Far East Journal of Mathematical Education
Volume 2, Number 2, 2008, Pages 103-113
Published online: December 20, 2008
This paper is available online at http://www.pphmj.com

MINIMAL SEMIGROUP GENERATING SETS WITH RESPECT TO GREATEST COMMON DIVISOR AND LEAST COMMON MULTIPLE

DAVID E. DOBBS and BRETT KATHLEEN LATHAM

Department of Mathematics
University of Tennessee
Knoxville, Tennessee 37996-1300, U. S. A.
e-mail: dobbs@math.utk.edu

John J. Lynch Middle School
Holyoke, Massachusetts 01040, U. S. A.
e-mail: bkm00@hampshire.edu

Abstract

Let $\mathbb{N}$ be the set of positive integers. As a semigroup under the binary operation given by $a * b = (a, b)$, the greatest common divisor of a and b, $\mathbb{N}$ does not have a minimal generating set. For each $n \in \mathbb{N}$, the subsemigroup $\{1, 2, ..., n\}$ (under the binary operation given by the greatest common divisor) has a unique minimal generating set T, and $T = \left\{k \in \mathbb{N} \mid \left\lfloor \frac{n}{3} \right\rfloor + 1 \leq k \leq n\right\}$. The asymptotics of this result are considered as $n \to \infty$. Analogues of the above results are considered for the binary operation given by least common multiple and for minimal generating sets in some algebraic categories other than semigroups. This note could find classroom/homework use as enrichment material in a variety of undergraduate courses, especially courses on abstract algebra or elementary number theory.

2000 Mathematics Subject Classification: Primary 20M99, 11A05; Secondary 13F15.

Keywords and phrases: minimal generating set, semigroup, greatest common divisor, least common multiple, natural numbers, prime number, cyclic group, vector space, unique factorization domain, polynomial ring.

Received April 27, 2008

1. Introduction

Our main purpose here is to study generating sets, with emphasis on minimal generating sets, in some semigroups that arise naturally in elementary number theory. This note could find classroom/homework use as enrichment material in a variety of undergraduate courses, such as abstract algebra or elementary number theory. Recall that a *semigroup* is a nonempty set with an associative binary operation. Let S be a semigroup relative to the binary operation $*$. If T is a nonempty subset of S, then the *subsemigroup of S generated by T* is $\langle T\rangle := \{a_1 * \cdots * a_n \,|\, n \in \mathbb{N}, a_i \in T \text{ if } 1 \le i \le n\}$. (As usual, $\mathbb{N}$ denotes the set of positive integers.) We say that T is a *generating set of S* if $\langle T\rangle = S$; and that a generating set T of S is a *minimal generating set of S* if no proper subset of T is a generating set of S.

Perhaps the most familiar semigroup is $\mathbb{N}$ relative to the binary operation of addition. It is clear that $\mathbb{N}$ has exactly one minimal generating set, namely, $\{1\}$. In fact, it is known (cf. [5, Theorem 2.4(2)]) that each subsemigroup S of $\mathbb{N}$ has a unique minimal generating set T and that T is finite. The proof of [5, Theorem 2.4(2)] uses the notion of the greatest common divisor (abbreviated gcd, also known as the highest common factor) of a set of integers. As usual, if $a_1, ..., a_n \in \mathbb{N}$, we let $(a_1, ..., a_n)$ denote the gcd of $a_1, ..., a_n$. It is well known that if $a, b, c \in \mathbb{N}$, then $((a, b), c) = (a, (b, c)) =: (a, b, c)$. In other words, $\mathbb{N}$ is a semigroup relative to the binary operation $*$ defined by $a * b := (a, b)$ for all $a, b \in \mathbb{N}$. The main results of this note concern this structure. Indeed, Theorem 2.2 shows, in contrast to the results on additive structure that were recalled above, that relative to the binary operation induced by gcd, $\mathbb{N}$ does not have a minimal generating set. On the other hand, if we consider the semigroup structure on $\mathbb{N}$ that is induced by least common multiple (abbreviated lcm), Proposition 2.3 shows that this semigroup has a unique minimal generating set (which consists of 1 and all the integral prime powers).

