GROWTH SEQUENCES OF FINITE SEMIGROUPS

JAMES WIEGOLD

Abstract

The growth sequence of a finite semigroup S is the sequence $\{d(S^n)\}$, where S^n is the nth direct power of S and d stands for minimum generating number. When S has an identity, $d(S^n) = d(T^n) + kn$ for all n, where T is the group of units and k is the minimum number of generators of $S \bmod T$. Thus $d(S^n)$ is essentially known since $d(T^n)$ is (see reference 4), and indeed $d(S^n)$ is then eventually piecewise linear. On the other hand, if S has no identity, there exists a real number $c > 1$ such that $d(S^n) \geqslant c^n$ for all $n \geqslant 2$.

1980 *Mathematics subject classification (Amer. Math. Soc.)*: 20 M 99.

1. Introduction

For a finitely generated semigroup S, the *growth sequence* is the sequence $\{d(S^n)\}$, where $d(S^n)$ means the minimum number of generators of the nth direct power S^n of S. In the spirit of [1], [2], [3], [4], [5], [6], where the growth sequences of finitely generated groups are discussed in detail, we ask: what is the growth sequence of a semigroup like?

Firstly, since S^n is always a homomorphic image of S^{n+1}, the sequence is monotonic increasing. However, that is about the only really simple observation to be made; for example, it is not true that $d(S^{n+m}) \leqslant d(S^n) + d(S^m)$ in general. In fact, S can be finitely generated without S^2 being finitely generated: the additive semigroup of positive integers is like this. To avoid such problems, we shall consider here only *finite* semigroups.

In the case of finite groups, there is a dichotomy between the imperfect and perfect cases (*op. cit.*). Roughly speaking, imperfect groups have eventually linear growth sequences, while those of perfect groups are essentially logarithmic, in that

they are majorised and minorised by logarithmic sequences. For finite semi-groups, there is also a dichotomy, but based this time on the existence or otherwise of an identity element.

Note that for finite groups, group generating sets and semigroup generating sets are the same, so there is no ambiguity in the notation in the following theorem.

THEOREM 1. *Let S be a finite semigroup with identity, T the subgroup of units, and k the minimum number of elements of S needed to generate S modulo T. Then for all $n \geqslant 1$,*

$$d(S^n) = d(T^n) + kn.$$

Since the asymptotic behaviour of $\{d(T^n)\}$ is known with great accuracy given certain structural ingredients [3], we can consider the case of semigroups with 1 to be solved. The results of [3] mean that $d(S^n) = (k + d(T/T'))n$ for large enough n if T is imperfect. If T is nontrivial and perfect, then $\{d(T^n)\}$ is essentially logarithmic, and so $\{d(S^n)\}$ is "piecewise-linear" with infinitely many discontinuities, and each linear section having gradient k.

Far less information is available for semigroups without identity. Indeed it is probably a very hard problem to decide this case. Some examples in §3 indicate possibilities. However, one has the broad picture:

THEOREM 2. *Let S be a finite semigroup of order t, without identity. Then for all $n \geqslant 2$,*

$$(2t/2t - 1)^n \leqslant d(S^n) \leqslant t^n.$$

Thus one can say that semigroup growth sequences are much faster than group growth sequences. Leaving out perfect groups, which have logarithmic-type sequences, the dichotomy is between linear-type sequences as in Theorem 1 (with $k \neq 0$), and exponential-type sequences as in Theorem 2. To be more precise, there are four types of behaviour, as indicated in the following table.

	Type of semigroup	Type of growth sequence
1.	Perfect group	Essentially logarithmic
2.	Semigroup with 1, imperfect or trivial group of units	Eventually linear
3.	Semigroup with 1, perfect group of units $\neq 1$	Eventually piecewise linear
4.	Semigroup without 1	Essentially exponential

2. Proofs

PROOF OF THEOREM 1. Firstly, it is clear that $d(S^n) \leqslant d(T^n) + kn$. This is because S has an identity element, 1 shall we say, and so S^n is generated by the n factors of the product. By the ith factor here we mean all "strings" in S^n whose components are all 1 outside the ith position.

Next, observe that any set X of generators for S^n must contain a set of generators for T^n, its group of units. The reason is that in any finite semigroup with identity, a product xy is a unit if and only if x an y are both units.

Take any element s of S. Then the element $\bar{s} := (s, 1, 1, \ldots, 1)$ of S^n is a product of elements of X, each of which will, of course, have elements of T in every component later than the first. Taking all the elements of X involved in expressions for all $\bar{s}$, one finds that they must include enough elements $(x, *, \ldots, *)$ so that the first components form a generating set for S, and the stars denote elements of T. In other words, X contains k elements $(u_1, *, \ldots, *)$, $\ldots, (u_k, *, \ldots, *)$, where $u_1, \ldots, u_k$ generate S modulo T. Similar arguments apply for the elements $(1, s, 1, \ldots, 1)$ etc., and we find that X contains kn elements which are different from each other and are not elements of T^n. By the remark at the beginning of the preceding paragraph, this means that $d(S^n) \geqslant kn + d(T^n)$, and so we have completed the proof of Theorem 1.

