(U)$, say $\tau(u) = \langle \tau_x(u(x)) : x \in X \rangle$. For $x \in X$, put $\sigma_x = \tau_{x_0}^{-1} \tau_x$, so that $\sigma_x \in \mathrm{Tw}_{\mathbf{A}}(U)$. Now we have $(\sigma_{x_1}(f(x_1)), \sigma_{x_1}(f'(x_1))) = (f'(x_0), f(x_0))$. Moreover, for all $x \in X \setminus \{x_0, x_1\}$, $\sigma_x(f(x)) = \sigma_x(f'(x)) = \tau_{x_0}^{-1}(c) \in \{f(x_0), f'(x_0)\}$. Thus conditions (i)–(iii) are fulfilled if $(f, f') \in \Theta$.

Conversely, if (i)–(iii) are satisfied, then by Lemma 7.1, there is $\tau \in \mathrm{Tw}_{\mathbf{D}}(D(U))$ with $\{\tau(f), \tau(f')\} = \{[c, d]_{x_0}, [c, d]_{x_1}\}$ where $c = e$ and $\{c, d\} = \{f(x_0), f'(x_0)\}$. Thus $(f, f') \in \Theta$ in this case.

Thus (1) is proved. Assertion (2) is an immediate consequence of (1). □

Definition 8.6. *For $p \in P_s^\diamond(\mathbf{A})$, we put $M(pt_0)$ equal to the set of pairs $(\bar{c}, \bar{d}) \in (A^m)^2$ such that $\emptyset \neq E(pt_0, \bar{c}, \bar{d}) \neq A$ and for all $\bar{c}', \bar{d}' \in A^m$, if $E(pt_0, \bar{c}, \bar{d}) < E(pt_0, \bar{c}', \bar{d}')$ then $E(pt_0, \bar{c}', \bar{d}') = A$.*

Claim 3: Suppose that $\nu s_{\bar{c}} \in P_s^\diamond(\mathbf{A})$ with $\tau \nu s_{\bar{c}} = s_{\bar{c}}$. Then for any $\bar{u}, \bar{v} \in A^m$,

$$E(\nu s_{\bar{c}} t_0, \bar{u}, \bar{v}) = E(s_{\bar{c}} t_0, \bar{u}, \bar{v}) \quad \text{and} \quad M(\nu s_{\bar{c}} t_0) = M(s_{\bar{c}} t_0)\,.$$

This claim is obvious. Recall that the numbers M_1, M_3 were defined in the fourth paragraph of this section.

Definition 8.7. *Let the polynomial σ of $\mathbf{R}$ belong to $P_s^\diamond(\mathbf{R})$. For $\bar{c}, \bar{d} \in (R^m)$, we put $(\bar{c}, \bar{d}) \in M'(\sigma t_0)$ if and only if the following are satisfied:*

(M′1): $\emptyset \neq E(\sigma t_0, \bar{c}, \bar{d}) < R$.

(M′2): *Let $\bar{c}', \bar{d}' \in (R^m)$ be such that $E(\sigma t_0, \bar{c}, \bar{d}) < E(\sigma t_0, \bar{c}', \bar{d}') < R$. Let*

$$T = \left\{ \sigma t_0(u, \bar{c}') : u \in E(\sigma t_0, \bar{c}, \bar{d}) \right\}\,.$$

Then the number of orbits under $Tw_{\mathbf{R}}(\sigma(R))$ containing members of T is at most M_1.

(M′3): *Let $\bar{c}', \bar{d}' \in (R^m)$ be such that $E(\sigma t_0, \bar{c}, \bar{d}) \setminus E(\sigma t_0, \bar{c}', \bar{d}') \neq \emptyset$. Let*

$$T = \left\{ \sigma t_0(u, \bar{c}) : u \in E(\sigma t_0, \bar{c}, \bar{d}) \setminus E(\sigma t_0, \bar{c}', \bar{d}') \right\} .$$

Then the number of orbits under $Tw_{\mathbf{R}}(\sigma(R))$ containing members of T is at least $M_3 - 2$.

(M′4): *The number of orbits under $Tw_{\mathbf{R}}(\sigma(R))$ of elements $\sigma t_0(u, \bar{c})$ with $u \in E(\sigma t_0, \bar{c}, \bar{d})$ is at least M_3.*

Claim 4: For any $\nu s_{\bar{\tau}} \in P_s^{\diamond}(\mathbf{R})$ (so that there exists a polynomial ξ with $\xi \nu s_{\bar{\tau}} = s_{\bar{\tau}}$), we have $M'(\nu s_{\bar{\tau}} t_0) = M'(s_{\bar{\tau}} t_0)$.

Claim 4 is straightforward to prove, and we leave that to the reader.

The next two claims assert much deeper properties of $M'(\sigma t_0)$. The proofs are lengthy. We state both claims, prove Claim 6 first, and then prove Claim 5.

Claim 5: Suppose that $(\bar{c}, \bar{d}) \in M'(s_{\bar{\tau}} t_0)$. There exists a unique point $x_0 \in X$ and a unique subset $S \subseteq A$ so that whenever $\bar{b} \in D^k$ and $\{\bar{h}, \bar{k}\} \subseteq D^m$ with $\bar{\tau} = \bar{b}/\Theta$, $\bar{c} = \bar{h}/\Theta$, $\bar{d} = \bar{k}/\Theta$, then

(1) $\{x \in X : E(s_{\bar{b}(x)} t_0, \bar{h}(x), \bar{k}(x)) \neq A\} = \{x_0\}$ and $(\bar{h}(x_0), \bar{k}(x_0))$ is in $M(s_{\bar{b}(x_0)} t_0)$;
(2) $S = E(s_{\bar{b}(x_0)} t_0, \bar{h}(x_0), \bar{k}(x_0))$, and for all $f \in D$, we have $f/\Theta \in E(s_{\bar{\tau}} t_0, \bar{c}, \bar{d})$ if and only if $f(x_0) \in S$.

Definition 8.8. *We define Λ to be the set of all systems*

$$\left(\bar{a}^0, \bar{a}^1, \bar{e}^0, \bar{e}^1, \bar{e}^2, w_0, w_1, w_2\right)$$

with $\bar{a}^i \in A^k$, $\bar{e}^i \in A^m$, $w_i \in A$ such that

(i) $(\bar{e}^0, \bar{e}^1) \in M(s_{\bar{a}^0} t_0)$.
(ii) $w_0 \notin E(s_{\bar{a}^0} t_0, \bar{e}^0, \bar{e}^1)$.
(iii) $s_{\bar{a}^1} t_0(w_1, \bar{e}^2) \overset{tw}{\not\sim} s_{\bar{a}^1} t_0(w_2, \bar{e}^2)$ *in* $s_{\bar{a}^1}(A)$.

Claim 6: Suppose that $x_0 \in X$ and $(\bar{a}^0, \bar{a}^1, \bar{e}^0, \bar{e}^1, \bar{e}^2, w_0, w_1, w_2) \in \Lambda$. Put $\bar{h} = [\bar{e}^2, \bar{e}^0]_{x_0}$, $\bar{k} = [\bar{e}^2, \bar{e}^1]_{x_0}$ so that $\bar{h}, \bar{k} \in D^m$, and put $\bar{b} = [\bar{a}^1, \bar{a}^0]_{x_0} \in D^k$. Finally, put $\bar{c} = \bar{h}/\Theta$, $\bar{d} = \bar{k}/\Theta$, $\bar{\tau} = \bar{b}/\Theta$.

Then $(\bar{c}, \bar{d}) \in M'(s_{\bar{\tau}} t_0)$. Moreover, if it happens that

$$s_{\bar{a}^0} t_0(w_0, \bar{e}^0) = s_{\bar{a}^1} t_0(w_1, \bar{e}^2) = a' ,$$

then where $f = [w_1, w_0]_{x_0}$ and $b' = s_{\bar{a}^0} t_0(w_0, \bar{e}^1)$, we have $s_{\bar{b}} t_0(f, \bar{h}) = \langle a' \rangle$ and $s_{\bar{b}} t_0(f, \bar{k}) = [a', b']_{x_0}$.

Remark 3: Suppose that $\bar{a}^0 \in A^k$ and $(\bar{e}^0, \bar{e}^1) \in M(s_{\bar{a}^0} t_0)$ and

$$s_{\bar{a}^0} t_0(w_0, \bar{e}^0) = a' \neq b' = s_{\bar{a}^0} t_0(w_0, \bar{e}^1) .$$

Choose $w \in E(s_{\bar{a}^0} t_0, \bar{e}^0, \bar{e}^1)$, say

$$s_{\bar{a}^0} t_0(w, \bar{e}^0) = s_{\bar{a}^0} t_0(w, \bar{e}^1) = c' .$$

By Lemma 7.6, $s_{\bar{a}^0}(A) = U'$ is an $(0_A, \mu)$-minimal set. Since $s_{\bar{a}^0} t_0(w, \bar{e}^0) = s_{\bar{a}^0} t_0(w, \bar{e}^1)$ and $\mathbf{A}/\mu$ is Abelian, then $(a', b') \in \mu$. Thus a' and b' lie in one of

the traces of U'. Lemma 7.7 applies in this situation and we conclude that c' cannot be twin-equivalent (relative to the group $\mathrm{Tw}_{\mathbf{A}}(U')$) to both a' and b'. It is easy to check that if $c' \overset{\mathrm{tw}}{\not\sim} a'$ then $(\bar{a}^0, \bar{a}^0, \bar{e}^0, \bar{e}^1, \bar{e}^0, w_0, w_0, w) \in \Lambda$, while if $c' \overset{\mathrm{tw}}{\not\sim} b'$ then $(\bar{a}^0, \bar{a}^0, \bar{e}^1, \bar{e}^0, \bar{e}^1, w_0, w_0, w) \in \Lambda$.

Proof of Claim 6. Throughout this proof, we shall write $p = s_{\bar{b}}$, $p_i = s_{\bar{a}^i}$ ($i \in \{0,1\}$). Now $E(s_{\bar{\tau}}t_0, \bar{c}, \bar{d}) \neq R$ since $pt_0(f, \bar{h})$ is not Θ-equivalent to $pt_0(f, \bar{k})$, as follows by Claim 1 and Remark 1. That $E(s_{\bar{\tau}}t_0, \bar{c}, \bar{d}) \neq \emptyset$ is a consequence of the fact that $E(p_0t_0, \bar{e}^0, \bar{e}^1) \neq \emptyset$. Thus we have verified (M′1).

To prove (M′4) for $s_{\bar{\tau}}, \bar{c}, \bar{d}$, choose pairwise disjoint two-element sets

$$\{y_i, z_i\} \subseteq X \setminus \{x_0\}\,,\ 0 \leq i < M = \lfloor (|X| - 1)/2 \rfloor\,.$$

For $i < M$, define $f_i \in D$ so that $f_i(x_0) \in E(p_0t_0, \bar{e}^0, \bar{e}^1)$, $f_i(y_i) = f_i(z_i) = w_1$ and $f_i(x) = w_2$ for all $x \in X \setminus \{x_0, y_i, z_i\}$. Now $u_i = f_i/\Theta$ belongs to $E(s_{\bar{\tau}}t_0, \bar{c}, \bar{d})$. We claim that where $v_i = s_{\bar{\tau}}t_0(u_i, \bar{c})$, then for $0 \leq i < j < M$, we have $v_i \overset{\mathrm{tw}}{\not\sim} v_j$ with respect to the group $\mathrm{Tw}_{\mathbf{R}}(s_{\bar{\tau}}(R))$. This follows from Remark 2 and the observation that there are four $x \in X$ for which

$$\{p_1t_0(f_i(x), \bar{h}(x)), p_1t_0(f_j(x), \bar{h}(x))\} = \{p_1t_0(w_1, \bar{e}^2), p_1t_0(w_2, \bar{e}^2)\}\,.$$

Now $M_3 \leq M$ since we required, in condition (E2) at the beginning of our proof of Theorem 7.3, that $|X| \geq 2M_3 + 1$. This concludes our proof of (M′4).

Notice that since $\bar{h}$ differs from $\bar{k}$ only at x_0, then for any $z \in D$, we have, by Remark 2, that

$$z/\Theta \in E(s_{\bar{\tau}}t_0, \bar{c}, \bar{d}) \Leftrightarrow pt_0(z, \bar{h}) = pt_0(z, \bar{k}) \Leftrightarrow$$

$$\Leftrightarrow p_0t_0(z(x_0), \bar{e}^0) = p_0t_0(z(x_0), \bar{e}^1) \Leftrightarrow z(x_0) \in E(p_0t_0, \bar{e}^0, \bar{e}^1)\,.$$

Next, to prove (M′2) for $s_{\bar{\tau}}, \bar{c}, \bar{d}$, assume that $\bar{f}/\Theta, \bar{g}/\Theta \in R^m$ ($\bar{f}, \bar{g} \in D^m$) are such that $E(s_{\bar{\tau}}t_0, \bar{c}, \bar{d}) < E(s_{\bar{\tau}}t_0, \bar{f}/\Theta, \bar{g}/\Theta) < R$. Choose $z_0 \in D$ such that $z_0/\Theta \in E(s_{\bar{\tau}}t_0, \bar{f}/\Theta, \bar{g}/\Theta) \setminus E(s_{\bar{\tau}}t_0, \bar{c}, \bar{d})$, and choose $z_1 \in D$ such that

$$z_1/\Theta \notin E(s_{\bar{\tau}}t_0, \bar{f}/\Theta, \bar{g}/\Theta)\,.$$

Now we look at cases.

