

# On the Growth of Generating Sets for Direct Powers of Semigroups

J.T. Hyde, N.J. Loughlin, M. Quick, N. Ruškuc, A.R. Wallis

August 15, 2011

## Abstract

For a semigroup  $S$  its  $\mathbf{d}$ -sequence is  $\mathbf{d}(S) = (d_1, d_2, d_3, \dots)$ , where  $d_i$  is the smallest number of elements needed to generate the  $i$ th direct power of  $S$ . In this paper we present a number of facts concerning the type of growth  $\mathbf{d}(S)$  can have when  $S$  is an infinite semigroup, comparing them with the corresponding known facts for infinite groups, and also for finite groups and semigroups.

*2000 Mathematics Subject Classification:* 20M05, 20M20.

## 1 Introduction

For a semigroup  $S$  let  $d(S)$  denote the smallest number of generators needed to generate  $S$ , and let

$$\mathbf{d}(S) = (d(S), d(S^2), d(S^3), \dots),$$

where  $S^n$  is  $n$ th direct power of  $S$ . In this paper we present some observations regarding the growth of the sequence  $\mathbf{d}(S)$  for infinite semigroups  $S$ .

Wiegold and various co-authors in a series of papers investigated the sequence  $\mathbf{d}(S)$ , mostly when  $S$  is a finite group [14, 15, 16, 17, 8], but also when it is a finite semigroup [18] or an infinite group [19, 13]. In the context of this paper we can summarise their main findings as follows. For a finite semigroup  $S$  we have:

(FG1) If  $S$  is trivial then  $\mathbf{d}(S) = (1, 1, 1, \dots)$ .

(FG2) If  $S$  is a non-trivial perfect group then  $\mathbf{d}(S)$  grows logarithmically.

(FG3) If  $S$  is a monoid which is not a perfect group then  $\mathbf{d}(S)$  grows linearly.

(FG4) If  $S$  is not a monoid then  $\mathbf{d}(S)$  grows exponentially.

For  $S$  an infinite group we have:

- (IG1) If  $S$  is an infinite simple group then  $\mathbf{d}(S)$  is eventually constant.
- (IG2) If  $S$  is an infinite perfect group then  $\mathbf{d}(S)$  is bounded above by a logarithmic function.
- (IG3) If  $S$  is an infinite non-perfect group then  $\mathbf{d}(S)$  grows linearly.

To grow *logarithmically* (resp. *linearly*, *exponentially*) throughout the paper means that the sequence is bounded both below and above by logarithmic (resp. linear, exponential) functions.

The results from above concerning groups largely carry over to other ‘classical’ algebraic structures, such as rings, associative and Lie algebras; this is the topic of [9]. The purpose of the present article is to present some results concerning the growth of  $\mathbf{d}(S)$  for an infinite semigroup or monoid  $S$ . We mention in passing that recently  $\mathbf{d}$ -sequences have (re)appeared in the context of Universal Algebra, in connection with quantified constraint satisfaction problems; see [5]. Also, Berman et al. [1] undertake an in-depth study of several sequences closely related to  $\mathbf{d}$  and to direct powers.

One recurring theme in the results we present is that infinite semigroups and monoids compare to groups in ways that are often rather different from the same comparison in the finite case. For example, adopting a convention that slower growth rates are ‘better’, we see from (FG1)–(FG3) that growth rates of perfect groups, which are logarithmic, are better than those of non-perfect groups and monoids, which are linear. For infinite monoids, however, we have:

- (IG4) There exists an infinite non-group monoid  $S$  such that  $\mathbf{d}(S)$  is constant (Theorem 5.1).
- (IG5) There exists an infinite non-group monoid  $S$  such that  $\mathbf{d}(S)$  is logarithmic (Corollary 5.2).

Of course, just like groups, there is a natural upper bound on the growth of  $\mathbf{d}$ -sequences of monoids:

- (IG6) If  $S$  is any monoid the sequence  $\mathbf{d}(S)$  is bounded above by a linear function.

This follows from the fact that if  $S = \langle A \rangle$  and  $T = \langle B \rangle$  are two monoids then  $S \times T$  is generated by the set  $(A \times \{1\}) \cup (\{1\} \times B)$ . We will use this fact without special mention throughout.

However, some caution is needed, as the same does not hold for semigroups without identity. Indeed, we saw in (FG4) that finite semigroups may have exponential  $\mathbf{d}$ -sequences, and that this is governed precisely by the presence or absence of an identity element. The situation for infinite semigroups is very different:

- (IG7) There exists an infinite semigroup  $S$  without identity such that  $\mathbf{d}(S)$  is eventually constant (Corollary 7.1).
- (IG8) There exists an infinite semigroup  $S$  without identity such that  $\mathbf{d}(S)$  is logarithmic (Corollary 7.2).
- (IG9) There exists an infinite semigroup  $S$  without identity such that  $\mathbf{d}(S)$  is linear (Corollary 7.2).

The worst growth rate that a finite semigroup (or indeed any finite structure) can have is exponential. For infinite semigroups it can happen that  $d(S^n) = \infty$ , even if  $S$  itself is finitely generated. However, we prove:

- (IG10) If, for a semigroup  $S$ , we have  $d(S^2) < \infty$  then  $d(S^n) < \infty$  for all  $n$  and the sequence  $\mathbf{d}(S)$  is bounded above by an exponential function (Corollary 6.4).

The next possible growth rate is linear:

- (IG11) The growth of the  $\mathbf{d}$ -sequence of a semigroup cannot be strictly between exponential and linear (Theorem 6.5).

From (FG1) and (IG1) we see that simplicity has a major effect on the growth rate of both finite and infinite groups. The analogue of simplicity for semigroups is congruence freeness – not having any proper homomorphic images. We show:

- (IG12) The polycyclic monoid  $P_k$  ( $k \geq 2$ ) is an infinite congruence free monoid for which the  $\mathbf{d}$ -sequence grows linearly (Theorem 3.1).
- (IG13) There exists an infinite congruence free semigroup  $S$  without identity such that  $\mathbf{d}(S)$  is constant (Corollary 7.1).

