J. Aust. Math. Soc. **89** (2010), 105–126
doi:10.1017/S1446788710001473

GROWTH OF GENERATING SETS FOR DIRECT POWERS OF CLASSICAL ALGEBRAIC STRUCTURES

MARTYN QUICK and N. RUŠKUC✉

(Received 1 December 2009; accepted 9 July 2010)

Communicated by M. G. Jackson

Dedicated to the memory of Jim Wiegold.

Abstract

For an algebraic structure $\boldsymbol{A}$ denote by $d(\boldsymbol{A})$ the smallest size of a generating set for $\boldsymbol{A}$, and let $\mathbf{d}(\boldsymbol{A}) = (d(\boldsymbol{A}), d(\boldsymbol{A}^2), d(\boldsymbol{A}^3), \ldots)$, where $\boldsymbol{A}^n$ denotes a direct power of $\boldsymbol{A}$. In this paper we investigate the asymptotic behaviour of the sequence $\mathbf{d}(\boldsymbol{A})$ when $\boldsymbol{A}$ is one of the classical structures—a group, ring, module, algebra or Lie algebra. We show that if $\boldsymbol{A}$ is finite then $\mathbf{d}(\boldsymbol{A})$ grows either linearly or logarithmically. In the infinite case constant growth becomes another possibility; in particular, if $\boldsymbol{A}$ is an infinite simple structure belonging to one of the above classes then $\mathbf{d}(\boldsymbol{A})$ is eventually constant. Where appropriate we frame our exposition within the general theory of congruence permutable varieties.

2000 *Mathematics subject classification*: primary 08A40; secondary 16S15, 17B99, 20F05.
Keywords and phrases: generating sets, growth, direct products, algebraic structures, universal algebra.

1. Introduction

For an algebraic structure $\boldsymbol{A}$, we denote by $d(\boldsymbol{A})$ the smallest cardinality of a generating set of $\boldsymbol{A}$, and by $\mathbf{d}(\boldsymbol{A})$ the sequence

$$\mathbf{d}(\boldsymbol{A}) = (d(\boldsymbol{A}), d(\boldsymbol{A}^2), d(\boldsymbol{A}^3), \ldots),$$

where $\boldsymbol{A}^n$ stands for the nth direct power of $\boldsymbol{A}$. For example, for the cyclic group $\boldsymbol{C}_m$ of order $m > 1$ we have $\mathbf{d}(\boldsymbol{C}_m) = (1, 2, 3, 4, \ldots)$.

In this paper we discuss the behaviour of $\mathbf{d}(\boldsymbol{A})$ when $\boldsymbol{A}$ is a *classical* algebraic structure. This will be given a technical meaning here of being a group, ring, module, algebra, or Lie algebra. The $\mathbf{d}$-sequences of groups have been investigated in considerable detail by Wiegold and various co-authors in a series of papers [18, 23, 25–28, 30]. Below we summarize their main findings.

For a nontrivial finite group $\boldsymbol{G}$, the following hold.

- If G is perfect (that is, it is equal to its derived subgroup), then $\mathbf{d}(G)$ grows logarithmically.
- If G is nonperfect, $\mathbf{d}(G)$ grows linearly.

For an infinite group G, the following hold.

- If G is simple, then $\mathbf{d}(G)$ is eventually constant.
- If G is nonperfect, then $\mathbf{d}(G)$ grows linearly.
- If G is perfect and has nontrivial finite images, then $\mathbf{d}(G)$ grows logarithmically.
- If G is perfect and has no nontrivial finite images, then $\mathbf{d}(G)$ is sandwiched between a constant and a logarithmic function.

Wiegold and his co-authors, of course, provide much more detailed information about the actual behaviour and values of the $\mathbf{d}$-sequences. As far as we are aware, the only other structures for which the $\mathbf{d}$-sequences have been studied are semigroups, for which Wiegold [29] shows the following: $\mathbf{d}(S)$ for a finite semigroup S grows linearly if S has an identity element, and otherwise grows exponentially. In this paper we shall see that exponential growth cannot occur in classical structures. The $\mathbf{d}$-sequences of semigroups will be investigated further in a separate paper [14].

Our main purpose is to take a broader look at the $\mathbf{d}$-sequences of classical algebraic structures, and put the above results about groups into a more general framework. Here is a summary of our main results.

- If A is a nontrivial finite classical structure then $\mathbf{d}(A)$ grows either logarithmically or linearly (Theorem 4.9, Corollaries 4.10–4.14).
- The finite structures displaying logarithmic growth are: perfect groups, rings R with $R \cdot R = R$, algebras A with $A \cdot A = A$, and perfect Lie algebras (Corollaries 4.10–4.14).
- The finite structures displaying linear growth are: nonperfect groups, rings with $R \cdot R \neq R$, modules, algebras with $A \cdot A \neq A$ and nonperfect Lie algebras (Corollaries 4.10–4.14).
- In the special case of simple finite classical structures the criteria for logarithmic growth are: being perfect for groups and Lie algebras, and the existence of an identity element for rings and algebras (Corollaries 3.5–3.9).
- The $\mathbf{d}$-sequence of an infinite, finitely generated, simple group, ring, algebra or Lie algebra is eventually constant (Corollary 5.4).
- If A is an Artinian simple algebra over an algebraically closed field then $\mathbf{d}(A) = (2, 2, 2, \ldots)$ (Theorem 6.9).
- There exist a finitely generated simple module and a finitely generated simple ring without identity with eventually constant $\mathbf{d}$-sequences (Examples 6.1 and 6.3).

The universal algebraic theory of congruence permutable and congruence uniform varieties provides a natural framework within which to develop this investigation. In fact, during its development this project has been moving steadily away from classical and towards universal algebra. Associating number sequences to algebraic structures has been one of the leitmotivs in this field, for example, the spectrum functions of

Shelah [22], G-spectra [1], p_n-sequences and free spectra [9]. In fact the **d**-sequence itself has made a recent appearance in the universal algebra literature [5], albeit without reference to Wiegold's pioneering work. The most recent major development in this direction, and closest to the present work, has been the seminal article by Berman *et al.* [2], in which three functions concerning direct powers of an algebraic structure $\boldsymbol{A}$ are introduced: $\mathrm{s}_{\boldsymbol{A}}(n)$, the base 2 logarithm of the number of substructures in $\boldsymbol{A}^n$; $\mathrm{g}_{\boldsymbol{A}}(n)$, the maximum of $\{d(\boldsymbol{B}) : \boldsymbol{B} \leq \boldsymbol{A}^n\}$; $\mathrm{i}_{\boldsymbol{A}}(n)$, the maximum size of an independent set in $\boldsymbol{A}^n$. The authors establish strong links between the three sequences, and use their growth rates as a 'classifying tool'. The division lines obtained in [2] are quite different from those arising in the present paper: to give but one example, the sequences s, g, i grow slowly (linearly) for *every* finite group, while the **d**-sequence growth divides finite groups into perfect (slow/logarithmic growth) and nonperfect (fast/linear growth). This indicates that any relations between the sequences s, g, i on one hand and **d** on the other are unlikely to be immediately obvious. This clearly invites further research, as does the obvious need to extend the present project further into the universal algebra territory, presumably via congruence permutable and congruence distributive varieties, variations of Mal'cev type term conditions, and tame congruence theory [12].

The paper is organized as follows. Section 2 introduces the definitions and notation for the rest of the paper and establishes the easy general bounds for the **d**-sequence. Our main results concerning finite structures are proved in Sections 3 and 4; we first treat simple structures using the notion of functional completeness, and then 'lift' our findings to arbitrary finite structures by adapting an old trick of Gaschütz. In Sections 5 and 6 we undertake a parallel development for infinite structures, using the concept of interpolation.

2. Preliminaries

Throughout we will develop some standard concepts and notations from universal algebra, largely following [3]. In order to avoid confusion between 'classical' algebras (over a field) and 'universal' algebras (sets with operations defined on them), we will designate the latter as *algebraic structures*. Algebraic structures will generally be denoted by bold letters $\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}, \ldots$. Unless specifically stated otherwise, it will be understood that the carrier set of a structure is the corresponding standard letter, for instance A will be the carrier set of the algebraic structure $\boldsymbol{A}$. An algebraic structure is said to be *simple* if it (is nontrivial and) has no proper congruences (or, equivalently, homomorphic images). The full and diagonal congruences (the 'improper' congruences) on an algebraic structure $\boldsymbol{A}$ will be denoted by Φ_A and Δ_A, respectively. The nth direct power of $\boldsymbol{A}$ will be denoted by $\boldsymbol{A}^n$, and $\boldsymbol{\Delta}^n(\boldsymbol{A})$ will denote the diagonal subalgebra of $\boldsymbol{A}^n$, which has carrier set

$$\Delta^n(A) = \{(a, \ldots, a) : a \in A\},$$

and which is isomorphic to $\boldsymbol{A}$.

A *term* is a formal expression made of variables (say, $x_1, \ldots, x_k$) and symbols representing basic operations of an algebraic structure $\boldsymbol{A}$. Every such expression induces a k-ary function from A^k to A; such functions are called *term operations*. Suppose that $t(x_1, \ldots, x_k, y_1, \ldots, y_l)$ is a term and $c_1, \ldots, c_l \in A$. Then the rule $(a_1, \ldots, a_k) \mapsto t(a_1, \ldots, a_k, c_1, \ldots, c_l)$ defines a function from A^k to A. Such functions are called *polynomial functions*. Term and polynomial functions clearly respect all congruences of $\boldsymbol{A}$. For an algebraic structure $\boldsymbol{A}$ let $\mathbf{EC}(\boldsymbol{A})$ denote the *extension by constants* of $\boldsymbol{A}$; it has the same carrier set as $\boldsymbol{A}$ and the same fundamental operations, to which one adds $|A|$ many constant symbols, one for each element of A. Clearly, polynomial functions on $\boldsymbol{A}$, term functions on $\mathbf{EC}(\boldsymbol{A})$, and polynomial functions on $\mathbf{EC}(\boldsymbol{A})$ all coincide. We say that two algebraic structures $\boldsymbol{A}$ and $\boldsymbol{B}$ are *polynomially equivalent* if $A = B$ and their respective sets of polynomial operations are equal. For example, $\boldsymbol{A}$ and $\mathbf{EC}(\boldsymbol{A})$ are polynomially equivalent.