Case 1: $E(p_0t_0, \bar{f}(x_0), \bar{g}(x_0)) = A$. In this case, we can choose $x_2 \in X \setminus \{x_0\}$ such that $p_1t_0(z_1(x_2), \bar{f}(x_2)) \neq p_1t_0(z_1(x_2), \bar{g}(x_2))$. Let $z \in D$ be any element such that $z(x_2) = z_1(x_2)$, $z(x_0) \in E(p_0t_0, \bar{e}^0, \bar{e}^1)$. Then $pt_0(z, \bar{f})(x_2) \neq pt_0(z, \bar{g})(x_2)$ but $pt_0(z, \bar{f})\Theta pt_0(z, \bar{g})$ (since $z \in E(pt_0, \bar{h}, \bar{k})$ and $E(s_{\bar{\tau}}t_0, \bar{c}, \bar{d}) \subseteq E(s_{\bar{\tau}}t_0, \bar{f}/\Theta, \bar{g}/\Theta)$). Thus by Remark 2, there is $x = x(z) \in X \setminus \{x_0, x_2\}$ such that $[\![pt_0(z, \bar{f}) \neq pt_0(z, \bar{g})]\!] = \{x, x_2\}$. Since D projects onto A^{M_2} at every set of M_2 coordinates (our choice of generators), it easily follows, by allowing z to vary, and using that no two elements of $p(D)$ which disagree at just one place, or at more than two places, are Θ-congruent (Remark 2), that $x(z)$ is independent of z—call it x_1, and that $E(p_1t_0, \bar{f}(x), \bar{g}(x))$ is A for all $x \notin \{x_1, x_2\}$, and is empty for $x \in \{x_1, x_2\}$.

Thus for $z \in D$ with $z(x_0) \in E(p_0t_0, \bar{e}_0, \bar{e}^1)$—i.e., with $z \in E(pt_0, \bar{h}, \bar{k})$, we have the pair

$$(f^z, g^z) = (pt_0(z, \bar{f}), pt_0(z, \bar{g}))$$

consisting of two functions which differ precisely at x_1 and x_2 and are Θ-equivalent. By Lemma 8.3, it follows that the elements f^z/Θ represent no more than $2|U|^2 =$

M_1 distinct $\overset{\text{tw}}{\sim}$-equivalence classes in $s_{\bar\tau}(R)$. This finishes the proof of (M′2) in Case 1.

Case 2: $E(p_0t_0, \bar e^0, \bar e^1) \subseteq E(p_0t_0, \bar f(x_0), \bar g(x_0)) \neq A$. In this case, since $(\bar e^0, \bar e^1) \in M(p_0t_0)$, then $E(p_0t_0, \bar e^0, \bar e^1) = E(p_0t_0, \bar f(x_0), \bar g(x_0))$. Hence, in this case,

$$p_0t_0(z_0(x_0), \bar f(x_0)) \neq p_0t_0(z_0(x_0), \bar g(x_0))\,.$$

Since $s_{\bar\tau}t_0(z_0, \bar f)\Theta s_{\bar\tau}t_0(z_0, \bar g)$, it follows that there is $x_2 \neq x_0$ such that

$$[\![s_{\bar\tau}t_0(z_0, \bar f) \neq s_{\bar\tau}t_0(z_0, \bar g)]\!] = \{x_0, x_2\}\,.$$

Now, letting z vary over all elements of D such that $z(x_0) \in E(p_0t_0, \bar e^0, \bar e^1)$, and $z(x_2) = z_0(x_2)$, we easily conclude, as in Case 1, that there are two distinct coordinates $x \in X \setminus \{x_0\}$ at which $E(p_1t_0, \bar f(x), \bar g(x))$ is empty and at all other coordinates in $X \setminus \{x_0\}$, this set is A. Now $|[\![pt_0(z_0, \bar f) \neq pt_0(z_0, \bar g)]\!]| = 3$, contradiction.

Case 3: $E(p_0t_0, \bar e^0, \bar e^1) \not\subseteq E(p_0t_0, \bar f(x_0), \bar g(x_0))$. In this case, choosing $p \in E(p_0t_0, \bar e^0, \bar e^1) \setminus E(p_0t_0, \bar f(x_0), \bar g(x_0))$ and considering arbitrary $z \in D$ such that $z(x_0) = p$, we find that there is $x_1 \neq x_0$ such that $E(p_1t_0, \bar f(x), \bar g(x))$ is A for all $x \notin \{x_0, x_1\}$ and this set is empty at $x = x_1$. Then it follows that at $x = x_0$, $E(p_0t_0, \bar f(x_0), \bar g(x_0))$ is disjoint from $E(p_0t_0, \bar e^0, \bar e^1)$. Thus the same argument used in Case 1 can now be applied, substituting $\{x_0, x_1\}$ for the set $\{x_1, x_2\}$ used there. This completes our proof that (M′2) holds.

Now to prove (M′3) for $s_{\bar\tau}, \bar c, \bar d$, suppose that $\bar f, \bar g \in (D^m)^2$ satisfy

$$E(s_{\bar\tau}t_0, \bar c, \bar d) \setminus E(s_{\bar\tau}t_0, \bar f/\Theta, \bar g/\Theta) \neq \emptyset\,.$$

For this proof, we take E_Θ to be the set of $z \in D$ such that z/Θ belongs to $E(s_{\bar\tau}t_0, \bar f/\Theta, \bar g/\Theta)$. We choose $z_0 \in E(pt_0, \bar h, \bar k) \setminus E_\Theta$; then we choose $x_1 \in X$ at which the functions $pt_0(z_0, \bar f)$ and $pt_0(z_0, \bar g)$ are unequal.

In this proof of (M′3), we will eventually find $z' \in E(pt_0, \bar h, \bar k) \setminus E_\Theta$; and a set Y of at most five points in X, including $\{x_0, x_1\}$, such that where D_Y denotes the set of all $z \in D$ such that $z|_Y = z'|_Y$, we have $D_Y \cap E_\Theta = \emptyset$. Then repeating the proof of (M′4) above, using functions in D_Y which take the value w_1 at two points outside Y, and the value w_2 at all other points outside Y, we can complete the proof of (M′3).

As a first approximation to the desired Y and z', take $Y = \{x_0, x_1\}$ and $z' = z_0$. (Note that we are not assuming that $x_0 \neq x_1$.) Let us assume that this doesn't work. Then there is $z_1 \in D$ with $z_1(x) = z_0(x)$ for $x \in \{x_0, x_1\}$ and $z_1 \in E_\Theta$. Thus there exists $x_2 \neq x_1$ such that $(x_1, x_2) \in E$ and $pt_0(z_1, \bar f)$ disagrees with $pt_0(z_1, \bar g)$ precisely at x_1 and x_2. (Note that it may be that $x_2 = x_0$.) Suppose that there is $z_2 \in D$ which agrees with z_1 at x_0, x_1, x_2 such that $pt_0(z_2, \bar f)$ disagrees with $pt_0(z_2, \bar g)$ at some point x_3 distinct from x_1 and x_2. Then by Claim 1, all $z \in D$ which agree with z_2 on $Y = \{x_0, x_1, x_2, x_3\}$ lie outside E_Θ, and so we are done in this case. Hence, we can assume that no such z_2 exists.

We now have that for all $x \notin \{x_0, x_1, x_2\}$,

$$E(p_1t_0, \bar f(x), \bar g(x)) = A\,.$$

Similarly, we can discard the possibility that $E(p_1t_0, \bar f(x), \bar g(x)) \neq \emptyset$ for some $x \in \{x_1, x_2\} \setminus \{x_0\}$. And so we now assume that

$$E(p_1t_0, \bar f(x), \bar g(x)) = \emptyset \;\text{ if } x \in \{x_1, x_2\} \setminus \{x_0\}\,.$$

Then if $pt_0(z_0, \bar{f})$ and $pt_0(z_0, \bar{g})$ agree at x_2, it follows that $x_2 = x_0$, and also that $pt_0(z_1, \bar{f})$ and $pt_0(z_1, \bar{g})$ agree at x_2, since $z_1(x_0) = z_0(x_0)$. This contradiction establishes that $x_2 \in [\![pt_0(z_0, \bar{f}) \neq pt_0(z_0, \bar{g})]\!]$. Similarly, we get a contradiction if $x_0 \notin \{x_1, x_2\}$ and $\{x_0, x_1, x_2\} \subseteq [\![pt_0(z_0, \bar{f}) \neq pt_0(z_0, \bar{g})]\!]$. Thus we have that

$$[\![pt_0(z_0, \bar{f}) \neq pt_0(z_0, \bar{g})]\!] = \{x_1, x_2\}\,.$$

To conclude the argument for (M′3), we make a translation from $p(D)$ to $D(U)$ via polynomial isomorphism. Recall that $\bar{a} \in A^k$ and $s_{\bar{a}}(A) = U$. Let $\bar{b}' = [\bar{a}, \bar{a}]_\emptyset \in D^k$. According to Lemma 7.6, $p|_{D(U)}$ and $s_{\bar{b}'}|_{p(D)}$ are bijections from $D(U)$ to $p(D)$, and from $p(D)$ to $D(U)$, respectively, and there is a polynomial q of $\mathbf{D}$ such that pq is the identity on $p(D)$ and qp is the identity on $D(U)$.

We are going to be able to take $z' = z_0$. Put $f = qpt_0(z_0, \bar{f})$, $f' = qpt_0(z_0, \bar{g})$. Thus $[\![f \neq f']\!] = \{x_1, x_2\}$ and $\{f, f'\} \subseteq D(U)$, $(f, f') \notin \Theta$. By Lemma 8.5, there is a set Y of at most five points, including $\{x_0, x_1, x_2\}$ such that whenever $\{u, u'\} \subseteq D(U)$ and $u(x) = f(x)$ and $u'(x) = f'(x)$ for all $x \in Y$ then $(u, u') \notin \Theta$. It follows that when $z \in D$ and z agrees with z_0 on Y, then $z \notin E_\Theta$. This concludes our proof of (M′3), and also ends the proof of Claim 6. □

Proof of Claim 5. Suppose that $(\bar{c}, \bar{d}) \in M'(s_{\bar{\tau}}t_0)$. We begin by assuming that $(\bar{c}, \bar{d}) = (\bar{h}/\Theta, \bar{k}/\Theta)$ with $\bar{h}, \bar{k} \in D^m$, and that $\bar{\tau} = \bar{b}/\Theta$ with $\bar{b} \in D^k$. We proceed to find the element $x_0 \in X$ and the set $S \subseteq A$ to satisfy statements (1) and (2) of this claim. Then we will need to demonstrate that x_0 and S are independent of the choice of $\bar{h}, \bar{k}, \bar{b}$.

For a while, we will operate under the following assumptions:

Assumption 1: For all $z \in D$,

$$z/\Theta \in E(s_{\bar{\tau}}t_0, \bar{h}/\Theta, \bar{k}/\Theta) \Leftrightarrow z \in E(s_{\bar{b}}t_0, \bar{h}, \bar{k})\,.$$

Assumption 2: There are $x_0, x_1 \in X$, $x_0 \neq x_1$, such that

$$E(s_{\bar{b}(x)}t_0, \bar{h}(x), \bar{k}(x)) \neq A \quad \text{for} \quad x \in \{x_0, x_1\}.$$

Employing (M′4), we choose $Z \subseteq D$, $|Z| = M_3$, so that

$$Z/\Theta \subseteq E(s_{\bar{\tau}}t_0, \bar{h}/\Theta, \bar{k}/\Theta)\,,$$

and for all $z \neq z'$, $\{z, z'\} \subseteq Z$,

$$s_{\bar{b}}t_0(z, \bar{h})/\Theta \quad \text{and } s_{\bar{b}}t_0(z', \bar{h})/\Theta \text{ are not } \overset{\text{tw}}{\sim}\text{-related in } s_{\bar{b}}(D)/\Theta\,.$$

For $z \in Z$ we write f^z for $s_{\bar{b}}t_0(z, \bar{h})$. We divide the set of two-element subsets of Z into two classes, C_1 and C_2, where $\{z, z'\} \in C_i$ iff the set of $x \in X$ such that $f^z(x)$ and $f^{z'}(x)$ are not $\overset{\text{tw}}{\sim}$-related in $s_{\bar{b}(x)}(A)$ is a one-element set ($i = 1$), or a set of at least two elements ($i = 2$). Since $s_{\bar{b}}(D)$ is polynomially isomorphic to $D(U)$, it follows by Lemma 7.1 that each set $\{z, z'\}$ belongs to one of these two classes.

By our choice of M_3 and M_1, for some $i \in \{1, 2\}$, there is a set $Z_i \subseteq Z$, $|Z_i| = 2M_1$, such that all two-element subsets from Z_i belong to C_i. Clearly, $i = 1$ is impossible, since $2M_1 > |U|$ and for all x, $|U| = |s_{\bar{b}(x)}(A)|$.

Thus $i = 2$. For each pair $z, z' \in Z_2$, $z \neq z'$, we can choose, by Lemma 8.4, a set $Y_{z,z'}$ of at most four elements of X so that whenever $u, u' \in s_{\bar{b}}(D)$ and u agrees with f^z on $Y_{z,z'}$ and u' agrees with $f^{z'}$ on the set $Y_{z,z'}$, then u/Θ and u'/Θ are not $\overset{\text{tw}}{\sim}$ related in $s_{\bar{\tau}}(R)$.

Define Y to be the union of all the sets $Y_{z,z'}$ and the set $\{x_0\}$. Thus

$$|Y| \leq 4 \cdot 2M_1^2 + 1 \leq M_2 \,.$$

We have that whenever $\{z_0, z_1\}$ is a two element subset of Z_2 and $\{u_0, u_1\} \subseteq s_{\bar{b}}(D)$ and $u_i = f^{z_i}$ on the set Y, then u_0/Θ and u_1/Θ are not $\overset{\text{tw}}{\sim}$ related in $s_{\bar{\tau}}(R)$.

Since $|Y| \leq M_2$, we can find $\bar{h}_0, \bar{k}_0 \in D^m$ such that $\bar{h}_0(x) = \bar{k}_0(x)$ for all $x \neq x_0$, $\bar{h}_0$ agrees with $\bar{h}$ at all $x \in Y$, and $\bar{k}_0(x_0) = \bar{k}(x_0)$. By Assumption 1 and Assumption 2 above, we have that

$$E(s_{\bar{\tau}} t_0, \bar{h}/\Theta, \bar{k}/\Theta) < E(s_{\bar{\tau}} t_0, \bar{h}_0/\Theta, \bar{k}_0/\Theta) < R \,.$$

Now $Z_2/\Theta \subseteq E(s_{\bar{\tau}} t_0, \bar{h}/\Theta, \bar{k}/\Theta)$. For $z \in Z_2$, put $f_0^z = s_{\bar{b}} t_0(z, \bar{h}_0)$. Then it is clear from the above observations that for $z \neq z'$, $\{z, z'\} \subseteq Z_2$, f_0^z/Θ and $f_0^{z'}/\Theta$ are not $\overset{\text{tw}}{\sim}$-related in $s_{\bar{\tau}}(R)$. Since $|Z_2| = 2M_1$, this contradicts (M′2) for $\bar{h}, \bar{k}$.