In fact, we compute the precise values for the  $\mathbf{d}$ -sequence of the polycyclic monoid  $P_k$  and its relative the bicyclic monoid (Theorem 2.1). We also present some observations regarding the  $\mathbf{d}$ -sequences of semigroup and group actions (Section 8), and propose some open problems which seem worthy of investigation (Section 9).

## 2 The bicyclic monoid

The *bicyclic monoid*  $B$  is defined by the presentation

$$B = \langle b, c \mid bc = 1 \rangle.$$

Each element of  $B$  can be uniquely expressed as  $c^n b^m$  with  $n, m \in \mathbb{N}_0$ . The bicyclic monoid is *simple* (i.e. has no proper ideals), but is not congruence

free: the mapping  $b \mapsto 1, c \mapsto -1$  induces an epimorphism  $\pi : B \rightarrow \mathbb{Z}$ . In particular, from (IG3) and (IG6) we know that  $\mathbf{d}(B)$  grows linearly. Here we determine  $\mathbf{d}(B)$  precisely:

**Theorem 2.1.** *For each  $n \in \mathbb{N}$ , the minimal number of generators for the direct power  $B^n$  of the bicyclic monoid  $B$  is  $n + 1$ ; that is,*

$$\mathbf{d}(B) = (2, 3, 4, \dots).$$

*Proof.* For  $i = 1, \dots, n$  let

$$\beta_i = (\underbrace{1, \dots, 1}_{i-1}, b, \underbrace{1, \dots, 1}_{n-i}), \quad \gamma_i = (\underbrace{1, \dots, 1}_{i-1}, c, \underbrace{1, \dots, 1}_{n-i}).$$

Note that  $\langle \beta_1, \dots, \beta_n, \gamma_1, \dots, \gamma_n \rangle = B^n$ . Furthermore, let  $\gamma = (c, \dots, c)$ . From

$$\gamma_i = \beta_1 \beta_2 \dots \beta_{i-1} \beta_{i+1} \dots \beta_n \gamma$$

it follows that  $B^n = \langle \beta_1, \dots, \beta_n, \gamma \rangle$ .

On the other hand, since  $\mathbb{Z}$  is a homomorphic image of  $B$ , it follows that  $\mathbb{Z}^n$  is a homomorphic image of  $B^n$ , and hence  $d(B^n) \geq d(\mathbb{Z}^n) = n + 1$  (remembering that we are considering  $\mathbb{Z}^n$  as a semigroup here).  $\square$

### 3 The polycyclic monoids

The *polycyclic monoid*  $P_k$  ( $k = 2, 3, \dots$ ) is defined by the presentation:

$$P_k = \langle b_1, \dots, b_k, c_1, \dots, c_k \mid b_i c_i = 1, b_i c_j = 0 \ (1 \leq i, j \leq k, i \neq j) \rangle$$

Every non-zero element of  $P_k$  can be uniquely expressed in the form  $\gamma\beta$ , where  $\gamma$  is a word over  $\{c_1, \dots, c_k\}$  and  $\beta$  is a word over  $\{b_1, \dots, b_k\}$ . It is known that  $P_k$  is a congruence free monoid; see [7, Theorem 9.3.5]. In this section we determine the  $\mathbf{d}$ -sequence of  $P_k$ , and observe that unlike the infinite simple groups which have eventually constant  $\mathbf{d}$ -sequences by (IG1), the sequence  $\mathbf{d}(P_k)$  is linear. More precisely, we prove:

**Theorem 3.1.** *Let  $k, n \in \mathbb{N}$  with  $k \geq 2$ . The minimal number of generators for the direct power  $P_k^n$  of the polycyclic monoid  $P_k$  is  $nk + 1$ . In other words,*

$$\mathbf{d}(P_k) = (k + 1, 2k + 1, 3k + 1, \dots).$$

Before proving Theorem 3.1 we record the following lemma concerning the  $\mathbf{d}$ -sequences of Rees quotients. For a semigroup  $S$  and an ideal  $I$  of  $S$ , the *Rees quotient*  $S/I$  is defined as the quotient of  $S$  by the congruence  $\{(s, s) : s \in S \setminus I\} \cup (I \times I)$ . It can be identified with the set  $(S \setminus I) \cup \{0\}$ , where  $s \in S \setminus I$  represents the singleton  $\{s\}$ , and  $0$  represents the class  $I$ .

**Lemma 3.2.** *Let  $S$  be a monoid, and let  $I$  be an ideal of  $S$ . If the set  $S \setminus I$  generates  $S$  then  $\mathbf{d}(S) = \mathbf{d}(S/I)$ .*

*Proof.* Let  $n \in \mathbb{N}$  be arbitrary. Since  $(S/I)^n$  is a homomorphic image of  $S^n$ , we have  $d((S/I)^n) \leq d(S^n)$ .