With the hope of finding a minimal generating set in a context determined by gcds, we next turn to the study of certain finite semigroups. For each $n \in \mathbb{N}$, we let $S(n) := \{k \in \mathbb{N} \mid 1 \leq k \leq n\}$. Observe that $S(n)$ has a relevant semigroup structure induced by gcd. Our main result, Theorem 2.5, states that if $n \in \mathbb{N}$, then $S(n)$ has a unique minimal generating set, and that this generating set is $\left\{k \in \mathbb{N} \mid \left\lfloor \frac{n}{3} \right\rfloor + 1 \leq k \leq n\right\}$. (As usual, $\lfloor ... \rfloor$ denotes the floor, or greatest integer, function.) On the other hand, Proposition 2.4 records that $S(n)$ is a semigroup relative to a binary operation induced by lcm if and only if n is either 1 or 2. Finally, Remark 2.6 collects a number of pedagogic comments, including some probabilistic interpretations arising from the asymptotics of the assertion in Theorem 2.5 and some ring-theoretic analogues of Proposition 2.3.

2. Results

We begin by stating a well-known number-theoretic fact that will be used later in some proofs.

Lemma 2.1. (a) *Let* $a, b, c \in \mathbb{N}$. *Then* $(ab, ac) = a(b, c)$.

As explained in the introduction, the negative conclusion of our next result stands in contrast to the classical theory for numerical semigroups given in [5, Theorem 2.4(2)].

Theorem 2.2. *Let* S *be the semigroup whose underlying set is* $\mathbb{N}$, *relative to the binary operation* $*$ *defined by* $a * b := (a, b)$ *for all positive integers* a, b. *Then* S *does not have a minimal generating set.*

Proof. We give an indirect proof. Suppose, by way of contradiction, that T is a minimal generating set of S. Let n denote the least element of T. Consider $T_1 := T \setminus \{n\}$. Note that T_1 is nonempty. (Otherwise, $T = \{n\}$, whence $S = \langle T \rangle = \{(n, n)\} = \{n\}$, a contradiction.) Since T_1 is a proper subset of T, we can contradict the minimality of T by showing that $T \subseteq \langle T_1 \rangle$, or equivalently, that $n \in \langle T_1 \rangle$. Observe via Lemma 2.1 that $(2n, 3n) = n(2, 3) = n \cdot 1 = n$. As $2n, 3n \in S = \langle T \rangle$ and $n < 2n < 3n$, it

follows that $2n, 3n \in \langle T_1 \rangle$. (The point is that if $m = (a_1, ..., a_\nu)$, then $m \leq a_j$ for each $j \in S(\nu)$). Therefore,

$$n = (2n, 3n) = (2n) * (3n) \in \langle T_1 \rangle,$$

the desired contradiction, completing the proof.

By using the $(2n) * (3n)$ construction that appeared in the proof of Theorem 2.2, one can also prove the following result. If $(S, *)$ is the semigroup considered in Theorem 2.2 and $n \in \mathbb{N}$, then there exists a (necessarily non-minimal) generating set T of S such that the least element of T is greater than n. The $(2n) * (3n)$ construction will also figure in the proof of Theorem 2.5.

Proposition 2.3 will give the analogue of Theorem 2.2 where "gcd" is replaced by "lcm" (which stands for "least common multiple"). As usual, if $a_1, ..., a_n \in \mathbb{N}$, we let $[a_1, ..., a_n]$ denote the lcm of $a_1, ..., a_n$. It is well known that if $a, b, c \in \mathbb{N}$, then $[[a, b], c] = [a, [b, c]] =: [a, b, c]$. In other words, $\mathbb{N}$ is a semigroup relative to the binary operation $*$ defined by $a * b := [a, b]$ for all $a, b \in \mathbb{N}$. Proposition 2.3 shows, in contrast to Theorem 2.2, that the semigroup structure induced on $\mathbb{N}$ by lcm has a unique minimal generating set.

Proposition 2.3. *Let S be the semigroup whose underlying set is $\mathbb{N}$, relative to the binary operation $*$ defined by $a * b := [a, b]$ for all positive integers a, b. Let $T_0 = \{1\} \cup \{p^i \mid p$ is a prime number and $i \in \mathbb{N}\}$. Then T_0 is the unique minimal generating set of S. Moreover, T_0 is a subset of any generating set of S.*

Proof. Observe that if m and n are distinct relatively prime positive integers, then $[m, n] = mn$. It therefore follows easily from the Fundamental Theorem of Arithmetic that $\langle T_0 \rangle = S$. Next, we shall show that if $\langle T \rangle = S$, then $T_0 \subseteq T$. Consider any element $k \in T_0$. Since $k \in \langle T \rangle$, there exist finitely many elements $a_1, ..., a_\nu \in T$ such that $k = [a_1, ..., a_\nu]$. In particular, $k \geq a_1$. If $k = 1$, then $1 = a_1 \in T$. In the remaining case, $k = p^i$ for some prime number p and $i \in \mathbb{N}$. As