The contradiction just obtained shows that Assumptions 1 and 2 above are not jointly tenable. Let us next assume for a moment that Assumption 1 fails. To handle this case, we can use Lemma 8.3.

Using the failure of Assumption 1, choose $z \in D$ so that

$$s_{\bar{b}} t_0(z, \bar{h}) \Theta s_{\bar{b}} t_0(z, \bar{k})$$

but these functions are unequal. Then choose $x_2 \neq x_3$ such that these functions differ precisely at x_2, x_3. Choose $\bar{h}_0, \bar{k}_0 \in D^m$ such that $\bar{h}_0 = \bar{k}_0$ at all $x \neq x_2$ and at x_2 these functions agree with $\bar{h}, \bar{k}$, respectively. Then

$$z/\Theta \in E(s_{\bar{\tau}} t_0, \bar{h}/\Theta, \bar{k}/\Theta) \setminus E(s_{\bar{\tau}} t_0, \bar{h}_0/\Theta, \bar{k}_0/\Theta) \,.$$

By (M′3) for $\bar{h}/\Theta, \bar{k}/\Theta$, and since $M_3 - 2 > 2|U|^2 = M_1$, we have $z_0, \ldots, z_{M_1}$ in D such that where

$$(f_i, g_i) = (s_{\bar{b}} t_0(z_i, \bar{h}), s_{\bar{b}} t_0(z_i, \bar{k})) \,,$$

we have $f_i \Theta g_i$, $f_i(x_2) \neq g_i(x_2)$, and for no $i < j$ do we have $f_i/\Theta \overset{\text{tw}}{\sim} f_j/\Theta$ in $s_{\bar{\tau}}(R)$. But this contradicts Lemma 8.3.

In this way, we have seen that Assumption 1 holds. Since Assumption 1 and Assumption 2 cannot both hold, then we have established that there is $x_0 \in X$ such that for all $x \neq x_0$, $E(s_{\bar{b}(x)} t_0, \bar{h}(x), \bar{k}(x)) = A$ and $\emptyset \neq E(s_{\bar{b}(x_0)} t_0, \bar{h}(x_0), \bar{k}(x_0)) \neq A$.

To finish the proof of Claim 5, statement (1), we must show that

$$(\bar{h}(x_0), \bar{k}(x_0)) \in M(s_{\bar{b}(x_0)} t_0) \,.$$

Assume not. Choose $\bar{u}, \bar{v} \in A^m$ such that

$$A \neq E(s_{\bar{b}(x_0)} t_0, \bar{u}, \bar{v}) > E(s_{\bar{b}(x_0)} t_0, \bar{h}(x_0), \bar{k}(x_0)) \,.$$

Then we can produce $\bar{h}_0, \bar{k}_0 \in D^m$ which are equal at all $x \neq x_0$ and take at x_0 the values $\bar{u}, \bar{v}$. Clearly, we have that

$$E(s_{\bar{\tau}} t_0, \bar{h}/\Theta, \bar{k}/\Theta) < E(s_{\bar{\tau}} t_0, \bar{h}_0/\Theta, \bar{k}_0/\Theta) < R \,.$$

We are aiming at contradicting (M′2) for $\bar{h}/\Theta, \bar{k}/\Theta$. To achieve the contradiction, we have to be rather precise about our choice of the tuple of functions $\bar{h}_0$ restricted to $x \neq x_0$. Here is how we do it.

As usual, let $f^z = s_{\bar{b}}t_0(z, \bar{h})$ and choose a set $Z \subseteq E(s_{\bar{b}}t_0, \bar{h}, \bar{k})$, $|Z| = M_3$, such that for $z \neq z'$ in Z, f^z/Θ and $f^{z'}/\Theta$ are not $\overset{\text{tw}}{\sim}$ related. Let T denote the set of all $x \in X \setminus \{x_0\}$ such that for some $z, z' \in Z$, $f^z(x)$ and $f^{z'}(x)$ are not $\overset{\text{tw}}{\sim}$-related in $s_{\bar{b}(x)}(A)$. Suppose that $|T| \leq 2M_1 + 1$. Since $|U|^{2M_1+2} < M_3$, there must then exist $z, z' \in Z$, $z \neq z'$, such that $f^z|_{T\cup\{x_0\}} = f^{z'}|_{T\cup\{x_0\}}$. But then, it follows from Lemma 7.1 that $f^z \overset{\text{tw}}{\sim} f^{z'}$ in $s_{\bar{b}}(D)$. This contradiction tells us that we can choose a set $Y \subseteq X \setminus \{x_0\}$, $|Y| = 2(M_1 + 1)$, such that for all $y \in Y$, there are $z, z' \in Z$ such that $f^z(y) \overset{\text{tw}}{\not\sim} f^{z'}(y)$. Write $Y = \{y_0, \ldots, y_{2M_1+1}\}$. For $y = y_i \in Y$, choose $z, z' \in Z$ with $f^z(y) \overset{\text{tw}}{\not\sim} f^{z'}(y)$, and put $(p_i, q_i) = (z(y_i), z'(y_i))$.

Of course, we choose $\bar{h}_0, \bar{k}_0$ so that $\bar{h}_0|_Y = \bar{k}_0|_Y = \bar{h}|_Y$, $\bar{h}_0(x) = \bar{k}_0(x) = \bar{u}$ for $x \in X \setminus (Y \cup \{x_0\})$ (and as we indicated, $\bar{h}_0(x_0) = \bar{u}$, $\bar{k}_0(x_0) = \bar{v}$). These functions belong to D since $2M_1 + 3 \leq M_2$. For $0 \leq j \leq M_1$, let $z_j \in D$ be such that $z_j(y_i) = p_i$ for $i \in \{2j, 2j + 1\}$ and $z_j(y_i) = q_i$ for $i \notin \{2j, 2j + 1\}$, and $z_j(x) = s$ for $x \notin Y$, where s is some fixed element in $E(s_{\bar{b}(x_0)}t_0, \bar{h}(x_0), \bar{k}(x_0))$. Now clearly, for $j < j' \leq M_1$, $z_j, z_{j'} \in E(s_{\bar{b}}t_0, \bar{h}, \bar{k})$ and the elements $s_{\bar{b}}t_0(z_j, \bar{h}_0)$ and $s_{\bar{b}}t_0(z_{j'}, \bar{h}_0)$ fail to be $\overset{\text{tw}}{\sim}$ equivalent at four distinct coordinates, so $s_{\bar{b}}t_0(z_j, \bar{h}_0)/\Theta$ and $s_{\bar{b}}t_0(z_{j'}, \bar{h}_0)/\Theta$ are not $\overset{\text{tw}}{\sim}$ equivalent. This is, finally, the desired contradiction of (M′2). It completes the proof of statement (1) of Claim 5.

Setting $S = E(s_{\bar{b}(x_0)}t_0, \bar{h}(x_0), \bar{k}(x_0))$, Statement (2) of Claim 5 becomes obvious, in view of statement (1) and Claim 1 and Remark 2.

Finally, we have to show that x_0 and S do not change when different representatives are chosen for $\bar{c}, \bar{d}, \bar{\tau}$. So let $\bar{c} = \bar{h}'/\Theta$, $\bar{d} = \bar{k}'/\Theta$, $\bar{\tau} = \bar{b}'/\Theta$. From the proof of (1), there is a unique $x_1 \in X$ such that $E(s_{\bar{b}'(x)}t_0, \bar{h}'(x), \bar{k}'(x)) \neq A$ iff $x = x_1$. By (2) [for $\bar{h}, \bar{k}, \bar{b}$ and also for $\bar{h}', \bar{k}', \bar{b}'$] we have, for all $f \in D$,

$$f(x_0) \in E(s_{\bar{b}(x_0)}t_0, \bar{h}(x_0), \bar{k}(x_0)) \quad \text{iff} \quad f(x_1) \in E(s_{\bar{b}'(x_1)}t_0, \bar{h}'(x_1), \bar{k}'(x_1))\,.$$

Also, each of these equality sets is a proper non-void subset of A. These facts clearly imply that $x_0 = x_1$ and

$$E(s_{\bar{b}(x_0)}t_0, \bar{h}(x_0), \bar{k}(x_0)) = E(s_{\bar{b}'(x_0)}t_0, \bar{h}'(x_0), \bar{k}'(x_0))\,.$$

Our proof of Claim 5 is finished. □

The next definition and pair of lemmas are the heart of this proof and justify all the work we have done.

Definition 8.9. *We define* Φ *to be the set of all systems*

$$\big(\sigma, z, u, v, \bar{c}, \bar{d}_i \ (0 \leq i \leq M_0)\big)$$

satisfying

(F1) $\sigma \in P_s^\diamond(\mathbf{R})$, $z, u, v \in R$ *and* $\bar{c}, \bar{d}_i \in R^m$ *(*$0 \leq i \leq M_0$*).*
(F2) $\sigma t_0(z, \bar{c}) = u$.

(F3) *For* $i \leq M_0$, $\sigma t_0(z, \bar{d}_i) = v \neq u$.
(F4) *For* $\{i, j\} \subseteq \{0, 1, \cdots, M_0\}$, $i \neq j$ *we have*

$$E(\sigma t_0, \bar{c}, \bar{d}_i) \not\subseteq E(\sigma t_0, \bar{c}, \bar{d}_j)\,.$$

(F5) *For all* $i \leq M_0$, *we have* $(\bar{c}, \bar{d}_i) \in M'(\sigma t_0)$.

Lemma 8.10. *Suppose that* $\sigma(g/\Theta) = p(g)/\Theta$ *for all* $g \in D$ *where* $p \in P_s^\diamond(\mathbf{D})$, *and*

$$\big(\sigma, z, u, v, \bar{c}, \bar{d}_i \ (0 \leq i \leq M_0)\big) \in \Phi\,.$$

Let $z = f/\Theta$, $\bar{c} = \bar{h}/\Theta$ *and* $\bar{d}_i = \bar{k}_i/\Theta$ *for* $i \leq M_0$; *and put* $w = pt_0(f, \bar{h})$, $w_i = pt_0(f, \bar{k}_i)$ *so that* $w/\Theta = u$ *and* $w_i/\Theta = v$. *Then there exist* $(a, b) \in \mu|_U$, $a \neq b$, *and a polynomial* q *of* $\mathbf{D}$ *with* $qp(D) = D(U)$, *and a block* B *of* E *and elements* $x_i \in B$ $(i \leq M_0)$ *so that*

$$q(w) = \langle a \rangle \quad \textit{and} \quad q(w_i) = [a, b]_{x_i} \quad \textit{for all } i\,.$$

Lemma 8.11. Φ *is non-empty.*

Proof of Lemma 8.10. By Claim 5, from (F5) we deduce that for each $i \leq M_0$, there is $x_i \in X$ such that $[\![E(pt_0, \bar{h}, \bar{k}_i) \neq A]\!] = \{x_i\}$ and $(\bar{h}(x_i), \bar{k}_i(x_i)) \in M(p_{x_i} t_0)$. Then $[\![w \neq w_i]\!] = \{x_i\}$. For any $\{i, j\} \subseteq \{0, \ldots, M_0\}$ with $x_i \neq x_j$, we must have $w_i \neq w_j$, and since $w_i \,\Theta\, w_j$, then $|[\![w_i \neq w_j]\!]| = 2$ by Remark 2. Since $w_i(x) = w(x) = w_j(x)$ for $x \notin \{x_i, x_j\}$, it follows that

$$\text{for } \{i, j\} \subseteq \{0, \ldots, M_0\}, \text{ either } x_i = x_j, \text{ or}$$

$$[\![w_i \neq w_j]\!] = \{x_i, x_j\} \quad \text{and} \quad (x_i, x_j) \in E\,.$$

Now (F4) implies that the map $i \mapsto (x_i, \bar{h}(x_i), \bar{k}_i(x_i))$ is one-to-one. Since $M_0 \geq 2|A|^{2m}$, it then follows that there must be $i_0 < i_1 < i_2 \leq M_0$ with $|\{x_{i_0}, x_{i_1}, x_{i_2}\}| = 3$.

Since $p(D)$ is polynomially isomorphic to $D(U)$ and $\{w_0, \ldots, w_{M_0}\} \subseteq w_0/\Theta$, then by Claim 1 and Remark 1, there is a polynomial q of $\mathbf{D}$ such that $q|_{p(D)}$ is a bijection of $p(D)$ with $D(U)$, and there are $(a, b) \in \mu|_U$, $a \neq b$ and there is a block B of the equivalence relation E and for all $i \leq M_0$ there is $y_i \in B$ so that $q(w_i) = [a, b]_{y_i}$.

Now for $\{j, k\} \subseteq \{0, 1, 2\}$, $j \neq k$, we have

$$[\![[a, b]_{y_{i_j}} \neq [a, b]_{y_{i_k}}]\!] = [\![w_{i_j} \neq w_{i_k}]\!] = \{x_{i_j}, x_{i_k}\}\,.$$

Hence $\{y_{i_0}, y_{i_1}, y_{i_2}\} = \{x_{i_0}, x_{i_1}, x_{i_2}\}$ is a three-element set and $q(w) \in D(U)$ differs from each $[a, b]_{y_{i_j}}$ at precisely one point in X. These facts force $q(w) = \langle a \rangle$. (Notice that for all $i \leq M_0$,

$$\{x_i\} = [\![w \neq w_i]\!] = [\![\langle a \rangle \neq [a, b]_{y_i}]\!] = \{y_i\}$$

so that $x_i = y_i$.) □

Proof of Lemma 8.11. Recall that we have $\bar{a} \in A^k$ with $s_{\bar{a}} = U$ and such that there are $\bar{e}_0, \bar{e}_1 \in A^m$ with $\emptyset < E(s_{\bar{a}}t_0, \bar{e}_0, \bar{e}_1) < A$. Obviously, we can select these elements so that $(\bar{e}_0, \bar{e}_1) \in M(s_{\bar{a}}t_0)$. As we observed in Remark 3, we can also select them in such a way that there are $w_1, w_2 \in A$ with $s_{\bar{a}}t_0(w_1, \bar{e}_0) \overset{\text{tw}}{\not\sim} s_{\bar{a}}t_0(w_2, \bar{e}_0)$ in U.

