NOTES

Edited by **Jimmie D. Lawson and William Adkins**

Number Theory and Semigroups of Intermediate Growth

Melvyn B. Nathanson

The semigroup S is *finitely generated* if it contains a finite subset A such that every element of S can be written as a product of not necessarily distinct elements of A. The *length* of an element $s \in S$ with respect to A, denoted $l_A(s)$, is the smallest integer m such that s can be written as the product of m elements of A. The length of the identity element is 0. The *growth function* $\gamma_A(n)$ of S with respect to A counts the number of elements $s \in S$ of length at most n, that is, $\gamma_A(n) = \text{card}\{s \in S : l_A(s) \leq n\}$.

The semigroup S has *polynomial growth* of degree k with respect to A if $\gamma_A(n) \leq c_0 n^k$ for some positive constant c_0 and all sufficiently large n. For example, if S is the free abelian semigroup of rank k generated by a set A of cardinality k, then the number of elements of length exactly m is $\binom{m+k-1}{k-1}$, and

$$\gamma_A(n) = \sum_{m=0}^{n} \binom{m+k-1}{k-1} = \binom{n+k}{k} = \frac{n^k}{k!} + O(n^{k-1}),$$

so S has polynomial growth of degree k.

The semigroup S has *exponential growth* with respect to A if there exists a real number $\theta > 1$ such that $\gamma_A(n) \geq \theta^n$ for all sufficiently large n. For example, if S is the free semigroup of rank $k \geq 2$ generated by a set A of cardinality k, then the number of elements of length exactly m is k^m, and

$$\gamma_A(n) = \sum_{m=0}^{n} k^m = \frac{k^{n+1} - 1}{k - 1} > k^n,$$

so S has exponential growth.

The semigroup S has *intermediate growth* with respect to A if, for every positive integer k and for every real number $\theta > 1$, we have

$$n^k < \gamma_A(n) < \theta^n \tag{1}$$

for all sufficiently large n. The purpose of this note is to give a simple and self-contained proof of the existence of semigroups of intermediate growth.

The rate of growth of a semigroup S is an intrinsic property of the semigroup, that is, the growth is independent of the choice of generating set. This is easy to prove, since if A and B are two generating sets for S, then each element of B can be written as a finite product of elements of A. Thus, there exists a constant $c > 0$ such that $l_A(b) \leq c$ for all $b \in B$. If $s \in S$ is a product of m elements of B, then s can be written as a product of at most cm elements of A, and so $l_A(s) \leq c l_B(s)$ for

all $s \in S$. Therefore, if $l_B(s) \leq n$, then $l_A(s) \leq cn$, and $\gamma_B(n) \leq \gamma_A(cn)$. Similarly, there exists a constant $c' > 0$ such that $\gamma_A(n) \leq \gamma_B(c'n)$. It follows that the functions $\gamma_A(n)$ and $\gamma_B(n)$ have the same growth rates (polynomial, exponential, or intermediate).

It is not obvious that semigroups of intermediate growth exist. In the analogous case of a group G generated by a finite set A, the length of an element $g \in G$ is the smallest number m such that g can be represented in the form

$$g = a_1^{\pm 1} \cdots a_m^{\pm 1},$$

where $a_1, \ldots, a_m \in A$. In a famous problem in this MONTHLY in 1968, Milnor [**5**] asked if there exist groups of intermediate growth. The question for groups was answered affirmatively by Grigorchuk [**1**, **2**, **4**]. Semigroups of intermediate growth have also been constructed, but the proofs that their growth functions satisfy (1) are complicated. The semigroup constructed in Theorem 1 is known, but the proof by means of elementary number theory is new. We prove the intermediate growth property using only Chebyshev's Theorem [**6**, Theorem 6.3] that $\pi(x)$, the number of primes up to x, satisfies the inequalities

$$\frac{c_1 x}{\log x} \leq \pi(x) \leq \frac{c_2 x}{\log x} \tag{2}$$

for all $x \geq 2$, and the following simple upper bound for the Hardy–Ramanujan partition function $p(n)$.

Lemma 1. *For every integer* $n \geq 2$, $p(n) < 2n^{2\sqrt{n}}$.