For the converse inequality, we first note that since  $S \setminus I$  generates  $S$ , and  $1 \in S \setminus I$ , it follows that

$$S^n = \langle (S \setminus I)^n \rangle. \quad (1)$$

Now suppose  $Y \subseteq (S/I)^n$  generates  $(S/I)^n$  and  $|Y| = d((S/I)^n)$ . The complement of the set  $(S \setminus I)^n$  in  $(S/I)^n$  is

$$J = \{(x_1, \dots, x_n) \in (S/I)^n : x_i = 0 \text{ for some } i\}.$$

This is an ideal in  $(S/I)^n$ , and so no elements of  $J$  can take part in generating an element outside of  $J$ . Therefore, the submonoid of  $(S/I)^n$  generated by  $Y \cap (S \setminus I)^n$  must contain the entire set  $(S \setminus I)^n$ . Interpreting this back in  $S$ , we see that  $\langle Y \cap (S \setminus I)^n \rangle$  certainly contains  $(S \setminus I)^n$ , which in turn generates the entire  $S^n$  by (1). Therefore

$$d(S^n) \leq |Y \cap (S \setminus I)^n| \leq |Y| = d((S/I)^n),$$

and the lemma is proved.  $\square$

*Proof of Theorem 3.1.* For any  $i, j$  with  $1 \leq i \leq n$  and  $1 \leq j \leq k$  let

$$\beta_{ij} = (\underbrace{1, \dots, 1}_{i-1}, b_j, \underbrace{1, \dots, 1}_{n-i}), \quad \gamma_{ij} = (\underbrace{1, \dots, 1}_{i-1}, c_j, \underbrace{1, \dots, 1}_{n-i}).$$

Clearly these elements generate  $P_k^n$ . In addition, let

$$\begin{aligned} \delta_j &= \beta_{n-1,j} \beta_{n,j+1} = (1, \dots, 1, b_j, b_{j+1}) \quad (1 \leq j < k), \\ \zeta_j &= (c_j, \dots, c_j) \quad (1 \leq j \leq k). \end{aligned}$$

We claim that the set

$$\begin{aligned} X &= \{\beta_{ij} : 1 \leq i \leq n-2, 1 \leq j \leq k\} \cup \{\beta_{n-1,k}, \beta_{n1}\} \\ &\quad \cup \{\delta_j : 1 \leq j < k\} \cup \{\zeta_j : 1 \leq j \leq k\} \quad (2) \end{aligned}$$

generates  $P_k^n$ . We prove this by showing that all  $\beta_{ij}$  and all  $\gamma_{ij}$  belong to  $\langle X \rangle$ . Obviously  $\beta_{ij}$  ( $1 \leq i \leq n-2, 1 \leq j \leq k$ ) belong to  $X$ , as do  $\beta_{n1}$  and  $\beta_{n-1,k}$ .

**Claim 1.**  $\beta_{nj} \in \langle X \rangle$  for all  $j = 1, \dots, k$ .

*Proof.* Induction on  $j$ , the case  $j = 1$  being trivial. Suppose  $\beta_{nj} \in \langle X \rangle$  for some  $j < k$ . Then  $\langle X \rangle$  contains

$$\begin{aligned} & \beta_{1j}\beta_{2j}\dots\beta_{n-2,j}\delta_j\beta_{nj}\zeta_j \\ &= (b_j, \dots, b_j, 1, 1)(1, \dots, 1, b_j, b_{j+1})(1, \dots, 1, 1, b_j)(c_j, \dots, c_j, c_j, c_j) \\ &= (1, \dots, 1, 1, b_{j+1}) = \beta_{n,j+1}, \end{aligned}$$

as required.  $\square$

**Claim 2.**  $\gamma_{nj} \in \langle X \rangle$  for all  $j = 1, \dots, k$ .

*Proof.* A ‘reverse’ induction on  $j$ , starting at  $k$  and going downwards. For  $j = k$  we have

$$\begin{aligned} \langle X \rangle &\ni \beta_{1k}\beta_{2k}\dots\beta_{n-2,k}\beta_{n-1,k}\zeta_k \\ &= (b_k, \dots, b_k, b_k, 1)(c_k, \dots, c_k, c_k, c_k) = (1, \dots, 1, 1, c_k) = \gamma_{nk}. \end{aligned}$$

Suppose that  $\gamma_{n,j+1} \in \langle X \rangle$  for some  $j \geq 1$ . We have

$$\begin{aligned} \langle X \rangle &\ni \beta_{1j}\beta_{2j}\dots\beta_{n-2,j}\delta_j\gamma_{n,j+1}\zeta_j \\ &= (b_j, \dots, b_j, b_j, b_{j+1})(1, \dots, 1, 1, c_{j+1})(c_j, \dots, c_j, c_j, c_j) \\ &= (1, \dots, 1, 1, c_j) = \gamma_{nj}, \end{aligned}$$

completing the induction.  $\square$

**Claim 3.**  $\beta_{n-1,j} \in \langle X \rangle$  for all  $j = 1, \dots, k-1$ .

*Proof.*  $\langle X \rangle \ni \delta_j\gamma_{n,j+1} = \beta_{n-1,j}$ .  $\square$

**Claim 4.**  $\gamma_{ij} \in \langle X \rangle$  for all  $i = 1, \dots, n-1, j = 1, \dots, k$ .

*Proof.* We have

$$\begin{aligned} \langle X \rangle &\ni \beta_{1j}\dots\beta_{i-1,j}\beta_{i+1,j}\dots\beta_{nj}\zeta_j \\ &= (b_j, \dots, b_j, 1, b_j, \dots, b_j)(c_j, \dots, c_j, c_j, c_j, \dots, c_j) \\ &= (1, \dots, 1, c_j, 1, \dots, 1) = \gamma_{ij}, \end{aligned}$$

as required.  $\square$

Claims 1–4 complete the proof of the fact that the set  $X$  generates  $P_k^n$ . Clearly, the size of  $X$  is  $(n-2)k + 2 + (k-1) + k = nk + 1$ , and we conclude that  $d(P_k^n) \leq nk + 1$ .