Now we put $p = s_{\bar{b}}$ where $\bar{b} \in D^k$ is the tuple for which $\bar{b}(x) = \bar{a}$ for all $x \in X$, and we put $\sigma(g/\Theta) = p(g)/\Theta$ for $g \in D$.

Next, we choose distinct elements x_i, $0 \leq i \leq M_0$, from one E-equivalence class in X. We put $\bar{h} = [\bar{e}_0, \bar{e}_0]_\emptyset$ and for each $i \leq M_0$, we put $\bar{k}_i = [\bar{e}_0, \bar{e}_1]_{x_i}$. Then we take $\bar{c} = \bar{h}/\Theta \in R^m$ and $\bar{d}_i = \bar{k}_i/\Theta$ for $i \leq M_0$. Finally, we choose $w \notin E(s_{\bar{a}}t_0, \bar{e}_0, \bar{e}_1)$, and we put $z = \langle w \rangle/\Theta$, $u = pt_0(\langle w \rangle, \bar{h})/\Theta$ and $v = pt_0(\langle w \rangle, \bar{k}_0)/\Theta$.

We have $(\sigma, z, u, v, \bar{c}, \bar{d}_i (0 \leq i \leq M_0)) \in \Phi$. Indeed, (F1)–(F4) are easily verified. For (F4), note that $pt_0(\langle w \rangle, \bar{k}_i) = [a_0, a_1]_{x_i}$ where $a_\varepsilon = s_{\bar{a}}t_0(w, \bar{e}_\varepsilon)$. Condition (F5) is a consequence of Claim 6 (see Remark 3). □

Definition 8.12. (1) *J is the set of all pairs $(\sigma, u) \in P_s^\diamond(\mathbf{R}) \times R$ which are first and third items in some $(\sigma, z, u, v, \bar{c}, \bar{d}_i\ (0 \leq i \leq M_0)) \in \Phi$.*

(2) *For $(\sigma, u) \in J$, we take $S(\sigma, u)$ to be the set of all systems $(\tau, z, \bar{c}, \bar{d}) \in P_s^\diamond(\mathbf{R}) \times R \times R^m \times R^m$ such that $\tau(R) = \sigma(R)$, $(\bar{c}, \bar{d}) \in M'(\tau t_0)$ and $u = \tau t_0(z, \bar{c}) \neq \tau t_0(z, \bar{d})$.*

(3) *For $(\sigma, u) \in J$, we take $T(\sigma, u)$ to be the set of all elements $v \in R$ such that there exists $(\tau, z, \bar{c}, \bar{d}) \in S(\sigma, u)$ with $\tau t_0(z, \bar{d}) = v$.*

(4) *For $(\sigma, u) \in J$ and $v \in T(\sigma, u)$, we take $I(\sigma, u, v)$ to be the set of all sets $E(\tau t_0, \bar{c}, \bar{d}) \subseteq R$ where $(\tau, z, \bar{c}, \bar{d}) \in S(\sigma, u)$ and $\tau t_0(z, \bar{d}) = v$.*

(5) *For $(\sigma, \mu) \in J$, we take*

$$L(\sigma, u) = (|I(\sigma, u, v)| : v \in T(\sigma, u)) \ .$$

It is obvious (from Lemma 8.11) that J is non-empty, and also obvious that for all $(\sigma, u) \in J$, the sets $S(\sigma, u)$ and $T(\sigma, u)$ are non-empty; and for all $v \in T(\sigma, u)$, the set $I(\sigma, u, v)$ is non-empty. Thus $L(\sigma, u)$ is a nonvoid list of positive integers.

We shall now occupy ourselves with developing an algorithm which, when presented with any $(\sigma, u) \in J$, invariably produces, from the list $L(\sigma, u)$, another list which is $\sim$-equivalent to the list of block sizes of (X, E).

It is first necessary to learn how to count the sets $T(\sigma, u)$ and $I(\sigma, u, v)$ correlated with $(\sigma, u) \in J$.

Lemma 8.13 (Normalization Lemma)**.** *Suppose that $(\sigma, u) \in J$ and ν, ξ are polynomials of $\mathbf{R}$ such that $\xi\nu\sigma = \sigma$ (so that $\nu\sigma \in P_s^\diamond(\mathbf{R})$). Then $(\nu\sigma, \nu(u)) \in J$, $\nu|_{T(\sigma,u)}$ is a bijection of $T(\sigma, u)$ onto $T(\nu\sigma, \nu(u))$, and for all $v \in T(\sigma, u)$, $I(\sigma, u, v) = I(\nu\sigma, \nu(u), \nu(v))$.*

Proof. Assume that $\sigma \in P_s^\diamond(\mathbf{R})$ and ν, ξ are polynomials with $\xi\nu\sigma = \sigma$. It is easy to check that for any $\bar{c}, \bar{d} \in R^m$ we have $E(\sigma t_0, \bar{c}, \bar{d}) = E(\nu\sigma t_0, \bar{c}, \bar{d})$, $M'(\sigma t_0) = M'(\nu\sigma t_0)$, and $(\sigma, z, u, v, \bar{c}, \bar{d}_i\ (0 \leq i \leq M_0)) \in \Phi$ iff $(\nu\sigma, z, \nu(u), \nu(v), \bar{c}, \bar{d}_i\ (0 \leq i \leq M_0)) \in \Phi$. This lemma follows from these facts. □

Now choose any $(\sigma, u) \in J$. Our analysis of $L(\sigma, u)$ begins with an application of Lemma 8.10. We can write $\sigma(g/\Theta) = p(g)/\Theta$ with $p \in P_s^\diamond(\mathbf{D})$. By Definition 8.12(1), we have a system $(\sigma, z, u, v, \bar{c}, \bar{d}\,(0 \le i \le M_0)) \in \Phi$. Since $p(D)$ is polynomially isomorphic with $D(U)$, then for the polynomial q with $qp(D) = D(U)$ produced by Lemma 8.10, there is a polynomial q' with $q'qp = p$. Taking $\nu(g/\Theta) = q(g)/\Theta$ and $\xi(g/\Theta) = q'(g)/\Theta$, we can apply the Normalization Lemma to this situation.

Thus $(\nu\sigma, \nu(u)) \in J$ and $L(\nu\sigma, \nu(u))$ is essentially the same list as $L(\sigma, u)$—it just uses a different, but bijective, index set, $T(\nu\sigma, \nu(u))$ instead of $T(\sigma, u)$. So we can work with $(\nu\sigma, \nu(u))$ in place of (σ, u). Equivalently, and notationally more convenient, we make the following assumption.

Normalization Assumption: We have $\sigma(g/\Theta) = p(g)/\Theta$ where $p(D) = D(U)$. We have an $(0_A, \mu)$-trace $N \subseteq U$ and an element $a \in N$ with $u = \langle a \rangle/\Theta$. As usual, $\bar{a} \in A^k$ denotes a fixed tuple such that $s_{\bar{a}}(A) = U$; and $\bar{b} \in D^k$ is the k-tuple with $\bar{b}(x) = \bar{a}$ for all x. Until the end of this section, we hold $p, \sigma, N, a, u, \bar{a}, \bar{b}$ fixed and they satisfy the conditions stipulated here.

We shall use the fact that, by Claim 1, $u \cap D(U) = \langle a \rangle/\Theta \cap D(U) = \{\langle a \rangle\}$.

Definition 8.14. (1) *$\overline{S}$ is the set of all systems*

$$(t, \bar{u}, \bar{v}, w, \bar{e}_0, \bar{e}_1)$$

where $\bar{u} \in A^n$ for some $n \ge 0$, t is an $n+1$-ary term, $\bar{v} \in A^k$, $w \in A$, $\{\bar{e}_0, \bar{e}_1\} \subseteq A^m$ and $s_{\bar{a}} \circ t_{\bar{u}} \circ s_{\bar{v}} \in P_s^\diamond(\mathbf{A})$, and such that $(\bar{e}_0, \bar{e}_1) \in M(s_{\bar{v}} t_0)$ and

$$s_{\bar{a}} t_{\bar{u}} s_{\bar{v}} t_0(w, \bar{e}_1) \neq s_{\bar{a}} t_{\bar{u}} s_{\bar{v}} t_0(w, \bar{e}_0) = a\,;$$

and for some $\bar{u}' \in A^n$, $\bar{v}' \in A^k$, $\bar{e}_2 \in A^m$, $w_1, w_2 \in A$ we have

$$a = s_{\bar{a}} t_{\bar{u}'} s_{\bar{v}'} t_0(w_1, \bar{e}_2) \overset{tw}{\nsim} s_{\bar{a}} t_{\bar{u}'} s_{\bar{v}'} t_0(w_2, \bar{e}_2)\,.$$

(2) *$\overline{T}$ is the set of all $b \in U$ such that for some $(t, \bar{u}, \bar{v}, w, \bar{e}_0, \bar{e}_1) \in \overline{S}$, we have $b = s_{\bar{a}} t_{\bar{u}} s_{\bar{v}} t_0(w, \bar{e}_1)$.*

(3) *For $b \in \overline{T}$, $\overline{I}(b)$ is the set of all sets $E(s_{\bar{v}} t_0, \bar{e}_0, \bar{e}_1)$ where for some $t, \bar{u}, w$ we have $(t, \bar{u}, \bar{v}, w, \bar{e}_0, \bar{e}_1) \in \overline{S}$ and $b = s_{\bar{a}} t_{\bar{u}} s_{\bar{v}} t_0(w, \bar{e}_1)$.*

Claim 7: An element $v \in R(U)$ belongs to $T(\sigma, u)$ iff for some $b \in \overline{T}$ and for some block B of E, $v \cap D(U) = \{[a, b]_x : x \in B\}$ (i.e., if and only if $v = [a, b]_x/\Theta$ for some $x \in X$). Such an element v will be written as $v = v(b, B)$.

Claim 8: For $v = v(b, B) \in T(\sigma, u)$,

$$I(\sigma, u, v) = \big\{ i(x_0, C) :\ x_0 \in B \text{ and } C \in \overline{I}(b) \big\}$$

where $i(x_0, C) = \{f/\Theta \in R : f(x_0) \in C\}$.

Proof of Claim 7. Suppose first that $v \in T(\sigma, u)$, and choose a system $(\tau, z, \bar{c}, \bar{d}) \in S(\sigma, u)$ with $\tau t_0(z, \bar{d}) = v$. Since $\tau(R) = R(U)$ and $\tau \in P_s^\diamond(\mathbf{R})$, there is a polynomial $q \in P_s^\diamond(\mathbf{D})$ with $q(D) = D(U)$ and $\tau(g/\Theta) = q(g)/\Theta$ for all $g \in D$. We can represent q as $q = s_{\bar{b}} \circ t_{\bar{u}} \circ s_{\bar{v}}$ for some term t, with $\bar{u} \in D^n$ (say) and $\bar{v} \in D^k$.

Also, we choose $\bar{h}, \bar{k} \in D^m$ with $\bar{c} = \bar{h}/\Theta$, $\bar{d} = \bar{k}/\Theta$, and we choose $f \in D$ with $z = f/\Theta$.

Now $q t_0(f, \bar{h}) \in D(U) \cap \langle a \rangle/\Theta$, so by Claim 1,

$$q t_0(f, \bar{h}) = \langle a \rangle\,.$$

We have $(\bar{c}, \bar{d}) \in M'(s_{\bar{v}/\Theta} t_0)$; so by Claim 5, there is a unique $x = x_0 \in X$ for which $E(s_{\bar{v}(x)} t_0, \bar{h}(x), \bar{k}(x)) \neq A$ and for this x_0, we have $(\bar{h}(x_0), \bar{k}(x_0)) \in M(s_{\bar{v}(x_0)} t_0)$. According to Claim 5, the pair

$$(x_0, C) = \big(x_0, E(s_{\bar{v}(x_0)} t_0, \bar{h}(x_0), \bar{k}(x_0))\big)$$

is determined by $\tau, \bar{c}, \bar{d}$ and, in turn, this pair determines $E(\tau t_0, \bar{c}, \bar{d})$—in fact, $E(\tau t_0, \bar{c}, \bar{d}) = i(x_0, C)$.

Now $v = \tau t_0(z, \bar{d}) = q t_0(f, \bar{k})/\Theta$ and the function $q t_0(f, \bar{k})$ differs from $\langle a \rangle$ precisely at x_0, so we have $q t_0(f, \bar{k}) = [a, b]_{x_0}$ for some $b \neq a$. Since $(\bar{h}(x_0), \bar{k}(x_0)) \in M(s_{\bar{v}(x_0)} t_0)$, then it follows by Claim 2 that $(a, b) \in \mu|_U$, which means that $b \in N$.

We need to show that $b \in \overline{T}$. To accomplish this, we prove that

$$\rho = \big(t, \bar{u}(x_0), \bar{v}(x_0), f(x_0), \bar{h}(x_0), \bar{k}(x_0)\big) = (t, \bar{u}', \bar{v}', w, \bar{e}_0, \bar{e}_1)$$

belongs to $\overline{S}$. To begin, we observe that $s_{\bar{a}} \circ t_{\bar{u}'} \circ s_{\bar{v}'} \in P_s^\diamond(\mathbf{A})$ (by Lemma 8.1 and the fact that $\tau(R) = R(U)$). Also, $(\bar{e}_0, \bar{e}_1) \in M(s_{\bar{v}'} t_0)$ by construction. It remains to verify the condition in Definition 8.14 that refers to $\overset{\text{tw}}{\sim}$. To do that, recall that the definition of the property $(\bar{c}, \bar{d}) \in M'(\tau t_0)$ certainly implies that there are z_1, z_2 in R with $\tau t_0(z_1, \bar{c}) \overset{\text{tw}}{\not\sim} \tau t_0(z_2, \bar{c})$ in $R(U)$. We can assume that $\tau t_0(z, \bar{c}) \overset{\text{tw}}{\not\sim} \tau t_0(z_1, \bar{c})$ (by exchanging z_1 and z_2 if necessary). Let $z_1 = f_1/\Theta$, $f_1 \in D$.