Proof: The function $p(n)$ counts the number of partitions of a positive integer n. A partition of n is a sequence of positive integers $u_1, \ldots, u_s$ such that $n = u_1 + u_2 + \cdots + u_s$ and $u_1 \geq u_2 \geq \cdots \geq u_s$. Associated to this partition is an array of points, called the Ferrers graph, consisting of u_1 points on the first row, u_2 points on the second row, $\ldots$, u_s points on the s–th row. For example, corresponding to the partition $19 = 7 + 5 + 4 + 2 + 1$ is the graph in Figure 1.

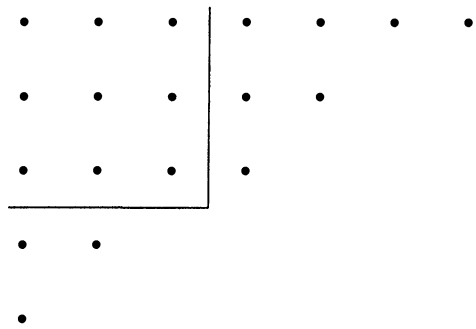

Figure 1

Consider the largest square array of dots that can be found in the upper left corner of the graph. In the example in Figure 1, this square consists of three lines, each with three points. The length of this square is some positive integer $r \leq \sqrt{n}$, and the square contains r^2 points. The remaining $n - r^2$ points in the graph must lie on the first r lines, to the right of the square, or on the first r columns, underneath the square. The number of ways to add these points to the graph is at most n^{2r}.

Therefore, the number of partitions of n satisfies

$$p(n) \leq \sum_{r=1}^{[\sqrt{n}]} n^{2r} < 2n^{2\sqrt{n}}.$$

Theorem 1. *Let S be the semigroup of 2×2 matrices generated by the set $A = \{a, b\}$, where*

$$a = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad b = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}.$$

Then

$$2^{2c_1\sqrt{n}/\log n} \leq \gamma_A(n) < n^2 p(n) < 2n^{2\sqrt{n}+2} \tag{3}$$

for some constant $c_1 > 0$ and all sufficiently large n. In particular, S has intermediate growth.

Proof: We observe that the matrices a and b satisfy the identities

$$b^2 = b,$$

$$a^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix},$$

and

$$ba^k b = \begin{pmatrix} k+1 & 0 \\ k+1 & 0 \end{pmatrix} = (k+1)b$$

for every positive integer k. Therefore, for any positive integers $k_1, \ldots, k_r$ we have

$$ba^{k_1}ba^{k_2}b \cdots ba^{k_r}b = \prod_{i=1}^{r} ba_i^{k_i}b = \left(\prod_{i=1}^{r}(k_i+1)\right)b. \tag{4}$$

Let $p_1, p_2, \ldots, p_r$ be distinct prime numbers not exceeding $\sqrt{n}$. Then

$$ba^{p_1-1}ba^{p_2-1}b \cdots ba^{p_r-1}b = \left(\prod_{i=1}^{r} p_i\right)b.$$

By Chebyshev's Theorem (2), the length of this element does not exceed

$$1 + \sum_{i=1}^{r} p_i \leq r\sqrt{n} + 1 \leq \sqrt{n}\,\pi(\sqrt{n}) + 1 \leq \frac{2c_2 n}{\log n} + 1 \leq n$$

for all sufficiently large n. Therefore, each of these elements is counted by the growth function $\gamma_A(n)$. These elements are distinct, since every positive integer is uniquely a product of primes, and so every subset of the primes up to $\sqrt{n}$ produces a different element of the semigroup S of length at most n. This gives the lower bound