An algebra is said to be *congruence permutable* if $\rho \circ \sigma = \sigma \circ \rho$ for all congruences ρ, σ on $\boldsymbol{A}$. All our classical structures are congruence permutable. A class of algebraic structures is *congruence permutable* if all the structures belonging to it are congruence permutable. It is a classical result of Mal'cev that a variety $\mathcal{V}$ is congruence permutable if and only if there exists a term m (called a *Mal'cev term*) such that

$$m(x, y, y) = m(y, y, x) = x \tag{2.1}$$

for all algebras $\boldsymbol{A} \in \mathcal{V}$ and all $x, y \in A$; see [3, Section II.12].

For two functions $f, g : \mathbb{N} \to \mathbb{R}$ we write $f \preceq g$ if $f(n) \leq g(n)$ for all sufficiently large n. Let $\mathcal{F}$ be a family of functions from $\mathbb{N}$ to $\mathbb{R}$, and let $f : \mathbb{N} \to \mathbb{R}$. We say that f has an $\mathcal{F}$-growth if there exist $f_1, f_2 \in \mathcal{F}$ such that $f_1 \preceq f \preceq f_2$. It is in this sense that we will be speaking of logarithmic or exponential growth of our sequences.

For an example, let us consider two algebraic structures $\boldsymbol{A}$ and $\boldsymbol{B}$ which are polynomially equivalent. Suppose that $\boldsymbol{A}^n = \langle G \rangle$ for some $G \subseteq A^n$. Thus, for every $\boldsymbol{a} \in A^n$ there exists a k-ary term function $t(x_1, \ldots, x_k)$ of $\boldsymbol{A}$ and elements $\boldsymbol{g}_1, \ldots, \boldsymbol{g}_k \in G^n$ such that $t(\boldsymbol{g}_1, \ldots, \boldsymbol{g}_k) = \boldsymbol{a}$. Polynomial equivalence implies that t is a polynomial function of $\boldsymbol{B}$. Thus there exist a $(k+l)$-ary term operation $s(x_1, \ldots, x_k, y_1, \ldots, y_l)$ of $\boldsymbol{B}$ and elements $c_1, \ldots, c_l \in B = A$ such that $t(x_1, \ldots, x_k) = s(x_1, \ldots, x_k, c_1, \ldots, c_l)$ for all $x_1, \ldots, x_k \in A$. Thus if we define $\boldsymbol{c}_i = (c_i, \ldots, c_i) \in \Delta^n(A)$ (where $i = 1, \ldots, l$),

$$\boldsymbol{a} = t(\boldsymbol{g}_1, \ldots, \boldsymbol{g}_k) = s(\boldsymbol{g}_1, \ldots, \boldsymbol{g}_k, \boldsymbol{c}_1, \ldots, \boldsymbol{c}_l).$$

It follows that

$$\boldsymbol{B}^n = \langle G \cup \Delta^n(A) \rangle,$$

and therefore

$$d(\boldsymbol{B}^n) \leq d(\boldsymbol{A}^n) + d(\boldsymbol{A}), \tag{2.2}$$

and, by symmetry,

$$d(\boldsymbol{A}^n) - d(\boldsymbol{B}) \leq d(\boldsymbol{B}^n). \tag{2.3}$$

Suppose now that $\mathcal{F}$ is a family of functions satisfying the following property: if $f \in \mathcal{F}$ and $c \in \mathbb{R}$ then $f + c$ has $\mathcal{F}$-growth. The families of all logarithmic, linear and exponential functions clearly satisfy this property. Then from (2.2) and (2.3) it follows that $\mathbf{d}(\boldsymbol{A})$ has $\mathcal{F}$-growth if and only if $\mathbf{d}(\boldsymbol{B})$ has $\mathcal{F}$-growth. In particular, $\mathbf{d}(\boldsymbol{A})$ has $\mathcal{F}$-growth if and only if $\mathbf{d}(\mathbf{EC}(\boldsymbol{A}))$ has $\mathcal{F}$-growth.

At various points in the text we will use another sequence $\mathbf{e}(\boldsymbol{A})$, closely related to $\mathbf{d}(\boldsymbol{A})$, and defined as follows: for $n \in \mathbb{N}$ we denote by $e(\boldsymbol{A}, n)$ the largest number $m \in \mathbb{N}$ such that $\boldsymbol{A}^m$ can be generated by n elements, and let

$$\mathbf{e}(\boldsymbol{A}) = (e(\boldsymbol{A}, 1), e(\boldsymbol{A}, 2), e(\boldsymbol{A}, 3), \ldots).$$

Both these sequences are nondecreasing and are linked with the formula

$$d(\boldsymbol{A}^{e(\boldsymbol{A},n)}) = n. \tag{2.4}$$

It therefore follows that:

(DE1) $\mathbf{d}(\boldsymbol{A})$ grows linearly if and only if $\mathbf{e}(\boldsymbol{A})$ grows linearly;

(DE2) $\mathbf{d}(\boldsymbol{A})$ grows logarithmically if and only if $\mathbf{e}(\boldsymbol{A})$ grows exponentially (and *vice versa*).

We end this section by recording the following easy general bounds for the $\mathbf{d}$-sequence.

PROPOSITION 2.1. *Let $\boldsymbol{A}$ be any algebraic structure.*

(i) *The sequence $\mathbf{d}(\boldsymbol{A})$ is nondecreasing.*

(ii) *If $\boldsymbol{A}$ is finite and nontrivial then $\mathbf{d}(\boldsymbol{A})$ is bounded below by a logarithmic function.*

(iii) *If $\boldsymbol{A}$ is a classical structure then $\mathbf{d}(\boldsymbol{A})$ is bounded above by a linear function.*

PROOF. (i) This follows from $\boldsymbol{A}^{n-1}$ being a homomorphic image of $\boldsymbol{A}^n$.

(ii) We shall prove that the sequence $\mathbf{e}(\boldsymbol{A})$ satisfies $e(\boldsymbol{A}, n) \leq |A|^n$ and then appeal to (DE2). Suppose that a set X of size n can generate $\boldsymbol{A}^q$ for some $q > |A|^n$. Suppose that the elements of X are $\boldsymbol{x}_i = (x_{i1}, \ldots, x_{iq})$ for $i = 1, \ldots, n$. By the pigeonhole principle, among the n-tuples $\boldsymbol{y}_j = (x_{1j}, \ldots, x_{nj})$ (for $j = 1, \ldots, q$) there must be two equal ones, say $\boldsymbol{y}_j = \boldsymbol{y}_k$. But then in any two elements from the subalgebra generated by X the jth and kth components coincide, contradicting $\langle X \rangle = \boldsymbol{A}^n$.

(iii) For any classical structures $\boldsymbol{B}$ and $\boldsymbol{C}$ of the same type we have

$$d(\boldsymbol{B} \times \boldsymbol{C}) \leq d(\boldsymbol{B}) + d(\boldsymbol{C}). \tag{2.5}$$

This follows from the fact that $\boldsymbol{B} \times \boldsymbol{C}$ is generated by natural copies of $\boldsymbol{B}$ and $\boldsymbol{C}$ inside it, which in turn is a consequence of the presence of an identity or zero. The assertion follows immediately from (2.5). □

REMARK 2.2. In the infinite case it is possible for $\mathbf{d}(\boldsymbol{A})$ to be (eventually) constant: Wiegold [30] observes that this is the case for any finitely generated infinite simple group. We will have more to say about this in Sections 5 and 6.

3. Finite simple structures and functional completeness

A finite algebraic structure $\boldsymbol{A}$ is said to be functionally complete if, for all $n \in \mathbb{N}$, all n-ary functions from A^n to A are polynomial. Obviously, every functionally complete algebraic structure is simple. For basic information on functional completeness the reader is referred to [3, Section IV.11].

THEOREM 3.1. *The* $\mathbf{d}$*-sequence of a nontrivial functionally complete algebraic structure* $\boldsymbol{A}$ *grows logarithmically.*

PROOF. We saw in Section 2 that the $\mathbf{d}$-sequences for $\boldsymbol{A}$ and its extension by constants $\boldsymbol{A}_C = \mathbf{EC}(\boldsymbol{A})$ have the same growth. Thus it is sufficient to prove that $\mathbf{d}(\boldsymbol{A}_C)$ grows logarithmically. By (DE2) of Section 2 it is sufficient to show that the $\mathbf{e}$-sequence of $\boldsymbol{A}_C$ grows exponentially. Let $N = |A|^n$. We will prove that $\boldsymbol{A}_C^N$ can be generated by n elements (so that $e(\boldsymbol{A}_C, n) \geq |A|^n$). Let $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_N$ be the list of all n-tuples of elements of A, say $\boldsymbol{y}_j = (y_{1j}, y_{2j}, \ldots, y_{nj})$. Define $\boldsymbol{x}_i = (y_{i1}, y_{i2}, \ldots, y_{iN})$, for $i = 1, \ldots, n$, and let $X = \{\boldsymbol{x}_i : i = 1, \ldots, n\}$. We claim that X generates $\boldsymbol{A}_C^N$. Indeed, let $(a_1, \ldots, a_N) \in A^N$ be arbitrary. Since $\boldsymbol{A}$ is functionally complete, there exists a polynomial function $f : A^n \to A$, satisfying $f(\boldsymbol{y}_j) = a_j$ for $j = 1, \ldots, N$. But a polynomial function for $\boldsymbol{A}$ is a term function for $\boldsymbol{A}_C$ and so $\langle X \rangle$ contains

$$f(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n) = (f(\boldsymbol{y}_1), \ldots, f(\boldsymbol{y}_N)) = (a_1, \ldots, a_N),$$

proving the result. □

In a congruence permutable variety, a finite algebraic structure $\boldsymbol{A}$ is functionally complete if and only if $\boldsymbol{A}^2$ has only the four 'obvious' congruences: $\Delta_A \times \Delta_A$ (the diagonal), $\Phi_A \times \Phi_A$ (the full relation), $\Delta_A \times \Phi_A$, $\Phi_A \times \Delta_A$ (two projection kernels). This was proved by Werner [24]; see also [3, Theorem IV.11.12]. If $\boldsymbol{A}$ is simple, then clearly there can be no congruences containing or contained in $\Delta_A \times \Phi_A$, $\Phi_A \times \Delta_A$, and so the only alternative to the above is that $\boldsymbol{A}^2$ contains a further congruence which is incomparable with these two. Thus, by [17, Lemma 4.154, Theorem 4.155], $\boldsymbol{A}$ is polynomially equivalent to a simple module over a finite ring with 1. Let us record this.