By Lemmas 7.1 and 8.2, there must be $x_1 \in X$ such that where $\bar{u}'' = \bar{u}_{x_1}$, $\bar{v}'' = \bar{v}_{x_1}$, $w_1 = f(x_1)$, $w_2 = f_1(x_1)$, $\bar{e}_2 = \bar{h}(x_1)$ then

$$a = s_{\bar{a}} t_{\bar{u}''} s_{\bar{v}''} t_0(w_1, \bar{e}_2) \overset{\text{tw}}{\not\sim} s_{\bar{a}} t_{\bar{u}''} s_{\bar{v}''} t_0(w_2, \bar{e}_2)\,.$$

This concludes our proof of the forward implication in Claim 7.

Now for the converse, suppose that $v = [a, b]_{x_0}/\Theta$ where $x_0 \in X$, $x_0/E = B$, and $b \in \overline{T}$. We can choose $(t, \bar{u}, \bar{v}, w, \bar{e}_0, \bar{e}_1) \in \overline{S}$ with $b = s_{\bar{a}} t_{\bar{u}} s_{\bar{v}} t_0(w, \bar{e}_1)$. Also, we choose $w_1, w_2, \bar{u}', \bar{v}', \bar{e}_2$ satisfying

$$a = s_{\bar{a}} t_{\bar{u}'} s_{\bar{v}'} t_0(w_1, \bar{e}_2) \overset{\text{tw}}{\not\sim} s_{\bar{a}} t_{\bar{u}'} s_{\bar{v}'} t_0(w_2, \bar{e}_2)\,.$$

We are going to employ Claim 6. Put $w_0 = w$, $\bar{a}_0 = \bar{v}$, $\bar{a}_1 = \bar{v}'$.

Now we have

$$(\bar{a}_0, \bar{a}_1, \bar{e}_0, \bar{e}_1, \bar{e}_2, w_0, w_1, w_2) \in \Lambda\,.$$

By Claim 6, we have $(\bar{c}, \bar{d}) \in M'(\lambda t_0)$ where $\bar{c} = [\bar{e}_2, \bar{e}_0]_{x_0}/\Theta$, $\bar{d} = [\bar{e}_2, \bar{e}_1]_{x_0}/\Theta$, and $\lambda(g/\Theta) = s_{\bar{\ell}}(g)/\Theta$ with $\bar{\ell} = [\bar{v}', \bar{v}]_{x_0}$. We have, say, that $\bar{u} \in A^n$. Let us now put $\bar{k} = [\bar{u}', \bar{u}]_{x_0} \in D^n$ and put $q = s_{\bar{b}} \circ t_{\bar{k}}$ and for all $g \in D$ put $\gamma(g/\Theta) = q(g)/\Theta$. Finally, take $\tau = \gamma \circ \lambda$.

It is easy to see that $\tau \in P_s^\diamond(\mathbf{R})$, $\tau(R) = R(U)$, and since $(\bar{c}, \bar{d}) \in M'(\lambda t_0)$ then $(\bar{c}, \bar{d}) \in M'(\tau t_0)$. Now taking $z = [w_1, w_0]_{x_0}/\Theta$, we can verify that $\tau t_0(z, \bar{c}) = u$ and $\tau t_0(z, \bar{d}) = v$. Thus we have established that $v \in T(\sigma, u)$, finishing our proof of Claim 7. □

Proof of Claim 8. Let $b \in \overline{T}$, $B \in X/E$, and $v = v(b, B)$. To prove this claim we first take any set $Y \in I(\sigma, u, v)$. A glance at Definition 8.12 tells us that we can choose $(\tau, z, \bar{c}, \bar{d}) \in S(\sigma, u)$ so that $\tau t_0(z, \bar{d}) = v$ and $Y = E(\tau t_0, \bar{c}, \bar{d})$. We have $\tau(g/\Theta) = q(g)/\Theta$ where $q = s_{\bar{b}} \circ t_{\bar{u}} \circ s_{\bar{w}}$ for all $g \in D$, for a certain term t, $\bar{u} \in D^n$, $\bar{w} \in D^k$. We write $\bar{c} = \bar{h}/\Theta, \bar{d} = \bar{k}/\Theta$, $z = f/\Theta$. There is a unique $x_0 \in X$ such that $E(s_{\bar{a}} t_{\bar{u}(x_0)} s_{\bar{w}(x_0)} t_0, \bar{h}(x_0), \bar{k}(x_0)) \neq A$. We have $q t_0(f, \bar{h}) = \langle a \rangle$ since these two

elements of $D(U)$ are Θ-congruent. The element $pt_0(f, \bar{k}) \in D(U)$ is in v and differs from $\langle a \rangle$ only at x_0; therefore $x_0 \in B$ and we have

$$(qt_0(f, \bar{h}), qt_0(f, \bar{k})) = (\langle a \rangle, [a, b]_{x_0}) .$$

It should be clear from our proof of Claim 7 that, here, we have

$$C = E(s_{\bar{a}} t_{\bar{u}(x_0)} s_{\bar{w}(x_0)} t_0, \bar{h}(x_0), \bar{k}(x_0)) \in \overline{I}(b) .$$

Statement (2) in Claim 5 tells us that $Y = i(x_0, C)$.

For the converse, assume that $Y = i(x_0, C)$ where $x_0 \in B$ and $C \in \overline{I}(b)$. The reader will easily verify that the proof of Claim 7 contains the proof that $Y \in I(\sigma, u, v)$. This finishes the proof of Claim 8. □

Claim 9: For $(b, B), (b', B') \in \overline{T} \times X/E$ we have $v(b, B) = v(b', B')$ iff $(b, B) = (b', B')$. For $(b, B) \in \overline{T} \times X/E$ and $(x, C), (x', C') \in B \times \overline{I}(b)$, we have $i(x, C) = i(x', C')$ iff $(x, C) = (x', C')$.

Proof. The first statement of Claim 9 follows directly by Claim 1. For the second, suppose that $(x, C) \neq (x', C')$ but $i(x, C) = i(x', C')$. We can write $C = E(s_{\bar{v}} t_0, \bar{e}_0, \bar{e}_1)$ and write $C' = E(s_{\bar{v}'} t_0, \bar{e}'_0, \bar{e}'_1)$; and we know that $\emptyset \neq C \neq A$ and the same for C'. If, say, $x = x'$ and $C \neq C'$, there is a constant function $f = \langle j \rangle$ in D with $j \in C \setminus C'$ (or exchange C and C'). Now $f/\Theta \in i(x, C) = i(x, C')$, hence there is $f' \in f/\Theta$ with $f'(x) \in C'$. Since $\mathbf{A}$ is subdirectly irreducible with monolith μ, there is a polynomial function p of $\mathbf{A}$ with $s_{\bar{a}} p(f(x)) \neq s_{\bar{a}} p(f'(x))$. Where $\bar{p}$ is the polynomial of $\mathbf{D}$ which acts like $s_{\bar{a}} p$ at every coordinate, we have that $(\bar{p}(f), \bar{p}(f')) \in \Theta|_{D(U)}$. This contradicts Claim 1 since these functions are not equal and $\bar{p}(f)$ is a constant function.

Thus, we can assume that $x \neq x'$. We now choose $f \in D$ with $f(x) \notin C$ and $f(x') \in C'$. Since $i(x, C) = i(x', C')$, there is $f' \in f/\Theta$ with $f'(x) \in C$. Now $\Theta \leq \mu_X$ so $(f(x), f'(x)) \in \mu$; also $f(x) \notin C$, $f'(x) \in C$. This contradicts the fact that $C = E(s_{\bar{v}} t_0, \bar{e}_0, \bar{e}_1)$ is a union of μ-blocks, which is a consequence of the fact that $C(\mu, 1_A; 0_A)$ (Corollary 7.8). We have now concluded our proof of Claim 9. □

Claims 7, 8, 9 give that

$$L(\sigma, u) \sim \left(|\overline{I}(b)| \cdot |B| : (b, B) \in \overline{T} \times (X/E) \right) = \bar{t} \cdot \bar{e} ,$$

where $\bar{t} = (|\overline{I}(b)| : b \in \overline{T})$ and $\bar{e} = (|B| : B \in X/E)$. Recall that at the beginning of this proof, as we defined $\mathbf{R} = \mathbf{R}(X, E)$, we assumed that in the multi-set $\bar{e}$, the integer 1 occurs as a value precisely once and that all other values are greater than $2|A|^{k+2m}$. It is also true that every entry of $\bar{t}$ is no greater than $|A|^{k+2m}$. Thus let

$$L'(\sigma, u) = (|I(\sigma, u, v)| : v \in T(\sigma, u) \quad \text{and } |I(\sigma, u, v)| \leq M_0) .$$

It follows from the displayed formulas and observations above that $L'(\sigma, u) \sim \bar{t}$, and so

$$L(\sigma, u) \sim L'(\sigma, u) \cdot \bar{e} .$$

Recall that (σ, u) is essentially arbitrary. Now it follows by the Lovász cancellation theorem [14] that for each $(\sigma, u) \in J$, $\bar{e}$ is, up to $\sim$-equivalence, the unique multi-set $\bar{m}$ such that $L(\sigma, u) \sim L'(\sigma, u) \cdot \bar{m}$. This paragraph has revealed our procedure for recovering (X, E) up to isomorphism from $L(\sigma, u)$ (completely formulated

in the preceding sentence), and also has concluded our proof that the procedure works as advertised.

To conclude, let $n \geq M_3$, and let X be a set of cardinality $(M_0+1)n+1$. Partitions of n can be encoded faithfully as equivalence relations on X by multiplying all numbers by M_0+1 and adding the integer 1 as a new entry. Thus $\pi(n)$ is no greater than the number of non-isomorphic equivalence relation structures (X, E) on the given universe X that satisfy our initial conditions (E1) and (E2). The size of the set $G(X)$ of generators of $\mathbf{D}(X, E)$ is bounded above by

$$(2n \cdot M_0)^{M_2} |A|^{M_2}.$$

Thus, we have proved that

$$\pi(n) \leq n^{CM_2} \cdot C'$$

for certain constants C and C', and for all n. This contradicts a known result, mentioned in Section 4. With this contradiction, our proof of Theorem 7.3 is concluded.

Theorem 8.15. *$\mathcal{V}$ is Abelian.*

Proof. This follows from Theorems 6.3 and 7.3. □

9. The transfer principles and the decomposition

Definition 9.1. *We say that $\mathcal{V}$ satisfies the $(\mathbf{1}, \mathbf{2})$-transfer principle if there do not exist congruences $\alpha \prec \beta \prec \gamma$ on a finite algebra $\mathbf{A} \in \mathcal{V}$ such that*

1. *typ$(\alpha, \beta) = \mathbf{1}$ and typ$(\beta, \gamma) = \mathbf{2}$ and*
2. *the interval $I[\alpha, \gamma]$ in $\mathbf{Con}(\mathbf{A})$ is $\{\alpha, \beta, \gamma\}$.*

An equivalent condition is that whenever congruences $\alpha \prec \beta \prec \gamma$ on a finite algebra $\mathbf{A} \in \mathcal{V}$ satisfy (1), then there exists a congruence δ such that $\alpha \prec \delta \leq \gamma$ and typ$(\alpha, \delta) = \mathbf{2}$.

The $(\mathbf{2}, \mathbf{1})$-transfer principle is defined in the same way, exchanging the roles of $\mathbf{1}$ and $\mathbf{2}$.

We can apply Theorems 2.7 and 2.8 in K. Kearnes [9] to conclude that $\mathcal{V}$ decomposes as $\mathcal{V} = \mathcal{A} \otimes \mathcal{S}$ where $\mathcal{A}$ is affine and $\mathcal{S}$ is strongly Abelian, as soon as we have shown that $\mathcal{V}$ satisfies the $(\mathbf{1}, \mathbf{2})$ and the $(\mathbf{2}, \mathbf{1})$ transfer principles and that the following lemma holds.

We remark that this lemma, which we prove directly, is a consequence of Corollary 4.1 of E. W. Kiss, M. Valeriote [13], showing that a locally finite Abelian variety has the congruence extension property (i.e., CEP), and Theorem 2.13 of K. Kearnes [7], which proves that Lemma 9.2 holds for varieties with the CEP.

Lemma 9.2. *Suppose that $\mathbf{B}$ is a finite subdirectly irreducible algebra in $\mathcal{V}$ with monolith μ, $\mathbf{A}$ is a subalgebra of $\mathbf{B}$, typ$(0_B, \mu) = \mathbf{2}$, and ν is a congruence of $\mathbf{A}$ with $0_A \prec \nu \leq \mu|_A$. Then typ$(0_A, \nu) = \mathbf{2}$.*

Proof. Assume that typ$(0_A, \nu) \neq \mathbf{2}$. Then typ$(0_A, \nu) = \mathbf{1}$ and ν is a strongly Abelian congruence of $\mathbf{A}$ (since $\mathcal{V}$ is Abelian).