PROOF OF THEOREM 2. Here S is a semigroup without identity of order t. There cannot be elements x and y of S such that $Sx = S = yS$, for some power of such an x would be a right identity and some power of y a left identity. Thus without loss of generality we may assume that $|Sx| \leqslant t - 1$ for all x in S. But this means that, for every z in S^n,

$$|S^n z| \leqslant (t - 1)^n.$$

Let $z_1, z_2, \ldots, z_r$ be any elements of S^n. The subsemigroup A they generate has order at most $r + r(t - 1)^n$, because A consists of the elements $z_1, z_2, \ldots, z_r$ and products of them. Since $|S^n| = t^n$, in order that $A = S^n$ it must be the case that $\{1 + (t - 1)^n\} r \geqslant t^n$, or $r \geqslant t^n / (1 + (t - 1)^n)$. Very elementary arithmetic shows that

$$\frac{t^n}{1 + (t - 1)^n} \geqslant \left(\frac{2t}{2t - 1}\right)^n \quad \text{for } n \geqslant 2,$$

and this completes the proof of Theorem 2.

Note that the proof of this theorem is extremely elementary. It is not surprising, therefore, that the exponentiation constant $2t/(2t - 1)$ is very small. The main amiable feature is that it exceeds unity, and no doubt it should be possible to replace it by a much larger constant. Some investigation of the intersections $S^n z_i \cap S^n z_j$ could be of value. Note too that no mention is made of $d(S)$ in the

statement; we could strengthen it by observing that $d(S^n) \geq d(S)$ for all n. All the examples provided in §3 have growth sequences very much faster than the lower bound provided in Theorem 2.

3. Examples

We shall restrict ourselves here to examples of semigroups that are not groups, since groups have been covered adequately in the papers referred to at the end.

Firstly, an example to illustrate Theorem 1.

EXAMPLE 1. *Let T be any finite group and k any positive integer. Then there exists a semigroup S with identity having T as group of units and such that k elements are required to generate S modulo T.*

The referee has suggested the following easier example than my original one: my thanks to him for this.

Define $S_0 = T$ and inductively

$$S_k = S_{k-1} \cup \{z_k\}, \qquad z_k \notin S_{k-1}$$

with $z_k x = x z_k = z_k$ for all x in S_k. Then S_k has T as group of units, and k elements are required to generate S modulo T.

As indicated previously, semigroups without identity are not so easy. Firstly note that the obvious upper bound t^n for $d(S^n)$ is sometimes attained. To see this, take $S = L_t$, the semigroup of order t of left zeros, that is, that satisfies the law $xy = x$. Then $S^n \cong L_{t^n}$, every subset of S^n is a subsemigroup, and so all the elements are needed to generate it.

Before giving our next example, we prove an auxiliary result, which should perhaps be viewed in conjunction with Theorem 2.

LEMMA. *Let S be a semigroup of order t having α elements that are not products. Then for all $n \geq 1$, $d(S^n) \geq t^n - (t - \alpha)^n$.*

PROOF. If $x = (x_1, x_2, \ldots, x_n)$ is an element of S^n where at least one x_i is a non-product in S, then x is a non-product in S^n. Every generating set for S^n contains every such element, and a quick count proves that there are $t^n - (t - \alpha)^n$ of these.

EXAMPLE 2. *Let S be a finite cyclic semigroup of order t that is not a group. Then $d(S^n) = t^n - (t - 1)^n$ for all $n \geq 1$.*

Let a be a generator for S. Then a is the only element of S that is not a product, and thus we have $d(S^n) \geq t^n - (t-1)^n$ by the lemma. However, the nonproducts in S^n, that is, the elements $(a^{\lambda_1}, a^{\lambda_2}, \ldots, a^{\lambda_n})$ where $\lambda_i = 1$ for at least one i, actually generate S^n. Take any $(a^{\mu_1}, a^{\mu_2}, \ldots, a^{\mu_n})$. If any μ_i is 1, there is nothing to prove; so assume that that $\mu_i \geq 2$ or all 1. Then

$$(a^{\mu_1}, \ldots, a^{\mu_n}) = (a, \ldots, a)(a^{\mu_1 - 1}, \ldots, a^{\mu_n - 1}),$$

and an easy induction on $\min(\mu_1, \ldots, \mu_n)$ gives the answer.

In Example 2, it is the existence of nonproducts that causes the growth sequence to be fast. However, I have not been able to find a semigroup S without identity such that $d(S^n)$ is significantly less than 2^n for large n. Perhaps this reflects the true picture.

References

[1] James Wiegold, 'Growth sequences of finite groups', *J. Austral. Math. Soc.* **17** (1974), 133–141.
[2] James Wiegold, 'Growth sequences of finite groups II', *J. Austral. Math. Soc.* **20** (1975), 225–229.
[3] James Wiegold, 'Growth sequences of finite groups III', *J. Austral. Math. Soc.* **25** (1978), 142–144.
[4] James Wiegold, 'Growth sequences of finite groups IV', *J. Austral. Math. Soc.* **29** (1980), 14–16.
[5] D. Meier and James Wiegold, 'Growth sequences of finite groups V', *J. Austral. Math. Soc.* **31** (1981), 374–375.
[6] James Wiegold and John Wilson, 'Growth sequences of finitely generated groups', *Arch. Math.* **30** (1978), 337–343.

Department of Pure Mathematics
University College
Cardiff CF1 1XL
Wales, United Kingdom