$$\gamma_A(n) \geq 2^{\pi(\sqrt{n})} \geq 2^{2c_1\sqrt{n}/\log n}.$$

Next we compute an upper bound. Let $s \in S$ have length $l_A(s) \leq n$. There are three possibilities. First, there are $n+1$ elements of the form $s = a^u$ with $0 \leq u \leq n$. Second, there are $\binom{n+1}{2}$ elements of the form $s = a^u ba^v$ with $u, v \geq 0$ and $0 \leq u + v \leq n-1$. Third, we can have $s = a^u s' a^v$, where $s' = ba^{k_1}ba^{k_2}b \cdots ba^{k_r}b$, u, v are nonnegative integers with $u + v \leq n-3$, and $r, k_1, \ldots, k_r$ are positive integers such that $k_1 + \cdots + k_r + r + 1 \leq n$. Equation (4) implies that $s' = ba^{k_{\sigma(1)}}ba^{k_{\sigma(2)}}b \cdots ba^{k_{\sigma(r)}}b$ for every permutation σ of $1, \ldots, r$, so we can

assume that $k_1 \geq \cdots \geq k_r \geq 1$. Let $k_i' = k_i + 1$. We associate the following partition of n to the semigroup element s': $n = k_1' + \cdots + k_r' + 1 + \cdots + 1$, where $k_1' \geq \cdots \geq k_r' \geq 2$ and the number of 1's in the partition is

$$n - \sum_{i=1}^{r} k_i' \geq 1.$$

This is a one-to-one mapping of the elements s' to partitions of n. It follows that there are at most $p(n)$ semigroup elements s' of the form (4) with $k_1 + \cdots + k_r + r + 1 \leq n$. Since $u + v \leq n - 3$, there are $\binom{n-1}{2}$ choices of nonnegative integers u, v, and so there are at most $\binom{n-1}{2}p(n)$ semigroup elements of the third type. By Lemma 1, for $n \geq 2$ we have

$$\gamma_A(n) \leq n + 1 + \binom{n+1}{2} + \binom{n-1}{2}p(n) \leq n^2 p(n) < 2n^{2\sqrt{n}+2}.$$

This gives the upper bound. The semigroup S has intermediate growth since the left side of inequality (3) grows faster than any polynomial, while the right side grows slower than any exponential function. ■

Let A be a finite subset of a group, with $1 \in A$. Let S be the semigroup generated by A, and let G be the group generated by A. Denote by A^n the set of all products of n elements of A. Denote by $A^{\pm n}$ the set of all elements of the form $a_1^{\pm 1} \cdots a_n^{\pm 1}$. The growth function of the semigroup S with respect to A is $\gamma_{A,S}(n) = |A^n|$, and the growth function of the group G with respect to A is $\gamma_{A,G}(n) = |A^{\pm n}|$, Clearly, $\gamma_{A,S}(n) \leq \gamma_{A,G}(n)$ for all n. It is natural to ask if these two functions must have similar growth rates. Grigorchuk [3] proved that if $\gamma_{A,S}(n)$ has polynomial growth of degree k, then $\gamma_{A,G}(n)$ also has polynomial growth of degree k. It is not known if it is possible for the semigroup function $\gamma_{A,S}(n)$ to have intermediate growth while the group function $\gamma_{A,G}(n)$ has exponential growth.

REFERENCES

1. R. I. Grigorchuk, On Burnside's problem on periodic groups, *Funktsional. Anal. i Prilozhen.*, 14(1):53–54, 1980. English translation: *Functional Analysis Appl.* **14** (1980) 41–43.
2. R. I. Grigorchuk, On Milnor's problem of group growth, *Doklady Akad. Nauk SSSR*, 271(1):31–33, 1983. English translation: *Soviet Math. Dokl.* **28** (1983) 23–26.
3. R. I. Grigorchuk, Cancellation semigroups of polynomial growth, *Matem. Zamet.*, 43:305–319, 1988. English translation: Math. Notes (1988) 175–183.
4. R. I. Grigorchuk, On growth in group theory, in *Proceedings of the International Congress of Mathematicians, Kyoto, Japan*, 1990, Springer–Verlag, Tokyo, 1991, pp. 325–338.
5. J. Milnor, Problem 5603, *Amer. Math. Monthly* **75** (1968) 685–686.
6. M. B. Nathanson, *Additive Number Theory: The Classical Bases*, volume 164 of *Graduate Texts in Mathematics*, Springer-Verlag, New York, 1996.

Lehman College (CUNY), Bronx, NY 10468
nathansn@alpha.lehman.cuny.edu