Let $U \in M_{\mathbf{B}}(0_B, \mu)$ and $(c, d) \in \nu \setminus 0_A$. Then $\mathbf{B}$ has a polynomial function f such that $(f(c), f(d)) \in U$, $f(c) \neq f(d)$. $\mathbf{B}$ has a polynomial (the pseudo-Maltsev

polynomial) $t(\bar{b}, x, y, z)$ such that $t(\bar{b}, f(c), f(d), f(d)) = t(\bar{b}, f(d), f(d), f(c))$ $(= f(c))$ while $t(\bar{b}, f(d), f(d), f(d)) \neq t(\bar{b}, f(d), f(d), f(c))$. Here $t(\bar{w}, x, y, z)$ is a term and $\bar{b}$ is a tuple listing all the elements of $\mathbf{B}$. We can also write $f(x) = s(\bar{b}, x)$ where $s(\bar{w}, x)$ is a term. Choosing any tuple $\bar{a}$ in $\mathbf{A}$, the Abelian property of $\mathbf{B}$ implies that

$$t(\bar{a}, s(\bar{a}, c), s(\bar{a}, d), s(\bar{a}, d)) = t(\bar{a}, s(\bar{a}, d), s(\bar{a}, d), s(\bar{a}, c)) \text{ while}$$
$$t(\bar{a}, s(\bar{a}, d), s(\bar{a}, d), s(\bar{a}, d)) \neq t(\bar{a}, s(\bar{a}, d), s(\bar{a}, d), s(\bar{a}, c))\,.$$

But this contradicts the assumption that ν is strongly Abelian in $\mathbf{A}$. □

We have found no quicker way to prove that $\mathcal{V}$ satisfies the $(\mathbf{1}, \mathbf{2})$ and the $(\mathbf{2}, \mathbf{1})$ transfer principles other than to repeat, with appropriate modifications, the arguments in R. McKenzie, M. Valeriote [15], Chapter 10. In [15], Chapter 8, it was shown that for any locally finite Abelian variety $\mathcal{W}$ that fails to satisfy one of these two transfer principles, some finite algebra in $\mathcal{W}$ contains one of three special configurations. With each configuration, a construction was given in Chapter 10 which served to semantically embed the class of all graphs into $\mathcal{W}$. We can use the same constructions, slightly altered, to produce a large number of non-isomorphic algebras, contradicting our assumption that $G_{\mathcal{V}}(n) \leq n^C$.

Configuration one. This is the configuraton of [15], Lemma 8.4, treated in Chapter 10 on pages 107–114: *We have a finite algebra* $\mathbf{A}$ *in* $\mathcal{V}$ *with congruences* $0_A \prec \alpha \prec \beta$ *such that typ*$(0_A, \alpha) = \mathbf{1}$ *and typ*$(\alpha, \beta) = \mathbf{2}$. *We have subsets* M, N, U, V *and elements* $0, 0', 1$ *satisfying* $N \subseteq V \subseteq U$, $M \subseteq U$, $M \cap N = \{0\}$, $0' \in M \setminus N$, *and* $1 \in N \setminus M$. M *is a* $(0_A, \alpha)$*-trace and* $U \in M_{\mathbf{A}}(0_A, \alpha)$. N *is a* (α, β)*-trace and* $V \in M_{\mathbf{A}}(\alpha, \beta)$.

Let n be a positive integer. There are pairwise non-isomorphic symmetric graphs without loops, $\mathbf{G}_1, \mathbf{G}_2, \ldots, \mathbf{G}_k$ $(k = n^n)$, such that every $\mathbf{G}_i$ has the same set G of vertices, $v = |G| = 2n + 9$, and every graph $\mathbf{G}_i$ has precisely $e = 5n + 5$ edges. (These graphs encode all the self-maps of an n-element set.) With each of these graphs $\mathbf{G} = \mathbf{G}_i$, we construct an algebra $\mathbf{A}(\mathbf{G}) \leq \mathbf{A}^X$, $|X| = v + 2$. This is the algebra constructed on page 109 of [15] with one minor difference. For generators, we take the set $G^\star = \{f_v : v \in G\}$, together with the set $E^\star = \{f_e^i : i \in \{1, 2\},\ \ e \text{ an edge of } \mathbf{G}\}$ and the set of all constant functions $\hat{a}$, $a \in A$, just as in [15]; but we replace the additional generators in the set $N^\star = \{f \in N^X : f(p_1) = f(p_2)\}$ by the subset of $N^\star$ consisting of the functions f'_v (identical with f_v except that $f'_v(p_2) = 0$) and the functions f'_e (identical to f_e^1 and to f_e^2 except that $f'_e(p_1) = f'_e(p_2) = 0$). Thus the algebra $\mathbf{A}(\mathbf{G})$ has

$$g = a + 2v + 3e = a + 19n + 33$$

generators altogether, where $a = |A|$.

Now the proof in [15], pp. 109–114, will show that $\mathbf{G}$ is recoverable from $\mathbf{A}(\mathbf{G})$ using second-order formulas with the parameters $\hat{a}$, $a \in A$. The formulas are identical to the first order formulas used in [15], except that we use quantification over the set of <u>all</u> "collapsing" polynomial functions, rather than the selected finite list of them. This means that in the next to the last paragraph on page 110, we simply have $\mu = t(\nu_1, \ldots, \nu_k)$, $\nu_j \in G^\star \cup E^\star$, and so we also have $\mu = t(\nu'_1, \ldots, \nu'_k)$, since t is a collapsing function, where $\nu'_j \in N^\star$ are among the functions we included as generators. This is the only modification that needs to be made in the argument.

Now write $\mathbf{A}_i$ for $\mathbf{A}(\mathbf{G}_i)$. Then where $\Phi(\bar{x})$ is the system of second-order formulas we are using to recover $\mathbf{G}$, and $\bar{a} \in (A^X)^a$ is the tuple of all constant functions, we have that $\mathbf{G}_i \cong \Phi^{\mathbf{A}_i}(\bar{a})$—the graph defined in $\mathbf{A}_i$ by the formulas $\Phi(\bar{a})$ with parameters $\bar{a}$. Suppose that $i_0 \neq i_1$ and $\mathbf{A}_{i_0} \cong \mathbf{A}_i \cong \mathbf{A}_{i_1}$ under maps $\sigma_{i_j} : \mathbf{A}_{i_j} \cong \mathbf{A}_i$. Then $\sigma_{i_0}(\bar{a}) \neq \sigma_{i_1}(\bar{a})$, since $\mathbf{G}_{i_j} \cong \Phi^{\mathbf{A}_i}(\sigma_{i_j}(\bar{a}))$ while $\mathbf{G}_{i_0} \ncong \mathbf{G}_{i_1}$. Hence the number of $\mathbf{A}_j$ with $\mathbf{A}_j \cong \mathbf{A}_i$ is no greater than $|A_i|^a$.

Recall from J. Berman, R. McKenzie, [3] that since $\mathbf{A}$ is Abelian, there is a constant c such that for all m, $|\mathbf{F}_{V(\mathbf{A})}(m)| \leq 2^{cm}$. Thus, the number of distinct a-tuples of elements of $\mathbf{A}_i$ is at most 2^{acg}. We conclude that among the $\mathbf{A}_i$ there are no fewer than

$$\frac{n^n}{2^{acg}} = \frac{n^n}{2^{ac(a+19n+33)}}$$

non-isomorphic algebras. I.e., we have that

$$G_{\mathcal{V}}(a+19n+33) \geq \frac{n^n}{2^{ac(a+19n+33)}} = 2^{n(\log n)-(b+dn)}\,,$$

for all n, for certain positive integral constants b and d. This is clearly impossible, because $G_{\mathcal{V}}(n) \leq n^C$, while $n(\log n) - (b + dn) \geq n$ for large n.

We remark that it follows from the above analysis that if configuration one can be found in some finite algebra of $\mathcal{V}$, then $G_{\mathcal{V}}(M) \geq M^{kM}$ for some positive constant k and for infinitely many values of M.

Configuration two. This is the configuration of [15], page 115, Lemma 10.2: *We have a finite algebra* $\mathbf{A}$ *in* $\mathcal{V}$ *and congruences* $0_A \prec \alpha \prec \beta$ *such that typ*$(0_A, \alpha) =$ **2** *and typ*$(\alpha, \beta) =$ **1**. *We have sets* $\{0,1\} \subseteq M \subseteq U, \{a,b\} \subseteq N \subseteq V$ *and a polynomial function* f *of* $\mathbf{A}$ *satisfying the following.* M *is a* $(0_A, \alpha)$*-trace and* $U \in M_{\mathbf{A}}(0_A, \alpha)$. N *is an* (α, β)*-trace and* $V \in M_{\mathbf{A}}(\alpha, \beta)$. $f(A) \subseteq U$, $f(N) \subseteq M$, $f(\alpha|_V) \subseteq 0_U$, *and* $0 = f(a) \neq f(b) = 1$.

Here, the construction and proof in [15], pages 115–120 require no changes. The concluding argument, to deduce that $G_{\mathcal{V}}$ is of exponential growth, is essentially the same as for the first configuration. This time, we are using $g = a + 1 + v + 2e$ and using $a + 1$ parameters.

Configuration three. This is the configuration of [15], page 121, Lemma 10.4: *We have a finite algebra* $\mathbf{A}$ *in* $\mathcal{V}$ *and congruences* $0_A \prec \alpha \prec \beta$ *such that typ*$(0_A, \alpha) =$ **2** *and typ*$(\alpha, \beta) =$ **1**. *We have subsets* $M \subseteq U \subseteq V$ *and* $\{a,b\} \subseteq N \subseteq V$ *and a polynomial function* f *of* $\mathbf{A}$ *satisfying the following.* M *is a* $(0_A, \alpha)$*-trace, and* $U \in M_{\mathbf{A}}(0_A, \alpha)$. N *is an* (α, β)*-trace* N*, and* $V \in M_{\mathbf{A}}(\alpha, \beta)$. $f(A) = f(U) = U$, $f(N) \subseteq M$ *and* $f = f^2$*; moreover* $(a,b) \in \beta \setminus \alpha$ *and* $(f(a), f(b)) \in \alpha \setminus 0_A$. *Finally, for every polynomial function* g *in* $\mathbf{A}$, *if* $g(\beta|_V) \subseteq \alpha$ *and* $g(\alpha|V) \subseteq 0_A$, *then* $g(\beta|_V) \subseteq 0_A$.

Here, the construction and proof in [15], pages 121–126 requires only the following modifications. We omit the subset $M^\star$ from the generators. It is not required since we are not restricted to first order formulas and can use quantification over the set of all collapsing functions. Then Lemma 10.5 is not required. In building the formula Alpha(x) for Claim 2 on page 123, we use quantification over all collapsing functions, rather than just over those belonging to I. The proof of Claim 2 is then simplified.

The concluding argument, to deduce that $G_{\mathcal{V}}$ is of exponential growth, is again almost the same as in the argument proceeding from the first configuration. This time, we are using $g = a + 2 + 2v + 2e$ and using $a + 2$ parameters.

Theorem 9.3. *$\mathcal{V}$ has the transfer principles.*

Proof. It follows from the arguments of R. McKenzie, M. Valeriote [15], modified as indicated above. □

Corollary 9.4. *$\mathcal{V}$ has an affine subvariety $\mathcal{A}$ and a strongly Abelian subvariety $\mathcal{S}$ such that $\mathcal{V} = \mathcal{A} \otimes \mathcal{S}$. We have $G_{\mathcal{V}}(n) = G_{\mathcal{A}}(n) \cdot G_{\mathcal{S}}(n)$ for all positive integers n.*

Proof. By Theorems 2.7 and 2.8 of K. Kearnes [9], it follows from Theorem 8.15, Lemma 9.2 and Theorem 9.3 that $\mathcal{V}$ factors as stated. The product formula for $G_{\mathcal{V}}(n)$ is immediate. □

10. The character of **S** and **A**

It is clear that $\mathcal{A} \otimes \mathcal{S}$ has polynomially many models iff each of $\mathcal{A}$ and $\mathcal{S}$ has this property. It is proved in P. Idziak, R. McKenzie [6] that a locally finite affine variety $\mathcal{A}$ has polynomially many models if and only if it is directly representable—that is, if and only if the ring of $\mathcal{A}$ is a finite ring of finite representation type.

We have now to deal with a locally finite strongly Abelian variety $\mathcal{S}$ with the property that $G_{\mathcal{S}}(n) \leq n^C$ for some positive integer C and all natural numbers $n \geq 2$. We will show that $\mathcal{S}$ decomposes as a varietal product of a sequence of varieties equivalent to matrix powers of varieties of H-sets, with constants, for various finite groups H. As a converse, we will show that for any variety $\mathcal{V}$ of this type, $G_{\mathcal{V}}$ is bounded by some polynomial.

Although the main result of this section does not refer to multi-sorted algebras and varieties, we deal with them at several intermediate steps in our proof. Recall that a multi-sorted algebra consists of a finite number of non-empty, pair-wise disjoint universes, along with a set of functions defined on those universes. Since we will be referring to parts of the book [15] in this section, we will adopt the formalism of Chapter 11 of that book when dealing with multi-sorted algebras and varieties. We also extend the scope of the function $G_{\mathcal{V}}$ to include multi-sorted varieties $\mathcal{V}$, in the expected manner.

An n-ary decomposition operation on a set A is a function $d(x_1, \ldots, x_n)$ which satisfies the equations:

$$\begin{aligned} d(x, \ldots, x) &\approx x \\ d(d(x_1^1, \ldots, x_n^1), \ldots, d(x_1^n, \ldots, x_n^n)) &\approx d(x_1^1, x_2^2, \ldots, x_n^n) \end{aligned}$$

A term $t(\bar{x})$ of a variety $\mathcal{V}$ is called a decomposition term for $\mathcal{V}$ if $t^{\mathbf{A}}$ is a decomposition operation on A for every algebra $\mathbf{A} \in \mathcal{V}$.

In Chapter 11 of [15] it is shown how to associate a k-sorted variety $\mathcal{V}[d]$ to a variety $\mathcal{V}$ equipped with a k-ary decomposition term d so that many properties are shared by $\mathcal{V}$ and $\mathcal{V}[d]$. In particular $\mathcal{V}$ and $\mathcal{V}[d]$ are equivalent (as categories) and one is strongly Abelian if and only if both are. It is also pointed out that every variety of k-sorted algebras is term equivalent to a variety of the form $\mathcal{W}[e]$ for some one-sorted variety $\mathcal{W}$ and some decomposition term $e(x_1, \ldots, x_k)$ of $\mathcal{W}$.

For d a decomposition term of $\mathcal{V}$ and any $\mathbf{A} \in \mathcal{V}$ we can define a k-sorted algebra $\mathbf{A}[d]$ that is intimately associated with $\mathbf{A}$. Since d is a decomposition term for $\mathcal{V}$ then we may assume that the universe of $\mathbf{A}$ is equal to the set $A_1 \times \cdots \times A_k$ for some sets A_i and such that $d^{\mathbf{A}}$ is equal to the decomposition operation on this product, i.e., $d(\vec{a}_1, \ldots, \vec{a}_k) = (a_1^1, a_2^2, \ldots, a_k^k)$ for all $\vec{a}_i = (a_i^1, a_i^2, \ldots, a_i^k) \in A$.