For the reverse inequality, let us consider the monoid  $F_k$  with presentation

$$F_k = \langle b_1, \dots, b_k, c_1, \dots, c_k \mid b_i c_i = 1 \ (1 \leq i \leq k) \rangle;$$

this is the free product of  $k$  copies of the bicyclic monoid  $B$ . The set of elements in  $F_k$  containing  $b_i c_j$  with  $i \neq j$  as a subword forms an ideal  $I$  of  $F_k$ , and the Rees quotient  $F_k/I$  is naturally isomorphic to  $P_k$ . By Lemma 3.2 we have  $d(F_k^n) = d(P_k^n)$ , since  $b_i, c_i \notin I$ . The free product  $F_k$  also has the direct power  $B^k$  as a homomorphic image (by adding the relations  $b_i b_j = b_j b_i$ ,  $b_i c_j = c_j b_i$  for all  $i \neq j$ ). Hence  $B^{kn}$  is a homomorphic image of  $F_k^n$ , and from Theorem 2.1 we know that  $d(B^{kn}) = kn + 1$ , so that

$$d(P_k^n) = d(F_k^n) \geq d(B^{kn}) = kn + 1,$$

completing the proof. □

#### 4 Diagonal acts

In what follows we will make use of the language of semigroup actions. Suppose that a semigroup  $S$  acts on a set  $X$  on the right via  $(x, s) \mapsto x \cdot s$ . A set  $A \subseteq X$  generates  $X$  if  $A \cdot S' = X$ , where  $S'$  denotes the monoid obtained by adjoining an identity to  $S$  if it does not already have one. By analogy to our definition for semigroups, let  $d(X)$  denote the smallest size of a generating set for  $X$ . If  $d(X) < \infty$  we say that  $X$  is *finitely generated*, and if  $d(X) = 1$  we say that  $X$  is *cyclic*. The  $n$ th direct power of  $X$  is the set  $X^n$  equipped with the 'diagonal' action

$$(x_1, \dots, x_n) \cdot s = (x_1 \cdot s, \dots, x_n \cdot s).$$

The  $\mathbf{d}$ -sequence of  $X$  is now

$$\mathbf{d}(X) = (d(X), d(X^2), d(X^3), \dots).$$

Analogous definitions can be made for left acts, and for bi-acts.

A semigroup  $S$  acts on itself by right multiplication and by left multiplication. This gives rise to three acts: the right regular representation, the left regular representation and the regular bi-representation. In order to distinguish these from the semigroup  $S$ , let us denote them by  $R_r(S)$ ,  $R_l(S)$ ,  $R_b(S)$  respectively. The direct powers of these acts are referred to in [10] as the *diagonal acts* of  $S$ .

Our main observation, linking the diagonal acts and the  $\mathbf{d}$ -sequences, is the following:

**Theorem 4.1.** *For a semigroup  $S$  and  $n \in \mathbb{N}$  we have*

$$d(S^n) \leq d(R_b(S)^n) + d(S).$$

*Proof.* Let  $A$  be a generating set for  $R_b(S)$  with  $|A| = d(R_b(S))$ , and let  $B$  be a generating set of  $S$  with  $|B| = d(S)$ . For  $s \in S$ , let  $\bar{s} = (s, \dots, s) \in S^n$ . The diagonal  $\bar{S} = \{\bar{s} : s \in S\}$  is a subsemigroup of  $S^n$  isomorphic to  $S$ ;

it is therefore generated by the set  $\bar{B}$ . We claim that  $S^n$  is generated by the set  $A \cup \bar{B}$ . Indeed, since  $A$  generates  $R_b(S)$ , for an arbitrary  $(x_1, \dots, x_n) \in S^n$  there exist  $(a_1, \dots, a_n) \in A$  and  $s, t \in S'$  such that  $s \cdot (a_1, \dots, a_n) \cdot t = (s_1, \dots, s_n)$ . But then in the semigroup  $S^n$  we have

$$\bar{s}(a_1, \dots, a_n)\bar{t} = s \cdot (a_1, \dots, a_n) \cdot t = (x_1, \dots, x_n).$$

Since clearly  $\bar{s}, \bar{t} \in \bar{S}' = \langle \bar{B} \rangle'$ , the theorem is proved.  $\square$

**Corollary 4.2.** *If  $S$  is a finitely generated semigroup satisfying  $d(R_r(S)^2) = 1$  or  $d(R_l(S)^2) = 1$  then  $d(S^n) \leq d(S) + 1$  for every  $n \in \mathbb{N}$ , and so  $\mathbf{d}(S)$  is eventually constant.*

*Proof.* Without loss of generality assume  $d(R_r(S)^2) = 1$ . By [11, Lemma 2.6] this implies  $d(R_r(S)^n) = 1$  for all  $n \in \mathbb{N}$ , and hence  $d(R_b(S)^n) = 1$ , so that the result follows from Theorem 4.1.  $\square$

## 5 Partially recursive functions in one variable

The first example of a finitely generated monoid with  $d(R_r(S)^2) = 1$  given in [10] is the monoid  $R_{\mathbb{N}}$  of all partially recursive functions  $\mathbb{N} \rightarrow \mathbb{N}$  in one variable. For basic facts about partially recursive functions, and especially the existence of universal partially recursive functions which are crucial for the argument below, we refer the reader to any standard text on computability, such as [6]. It is shown in [10] that  $R_{\mathbb{N}}$  can be generated by four mappings; Corollary 4.2 implies that  $d(R_{\mathbb{N}}^n) \leq 5$  for all  $n$ . In fact, we can prove:

**Theorem 5.1.** *Every direct power of the monoid  $R_{\mathbb{N}}$  of all partially recursive functions can be generated by two elements, i.e.*

$$\mathbf{d}(R_{\mathbb{N}}) = (2, 2, 2, \dots).$$

*Proof.* Let  $\psi : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$  be a universal partially recursive function for the family of all partially recursive functions in one variable. Thus for every  $f \in R_{\mathbb{N}}$  there exists  $i \in \mathbb{N}$  such that  $xf = (i, x)\psi$  for all  $x \in \mathbb{N}$ . Let  $p_1, p_2, p_3, \dots$  be the sequence of prime numbers. Every  $x \in \mathbb{N}$  can be uniquely represented as a product  $\prod_{i=1}^{\infty} p_i^{x_i}$  where  $x_i \in \mathbb{N}_0$  and all but finitely many are equal to 0.