$p^i = [a_1, ..., a_\nu]$, it follows from a standard formula for lcm [8, p. 44, line −5] (and from the Fundamental Theorem of Arithmetic) that there exists $j \in S(\nu)$ such that $p^i = a_j \in T$, to complete the proof. □

Given the positive nature of the conclusion of Proposition 2.3, it seems natural to ask if some variant of the context studied in Theorem 2.2 in terms of gcds can also lead to a minimal generating set. Such a result is given in Theorem 2.5. First, an easier analogue of it in terms of lcms is given in Proposition 2.4. Recall that if $n \in \mathbb{N}$, then $S(n)$ denotes $\{k \in \mathbb{N} \mid 1 \leq k \leq n\}$.

Proposition 2.4. *Let* $n \in \mathbb{N}$. *Then* $a * b := [a, b]$ *for all* $a, b \in S(n)$ *defines a binary operation on* $S(n)$ *if and only if* n *is either* 1 *or* 2. *If* n *is either* 1 *or* 2, *this induced binary operation on* $S(n)$ *is associative and so induces the structure of a semigroup whose underlying set is* $S(n)$. *Moreover, if* n *is either* 1 *or* 2, *the only* (*necessarily minimal*) *generating set of this semigroup is* $S(n)$.

Proof. By the comment about associativity that preceded the statement of Proposition 2.3, lcm induces a semigroup structure on $S(n)$ if and only if the corresponding "product" satisfies the closure property, that is, if and only if $[a, b] \in S(n)$ whenever $a, b \in S(n)$. As $[1, 1] = 1$ and $[2, 2] = 2$, it suffices to show that if $3 \leq n \in \mathbb{N}$, then there exist $a, b \in S(n)$ such that $[a, b] \notin S(n)$, that is, that there exist positive integers $a, b \leq n$ such that $[a, b] > n$. If there exists a prime number p such that $p \leq n$ and p does not divide n, then $[p, n] = pn > n$, in which case it suffices to take $a := p$ and $b := n$. Accordingly, it remains only to rule out the case that $3 \leq n \in \mathbb{N}$ and n is divisible by each prime number q such that $q \leq n$. However, in this case, the Fundamental Theorem of Arithmetic would imply that each integer m such that $2 \leq m \leq n$ is a product of prime numbers (possibly with repetition) each of which divides n. It would follow that 1 is the only member of $S(n)$ that is relatively prime to n and, hence, from the definition of the Euler phi-function [8, p. 53] that $\varphi(n) = 1$. However, the standard formula for this function

[8, Theorem 3.8] easily yields that $\varphi(k) > 1$ whenever $3 \leq k \in \mathbb{N}$. This completes the proof. □

We next present our main result.

Theorem 2.5. *Let* $n \in \mathbb{N}$. *Then* $a * b := (a, b)$ *for all* $a, b \in S(n)$ *defines an associative binary operation on* $S(n)$. *The resulting semigroup with underlying set* $S(n)$ *has a unique minimal generating set* $T(n) := \left\{k \in \mathbb{N} \mid \left\lfloor \frac{n}{3} \right\rfloor + 1 \leq k \leq n\right\}$. *Moreover,* $T(n)$ *is a subset of any generating set of this semigroup.*

Proof. Recall that $((a, b), c) = (a, (b, c))$ for all $a, b, c \in \mathbb{N}$. Since $(a, b) \leq \min(a, b)$, it follows that $*$ induces the structure of a semigroup on $S(n)$. Consider $T(n) := \left\{k \in \mathbb{N} \mid \left\lfloor \frac{n}{3} \right\rfloor + 1 \leq k \leq n\right\}$. We claim that if T is any generating set of $S(n)$ (with respect to the binary operation induced by gcd), then $T(n) \subseteq T$.

If the claim fails, then there exists a positive integer i such that $1 \leq i \leq n - \left\lfloor \frac{n}{3} \right\rfloor$ and $\left\lfloor \frac{n}{3} \right\rfloor + i$ is the gcd of a nonempty subset $\mathcal{U}$ of (the integers in) $T \setminus \left\{\left\lfloor \frac{n}{3} \right\rfloor + i\right\}$. It follows from the definition of gcd that $\mathcal{U}$ must contain at least two distinct nontrivial integral multiples of $\left\lfloor \frac{n}{3} \right\rfloor + i$. Thus, $3\left(\left\lfloor \frac{n}{3} \right\rfloor + i\right) \leq n$. But the definition of the floor function ensures that $\left\lfloor \frac{n}{3} \right\rfloor \geq \frac{n}{3} - \frac{2}{3}$ (To see this, it may help to note that $n = 3q + r$ for some non-negative integer q and some $r \in \{0, 1, 2\}$). It follows that

$$n \geq 3\left(\left\lfloor \frac{n}{3} \right\rfloor + i\right) \geq 3\left(\frac{n}{3} - \frac{2}{3} + i\right) = n - 2 + 3i > n,$$

with the last inequality holding since $i > \frac{2}{3}$. This contradiction proves the above claim.