PROPOSITION 3.2. *A finite simple algebra in a congruence permutable variety is either functionally complete or else it is polynomially equivalent to a simple module over a finite ring with* 1.

In the light of Proposition 3.2, we need to understand the $\mathbf{d}$-sequences of simple modules. It is clear that the $\mathbf{d}$-sequences of vector spaces are linear, and it is no great surprise that this carries over to arbitrary simple modules (and indeed to the nonsimple as well; see Corollary 3.7).

LEMMA 3.3. *Let* $\boldsymbol{M}$ *be a finite simple module over a ring* $\boldsymbol{R}$ *with* 1. *Then the sequence* $\mathbf{d}(\boldsymbol{M})$ *grows linearly.*

PROOF. A linear upper bound has been established in Proposition 2.1. So we concentrate on establishing a linear lower bound. For the sake of a concrete framework, we work here with left modules, but the result is equally valid for right modules.

As $\boldsymbol{M}$ is finite, we may if necessary replace $\boldsymbol{R}$ by the quotient by the annihilator of M and so there is no loss of generality in assuming that $\boldsymbol{R}$ is finite and certainly therefore Artinian. Then since $\boldsymbol{M}$ is simple it can be expressed as $\boldsymbol{M} \cong \boldsymbol{R}/L$, where L is a maximal left ideal of $\boldsymbol{R}$. The Jacobson radical J of $\boldsymbol{R}$ is contained in L, and so there is a natural $\boldsymbol{R}/J$-module structure on M, with exactly the same $\mathbf{d}$-sequence. So, without loss of generality, we may assume that the ring $\boldsymbol{R}$ is (Jacobson) semisimple. As such, by the Wedderburn–Artin theorem (see, for example, [10, Theorem 2.1.6]), it is isomorphic to the direct sum of full matrix rings over fields: $\boldsymbol{R} \cong \boldsymbol{M}_{r_1}(\boldsymbol{F}_1) \oplus \cdots \oplus \boldsymbol{M}_{r_n}(\boldsymbol{F}_n)$.

Since L is maximal, it follows without loss of generality that it has the form

$$L = L_1 \oplus \boldsymbol{M}_{r_2}(\boldsymbol{F}_2) \oplus \cdots \oplus \boldsymbol{M}_{r_n}(\boldsymbol{F}_n)$$

where L_1 is a maximal left ideal of $\boldsymbol{M}_{r_1}(\boldsymbol{F}_1)$. Hence we see that $\boldsymbol{M}$ has the form $\boldsymbol{M}_1 \oplus 0 \oplus \cdots \oplus 0$, where $\boldsymbol{M}_1$ is the vector space $\boldsymbol{F}_1^{r_1}$ viewed as an $\boldsymbol{M}_{r_1}(\boldsymbol{F}_1)$-module. Clearly $\mathbf{d}(\boldsymbol{M}) = \mathbf{d}(\boldsymbol{M}_1)$. To put it differently, we can now assume without loss of generality that our original ring $\boldsymbol{R}$ is actually a full matrix ring $\boldsymbol{M}_r(\boldsymbol{F})$ over a finite field $\boldsymbol{F}$, and that our module $\boldsymbol{M}$ is the r-dimensional $\boldsymbol{F}$-vector space on which $\boldsymbol{R}$ acts via its natural action.

To prove that $\mathbf{d}(\boldsymbol{M})$ is bounded below by a linear function, we will demonstrate that $\mathbf{e}(\boldsymbol{M})$ is bounded above by a linear function, namely

$$e(\boldsymbol{M}, n) \leq nr, \tag{3.1}$$

and then appeal to (DE1) in Section 2. Suppose that $\boldsymbol{M}^{nr+1}$ can be generated by n elements, say $\boldsymbol{M}^{nr+1} = \langle \boldsymbol{v}_1, \ldots, \boldsymbol{v}_n \rangle$, where $\boldsymbol{v}_i = (\boldsymbol{v}_{i1}, \ldots, \boldsymbol{v}_{i,nr+1})$ for $i = 1, \ldots, n$. Each $\boldsymbol{v}_{ij}$ (for $1 \leq i \leq n$, $1 \leq j \leq nr+1$) is a vector in the r-dimensional vector space M. So each $\boldsymbol{y}_j = (\boldsymbol{v}_{1j}, \boldsymbol{v}_{2j}, \ldots, \boldsymbol{v}_{nj})$, for $j = 1, \ldots, nr+1$, can be regarded as a vector in an nr-dimensional vector space over $\boldsymbol{F}$. Since there are $nr+1$ such vectors, they must be linearly dependent, so for some j the vector $\boldsymbol{y}_j$ is a linear combination of the others. This implies that in the submodule generated by $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ the jth component of any element is uniquely determined by the other components, contradicting the assumption that $\boldsymbol{M}$ is generated by this set. □

By combining all the above considerations we obtain the following main result of this section.

THEOREM 3.4. *Let $\boldsymbol{A}$ be a finite simple algebraic structure in a congruence permutable variety. The sequence $\mathbf{d}(\boldsymbol{A})$ grows either logarithmically (if $\boldsymbol{A}$ is functionally complete) or linearly (if $\boldsymbol{A}$ is polynomially equivalent to a simple module).*

Specializing to each of five kinds of classical structures, we obtain the following corollaries.

COROLLARY 3.5. *Let $\boldsymbol{G}$ be a finite simple group. If $\boldsymbol{G}$ is cyclic of prime order then $\mathbf{d}(\boldsymbol{G})$ grows linearly, while if $\boldsymbol{G}$ is nonabelian the sequence $\mathbf{d}(\boldsymbol{G})$ grows logarithmically.*

PROOF. $\boldsymbol{G}$ is functionally complete if and only if it is nonabelian; see [16] or [3, Corollary 11.13]. □

COROLLARY 3.6. *Let $\boldsymbol{R}$ be a finite simple ring. If $\boldsymbol{R}$ has an identity then $\mathbf{d}(\boldsymbol{R})$ grows logarithmically, otherwise ($\boldsymbol{R}$ is a zero ring and) $\mathbf{d}(\boldsymbol{R})$ grows linearly.*

PROOF. $\boldsymbol{R}$ is functionally complete if and only if it is not a zero ring by [24, Example D], in which case it has an identity element by the Wedderburn–Artin theorem. □

COROLLARY 3.7. *Let $\boldsymbol{M}$ be a finite simple module over a ring $\boldsymbol{R}$. The sequence $\mathbf{d}(\boldsymbol{R})$ grows linearly.*

PROOF. Let $\boldsymbol{E}$ be the ring (with identity) of endomorphisms of the additive abelian group of $\boldsymbol{M}$. The action of $\boldsymbol{E}$ on M induces a module structure $\overline{\boldsymbol{M}}$ on it. Clearly $d(\boldsymbol{M}^n) \geq d(\overline{\boldsymbol{M}}^n)$ for all n. The assertion now follows from Lemma 3.3. □

COROLLARY 3.8. *Let $\boldsymbol{A}$ be a finite simple algebra over a (finite) field $\boldsymbol{F}$. If $\boldsymbol{A}$ has an identity then $\mathbf{d}(\boldsymbol{A})$ grows logarithmically, otherwise ($\boldsymbol{A}$ is a zero algebra and) $\mathbf{d}(\boldsymbol{A})$ grows linearly.*

PROOF. The same as Corollary 3.6. □

COROLLARY 3.9. *Let $\boldsymbol{L}$ be a finite simple Lie algebra over a (finite) field $\boldsymbol{F}$. If $\boldsymbol{L}$ is perfect then $\mathbf{d}(\boldsymbol{L})$ grows logarithmically, otherwise ($\boldsymbol{L}$ is abelian and) $\mathbf{d}(\boldsymbol{L})$ grows linearly.*

PROOF. It is obvious that an abelian simple Lie algebra is polynomially equivalent to a vector space, and so $\mathbf{d}(\boldsymbol{L})$ grows linearly in this case. Suppose that $\boldsymbol{L}$ is perfect; in particular, the term operation $[x, y]$ is nonconstant. On the other hand, $[x, 0] = [0, x] = 0$. Of course, $\boldsymbol{L}$ has a Mal'cev term. It follows that $\boldsymbol{L}$ is functionally complete from Proposition 5.1 below specialized to the finite case. □

4. Finite structures and Gaschütz's lemma

Wiegold's second proof of the logarithmic/linear dichotomy for groups, which he gives in [26], relies on a result known as Gaschütz's lemma from [7]. With small modifications this works in greater generality, and this is the path we take in this section.

We will say that a congruence ρ on an algebraic structure $\boldsymbol{A}$ is *uniform* if all the ρ-classes have the same size. If all the congruences on $\boldsymbol{A}$ are uniform we say that $\boldsymbol{A}$ itself is *congruence-uniform*. If all the members of a class $\mathcal{K}$ of algebraic structures are uniform we say that $\mathcal{K}$ is *congruence-uniform*. All classical structures certainly have this property.

The following lemma is a modification of Gaschütz's lemma [7, Satz 1] to our more general setting.