Let  $n \in \mathbb{N}$  be fixed. Let us define two tuples  $\bar{g} = (g, \dots, g)$  and  $h = (h_1, \dots, h_n)$  from  $R_{\mathbb{N}}^n$  as follows:

$$\left( \prod_{i=1}^{\infty} p_i^{x_i} \right) g = \prod_{i=1}^{\infty} p_{i+1}^{x_i}, \quad (3)$$

$$\left( \prod_{i=1}^{\infty} p_i^{x_i} \right) h_k = \begin{cases} p_1^{x_1+1} \prod_{i=2}^{\infty} p_i^{x_i} & \text{if } x_2 = 0 \\ (x_{2k}, \prod_{i=1}^{\infty} p_i^{x_{2n+1+i}}) \psi & \text{if } x_2 \neq 0. \end{cases} \quad (4)$$



It is a routine exercise to verify that  $g, h_1, \dots, h_k$  are all partially recursive.

We claim that  $R_{\mathbb{N}}^n$  is generated by  $\bar{g}$  and  $h$ . To this end let  $f = (f_1, \dots, f_n) \in R_{\mathbb{N}}^n$ . Let  $m_1, \dots, m_n \in \mathbb{N}$  be such that

$$(m_j, x)\psi = x f_j \quad (1 \leq j \leq n, x \in \mathbb{N}). \quad (5)$$

Let us consider the product

$$\bar{g}^2 h^{m_n} \bar{g}^2 h^{m_{n-1}} \dots \bar{g}^2 h^{m_1} \bar{g} h \in R_{\mathbb{N}}^n. \quad (6)$$

Its  $k$ th component ( $1 \leq k \leq n$ ) is

$$g^2 h_k^{m_n} g^2 h_k^{m_{n-1}} \dots g^2 h_k^{m_1} g h_k.$$

Let us determine how this mapping acts on an arbitrary  $x = \prod_{i=1}^{\infty} p_i^{x_i} \in \mathbb{N}$ :

$$\begin{aligned} & \left( \prod_{i=1}^{\infty} p_i^{x_i} \right) g^2 h_k^{m_n} g^2 h_k^{m_{n-1}} \dots g^2 h_k^{m_1} g h_k \\ &= \left( p_1^0 p_2^0 \prod_{i=1}^{\infty} p_{i+2}^{x_i} \right) h_k^{m_n} g^2 h_k^{m_{n-1}} \dots g^2 h_k^{m_1} g h_k && \text{(by (3))} \\ &= \left( p_1^{m_n} p_2^0 \prod_{i=1}^{\infty} p_{i+2}^{x_i} \right) g^2 h_k^{m_{n-1}} \dots g^2 h_k^{m_1} g h_k && \text{(by (4))} \\ &= \left( p_1^0 p_2^0 p_3^{m_n} p_4^0 \prod_{i=1}^{\infty} p_{i+4}^{x_i} \right) h_k^{m_{n-1}} \dots g^2 h_k^{m_1} g h_k && \text{(by (3))} \\ &= \left( p_1^{m_{n-1}} p_2^0 p_3^{m_n} p_4^0 \prod_{i=1}^{\infty} p_{i+4}^{x_i} \right) g^2 \dots g^2 h_k^{m_1} g h_k && \text{(by (4))} \\ & \vdots \\ &= \left( p_1^{m_1} p_2^0 \dots p_{2n-3}^{m_{n-1}} p_{2n-2}^0 p_{2n-1}^{m_n} p_{2n}^0 \prod_{i=1}^{\infty} p_{2n+i}^{x_i} \right) g h_k \\ &= \left( p_1^0 p_2^{m_1} p_3^0 \dots p_{2n-2}^{m_{n-1}} p_{2n-1}^0 p_{2n}^{m_n} p_{2n+1}^0 \prod_{i=1}^{\infty} p_{2n+i+1}^{x_i} \right) h_k && \text{(by (3))} \\ &= \left( m_k, \prod_{i=1}^{\infty} p_i^{x_i} \right) \psi && \text{(by (4))} \\ &= \left( \prod_{i=1}^{\infty} p_i^{x_i} \right) f_k. && \text{(by (5))} \end{aligned}$$

It then follows that the product (6) is actually equal to  $f = (f_1, \dots, f_n)$  and the theorem is proved.  $\square$

A further corollary of this and Theorem 4.1 is:

**Corollary 5.2.** *There exists an infinite non-group monoid  $S$  such that  $\mathbf{d}(S)$  grows logarithmically.*

*Proof.* Let  $T$  be any monoid such that  $\mathbf{d}(T)$  is (eventually) constant (such as  $R_{\mathbb{N}}$ , say), and let  $G$  be any group such that  $\mathbf{d}(G)$  is logarithmic (such as any finite non-abelian simple group). Then  $\mathbf{d}(T \times G)$  is bounded below by  $\mathbf{d}(G)$  and above by  $\mathbf{d}(T) + \mathbf{d}(G)$ , two logarithmic functions.  $\square$

## 6 Semigroups without identity

Robertson, Ruškuc and Wiegold [12] describe necessary and sufficient conditions for the direct product of two semigroups to be finitely generated or finitely presented. Here we will make use of their findings regarding the generators.