Every n-ary operation on A is determined by the sequence of k multi-sorted functions $\langle p_1 f, \ldots, p_k f \rangle$, where

$$p_i f : A_1^n \times \cdots \times A_k^n \longrightarrow A_i,$$

has the property that if $\vec{a}_i = (a_i^1, \ldots, a_i^k) \in A$, for $1 \leq i \leq n$, and if

$$\vec{b} = (a_1^1, \ldots, a_n^1, \ldots, a_1^k, \ldots, a_n^k),$$

then

$$f(\vec{a}_1, \ldots, \vec{a}_n) = (p_1 f(\vec{b}), \ldots, p_k f(\vec{b})).$$

We define the type T of $\mathbf{A}[d]$ by first supposing that $\mathcal{V}$ is a variety in the language $\mathsf{L} = (\Phi, \rho)$. We put $\mathsf{T} = (k, \Phi', \tau)$, where $\Phi' = \Phi \times \{1, \ldots, k\}$, and for $\langle f, j \rangle \in \Phi'$ we put

$$\tau(\langle f, j \rangle) = \langle 1, \ldots, 1, 2, \ldots, 2, \ldots, k, \ldots, k, j \rangle,$$

consisting of n occurrences each of 1, 2, $\ldots, k$ and a final j, where $n = \rho(f)$, the arity of the function symbol f. Now we define

$$\mathbf{A}[d] = \langle A_1, \ldots, A_k; p_j f^{\mathbf{A}}(\langle f, j \rangle \in \Phi') \rangle,$$

a k-sorted algebra of type T. So, the basic operations of $\mathbf{A}[d]$ consist of the projections of the basic operations of $\mathbf{A}$ onto each of the factors A_i.

If we denote the class of all k-sorted algebras of type T which are isomorphic to an algebra of the form $\mathbf{A}[d]$ for some $\mathbf{A} \in \mathcal{V}$ by $\mathcal{V}[d]$ then Lemma 11.8 of [15] shows that $\mathcal{V}[d]$ is a variety of k-sorted algebras.

For a locally finite strongly Abelian variety $\mathcal{V}$ there is a natural number N such that no term operation of any member of $\mathcal{V}$ can depend on more than N variables (see Lemma 10.2). From this it follows that there is a largest integer n such that $\mathcal{V}$ has an n-ary decomposition term $d(\bar{x})$ which depends on all of its variables. Theorem 11.9 of [15] states that if $\mathcal{V}[d]$ is not essentially unary, then the variety $\mathcal{V}$ is hereditarily undecidable. This theorem is established by showing that if $\mathcal{V}[d]$ is not essentially unary, then the class of bi-partite graphs can be semantically embedded into $\mathcal{V}[d]$ (and hence into $\mathcal{V}$). By using essentially the same techniques and arguments we prove:

Theorem 10.1. *If $\mathcal{V}$ is a locally finite strongly Abelian variety with $G_{\mathcal{V}}$ bounded by a polynomial and $d(x_1, \ldots, x_n)$ is an essentially n-ary decomposition term for $\mathcal{V}$ of maximal arity then the n-sorted variety $\mathcal{V}[d]$ is essentially unary.*

Before proving this theorem we first point out useful, but elementary facts about strongly Abelian varieties.

Lemma 10.2. *Let $\mathcal{V}$ be a locally finite strongly Abelian variety and let $d(\bar{x})$ be an n-ary decomposition term of $\mathcal{V}$.*

1. *There is a finite upper bound to the number of variables any term of $\mathcal{V}$ or $\mathcal{V}[d]$ depends upon.*
2. *The size of the finitely generated $\mathcal{V}$ ($\mathcal{V}[d]$)-free algebras can be bounded by a polynomial in the number of free generators.*

(3) *$G_{\mathcal{V}}$ is bounded by a polynomial if and only if $G_{\mathcal{V}[d]}$ is.*

Proof. A proof of item (1) (for $\mathcal{V}$) may be found in [15], Theorem 0.17. The multi-sorted version follows from the fact that every term of $\mathcal{V}[d]$ arises as a projection of a term from $\mathcal{V}$ and so cannot depend on more than n-times the number of variables that the original term depended on.

Item (2) follows from (1) since the elements of a k-generated $\mathcal{V}$ or $\mathcal{V}[d]$-free algebra correspond to the number of distinct terms over a set of k variables (up to $\mathcal{V}$ or $\mathcal{V}[d]$-equivalence). As the number of variables that any term can depend on in the variety is bounded by a fixed integer then the number of terms (up to equivalence in the variety) is bounded by some polynomial.

Let $\mathbf{A}$ be a k-generated element of $\mathcal{V}$. We may assume that the universe of $\mathbf{A}$ is equal to the product $A_1 \times \cdots \times A_n$ for some nonempty sets A_i and that $d^{\mathbf{A}}$ is equal to the decomposition operation on this product. The associated algebra $\mathbf{A}[d]$ is generated by at most kn elements, namely, the set of kn components of the k generators of $\mathbf{A}$. From this we can deduce that $G_{\mathcal{V}}(k) \leq G_{\mathcal{V}[d]}(kn)$ for all k.

Conversely, let $\mathbf{B}$ be a k-generated member of $\mathcal{V}[d]$ and suppose that it is generated by the k elements $b_1, \ldots, b_k$. We may assume that $\mathbf{B}$ is equal to an algebra of the form $\mathbf{A}[d]$ for some algebra $\mathbf{A} \in \mathcal{V}$. Let a be some arbitrary member of A and, for each generator b_i, define a_i to be the unique element of A which is equal to a in every coordinate except possibly at $\sigma(b_i)$, where it is equal to b_i. For $b \in B$, $\sigma(b)$ denotes the sort of the element b.

We claim that the elements $a_1, \ldots, a_k$ of A form a generating set for $\mathbf{A}$. If we let $\mathbf{C}$ be the subalgebra of $\mathbf{A}$ that these elements generate then we see that $\mathbf{C}[d]$ (a subalgebra of $\mathbf{A}[d]$) will contain the b_i and so must be equal to $\mathbf{A}[d]$. From this it follows that $\mathbf{C}$ is equal to $\mathbf{A}$, as required. We can conclude from this that $G_{\mathcal{V}[d]}(k) \leq G_{\mathcal{V}}(k)$ for all k since each k-generated member of $\mathcal{V}[d]$ arises from a k-generated member of $\mathcal{V}$.

Thus if either of $G_{\mathcal{V}}$ or $G_{\mathcal{V}[d]}$ can be bounded by a polynomial then both of them can. □

Proof of Theorem 10.1. Let $d(x_1, \ldots, x_n)$ be a decomposition term for $\mathcal{V}$ of maximal arity. By Lemma 10.2 (3) it suffices to show that if $\mathcal{V}[d]$ is not essentially unary then $G_{\mathcal{V}[d]}$ is not bounded by a polynomial.

Under the assumption that $\mathcal{V}[d]$ is not essentially unary, the proof of Theorem 11.9 from [15] provides a method for building a finite algebra $\mathbf{S}[\mathbf{G}] \in \mathcal{V}[d]$, for every finite bi-partite graph $\mathbf{G}$, from which $\mathbf{G}$ can be recovered, up to isomorphism, using a first order interpretation scheme. The algebra $\mathbf{S}[\mathbf{G}]$ is generated by at most $2k^2 + k + n$ elements, where $|G| = k$.

Since the interpretation scheme that is employed in Theorem 11.9 to recover $\mathbf{G}$ employs a fixed number of parameters (independent of the size of $\mathbf{G}$) then we cannot conclude that the isomorphism type of $\mathbf{S}[\mathbf{G}]$ determines the isomorphism type of $\mathbf{G}$. What we now argue is that the isomorphism type of the algebra determines a "small" number of bi-partite graphs, up to isomorphism. Each choice of a sequence of parameters from $\mathbf{S}[\mathbf{G}]$ will determine some (possibly degenerate) finite bi-partite graph and so it will suffice to show that the number of sequences that can be selected is small, relative to the number of k-element bi-partite graphs.

Let $\mathbf{G}$ be a finite bi-partite graph of size k and let $f(x)$ be a polynomial that bounds the size of the $\mathcal{V}[d]$-free algebras, as a function of the number of free generators of the algebra (see Lemma 10.2(2)). Since $\mathbf{S}[\mathbf{G}]$, the algebra constructed from $\mathbf{G}$ in the proof of Theorem 11.9 of [15], is generated by at most $2k^2 + k + n$ elements then the size of this algebra is bounded by $f(2k^2 + k + n)$.

Let N be the number of parameters that are used in the interpretation scheme found in the proof of Theorem 11.9. (N is equal to the number of elements of a certain finite member of $\mathcal{V}[d]$.) If we let $p(k)$ denote the polynomial $f(2k^2+k+n)^N$ then we know that there are at most $p(k)$ distinct sequences of elements from $\mathbf{S}[\mathbf{G}]$ of length N. Using the interpretation scheme from the proof of Theorem 11.9, each such sequence determines some finite bi-partite graph and so the set of finite bi-partite graphs that can be recovered, up to isomorphism, from $\mathbf{S}[\mathbf{G}]$ using the interpretation scheme from Theorem 11.9 and some choice of parameters is bounded by $p(k)$.

Up to isomorphism, the number of algebras of the form $\mathbf{S}[\mathbf{G}]$ for some k-element bi-partite graph $\mathbf{G}$ is at most $G_{\mathcal{V}[d]}(2k^2+k+n)$, since each such algebra is generated by at most $2k^2+k+n$ elements. Since the isomorphism type of each algebra of this kind determines (using the interpretation scheme) a set of finite bi-partite graphs of size at most $p(k)$ and each k-element bi-partite graph lies in at least one of these sets, then an upper bound for the number of isomorphism types of k-element bi-partite graphs is given by:

$$G_{\mathcal{V}[d]}(2k^2 + k + n)p(k).$$

If $k = 4m$ then a lower bound for the number of isomorphism types of k-element bi-partite graphs is given by m^m and so we conclude that

$$m^m \leq G_{\mathcal{V}[d]}(32m^2 + 4m + n)p(4m)$$

for all natural numbers m. Since $p(x)$ is a polynomial, it follows that the function $G_{\mathcal{V}[d]}$ cannot be bounded by any polynomial. □

We now set out to prove that unless all non-constant unary terms of a multi-sorted unary variety $\mathcal{V}$ are invertible then the function $G_{\mathcal{V}}(n)$ cannot be bounded by a polynomial.

Definition 10.3. *Let $\mathcal{V}$ be a multi-sorted unary variety.*

1. *Call a term $t(x)$ of $\mathcal{V}$ invertible if there is a term $s(y)$ (of the appropriate sort) such that $\mathcal{V} \models s(t(x)) \approx x$.*
2. *The term $t(x)$ of $\mathcal{V}$ will be called constant if $\mathcal{V} \models t(x) \approx t(y)$.*
3. *A sort i of $\mathcal{V}$ will be called non-invertible if there is a non-invertible, non-constant term $t(x)$ of $\mathcal{V}$ with the sort of the variable x equal to i.*
4. *The scope of a sort i of $\mathcal{V}$, denoted by $\mathsf{Scope}(i)$, is defined to be*

$$\{j : \text{there is some term } t(x) \text{ with domain of sort } i \text{ and range of sort } j\}$$

$$\cup \{j : \text{there is a constant symbol of } \mathcal{V} \text{ of sort } j\}.$$

For $\mathbf{A} \in \mathcal{V}$ and $a \in A$, $\mathsf{Scope}(a)$ is set to $\mathsf{Scope}(i)$, where i is the sort of a.

Theorem 10.4. *Let $\mathcal{V}$ be an n-sorted unary variety with the function $G_{\mathcal{V}}$ bounded by a polynomial. Then all non-constant unary terms $t(x)$ of $\mathcal{V}$ are invertible.*

Proof. Without loss of generality we may assume that each sort of $\mathcal{V}$ is non-trivial and so if $\mathcal{V} \models x \approx y$ then the variables x and y are the same. Assume that some non-constant term of $\mathcal{V}$ is not invertible. We will interpret finite equivalence relations into $\mathcal{V}$ in a manner that will allow us to conclude that $G_{\mathcal{V}}$ cannot be bounded by a polynomial.

For $\mathbf{A} \in \mathcal{V}$ and $a \in A$ let $S(a)$ denote the subuniverse of $\mathbf{A}$ generated by $\{a\}$. Note that $S(a)$ is the universe of a subalgebra of $\mathbf{A}$ if and only if $\mathsf{Scope}(a) = \{1, \dots, n\}$. Define the quasi-order $\preceq$ on A by: $a \preceq b$ if and only if $S(a) \subseteq S(b)$ and write $a \simeq b$ if and only if $S(a) = S(b)$. So, $a \preceq b$ if and only if there is some term $t(x)$ with $t(b) = a$ or a is a constant of $\mathbf{A}$.

For each $i \leq n$, let $\mathbf{x_i}$ be a free generator of sort i and let $\mathbf{F}$ be the $\mathcal{V}$-free algebra generated by $\{\mathbf{x_1}, \dots, \mathbf{x_n}\}$. Select a non-invertible sort i with the property that: $\mathsf{Scope}(i)$ is maximal in the set

$$\{\mathsf{Scope}(j) : j \text{ is a non-invertible sort}\}.$$

We may assume that $i = 1$. By the maximality of $\mathsf{Scope}(1)$ we can conclude that if $j \notin \mathsf{Scope}(1)$ then there is no non-constant unary term of $\mathcal{V}$ with domain of sort j and range 1.

Let $\mathbf{E} = \langle X, E \rangle$ be an equivalence relation on the finite set X and let $\mathbf{F}_X$ be the $\mathcal{V}$-free algebra freely generated by the set $X \cup \{\mathbf{y_j} : j \notin \mathsf{Scope}(1)\}$, where the elements of X are treated as elements of sort 1 and $\mathbf{y_j}$ an element of sort j. We may assume that the $\mathbf{y_j}$ are not members of X. Note that by design each sort of $\mathbf{F}_X$ will be non-empty since we have included elements $\mathbf{y_j}$ of all sorts j which are not in $\mathsf{Scope}(1)$.