LEMMA 4.1. *Let $\boldsymbol{A}$ be a finite algebraic structure belonging to a congruence-uniform variety $\mathcal{V}$, let $f : \boldsymbol{A} \to \boldsymbol{B}$ be a surjective homomorphism, and let $n \in \mathbb{N}$. If both $\boldsymbol{A}$ and $\boldsymbol{B}$ can be generated by n elements, then for every generating set $\{y_1, \ldots, y_n\}$ of $\boldsymbol{B}$ there exists a generating set $\{x_1, \ldots, x_n\}$ of $\boldsymbol{A}$ such that $f(x_i) = y_i$ for $i = 1, \ldots, n$.*

PROOF. Our proof is a modification of that given in [21, Proposition 2.5.4]. For an arbitrary (ordered) generating set $\boldsymbol{y} = (y_1, \ldots, y_n)$ of $\boldsymbol{B}$ and for every subalgebra $\boldsymbol{C} \leq \boldsymbol{A}$, let $\lambda(\boldsymbol{C}, \boldsymbol{y})$ denote the number of ways in which $\boldsymbol{y}$ can be lifted to a generating set of $\boldsymbol{C}$:

$$\lambda(\boldsymbol{C}, \boldsymbol{y}) = |\{(x_1, \ldots, x_n) \in C^n : \langle x_1, \ldots, x_n \rangle = \boldsymbol{C},\ f(x_i) = y_i \text{ for } i = 1, \ldots, n\}|.$$

Clearly, if $f(C) \neq B$ we have $\lambda(\boldsymbol{C}, \boldsymbol{y}) = 0$ for any $\boldsymbol{y}$. Otherwise, let ρ be the kernel of $f \restriction_C$, and let c be the common size of the equivalence classes of ρ. The number of n-tuples that are mapped onto $\boldsymbol{y}$ is c^n. Each such tuple generates either $\boldsymbol{C}$ or a proper subalgebra of C; therefore

$$\lambda(\boldsymbol{C}, \boldsymbol{y}) = c^n - \sum_{\boldsymbol{D} < \boldsymbol{C}} \lambda(\boldsymbol{D}, \boldsymbol{y}). \tag{4.1}$$

An inductive argument based on (4.1) shows that $\lambda(\boldsymbol{C}, \boldsymbol{y})$ does not depend on $\boldsymbol{y}$; in particular, $\lambda(\boldsymbol{A}, \boldsymbol{y})$ does not depend on $\boldsymbol{y}$. However, if we were to start with an (ordered) generating set $\boldsymbol{x} = (x_1, \ldots, x_n)$ of $\boldsymbol{A}$ then the set $\boldsymbol{y} = (f(x_1), \ldots, f(x_n))$ generates $\boldsymbol{B}$ and satisfies $\lambda(\boldsymbol{A}, \boldsymbol{y}) > 0$. Hence $\lambda(\boldsymbol{A}, \boldsymbol{y}) > 0$ holds for *all* $\boldsymbol{y}$. □

Both finiteness and congruence-uniformity are necessary hypotheses, as the following two examples show.

EXAMPLE 4.2. Consider the natural epimorphism $f : \mathbb{Z} \to \mathbb{Z}_5$ of additive cyclic groups. The generating set $\{2\}$ of $\mathbb{Z}_5$ cannot be lifted to a generating set of $\mathbb{Z}$.

EXAMPLE 4.3. Let $\boldsymbol{S}$ be the monogenic semigroup defined by the presentation $\langle a \mid a^5 = a^2 \rangle$; it is easily seen not to be congruence-uniform. There is an epimorphism $f : \boldsymbol{S} \to \boldsymbol{G}$, $a \mapsto b$, onto the cyclic group $\boldsymbol{G}$ of order three generated by b. But $\boldsymbol{G}$ can also be generated by b^2, while $\boldsymbol{S}$ has a unique singleton generating set.

For an arbitrary nontrivial finite algebraic structure $\boldsymbol{A}$ with maximal proper congruences $\rho_1, \ldots, \rho_k$, let

$$R(\boldsymbol{A}) = \bigcap_{i=1}^{k} \rho_i$$

be their intersection, and let $\boldsymbol{A}^* = \boldsymbol{A}/R(\boldsymbol{A})$ be the corresponding quotient.

LEMMA 4.4. *If $\boldsymbol{A}$ is a finite algebraic structure in a congruence permutable variety then $\boldsymbol{A}^*$ is isomorphic to the direct product of simple algebraic structures which are quotients of $\boldsymbol{A}$.*

PROOF. If $\rho_1, \ldots, \rho_k$ are the maximal congruences of $\boldsymbol{A}$ then $\boldsymbol{A}^* = \boldsymbol{A}/R(\boldsymbol{A})$ is isomorphic to a subdirect product of simple quotients $\boldsymbol{A}/\rho_1, \ldots, \boldsymbol{A}/\rho_k$. By [3, Corollary IV.10.2] every subdirect product of simple algebraic structures in a congruence permutable variety is isomorphic to the direct product of such structures. □

LEMMA 4.5. *Let $\boldsymbol{A}$ and $\boldsymbol{B}$ be two algebraic structures in a congruence permutable variety $\mathcal{V}$, and let ρ be a congruence on $\boldsymbol{A} \times \boldsymbol{B}$.*

(i) *For $a_1, a_2 \in A$ there exists $b \in B$ such that $((a_1, b), (a_2, b)) \in \rho$ if and only if for all $b \in B$ we have $((a_1, b), (a_2, b)) \in \rho$.*

(ii) *The relation*

$$\overline{\rho} = \{(a_1, a_2) \in A \times A : (a_1, b) = (a_2, b) \text{ for some (and hence all) } b \in B\}$$

is a congruence on $\boldsymbol{A}$.

PROOF. (i) Only the direct implication needs proving. Let $((a_1, b), (a_2, b)) \in \rho$ for some $b \in B$, let $a \in A$, $b_1 \in B$ be arbitrary, and suppose that m is a Mal'cev term for $\mathcal{V}$. Then

$$\begin{aligned} \rho &\ni (m((a_1, b), (a, b), (a, b_1)), m((a_2, b), (a, b), (a, b_1))) \\ &= ((m(a_1, a, a), m(b, b, b_1)), (m(a_2, a, a), m(b, b, b_1))) \\ &= ((a_1, b_1), (a_2, b_1)). \end{aligned}$$

(ii) It is clear that $\overline{\rho}$ is an equivalence relation. Let $(a_1, c_1), \ldots, (a_k, c_k) \in \overline{\rho}$ and suppose that f is a k-ary fundamental operation of $\mathcal{V}$. From the definition of $\overline{\rho}$ we have $((a_i, b_i), (c_i, b_i)) \in \rho$ for some (and hence all) $b_i \in B$. Since ρ is a congruence on $\boldsymbol{A} \times \boldsymbol{B}$ we see that

$$\begin{aligned} \rho &\ni (f((a_1, b_1), \ldots, (a_k, b_k)), f((c_1, b_1), \ldots, (c_k, b_k))) \\ &= ((f(a_1, \ldots, a_k), b), (f(c_1, \ldots, c_k), b)), \end{aligned}$$

for $b = f(b_1, \ldots, b_k)$, and so $(f(a_1, \ldots, a_k), f(c_1, \ldots, c_k)) \in \overline{\rho}$. □

LEMMA 4.6. *If $\boldsymbol{A}_1, \ldots, \boldsymbol{A}_k$ are finite algebraic structures belonging to the same congruence permutable variety then*

$$R(\boldsymbol{A}_1 \times \cdots \times \boldsymbol{A}_k) = R(\boldsymbol{A}_1) \times \cdots \times R(\boldsymbol{A}_k), \tag{4.2}$$

$$(\boldsymbol{A}_1 \times \cdots \times \boldsymbol{A}_k)^* \cong \boldsymbol{A}_1^* \times \cdots \times \boldsymbol{A}_k^*. \tag{4.3}$$

PROOF. Clearly it suffices to only prove (4.2) and this only for $k = 2$. To simplify notation, we will be proving $R(\boldsymbol{A} \times \boldsymbol{B}) = R(\boldsymbol{A}) \times R(\boldsymbol{B})$. By the correspondence theorem (see [3, Theorem II.6.20]) we have $R(\boldsymbol{A} \times \boldsymbol{B}) \subseteq R(\boldsymbol{A}) \times R(\boldsymbol{B})$.

For the converse inclusion suppose that μ is any maximal congruence on $\boldsymbol{A} \times \boldsymbol{B}$, and let $\gamma = \mu \cap (\Phi_A \times \Delta_B)$. Define $\overline{\gamma}$, a congruence on $\boldsymbol{A}$, as in Lemma 4.5(ii).

Suppose that $\overline{\gamma}$ is properly contained in a maximal congruence δ of $\boldsymbol{A}$, and let $(a_1, a_2) \in \delta \setminus \overline{\gamma}$. Clearly $((a_1, b), (a_2, b)) \notin \mu$ for any $b \in B$. On the other hand,

$$((a_1, b), (a_2, b)) \in \delta \times \Delta_B \subseteq \mu \circ (\delta \times \Delta_B).$$

Thus μ is properly contained in this last congruence, which is not equal to $\Phi_{A\times B}$, since if $((a_1, b), (a_2, b)) \in \mu \circ (\delta \times \Delta_B)$ then $(a_1, a_2) \in \bar{\gamma} \circ \delta = \delta$. This contradicts the choice of μ as maximal, and implies that $\overline{\gamma}$ is either maximal or else equal to $\Phi_{A\times B}$. In either case $R(\boldsymbol{A}) \subseteq \overline{\gamma}$.

Now we have $R(\boldsymbol{A}) \times \Delta_B \subseteq \gamma \subseteq \mu$, and, by symmetry, $\Delta_A \times R(\boldsymbol{B}) \subseteq \mu$. But this implies that

$$R(\boldsymbol{A}) \times R(\boldsymbol{B}) = (R(\boldsymbol{A}) \times \Delta_B) \circ (\Delta_A \times R(\boldsymbol{B})) \subseteq \mu.$$

Therefore $R(\boldsymbol{A}) \times R(\boldsymbol{B})$ is contained in every maximal congruence of $\boldsymbol{A} \times \boldsymbol{B}$, and hence also in the intersection of all such congruences, which is precisely $R(\boldsymbol{A} \times \boldsymbol{B})$. □

LEMMA 4.7. *Let $\boldsymbol{A}_1, \ldots, \boldsymbol{A}_k$ (where $k \geq 2$) be nontrivial finite algebraic structures belonging to a congruence permutable, congruence uniform variety $\mathcal{V}$, and suppose that $n \in \mathbb{N}$. If $d(\boldsymbol{A}_i) \leq n$ (for $i = 1, \ldots, k$) and $d(\boldsymbol{A}_1^* \times \cdots \times \boldsymbol{A}_k^*) \leq n$ then $d(\boldsymbol{A}_1 \times \cdots \times \boldsymbol{A}_k) \leq n$.*

PROOF. Both the statement and the proof are modifications of [7, Satz 2].