An element  $s$  of a semigroup  $S$  is said to be *indecomposable* if  $s \neq uv$  for any  $u, v \in S$ . Clearly, an indecomposable element must belong to every generating set of  $S$ . Now suppose that  $S$  and  $T$  are infinite semigroups. If  $s \in S$  is indecomposable then  $(s, t)$  is indecomposable in  $S \times T$  for every  $t \in T$ , and so  $S \times T$  is not finitely generated. Suppose, on the other hand that neither  $S$  nor  $T$  have any indecomposable elements. Take any generating sets  $A$  and  $B$  of  $S$  and  $T$  respectively, and write

$$a = \zeta(a)\sigma(a) \ (a \in A), \ b = \theta(b)\tau(b) \ (b \in B),$$

where  $\zeta(a) \in A, \sigma(a) \in S, \theta(b) \in B, \tau(b) \in T$ . With this notation we have:

**Proposition 6.1** ([12, Proposition 2.5]). *The direct product  $S \times T$  is generated by the set*

$$(A \cup \{\sigma(a) : a \in A\}) \times (B \cup \{\tau(b) : b \in B\}).$$

**Corollary 6.2** ([12, Theorem 2.1]). *The direct product  $S \times T$  of two infinite semigroups is finitely generated if and only if both  $S$  and  $T$  are finitely generated and neither has any indecomposable elements.*

**Corollary 6.3.** *For any two infinite semigroups  $S$  and  $T$  with no indecomposable elements we have*

$$d(S \times T) \leq 4d(S)d(T).$$

The first corollary for the growth of  $\mathbf{d}$ -sequences is as follows.

**Corollary 6.4.** *Let  $S$  be an infinite semigroup. If  $S^2$  is finitely generated then  $S^n$  is finitely generated for every  $n \in \mathbb{N}$ , and the sequence  $\mathbf{d}(S)$  is bounded above by an exponential function.*

*Proof.* By Corollaries 6.2, 6.3,  $S^2$  is finitely generated if and only if  $S$  is finitely generated and has no indecomposable elements, in which case we have

$$d(S^2) \leq 4d(S)^2.$$

It is easily seen that  $S$  having no indecomposable elements implies that  $S^n$  has no indecomposable elements, and so an easy induction shows that

$$d(S^n) \leq 4^{n-1}d(S)^n,$$

proving the corollary.  $\square$

We can also prove that the growth of the  $\mathbf{d}$ -sequence of a semigroup cannot be strictly between linear and exponential:

**Theorem 6.5.** *Let  $S$  be a finitely generated semigroup. If there exist  $p, q \in S$  such that  $pS = Sq = S$  then  $\mathbf{d}(S)$  is bounded above by a linear function, and otherwise it is bounded below by an exponential function.*

*Proof.* Suppose first that  $pS = Sq (= pSq) = S$  for some  $p, q \in S$ . Let  $e, f \in S$  be such that  $pe = p$  and  $fq = q$ . Let  $A$  be any finite generating set of  $S$ . In the direct power  $S^n$  ( $n > 1$ ) define the following tuples:

$$\begin{aligned} \Delta_p &= (p, \dots, p), \quad \Delta_q = (q, \dots, q), \\ \alpha_{i,a} &= (\underbrace{f, \dots, f}_{i-1}, a, \underbrace{e, \dots, e}_{n-i}) \quad (a \in A, i = 1, \dots, n). \end{aligned}$$

We claim that  $S^n$  is generated by the set

$$X = \{\Delta_p, \Delta_q\} \cup \{\alpha_{i,a} : a \in A, i = 1, \dots, n\},$$

from which it will immediately follow that  $d(S^n) \leq 2 + n|A|$ , a linear upper bound as required.

Let  $\sigma = (s_1, \dots, s_n) \in S^n$  be arbitrary, and let  $t_1, \dots, t_n \in S$  be such that  $pt_iq = s_i$ . Each  $t_i$  is a product of generators from  $A$ , say of length  $l_i$ . Replacing each  $a \in A$  by  $\alpha_{i,a}$  in this product, we obtain

$$\tau_i = (\underbrace{f^{l_i}, \dots, f^{l_i}}_{i-1}, t_i, \underbrace{e^{l_i}, \dots, e^{l_i}}_{n-i}) \in \langle X \rangle.$$

Letting  $m_i = l_1 + \dots + l_{i-1}$  and  $n_i = l_{i+1} + \dots + l_n$ , and multiplying the above tuples we obtain

$$\langle X \rangle \ni \tau_1 \dots \tau_n = (t_1 f^{m_1}, e^{m_2} t_2 f^{m_2}, \dots, e^{m_i} t_i f^{m_i}, \dots, e^{m_n} t_n).$$

Finally, pre- and postmultiplying by  $\Delta_p$  and  $\Delta_q$  respectively, proves that

$$\Delta_p \tau_1 \dots \tau_n \Delta_q = (pt_1q, \dots, pt_nq) = (s_1, \dots, s_n) = \sigma$$

belongs to  $\langle X \rangle$ , and so  $\langle X \rangle = S^n$  as required.

For the second assertion, without loss of generality assume that  $pS \neq S$  for all  $p \in S$ . Also, by Corollary 6.2, we may assume without loss that  $S$

has no indecomposable elements. Since  $S$  is finitely generated it follows that  $S$  has maximal principal right ideals, and that they are of the form  $aS$  for some  $a \in A$ . Since  $S$  itself is not a principal right ideal by assumption, it follows that there exist  $a_1, a_2 \in S$  such that  $a_1S$  and  $a_2S$  are two distinct maximal principal right ideals. Let  $R_j$  ( $j = 1, 2$ ) be the *strong orbit* (or  *$\mathcal{R}$ -class*) of  $a_j$ :

$$R_j = \{x \in S : xS = a_jS\}.$$

From the foregoing discussion it follows that  $R_1 \cap R_2 = \emptyset$  and

$$a_j \in xS \Rightarrow x \in R_j.$$

Let  $n \geq 1$ , and let  $X$  be any generating set of  $S^n$ . We claim that for any  $j_1, \dots, j_n \in \{1, 2\}$  there exists a generator  $\xi = (x_1, \dots, x_n) \in X$  such that  $x_i \in R_{j_i}$ . Since there are  $2^n$  choices for  $j_1, \dots, j_n$ , an exponential lower bound follows as required.