Let θ_E be the congruence of $\mathbf{F}_X$ generated by the set

$$\{(t(u), t(v)) \quad : \quad t(x) \text{ is a non-invertible term of } \mathcal{V} \text{ with domain of sort 1 and } (u, v) \in E\}.$$

Let $\mathbf{A}[\mathbf{E}]$ be the algebra $\mathbf{F}_X/\theta_E$.

Claim 1:

(1) If $u \in X$ and $t(x)$ is an invertible term of $\mathcal{V}$ with domain of sort 1 then $t(u)/\theta_E = \{t(u)\}$.
(2) If $u \in X$ and $t(x)$ is a non-invertible term of $\mathcal{V}$ with domain of sort 1 then $t(u)/\theta_E = \{t(v) : (u, v) \in E\}$.
(3) The elements of X are in one-to-one correspondence with the $\simeq$-classes of the elements of $\mathbf{A}[\mathbf{E}]_1$ which are maximal in $\mathbf{A}[\mathbf{E}]$ with respect to the quasi-order $\preceq$.

To show (1), suppose that $c \in \mathbf{F}_X$ with $(t(u), c) \in \theta_E$ and $t(u) \neq c$. Then there are unary terms $r(y)$ and $s(x)$ and $(a, b) \in E$ with s non-invertible and $rs(a) = t(u) \neq rs(b)$. Since t is invertible and both a and u are free generators of $\mathbf{F}_X$ then we conclude that $a = u$ and that the term s must be invertible, contrary to our assumptions.

To establish (2) it suffices to show that if $(a, b) \in E$ and $s(x)$ is a non-invertible term with domain of sort 1 and $r(y)$ is any term of $\mathcal{V}$ with $rs(a) = t(v)$ for some $v \in X$ with $(u, v) \in E$ then $rs(b) = t(w)$ for some $w \in X$ with $(u, w) \in E$. If t is a constant term of $\mathcal{V}$ then we also have that $rs(b) = t(v)$, as required. If t is not constant then since a and v are free generators of $\mathbf{F}_X$ we have that $a = v$ and so $(v, b) \in E$ and $rs(b) = t(b)$, as required.

For (3), we will first establish that $\bar{u} = u/\theta_E$ is maximal with respect to $\preceq$ in $\mathbf{A}[\mathbf{E}]$ for any $u \in X$. Suppose that there is some element $a \in \mathbf{A}[\mathbf{E}]$ with $\bar{u} \preceq a$. Then there is some term $t(x)$ with $\bar{u} = t(a)$ and some element $c \in \mathbf{F}_X$ with $a = c/\theta_E$. Then we have that $(u, t(c)) \in \theta_E$ and so $u = t(c)$ by (1). Either c is the value of some constant of $\mathcal{V}$ or it can be written as $r(b)$ for some free generator b of $\mathbf{F}_X$ and some non-constant term r. The former can't hold since the free generator u would be constant and if the latter holds, then we would have that $u = t(r(b))$ holds in $\mathbf{F}_X$. As u and b are free generators, we conclude that $u = b$ and thus $r(\bar{u}) = a$ in $\mathbf{A}[\mathbf{E}]$. So, $a \preceq \bar{u}$ as required.

By choice, the sort 1 has the property that $\mathsf{Scope}(1)$ is maximal amongst those sorts which are non-invertible, and so if j is not a member of this set, then there is no non-constant term $t(x)$ whose range is of sort 1 and whose domain is of sort j. If $a \in \mathbf{A}[\mathbf{E}]_1$ then it is either the value of some constant term of $\mathcal{V}$ or it is of the form $t(g/\theta_E)$ for some (free) generator g of $\mathbf{F}_X$ and some non-constant term t whose range has sort 1. If the former holds, then the $\simeq$-class of a cannot be maximal with respect to $\preceq$. In the latter case we have that $a \preceq g/\theta_E$. As t is non-constant, then the generator g must belong to the set X since, as noted earlier, there is no non-constant unary term whose range is of sort 1 and whose domain has some sort not in $\mathsf{Scope}(1)$. Thus, the only maximal elements of $\mathbf{A}[\mathbf{E}]_1$ with respect to $\preceq$ are $\simeq$-related to x/θ_E for some $x \in X$.

To conclude the proof of (3) we need only establish that if $a \neq b \in X$ then $a/\theta_E \not\simeq b/\theta_E$. If, on the contrary, $a/\theta_E \simeq b/\theta_E$ then there is some unary term $t(x)$ with $t(a/\theta_E) = b/\theta_E$, or $(t(a), b) \in \theta_E$. Since b is a free generator of $\mathbf{F}_X$ we have that $t(a) = b$ and so we must have that $a = b$.

The claim establishes that we can recover the set of vertices of the graph $\mathbf{E}$ from the isomorphism type of $\mathbf{A}[\mathbf{E}]$ and the next claim shows that the edge relation can also be recovered.

Claim 2: For u, $v \in X$, $(u, v) \in E$ if and only if there are a, $b \in \mathbf{A}[\mathbf{E}]_1$ with $a \simeq u/\theta_E$, $b \simeq v/\theta_E$ and $t(a) = t(b)$ for all non-invertible terms $t(x)$ of $\mathcal{V}$ with domain of sort 1.

One direction of this claim is immediate from the definition of the congruence θ_E. For the converse, suppose that $a \simeq u/\theta_E$ and $b \simeq v/\theta_E$. Then there are invertible terms r and s with $a = r(u/\theta_E)$ and $b = s(v/\theta_E)$. Let $t(x)$ be some non-invertible, non-constant term of $\mathcal{V}$ with domain of sort 1. The equality $t(a) = t(b)$ implies that $(t(r(u)), t(s(v)) \in \theta_E$. Since the term $t(r(x))$ is non-invertible, then by (2) of Claim 1 we conclude that $t(s(v)) = t(r(w))$ for some $w \in X$ with $(u, w) \in E$. Since t is non-constant and r and s are invertible, then ts and tr are non-constant and so $v = w$, as required.

Thus the isomorphism type of the equivalence relation $\mathbf{E}$ can be recovered from the isomorphism type of the algebra $\mathbf{A}[\mathbf{E}]$. Since this algebra is generated by at most $|X|+n$ elements then a lower bound for the function $G_{\mathcal{V}}(k+n)$ is the function $\Pi(k)$, the number of k-element equivalence relations, up to isomorphism. It was noted earlier that

$$\Pi(k) \sim \frac{1}{4k\sqrt{3}} e^{\left(\pi\sqrt{\frac{2k}{3}}\right)}.$$

and so $\Pi(k)$ cannot be bounded from above by any polynomial. Thus the function $G_V(k)$ cannot have this property if $\mathcal{V}$ has a non-constant, non-invertible term. $\square$

Theorem 10.5. *Let $\mathcal{V}$ be a locally finite strongly Abelian variety. Then $G_{\mathcal{V}}$ is bounded above by a polynomial if and only if $\mathcal{V}$ is term equivalent to a varietal product of a sequence of matrix powers of H-sets, with constants, for various finite groups H.*

Proof. It is an easy exercise to check that the varietal product and matrix product operations on varieties preserves the property of having a polynomially bounded G-spectrum. In fact, a variety $\mathcal{W}$ and its matrix power $\mathcal{W}^{[k]}$ have identical G-spectra while the G-spectrum of the varietal product of two varieties $\mathcal{W}_1$ and $\mathcal{W}_2$ is equal to the product of $G_{\mathcal{W}_1}$ and $G_{\mathcal{W}_2}$. It is even easier to check that the G-spectrum of a variety of pointed H-sets for some finite group H is polynomially bounded and so we have established one half of the theorem.

Conversely, assume that $\mathcal{V}$ is a locally finite strongly Abelian variety with $G_{\mathcal{V}}$ bounded by a polynomial and let $\mathbf{A}$ be a finite algebra that generates $\mathcal{V}$. If we let $d(x_1, \dots, x_n)$ be a decomposition term for $\mathcal{V}$ of maximal arity then by Theorems 10.1 and 10.4 we know that $\mathcal{V}[d]$ is an essentially unary n-sorted variety with the property that every non-constant unary term of $\mathcal{V}[d]$ is invertible.

We may assume that $A = A_1 \times \cdots \times A_n$ for some non-empty sets A_i and that $d(\bar{x})$ is the decomposition operation with respect to this cartesian product. For each i, let G_i be the group of non-constant unary term operations of $\mathbf{A}[d]$ with domain and range of sort i. For $i \leq n$, let C_i be the set of elements from A_i that are equal to the value of some term of $\mathbf{A}[d]$ that is constant and that has range of sort i.

Define the binary relation $\sim$ on $\{1, 2, \dots, n\}$ by: $i \sim j$ if and only if there is a non-constant unary term of $\mathbf{A}[d]$ with domain A_i and range A_j. Since all non-constant terms of $\mathbf{A}[d]$ are invertible, it is not hard to see that $\sim$ is an equivalence relation. Without loss of generality, we may assume that the equivalence classes of $\sim$ are intervals and that $i \sim j$ if and only if $A_i = A_j$.

If $i \sim j$ then there are unary term operations of $\mathbf{A}[d]$ which provide bijections between A_i and A_j. By permuting elements of the A_k's as necessary we may in fact assume that for $i \sim j$ the identity map between A_i and A_j is a term operation of $\mathbf{A}[d]$. It then follows that the groups G_i and G_j and the sets C_i and C_j are identical in this case.

Let m be the number of $\sim$-classes and for $i \leq m$, let σ_i be the smallest member of the ith $\sim$-class and k_i the size of this class. Then

$$A = A_{\sigma_1}^{k_1} \times A_{\sigma_2}^{k_2} \times \cdots \times A_{\sigma_m}^{k_m}$$

The theorem follows from the following claim.

Claim: The algebra $\mathbf{A}$ is term equivalent to the algebra $\mathbf{B}$ obtained by taking the non-indexed product of the k_ith matrix powers of the pointed G-sets $\langle A_{\sigma_i}, G_{\sigma_i}, C_{\sigma_i} \rangle$ for $i \leq m$.

Note that $\mathbf{A}$ and $\mathbf{B}$ have the same universe. By unravelling how the matrix power and non-indexed product work it can be seen that a p-ary operation $f(x_1, \dots, x_p)$ on A will be a term operation of $\mathbf{B}$ if and only if for each $i \leq n$, the projection of f onto the ith coordinate of A,

$$p_i f(x_1^1, x_2^1, \dots, x_p^1, \dots, x_1^n, \dots, x_p^n) : A_1^p \times \cdots \times A_n^p \to A_i$$

is either constant and takes on one of the values in C_i or is essentially unary and depends on some variable x_q^j with $i \sim j$ and such that this unary map from A_j into A_i is a member of the group G_i.

By appealing to the definitions of the groups G_i, the sets C_i and the relation $\sim$, and using the decomposition operation $d(\bar{x})$ one obtains an identical description for the p-ary members of the clone of $\mathbf{A}$. □

References

1. George E. Andrews, *The theory of partitions*, Encyclopedia of Mathematics and its Applications, Vol. 2, Addison-Wesley, Reading, Mass. 1976. MR 0557013 (58 #27738)
2. Joel Berman and Paweł M. Idziak, *Generative complexity in algebra*, Mem. Amer. Math. Soc. **175** (2005), no. 828, viii+159. MR 2130585 (2006a:08001)
3. Joel Berman and Ralph McKenzie, *Clones satisfying the term condition*, Discrete Math. **52** (1984), no. 1, 7–29. MR 765281 (86m:08005)
4. Marcin Bilski, *Generative complexity in semigroup varieties*, J. Pure Appl. Algebra **165** (2001), no. 2, 137–149. MR 1865962 (2002h:20082)
5. David Hobby and Ralph McKenzie, *The structure of finite algebras*, Contemporary Mathematics, vol. 76, American Mathematical Society, Providence, RI, 1988, Revised edition: 1996. MR 958685 (89m:08001)
6. P. Idziak and R. McKenzie, *Varieties with polynomially many models. I*, Fund. Math. **170** (2001), no. 1-2, 53–68, Dedicated to the memory of Jerzy Łoś. MR 1881368 (2003e:08002)
7. Keith A. Kearnes, *Type-preservation in locally finite varieties with the CEP*, Canadian J. Math. **43** (1991) no. 4, 748–769. MR 1127028 (92m:08005)
8. ———, *An order-theoretic property of the commutator*, Internat. J. Algebra Comput. **3** (1993), no. 4, 491–533. MR 1250248 (95c:08002)
9. ———, *Locally solvable factors of varieties*, Proc. Amer. Math. Soc. **124** (1996), no. 12, 3619–3625. MR 1343705 (97b:08007)
10. ———, *A Hamiltonian property for nilpotent algebras*, Algebra Universalis **37** (1997), no. 4, 403–421. MR 1465297 (98k:08001)
11. Keith A. Kearnes and Emil W. Kiss, *Modularity prevents tails*, Proc. Amer. Math. Soc. **127** (1999), no. 1, 11–19. MR 1625765 (99m:08003)
12. ———, *Residual smallness and weak centrality*, Internat. J. Algebra Comput. **13** (2003), no. 1, 35–59. MR 1970866 (2004c:08012)
13. E. W. Kiss, M. Valeriote, *Abelian algebras and the Hamiltonian property*, Journal of Pure and Applied Algebra **87** (1993), 37–49. MR 1222175 (94d:08002)
14. L. Lovász, *Operations with structures*, Acta Math. Acad. Sci. Hungar. **18** (1967), 321–328. MR 0214529 (35 #5379)
15. Ralph McKenzie and Matthew Valeriote, *The structure of decidable locally finite varieties*, Progress in Mathematics, vol. 79, Birkhäuser Boston Inc., Boston, MA, 1989. MR 1033992 (92j:08001)

Department of Theoretical Computer Science, Jagiellonian University, Kraków, Poland

E-mail address: idziak@tcs.uj.edu.pl

Department of Mathematics, Vanderbilt University, Nashville, Tennessee, USA 37240

E-mail address: ralph.n.mckenzie@vanderbilt.edu

Department of Mathematics & Statistics, McMaster University, Hamilton, Ontario, Canada L8S 4K1

E-mail address: matt@math.mcmaster.ca