Because of Lemma 4.6, it is sufficient to prove the statement for $k = 2$. Let $\boldsymbol{F}$ be the $\mathcal{V}$-free algebraic structure on n generators. Since $\boldsymbol{A}_1^* \times \boldsymbol{A}_2^*$ is n-generated, there exist congruences ρ_1, ρ_2 on $\boldsymbol{F}$ such that $\boldsymbol{F}/(\rho_1 \cap \rho_2) \cong \boldsymbol{A}_1^* \times \boldsymbol{A}_2^*$, $\boldsymbol{F}/\rho_i \cong \boldsymbol{A}_i^*$ (for $i = 1, 2$) and $\rho_1 \circ \rho_2 = \Phi_F$.

By Lemma 4.1 the n generators of $\boldsymbol{A}_i^*$ so provided can be lifted to n generators of $\boldsymbol{A}_i$. In other words, there are congruences $\sigma_i \subseteq \rho_i$ on $\boldsymbol{F}$ such that $\boldsymbol{F}/\sigma_i \cong \boldsymbol{A}_i$ (for $i = 1, 2$).

We claim that $\sigma_1 \circ \sigma_2 = \Phi_F$. Suppose otherwise, and let μ be a maximal congruence on $\boldsymbol{F}$ containing $\sigma_1 \circ \sigma_2$. By the correspondence theorem the factor congruence μ/σ_i is a maximal congruence on $\boldsymbol{F}/\sigma_i \cong \boldsymbol{A}_i$, and so

$$\rho_i/\sigma_i = R(\boldsymbol{F}/\sigma_i) \subseteq \mu/\sigma_i.$$

Again by the correspondence theorem we conclude that $\rho_i \subseteq \mu$ for $i = 1, 2$, which implies that $\rho_1 \circ \rho_2 \subseteq \mu$, contradicting $\rho_1 \circ \rho_2 = \Phi_F$.

We now have

$$\frac{\boldsymbol{F}}{\sigma_1 \cap \sigma_2} \cong \frac{\boldsymbol{F}}{\sigma_1} \times \frac{\boldsymbol{F}}{\sigma_2} \cong \boldsymbol{A}_1 \times \boldsymbol{A}_2,$$

which implies that $\boldsymbol{A}_1 \times \boldsymbol{A}_2$ is n-generated. □

LEMMA 4.8. *If $\boldsymbol{A}$ is a finite algebraic structure in a congruence permutable, congruence uniform variety then $d(\boldsymbol{A}^k) = \mathbf{d}((\boldsymbol{A}^*)^k)$ for all $k \geq 2$.*

PROOF. An immediate corollary of Lemma 4.7. □

We can now prove the main result of this section, which is a general version of 'Wiegold dichotomy'.

THEOREM 4.9. *Let $\boldsymbol{A}$ be a nontrivial finite group, ring, module, algebra or a Lie algebra. Suppose that $\boldsymbol{S}_1, \ldots, \boldsymbol{S}_k$ are all the distinct isomorphism types of simple quotients of $\boldsymbol{A}$. If $\mathbf{d}(\boldsymbol{S}_i)$ grows logarithmically for all i then $\mathbf{d}(\boldsymbol{A})$ grows logarithmically as well; otherwise $\mathbf{d}(\boldsymbol{A})$ grows linearly.*

PROOF. From Theorem 3.4 we know that each $\mathbf{d}(\boldsymbol{S}_i)$ grows either logarithmically or linearly. If some $\mathbf{d}(\boldsymbol{S}_i)$ grows linearly, then combining the fact that $d(\boldsymbol{S}_i^n) \leq d(\boldsymbol{A}^n)$ and Proposition 2.1(iii), we conclude that $\mathbf{d}(\boldsymbol{A})$ grows linearly.

So let us now suppose that all sequences $\mathbf{d}(\boldsymbol{S}_i)$ grow logarithmically. From Lemma 4.8 we know that $\mathbf{d}(\boldsymbol{A})$ and $\mathbf{d}(\boldsymbol{A}^*)$ are eventually equal, and from Lemma 4.4 that $\boldsymbol{A}^* \cong \boldsymbol{S}_{i_1} \times \cdots \times \boldsymbol{S}_{i_l}$, where $\{i_1, \ldots, i_l\} = \{1, \ldots, k\}$. We now have, for $n \geq 2$,

$$d(\boldsymbol{A}^n) = d((\boldsymbol{A}^*)^n) = d(\boldsymbol{S}_{i_1}^n \times \cdots \times \boldsymbol{S}_{i_l}^n) \leq d(\boldsymbol{S}_{i_1}^n) + \cdots + d(\boldsymbol{S}_{i_l}^n).$$

This is a sum of l logarithmic functions, and so has a logarithmic upper bound. □

Combining this theorem with Corollaries 3.5–3.9 and with Lemma 3.3, we obtain the following corollaries.

COROLLARY 4.10. *For a nontrivial finite group $\boldsymbol{G}$ the sequence $\mathbf{d}(\boldsymbol{G})$ grows logarithmically if $\boldsymbol{G}$ is perfect, and linearly otherwise.*

COROLLARY 4.11. *For a nontrivial finite ring $\boldsymbol{R}$ the sequence $\mathbf{d}(\boldsymbol{R})$ grows logarithmically if the ideal $\boldsymbol{R} \cdot \boldsymbol{R}$ generated by $\{rs : r, s \in R\}$ is equal to $\boldsymbol{R}$, and grows linearly otherwise. In particular, if $\boldsymbol{R}$ has a (left or right) identity then $\mathbf{d}(\boldsymbol{R})$ grows logarithmically.*

PROOF. If $\boldsymbol{R} \cdot \boldsymbol{R} = \boldsymbol{R}$ then the same property holds for every simple quotient of $\boldsymbol{R}$. So every simple quotient of $\boldsymbol{R}$ has an identity by the Wedderburn–Artin theorem, and it follows that $\mathbf{d}(\boldsymbol{R})$ grows logarithmically by Theorem 4.9 and Corollary 3.6. If $\boldsymbol{R} \cdot \boldsymbol{R} \neq \boldsymbol{R}$ then $\boldsymbol{R}/(\boldsymbol{R} \cdot \boldsymbol{R})$ is a nontrivial zero ring, and so $\boldsymbol{R}$ has a simple quotient with zero multiplication, implying that $\mathbf{d}(\boldsymbol{R})$ grows linearly. □

COROLLARY 4.12. *For a nontrivial finite module $\boldsymbol{M}$ over a ring $\boldsymbol{R}$ the sequence $\mathbf{d}(\boldsymbol{M})$ grows linearly.*

COROLLARY 4.13. *For a nontrivial finite algebra $\boldsymbol{A}$ over a field $\boldsymbol{F}$ the sequence $\mathbf{d}(\boldsymbol{A})$ grows logarithmically if $\boldsymbol{A} \cdot \boldsymbol{A} = \boldsymbol{A}$, and linearly otherwise. In particular, if $\boldsymbol{A}$ has a (left or right) identity then $\mathbf{d}(\boldsymbol{A})$ grows logarithmically.*

COROLLARY 4.14. *For a nontrivial finite Lie algebra $\boldsymbol{L}$ over a field $\boldsymbol{F}$ the sequence $\mathbf{d}(\boldsymbol{L})$ grows logarithmically if $\boldsymbol{L}$ is perfect, and linearly otherwise.*

REMARK 4.15. For 'nonclassical' algebraic structures $\mathbf{d}$-sequences can also have exponential growth; for example, this is the case with semigroups without identity

(see [29]). At present no finite algebraic structure is known for which the **d**-sequence does not have one of logarithmic, linear or exponential growth.

5. Infinite structures

In [23, 30] Wiegold, with Stewart and Wilson respectively, investigates the sequence $\mathbf{d}(\boldsymbol{G})$ for (finitely generated) infinite groups $\boldsymbol{G}$. The following main fundamental observation is that another type of growth—constant—makes its appearance.

- If $\boldsymbol{G}$ is nonperfect, $\mathbf{d}(\boldsymbol{G})$ grows linearly (as before).
- If $\boldsymbol{G}$ is simple, $\mathbf{d}(\boldsymbol{G})$ is (eventually) constant.
- If $\boldsymbol{G}$ is perfect, $\mathbf{d}(\boldsymbol{G})$ is bounded below by a constant and above by a logarithmic function.

The completeness of information here, however, is much less than in the finite case, and several interesting problems remain. We will discuss some of these in our more general context in the following section. In this section we will show how to utilize the notion of interpolation to prove that the **d**-sequences of infinite simple classical structures (with the exception of modules) are eventually constant.

Let $\boldsymbol{A}$ be an algebraic structure, and let $f : A^k \to A$ be a k-ary function. We say that f has the *interpolation property* if for every finite subset $F \subseteq A^k$ there exists a k-ary polynomial function p on $\boldsymbol{A}$ such that $f\restriction_F = p\restriction_F$. We say that $\boldsymbol{A}$ has the *k-ary interpolation property* if every k-ary function from A^k to A has the interpolation property; $\boldsymbol{A}$ has the *interpolation property* if this is the case for every $k \geq 1$. Clearly, for a finite structure, the interpolation property is equivalent to being functionally complete.

Istinger *et al.* [15] prove the following criterion for the interpolation property.

PROPOSITION 5.1 [15, Corollary 3.5]. *An algebraic structure $\boldsymbol{A}$ has the interpolation property if and only if the following conditions are satisfied.*

(i) *$\boldsymbol{A}$ is simple.*

(ii) *There exists a Mal'cev function from A^3 to A which has the interpolation property.*

(iii) *There exists a nonconstant function $q : A^2 \to A$ which has the interpolation property and for which there exists $a \in A$ such that $q(x, a) = q(a, x) = a$ for all $x \in A$.*

REMARK 5.2. If $\boldsymbol{A}$ is an infinite group, ring, algebra or Lie algebra then $\boldsymbol{A}$ has the interpolation property if and only if it is simple. Indeed, for the function q and element a appearing in Proposition 5.1(iii), we can choose $q = x^{-1}y^{-1}xy$, $a = 1$ for groups; $q = xy$, $a = 0$ for rings and algebras; and $q = [x, y]$, $a = 0$ for Lie algebras.