To prove our claim, consider the element  $\alpha = (a_{j_1}, \dots, a_{j_n}) \in S^n$ . If  $\alpha \in X$  there is nothing to prove. Otherwise,  $\alpha$  can be written as a product of elements of  $X$ . Let  $\xi = (x_1, \dots, x_n)$  be the leftmost generator in this product. Clearly we have  $a_{j_i} \in x_iS$ , which implies  $x_i \in R_{j_i}$ , as desired.  $\square$

Further corollaries will be derived in the next section.

## 7 Semigroups with slowly growing $d$ -sequences

In order to establish various examples of semigroups without identity, as required for (IG7)–(IG9), we utilise a construction introduced in [9] as a modification of an earlier construction by Byleen [2]. 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  $a_1, \dots, a_n \in A$  of distinct indices, and every collection  $c_1, \dots, c_n \in A \cup B \cup \{0\}$  there exist infinitely many distinct  $b \in B$  such that  $p_{a_i b} = c_i$  for all  $i = 1, \dots, n$ .
- (P2) Dually, for every  $n \geq 1$ , every collection  $b_1, \dots, b_n \in B$  of distinct indices, and every collection  $c_1, \dots, c_n \in A \cup B \cup \{0\}$  there exist infinitely many distinct  $a \in A$  such that  $p_{a b_i} = c_i$  for all  $i = 1, \dots, n$ .
- (P3) If  $a'_1, a'_2, \dots$  and  $b'_1, b'_2, \dots$  are fixed enumerations of  $A$  and  $B$  respectively,  $p_{a'_i b'_i} = b'_{i+1}$ ,  $p_{a'_i b'_{i+1}} = a'_{i+1}$  for all  $i = 1, 2, \dots$

The semigroup  $S = \mathcal{S}(A, B; P)$  is then defined by the following presentation:

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

The following properties of this semigroup are established in [9, Lemmas 6.6, 6.7]:

- (S1)  $S$  is finitely generated.
- (S2)  $S$  is congruence free.
- (S3)  $S$  has no identity element.
- (S4) For every  $n \in \mathbb{N}$ , any  $n$  distinct non-zero elements  $s_1, \dots, s_n \in S \setminus \{0\}$ , and any  $n$  elements  $t_1, \dots, t_n \in S$ , there exist  $u, v \in S$  such that  $us_i v = t_i$  for  $i = 1, \dots, n$ .

The property (S4) clearly implies

- (S5) Every bi-act  $R_b(S)^n$  is cyclic.

Combining this with Theorem 4.1 yields:

**Corollary 7.1.** *There exists a finitely generated, infinite, congruence free semigroup  $S$  with zero, but without identity, such that  $\mathbf{d}(S)$  is eventually constant.*

**Corollary 7.2.** *Let  $S$  be a semigroup without identity such that  $\mathbf{d}(S)$  is eventually constant, and let  $G$  be an infinite finitely generated group. Then the semigroup  $T = S \times G$  has no identity. Moreover, if  $\mathbf{d}(G)$  grows logarithmically then  $\mathbf{d}(T)$  grows logarithmically, while if  $\mathbf{d}(G)$  grows linearly then  $\mathbf{d}(T)$  grows linearly.*

*Proof.* The first assertion is trivial, and for the remaining two, if  $d(S^n) \leq c$  for all  $n \in \mathbb{N}$ , we have

$$d(G^n) \leq d(T^n) = d(S^n \times G^n) \leq 4d(S^n)d(G^n) \leq 4cd(G^n),$$

by Corollary 6.3. □

## 8 Some remarks on $\mathbf{d}$ -sequences of acts

As indicated in Section 4, group and semigroup actions can be considered as algebraic structures in their own right, and the  $\mathbf{d}$ -sequences of these structures can be investigated. For a group  $G$  acting on a set  $X$ , the number  $d(X^n)$  is simply the number of orbits of the action of  $G$  on the  $n$ -tuples of elements of  $X$ . The condition of  $\mathbf{d}(X)$  consisting of finite numbers is then equivalent to the action of  $G$  being *oligomorphic*; see [4, Section 4.1] or [3, Section 5.2]. There has been quite a lot of work concerning the growth of various sequences related to an oligomorphic group; see the references cited in [4]. We just record a trivial lower bound:

**Proposition 8.1.** *Let  $G$  be an oligomorphic permutation group acting on a set  $X$ . Then  $d(X^n) \geq B(n)$ , the  $n$ th Bell number.*

In particular, this gives us examples of  $\mathbf{d}$ -sequences growing faster than exponential, which, as we saw earlier, cannot happen for groups and semigroups themselves, or indeed any finite structures.

Our second observation relies on [4, Theorem 3.4]: *For every positive integer  $k$ , there is a permutation group  $G$  acting on an infinite set  $X$  which is  $k$ -transitive, and in which the stabiliser of any  $k + 1$  points is trivial.* Clearly, for such  $G$  and  $X$  we have  $d(X^n) < \infty$  for  $n = 1, \dots, k$ . Also, given any  $k + 1$  distinct points  $x_1, \dots, x_{k+1}$ , since their stabiliser is trivial, it follows that all the  $(k + 2)$ -tuples  $(x_1, \dots, x_{k+1}, y)$  ( $y \in X$ ) belong to different orbits, and hence  $d(X^n) = \infty$  for  $n \geq k + 2$ .

**Proposition 8.2.** *For every  $k \in \mathbb{N}$  there exists a group  $G$  acting on an infinite set  $X$  such that  $d(X^n) < \infty$  for  $n \leq k$  and  $d(X^n) = \infty$  for  $n \geq k + 2$ .*

For semigroup actions on finite sets we have

**Proposition 8.3.** *If a semigroup  $S$  acts on a finite set  $X$  with  $|X| > 1$  then  $\mathbf{d}(X)$  grows exponentially.*

*Proof.* Every element  $u = (x_1, \dots, x_n) \in X^n$  induces an equivalence relation  $\pi(u)$  on  $\{1, \dots, n\}$  as follows:

$$\pi(u) = \{(i, j) : x_i = x_j\}$$

with at most  $|X|$  equivalence classes. Furthermore, for every  $u \in X^n$  and every  $s \in S$  we have  $\pi(u) \subseteq \pi(u \cdot s)$ .