THEOREM 5.3. *If $\boldsymbol{A}$ is a finitely generated infinite algebraic structure, and if it has the unary interpolation property, then*

$$d(\boldsymbol{A}) \leq d(\boldsymbol{A}^n) \leq d(\boldsymbol{A}) + 1 \quad (n \in \mathbb{N}),$$

and so the sequence $\mathbf{d}(\boldsymbol{A})$ is eventually constant.

PROOF. Let $a_1, \ldots, a_n \in A$ be n distinct elements. We claim that

$$\boldsymbol{A}^n = \langle \Delta^n(A) \cup \{(a_1, \ldots, a_n)\}\rangle,$$

from which the theorem readily follows.

Let $(b_1, \ldots, b_n) \in A^n$ be arbitrary. Since $\boldsymbol{A}$ has the unary interpolation property there exists a polynomial function $f : A \to A$ such that $f(a_i) = b_i$ (when $i = 1, \ldots, n$). So there exist a term $t(x, y_1, \ldots, y_k)$ and elements $c_1, \ldots, c_k \in A$ such that $f(x) = t(x, c_1, \ldots, c_k)$ for all $x \in A$. Let $\hat{\boldsymbol{c}}_j = (c_j, \ldots, c_j) \in \Delta^n(A)$ for $j = 1, \ldots, k$. In $\boldsymbol{A}^n$ we have

$$\begin{aligned} t((a_1, \ldots, a_n), \hat{\boldsymbol{c}}_1, \ldots, \hat{\boldsymbol{c}}_k) &= (t(a_1, c_1, \ldots, c_k), \ldots, t(a_n, c_1, \ldots, c_k)) \\ &= (f(a_1), \ldots, f(a_n)) = (b_1, \ldots, b_n). \end{aligned}$$

Thus $(b_1, \ldots, b_n) \in \langle \Delta^n(A) \cup \{(a_1, \ldots, a_n)\}\rangle$, and the proof is complete. □

COROLLARY 5.4. *If $\boldsymbol{A}$ is an infinite, finitely generated simple group, ring, algebra or Lie algebra, the sequence $\mathbf{d}(\boldsymbol{A})$ is eventually constant.*

REMARK 5.5. There are many examples of finitely generated simple groups in the literature: Tarski monsters [19] and Thompson–Higman groups [11] are probably best known. Simple Artinian algebras over a field $\boldsymbol{F}$ are central in algebra via the Wedderburn–Artin theorem. We determine their $\mathbf{d}$-sequences precisely in the algebraically closed case in the following section. There are many other examples of finitely generated simple algebras, the best-known ones being the Weyl algebras [8, Corollary 1.15]. Likewise, simple Lie algebras play a central role within the theory of Lie algebras; see, for example, [13]. Perhaps somewhat surprisingly, finitely generated infinite simple rings seem less ubiquitous. O'Meara *et al.* [20] deduce the existence of such rings with identity as a consequence of their embedding theorem. We construct an example of a finitely generated infinite simple ring without identity in the following section.

The information about the growth rates of $\mathbf{d}$-sequences for the nonsimple case is by no means complete. As already stated, for groups, the nonperfect ones, of course, still have linear growth, but for perfect ones there is a gap. Wiegold and Wilson [30, Theorem 3.2] prove that the $\mathbf{d}$-sequence of an infinite perfect group is bounded above by a logarithmic function. This has a consequence that if a perfect simple group has a finite nontrivial homomorphic image then its $\mathbf{d}$-sequence does grow logarithmically. But in the absence of such a homomorphic image, at present, one cannot even guarantee that the growth is either logarithmic or constant, instead of something in between the two.

We can prove the following analogues of [30, Theorem 3.2] for rings with identity, algebras with identity and Lie algebras.

THEOREM 5.6. *Let $\boldsymbol{R}$ be a finitely generated ring with identity. The sequence $\mathbf{d}(\boldsymbol{R})$ is bounded above by a logarithmic function.*

PROOF. This is a very simplified version of the argument in [30, Section 3]. We will prove that for every $n \geq 0$ we have $d(\boldsymbol{R}^{2^{n+1}}) \leq d(\boldsymbol{R}^{2^n}) + 1$, from which the assertion follows readily. Define $\delta : R^{2^n} \to R^{2^{n+1}}$ by $\delta(\boldsymbol{r}) = (\boldsymbol{r}, \boldsymbol{r})$ and suppose that $G = \{\boldsymbol{g}_1, \ldots, \boldsymbol{g}_m\}$ is a generating set for $\boldsymbol{R}^{2^n}$. Let $\mathbf{1} = (1, \ldots, 1)$ and $\mathbf{0} = (0, \ldots, 0)$, two elements of R^{2^n}, and let $\boldsymbol{g} = (\mathbf{1}, \mathbf{0})$. We claim that $\langle \delta(G) \cup \{\boldsymbol{g}\}\rangle = \boldsymbol{R}^{2^{n+1}}$. Indeed, let $(\boldsymbol{r}, \boldsymbol{s}) \in R^{2^{n+1}}$, with $\boldsymbol{r}, \boldsymbol{s} \in R^{2^n}$, be arbitrary. We have

$$(\boldsymbol{r}, \boldsymbol{s}) = \delta(\boldsymbol{r}) \cdot \boldsymbol{g} + \delta(\boldsymbol{s}) \cdot (\delta(\mathbf{1}) - \boldsymbol{g}) \in \langle \delta(G) \cup \{\boldsymbol{g}\}\rangle,$$

completing the proof. □

In the same way one proves the following result.

THEOREM 5.7. *Let $\boldsymbol{A}$ be a finitely generated algebra with identity over a field $\boldsymbol{F}$. The sequence $\mathbf{d}(\boldsymbol{A})$ is bounded above by a logarithmic function.*

For Lie algebras the proof relies on the same idea as the proof of Theorem 5.6, but is closer to the original proof of Wiegold and Wilson in [30].

THEOREM 5.8. *Let $\boldsymbol{L}$ be a finitely generated Lie algebra over a field $\boldsymbol{F}$. If $\boldsymbol{L}$ is nonperfect the sequence $\mathbf{d}(\boldsymbol{A})$ grows linearly, while if $\boldsymbol{L}$ is perfect the sequence $\mathbf{d}(\boldsymbol{A})$ is bounded above by a logarithmic function.*

PROOF. If $\boldsymbol{L}$ is nonperfect then it has an abelian quotient, and the theorem follows. So suppose that $\boldsymbol{L}$ is perfect, that is, $\boldsymbol{L} = [\boldsymbol{L}, \boldsymbol{L}]$. This time we prove that

$$d(\boldsymbol{L}^{2^{n+1}}) \leq d(\boldsymbol{L}^{2^n}) + d(\boldsymbol{L}).$$

Let $G = \{\boldsymbol{g}_1, \ldots, \boldsymbol{g}_m\}$ be a generating set for $\boldsymbol{L}^{2^n}$ and, similarly to before, define $\delta : L^{2^n} \to L^{2^{n+1}}$ by $\boldsymbol{x} \mapsto (\boldsymbol{x}, \boldsymbol{x})$. In addition, let H be a generating set for $\boldsymbol{L}$, and for $x \in L$ define

$$\beta(x) = (x, 0, \ldots, 0) \in L^{2^n},$$
$$\gamma(x) = (x, \ldots, x, 0, \ldots, 0) \in L^{2^{n+1}},$$

where $\beta(x)$ has $2^n - 1$ zeros, while $\gamma(x)$ has 2^n entries equal to x and 2^n entries equal to 0. We claim that

$$\boldsymbol{L}^{2^{n+1}} = \langle \delta(L^{2^n}) \cup \gamma(L)\rangle = \langle \delta(G) \cup \gamma(H)\rangle.$$

Indeed, for arbitrary $a, b \in L$,

$$\beta([a, b]) = [\delta(\beta(a)), \gamma(b)] \in \langle \delta(L^{2^n}) \cup \gamma(L)\rangle.$$

Since $\boldsymbol{L}$ is perfect,

$$\langle \delta(L^{2^n}) \cup \gamma(L)\rangle \supseteq \langle \{\beta([a, b]) : a, b \in L\}\rangle = \beta([\boldsymbol{L}, \boldsymbol{L}]) = \boldsymbol{L} \oplus \mathbf{0}^{2^{n-1}}.$$

In an analogous way we can generate any $\mathbf{0}^i \oplus \boldsymbol{L} \oplus \mathbf{0}^{2^{n+1}-i}$ for $i = 1, \ldots, 2^n$. To generate $\mathbf{0}^i \oplus \boldsymbol{L} \oplus \mathbf{0}^{2^{n+1}-i}$ for $i = 2^n + 1, \ldots, 2^{n+1}$ we note that

$$(\underbrace{0, \ldots, 0}_{2^n}, \underbrace{x, \ldots, x}_{2^n}) = \delta((x, \ldots, x)) - \gamma(x),$$

and repeat the above argument. Adding all these subalgebras together gives us $\boldsymbol{L}^{2^{n+1}}$. □

6. Further remarks concerning infinite rings, modules and algebras

Modules were absent from our considerations in the previous section. They certainly can never have the interpolation property, not even the unary one. In Section 4 we saw that finite modules always have linearly growing **d**-sequences (Corollary 4.12). Nonetheless, infinite modules *can* have constant **d**-sequences, as the following example shows.

EXAMPLE 6.1. Let $\boldsymbol{V}$ be an infinite-dimensional vector space over a field $\boldsymbol{F}$. Consider $\boldsymbol{V}$ as an $\boldsymbol{E}$-module $\bar{\boldsymbol{V}}$, where $\boldsymbol{E}$ is the endomorphism ring of $\boldsymbol{V}$. Then $\mathbf{d}(\bar{\boldsymbol{V}}) = (1, 1, 1, 1, \ldots)$. Indeed, if $e_1, e_2, \ldots$ are distinct elements in an $\boldsymbol{F}$-basis for $\boldsymbol{V}$ then $\bar{\boldsymbol{V}}^n = \langle (e_1, \ldots, e_n) \rangle$.

QUESTION 6.2. What other growth rates are possible for infinite simple modules?

In Section 3 we saw that the **d**-sequences of nontrivial finite simple classical structures are always logarithmic or linear. Furthermore, we saw that this dichotomy corresponds precisely to the following: perfect/nonperfect for groups and Lie algebras; identity element/no identity element for rings and algebras. Furthermore, in Section 5 we saw that this dichotomy persists for infinite groups and Lie algebras. We will now demonstrate that this is not the case with rings, by means of exhibiting a finitely generated infinite simple ring without identity, which by Corollary 5.4 must have an eventually constant **d**-sequence.

EXAMPLE 6.3. We begin by constructing a semigroup, modifying (and simplifying at the same time, since we are just after a single particular example) ideas from Byleen [4]. Let A and B be two (disjoint) countably infinite alphabets. Let $P = (p_{ij})_{A \times B}$ be a matrix with entries from the set $A \cup B \cup \{0\}$, satisfying the following properties.

(P1) For every $n \geq 1$, every collection $a_1, \ldots, a_n \in A$ of distinct indices, and every collection $c_1, \ldots, c_n \in A \cup B \cup \{0\}$, there exist infinitely many distinct $b \in B$ such that $p_{a_i,b} = c_i$ for all $i = 1, \ldots, n$.

(P2) Dually, for every $n \geq 1$, every collection $b_1, \ldots, b_n \in B$ of distinct indices, and every collection $c_1, \ldots, c_n \in A \cup B \cup \{0\}$, there exist infinitely many distinct $a \in A$ such that $p_{a,b_i} = c_i$ for all $i = 1, \ldots, n$.

(P3) If $a'_1, a'_2, \ldots$ and $b'_1, b'_2, \ldots$ are fixed enumerations of A and B respectively, then $p_{a'_i,b'_i} = b'_{i+1}$, $p_{a'_i,b'_{i+1}} = a'_{i+1}$ for all $i = 1, 2, \ldots$.

In order to see that such a matrix exists one may reason as follows. Condition (P3) completely determines the main diagonal and the diagonal immediately above it in P. Now consider the countable set

$$T = \{(m, a_1, \ldots, a_n, c_1, \ldots, c_n) : m, n \in \mathbb{N}, \\ a_1, \ldots, a_n \in A, a_i \neq a_j \ (i \neq j), c_1, \ldots, c_n \in A \cup B \cup \{0\}\},$$

and let $\boldsymbol{t}_1, \boldsymbol{t}_2, \ldots$ be an enumeration of it. For each

$$\boldsymbol{t}_k = (m, a_1, \ldots, a_n, c_1, \ldots, c_n) \quad (k = 1, 2, \ldots)$$

we find a column $b \in B$ which is to the right of the columns used for all the previous $\boldsymbol{t}_l$, and such that all the coordinates (a_i, b) (where $i = 1, \ldots, n$) are above the second main diagonal. Then we set $p_{a_i,b} = c_i$ (where $i = 1, \ldots, n$). This choice ensures that condition (P1) is satisfied. It also leaves all the entries below the main diagonal undefined; these entries can be used in an analogous way to ensure that (P2) is satisfied. Finally, the entries remaining undefined may now be defined arbitrarily.

Let $\boldsymbol{S}$ be the semigroup with zero 0 defined by the presentation

$$\langle A, B \mid ab = p_{ab} \ (a \in A, b \in B)\rangle.$$

A routine verification shows that

$$(\{\beta\alpha : \alpha \in A^*, \beta \in B^*\} \cup \{0\}) \setminus \{\epsilon\},$$

where ϵ denotes the empty word, is a set of unique normal forms for S. (This is probably most easily accomplished by verifying that the above presentation, with the addition of relations $c0 = 0c = 0$, for $c \in A \cup B \cup \{0\}$, is a terminating, confluent rewriting system.)

LEMMA 6.4. *For every $n \in \mathbb{N}$, every collection $\alpha_1, \ldots, \alpha_n \in A^+$ of distinct words, and every finite subset $B_0 \subseteq B$ there exists $b \in B$ such that*

$$b, \alpha_1 b, \alpha_2 b, \ldots, \alpha_n b$$

are distinct elements of $B \setminus B_0$.

PROOF. Proceed by induction on the combined length L of all the α_j. Case $L = 1$ means that $n = 1$ and $\alpha_1 \in A$; the assertion then follows from (P1). Consider now arbitrary $\alpha_1, \ldots, \alpha_n$ with combined length greater than 1, and suppose that the assertion is true for all collections with a smaller combined length. Suppose that $a_1, \ldots, a_k$ are the distinct final letters appearing in $\alpha_1, \ldots, \alpha_n$, so that we can write

$$\{\alpha_1, \ldots, \alpha_n\} = \{\alpha'_{ij} a_j : j = 1, \ldots, k, i = 1, \ldots, p_j\}.$$

Notice that some α'_{ij}, at most one for every j, may be empty. By induction, for every $j = 1, \ldots, k$, there exists $b_j \in B$ such that

$$b_j, \alpha'_{ij} b_j \quad (i = 1, \ldots, p_j)$$

are distinct elements of the set

$$B \setminus (\{b_l, \alpha'_{il} b_l : l < j, i = 1, \ldots, p_l\} \cup B_0).$$

By (P1) there exists

$$b \in B \setminus (\{\alpha'_{ij} b_j : j = 1, \ldots, k, i = 1, \ldots, p_k\} \cup B_0)$$

such that

$$p_{a_j, b} = b_j \quad \text{for } j = 1, \ldots, k.$$

But then

$$\begin{aligned} \{\alpha_1 b, \ldots, \alpha_n b\} &= \{\alpha'_{ij} a_j b : j = 1, \ldots, k, i = 1, \ldots, p_k\} \\ &= \{\alpha'_{ij} b_j : j = 1, \ldots, k, i = 1, \ldots, p_k\}, \end{aligned}$$

a set of n distinct elements from $B \setminus B_0$, and all distinct from b. □

LEMMA 6.5. *For every $n \in \mathbb{N}$, every collection $\beta_1, \ldots, \beta_n \in A^+$ of distinct words, and every finite subset $A_0 \subseteq A$, there exists $a \in A$ such that*

$$a, a\beta_1, a\beta_2, \ldots, a\beta_n$$

are distinct elements of $A \setminus A_0$.

PROOF. This is dual to Lemma 6.4. □

LEMMA 6.6. *For every $n \in \mathbb{N}$, any n distinct nonzero elements $s_1, \ldots, s_n \in S \setminus \{0\}$, and any n elements $t_1, \ldots, t_n \in S$, there exist $u, v \in S$ such that*

$$u s_i v = t_i \quad \text{for } i = 1, \ldots, n.$$

PROOF. Write $s_i = \beta_i \alpha_i$, with $\alpha_i \in A^*$, $\beta_i \in B^*$. By Lemma 6.4 there exists $b \in B$ such that all $\alpha_i b$ belong to B, and in addition

$$\alpha_i \neq \alpha_j \Rightarrow \alpha_i b \neq \alpha_j b.$$

Thus, the elements

$$\beta_1(\alpha_1 b), \beta_2(\alpha_2 b), \ldots, \beta_n(\alpha_n b) \in B^+$$

are all distinct. By Lemma 6.5 there exists $a \in A$ such that

$$a_1 = a\beta_1\alpha_1 b, a_2 = a\beta_2\alpha_2 b, \ldots, a_n = a\beta_n\alpha_n b$$

are n distinct elements of A. By (P1) there exists $c \in B$ such that

$$p_{a_j, c} = t_j \quad \text{for } j = 1, \ldots, n.$$

Setting $u = a$ and $v = bc$ completes the proof. □

LEMMA 6.7. *The semigroup* $\boldsymbol{S}$ *has the following properties.*

(i) $\boldsymbol{S}$ *is finitely generated.*
(ii) $\boldsymbol{S}$ *is congruence free.*
(iii) $\boldsymbol{S}$ *has a zero.*
(iv) $\boldsymbol{S}$ *has no identity element.*

PROOF. (i) An easy inductive argument based on property (P3) shows that $\boldsymbol{S} = \langle a_1, b_1 \rangle$.

(ii) An immediate consequence of Lemma 6.6.

(iii) Follows directly from the definition of S.

(iv) Consider an arbitrary element $\beta\alpha \in S$. If α is nonempty then $\beta\alpha a \neq a$ for any $a \in A$, while if β is nonempty then $b\beta\alpha \neq b$ for any $b \in B$. In any case, $\beta\alpha$ is not an identity element. □

Let us now consider the semigroup ring $\mathbb{Z}_2\boldsymbol{S}$. The set $I = \{0, 1 \cdot 0\}$ is an ideal in this ring, and we can factor it out to obtain the ring $\boldsymbol{R} = \mathbb{Z}_2\boldsymbol{S}/I$. Every nonzero element of $\boldsymbol{R}$ has the form $s_1 + \cdots + s_n$, where $s_1, \ldots, s_n$ are distinct nonzero elements of S.

Clearly $\boldsymbol{R}$ is generated by S, and so it is finitely generated. We claim that $\boldsymbol{R}$ is simple. Indeed, suppose that J is a nonzero ideal of $\boldsymbol{R}$, with $0 \neq s_1 + \cdots + s_n \in J$. Let $s \in S$ be arbitrary. By Lemma 6.6 there exist $u, v \in S$ such that

$$us_1v = s, \quad us_iv = 0 \quad \text{for } i = 2, \ldots, n.$$

But then J contains

$$u(s_1 + \cdots + s_n)v = us_1v + us_2v + \cdots + us_nv = s.$$

It follows that $S \subseteq J$, and hence $J = R$. Thus $\boldsymbol{R}$ indeed is simple, and it follows from Corollary 5.4 that $\mathbf{d}(\boldsymbol{R})$ is constant.