Suppose  $A$  is a generating set for  $X^n$ . For every equivalence relation  $\pi$  on  $\{1, \dots, n\}$  there must exist  $u \in A$  such that  $\pi(u) = \pi$ . Thus  $|A|$  is bounded below by  $S(n, |X|)$ , the Stirling number of the second kind, and hence by an exponential function. A trivial exponential upper bound is provided by  $|A| \leq |X|^n$ .  $\square$

But the actions of semigroups on infinite sets can behave very differently from group actions or semigroup actions on finite sets:

**Proposition 8.4.** *Let  $X$  be an arbitrary infinite set, and consider  $X$  as a  $T_X$ -act, where  $T_X$  is the full transformation monoid on  $X$ . Then*

$$\mathbf{d}(X) = (1, 1, 1, \dots).$$

*Proof.* For every  $n \in \mathbb{N}$ , the act  $X^n$  is generated by  $(x_1, \dots, x_n)$ , where  $x_1, \dots, x_n$  are arbitrary distinct elements of  $X$ .  $\square$

Further examples are provided by cyclic diagonal acts which we encountered in Section 4.

## 9 Concluding remarks and open problems

This paper demonstrates interesting possibilities for the behaviour of the  $\mathbf{d}$ -sequences of semigroups which parallel and contrast with the existing knowledge for groups. In our opinion the most interesting remaining questions concern possible intermediate rates of growth:

- Does there exist a group  $G$  such that the growth of  $\mathbf{d}(G)$  is strictly between constant and logarithmic?
- Does there exist a monoid  $S$  such that the growth of  $\mathbf{d}(S)$  is strictly between constant and logarithmic?
- Does there exist a monoid  $S$  such that the growth of  $\mathbf{d}(S)$  is strictly between logarithmic and linear?
- Does there exist a semigroup  $S$  acting on a set  $X$  such that  $\mathbf{d}(X)$  is: (a) logarithmic; (b) linear; (c) strictly between logarithmic and linear; (d) strictly between constant and logarithmic?

**Acknowledgements.** Most of the work on this project was done during the St Andrews Summer Research School 2008, of which the first, second and fifth authors were participants. We would like to thank the other participants: Zoe O'Connor, Alison Shaw, Alan Logan, Luke Blackburn, Geoffrey Beresford, Sam Baynes, Jonathan Fraser, Iain Nicol and Louis Morgan. The authors would also like to thank Robert Gray for a number of useful conversations, ideas, and pointers to literature.

## References

- [1] 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.
- [2] K. Byleen, Embedding any countable semigroup in a 2-generated congruence-free semigroup, *Semigroup Forum* 41 (1990), 145–153.
- [3] P.J. Cameron, *Permutation Groups*, LMS Student Texts 45, CUP, Cambridge, 1999.
- [4] P.J. Cameron, Aspects of infinite permutation groups, in *Groups St. Andrews 2005 Vol. 1*, C.M. Campbell et al. (eds.), London Math. Soc. Lecture Note Ser. 339, Cambridge Univ. Press, Cambridge, 2007, 1–35.
- [5] H. Chen, 'Quantified constraint satisfaction and the polynomially generated powers property', in L. Aceto et al. (eds.), *ICALP 2008, Part II*, *Lecture Notes in Computer Science* **5126**, 2008, pp. 197–208.

- [6] D.E. Cohen, *Computability and logic*, Ellis Horwood Ltd, Chichester, 1987.
- [7] M.V. Lawson, *Inverse Semigroups*, World Scientific, River Edge NJ, 1998.
- [8] D. Meier and J. Wiegold, Growth sequences of finite groups V, *J. Austral. Math. Soc. (Ser. A)* 31 (1981), 374–375.
- [9] M.R. Quick and N. Ruškuc, Growth of generating sets for direct powers of classical algebraic structures, *J. Austral. Math. Soc.* 89 (2010), 105–126.
- [10] E.F. Robertson, N. Ruškuc and M.R. Thomson, Diagonal acts of monoids, *Bull. Austral. Math. Soc.* 63 (2001), 167–175.
- [11] E.F. Robertson, N. Ruškuc and M.R. Thomson, On finite generation and other finiteness conditions for wreath products of semigroups, *Comm. Alg.* 30 (2002), 3851–3873.
- [12] E.F. Robertson, N. Ruškuc and J. Wiegold, Generators and relations of direct products of semigroups, *Trans. Amer. Math. Soc.* 350 (1998), 2665–2685.
- [13] A.G.R. Stewart and J. Wiegold, Growth sequences of finitely generated groups II, *Bull. Austral. Math. Soc.* 40 (1989), 323–329.
- [14] J. Wiegold, Growth sequences of finite groups, Collection of articles dedicated to the memory of Hanna Neumann, VI. *J. Austral. Math. Soc.* 17 (1974), 133–141.
- [15] J. Wiegold, Growth sequences of finite groups II, *J. Austral. Math. Soc.* 20 (1975), 225–229.
- [16] J. Wiegold, Growth sequences of finite groups III, *J. Austral. Math. Soc. (Ser. A)* 25 (1978), 142–144.
- [17] J. Wiegold, Growth sequences of finite groups IV, *J. Austral. Math. Soc. (Ser. A)* 29 (1980), 14–16.
- [18] J. Wiegold, Growth sequences of finite semigroups, *J. Austral. Math. Soc. (Ser. A)* 43 (1987), 16–20.
- [19] J. Wiegold and J.S. Wilson, Growth sequences of finitely generated groups, *Arch. Math. (Basel)* 30 (1978), 337–343.