Finally, we claim that $\boldsymbol{R}$ has no identity element. By Lemma 6.7(iv) no element of S is an identity. Suppose that $e = s_1 + \cdots + s_n$, with $n > 1$, is an identity of $\boldsymbol{R}$. By Lemma 6.6 there exist $u, v \in S$ such that $us_iv = s_i$ for all $i = 1, \ldots, n$. But then $uv \in S$ and

$$uv = uev = us_1v + \cdots + us_nv = s_1 + \cdots + s_n \notin S,$$

a contradiction. This completes Example 6.3.

The reader will recall from Theorem 5.3 and Corollary 5.4 that for any infinite simple group, ring or algebra $\boldsymbol{A}$ we have $d(\boldsymbol{A}^n) \leq d(\boldsymbol{A}) + 1$. Even for groups, it remains an open question whether there actually exist an infinite, finitely generated simple group $\boldsymbol{G}$ and $n \in \mathbb{N}$ such that $d(\boldsymbol{G}^n) = d(\boldsymbol{G}) + 1$.

EXAMPLE 6.8. It is very easy to construct a simple 'group-like' structure $\boldsymbol{A}$ such that $d(\boldsymbol{A}^2) = d(\boldsymbol{A}) + 1$. Indeed, just take any infinite simple group $\boldsymbol{G}$, and let $\boldsymbol{A} = \mathbf{EC}(\boldsymbol{G})$ be its extension by constants; then $d(\boldsymbol{A}) = 0$ and $d(\boldsymbol{A}^2) = 1$.

The analogue of the above question for other classical structures is also interesting. As an initial contribution we show the following result.

THEOREM 6.9. *If $\boldsymbol{A}$ is an Artinian simple algebra over an algebraically closed field $\boldsymbol{F}$ then* $\mathbf{d}(\boldsymbol{A}) = (2, 2, 2, \ldots)$.

PROOF. According to the Wedderburn–Artin theorem, the algebra $\boldsymbol{A}$ is isomorphic to the algebra $\boldsymbol{M}_k(\boldsymbol{F})$ of all $k \times k$ matrices over $\boldsymbol{F}$ for some k. In [6] the following result is proved for the case $\mathrm{char}(\boldsymbol{F}) \neq 2$: for any nonscalar matrix $B \in \boldsymbol{M}_k(\boldsymbol{F})$, there exists a matrix $C \in \boldsymbol{M}_k(\boldsymbol{F})$ such that $\langle B, C\rangle = \boldsymbol{M}_k(\boldsymbol{F})$. This can actually be proved without the extra supposition on the characteristic [Laffey, personal communication]. In particular, $d(\boldsymbol{M}_2(\boldsymbol{F})) = 2$.

Now let $B = (b_{ij})_{k\times k}$ be the matrix with $b_{11} = 1$ and $b_{ij} = 0$ otherwise, and let C be any matrix such that $\langle B, C\rangle = \boldsymbol{M}_k(\boldsymbol{F})$. Furthermore, let $p \in \boldsymbol{F}[x]$ be a polynomial such that $p(0) = 0$ and $p(d_1) = \cdots = p(d_n) = 1$, where $d_1, \ldots, d_n \in F$ are distinct. For each $t = 1, \ldots, n$ define a matrix $D_t = (d_{ij}^{(t)})_{k\times k}$ by $d_{11}^{(t)} = d_t$ and $d_{ij}^{(t)} = 0$ otherwise. From the proof of Theorem 5.3 we know that

$$\boldsymbol{M}_k(\boldsymbol{F})^n = \langle \hat{\boldsymbol{B}}, \hat{\boldsymbol{C}}, (D_1, \ldots, D_n)\rangle,$$

where $\hat{\boldsymbol{B}} = (B, \ldots, B)$ and $\hat{\boldsymbol{C}} = (C, \ldots, C)$. But $p(D_i) = B$, and hence $p((D_1, \ldots, D_n)) = \hat{\boldsymbol{B}}$. It follows that

$$\boldsymbol{M}_k(\boldsymbol{F})^n = \langle \hat{\boldsymbol{C}}, (D_1, \ldots, D_n)\rangle,$$

and the proof is complete. □

Acknowledgements

The authors are grateful to an anonymous referee and Peter Mayr for their thorough and sympathetic reading of the paper, and several helpful suggestions regarding both the presentation and specific results. The authors would also like to thank Robert Gray, Edmund Robertson, Max Neunhöffer and Arthur Geddes for many helpful conversations, and Thomas Laffey for the private communication appearing in the proof of Theorem 6.9.

References

[1] J. Berman and P. M. Idziak, 'Generative complexity in algebra', *Mem. Amer. Math. Soc.* **175** (2005).
[2] J. Berman, P. Idziak, P. Marković, R. McKenzie, M. Valeriote and R. Willard, 'Varieties with few subalgebras of powers', *Trans. Amer. Math. Soc.* **362** (2010), 1445–1473.
[3] S. Burris and H. P. Sankappanavar, *A Course in Universal Algebra* (Springer, New York, 1981).
[4] K. Byleen, 'Embedding any countable semigroup in a 2-generated congruence-free semigroup', *Semigroup Forum* **41** (1990), 145–153.

[5] H. Chen, 'Quantified constraint satisfaction and the polynomially generated powers property', in: *ICALP 2008, Part II*, Lecture Notes in Computer Science, 5126 (eds. L. Aceto *et al.*) (Springer, Berlin–Heidelberg, 2008), pp. 197–208.
[6] F. Gaines, 'Some generators for the algebra of $n \times n$ matrices', *Linear and Multilinear Algebra* **5** (1977/78), 95–98.
[7] W. Gaschütz, 'Zu einem von B. H. und H. Neumann gestellten Problem', *Math. Nachr.* **14** (1955), 249–252.
[8] K. R. Goodearl and R. B. Warfield Jr, *An Introduction to Noncommutative Noetherian Rings*, London Mathematical Society Student Texts, 16 (Cambridge University Press, Cambridge, 1989).
[9] G. Grätzer and A. Kisielewicz, 'A survey of some open problems on p_n-sequences and free spectra of algebras and varieties', in: *Universal Algebra and Quasigroup Theory (Jadwisin, 1989)*, Research and Exposition in Mathematics, 19 (Heldermann, Berlin, 1992), pp. 57–88.
[10] I. N. Herstein, *Noncommutative Rings*, Carus Mathematical Monographs, 15 (Mathematical Association of America, New York, 1968).
[11] G. Higman, *Finitely Presented Infinite Simple Groups*, Notes on Pure Mathematics, 8 (The Australian National University, Canberra, 1974).
[12] D. Hobby and R. McKenzie, *The Structure of Finite Algebras*, Contemporary Mathematics, 76 (American Mathematical Society, Providence, RI, 1988).
[13] J. E. Humphreys, *Introduction to Lie Algebras and Representation Theory*, Graduate Texts in Mathematics, 9 (Springer, New York–Berlin, 1980).
[14] J. Hyde, N. Loughlin, M. Quick, N. Ruškuc and A. Wallis, 'On generating direct powers of semigroups', in preparation.
[15] M. Istinger, H. K. Keiser and A. P. Pixley, 'Interpolation in congruence permutable algebras', *Math. Colloq.* **42** (1979), 229–239.
[16] W. D. Maurer and J. L. Rhodes, 'A property of finite simple nonabelian groups', *Proc. Amer. Math. Soc.* **16** (1965), 552–554.
[17] R. N. McKenzie, G. F. McNulty and W. F. Taylor, *Algebras, Lattices, Varieties,* Vol. I (Wadsworth, Monterey, CA, 1987).
[18] D. Meier and J. Wiegold, 'Growth sequences of finite groups V', *J. Aust. Math. Soc. (Ser. A)* **31** (1981), 374–375.
[19] A. Yu. Ol'šanskiĭ, 'An infinite group with subgroups of prime orders', *Izv. Akad. Nauk. SSSR Ser. Mat.* **44** (1980), 309–321 (in Russian); English translation: *Math. USSR-Izv.* **16** (1981), 279–289.
[20] K. C. O'Meara, C. I. Vinsonhaler and W. J. Wickless, 'Identity-preserving embeddings of countable rings into 2-generator rings', *Rocky Mountain J. Math.* **19** (1989), 1095–1105.
[21] L. Ribes and P. Zalesskii, *Profinite Groups* (Springer, Berlin, 2000).
[22] S. Shelah, *Classification Theory and the Number of Nonisomorphic Models*, Studies in Logic and the Foundations of Mathematics, 92 (North Holland, Amsterdam, 1990).
[23] A. G. R. Stewart and J. Wiegold, 'Growth sequences of finitely generated groups II', *Bull. Aust. Math. Soc.* **40** (1989), 323–329.
[24] H. Werner, 'Congruences on products of algebras and functionally complete algebras', *Algebra Universalis* **4** (1974), 99–105.
[25] J. Wiegold, 'Growth sequences of finite groups: collection of articles dedicated to the memory of Hanna Neumann, VI', *J. Aust. Math. Soc.* **17** (1974), 133–141.
[26] J. Wiegold, 'Growth sequences of finite groups II', *J. Aust. Math. Soc.* **20** (1975), 225–229.
[27] J. Wiegold, 'Growth sequences of finite groups III', *J. Aust. Math. Soc. (Ser. A)* **25** (1978), 142–144.
[28] J. Wiegold, 'Growth sequences of finite groups IV', *J. Aust. Math. Soc. (Ser. A)* **29** (1980), 14–16.
[29] J. Wiegold, 'Growth sequences of finite semigroups', *J. Aust. Math. Soc. (Ser. A)* **43** (1987), 16–20.
[30] J. Wiegold and J. S. Wilson, 'Growth sequences of finitely generated groups', *Arch. Math. (Basel)* **30** (1978), 337–343.

MARTYN QUICK, School of Mathematics and Statistics, University of St Andrews, St Andrews, KY16 9SS, UK
e-mail: martyn@mcs.st-and.ac.uk

N. RUŠKUC, School of Mathematics and Statistics, University of St Andrews, St Andrews, KY16 9SS, UK
e-mail: nik@mcs.st-and.ac.uk