It remains only to prove that $\left\{k \in \mathbb{N} \mid k \leq \left\lfloor \frac{n}{3} \right\rfloor\right\} \subseteq \langle T(n) \rangle$. Suppose that $k \in \mathbb{N}$ is such that $k \leq \left\lfloor \frac{n}{3} \right\rfloor$. Let m denote the least integer such that $mk > \left\lfloor \frac{n}{3} \right\rfloor$ (Of course, m exists by the well-ordering principle for $\mathbb{N}$ since $\lim_{m \to \infty} mk = \infty$; note also that $m \geq 2$). By the minimality of m, we have that $(m-1)k \leq \left\lfloor \frac{n}{3} \right\rfloor$. Therefore,

$$(m+1)k = (m-1)k + 2k \leq \left\lfloor \frac{n}{3} \right\rfloor + 2\left\lfloor \frac{n}{3} \right\rfloor = 3\left\lfloor \frac{n}{3} \right\rfloor \leq n.$$

Hence, $\langle T(n) \rangle$ contains $(mk, (m+1)k)$, which, by Lemma 2.1, is just $k(m, m+1) = k \cdot 1 = k$, as desired. This completes the proof. □

In closing, we collect several comments that could be used in a variety of courses. These feature, in particular, an analysis of the asymptotics related to the formula for $T(n)$ in the statement of Theorem 2.5 and a polynomial-theoretic analogue of Proposition 2.3.

Remark 2.6. (a) Despite the last three results (and [5, Theorem 2.4(2)]), it is not rare for a semigroup to have more than one minimal generating set. For instance, take the semigroup S to be the Klein four-group, and note that any subset of S consisting of two distinct nonzero elements of S is a minimal generating set of S. In (b), we shall give another example of this behaviour by introducing a different semigroup that is constructed more in the spirit of Proposition 2.3.

The above type of phenomenon is also exhibited by the notion of "minimal generating set" in several algebraic contexts other than that of semigroups. For instance, if G is a finite cyclic group with exactly $n > 1$ elements, then G has $\varphi(n)$ minimal generating sets (in the sense of group theory), and each of these minimal generating sets has cardinality 1. Thus, a typical minimal generating set of a "large" finite cyclic group G can be viewed as constituting a negligible subset of G, in the sense that $\lim_{n \to \infty} \frac{1}{n} = 0$. A similar comment can be made about "minimal

generating sets" in the sense of linear algebra. Indeed, let F be a finite field with exactly q elements and let V be a finite-dimensional vector space over F of dimension n. Then any "minimal generating set" of V, in the sense of vector space theory, is just an F-basis of V, and hence has exactly n elements. Since V has cardinality q^n and $\lim_{n\to\infty} \frac{n}{q^n} = 0$, one can also conclude that a typical minimal generating set of a "large" finite-dimensional vector space V over a given finite field can be viewed as constituting a negligible subset of V. (To show that $\lim_{n\to\infty} \frac{n}{q^n} = 0$, one notes that $q \geq 2$ and then uses L'Hôpital's Rule.)

Semigroups behave differently from groups or vector spaces. Consider the (unique) minimal generating set $T(n)$ that was constructed for $S(n)$ in Theorem 2.5. As the cardinalities of $T(n)$ and $S(n)$ are $n - \left\lfloor \frac{n}{3} \right\rfloor$ and n, respectively, we are led by the examples in the preceding paragraph to consider $\lim_{n\to\infty} \frac{n - \left\lfloor \frac{n}{3} \right\rfloor}{n}$. Contrary to the limits in those earlier examples, this limit is not 0. It is, in fact, $\frac{2}{3}$. (The proof of this is an instructive exercise in elementary real analysis. Since $\left\lfloor \frac{n}{3} \right\rfloor$ is either $\frac{n}{3}$, $\frac{n}{3} - \frac{1}{3}$ or $\frac{n}{3} - \frac{2}{3}$, one can calculate this limit by showing that the three obvious subsequences each have limit equal to $\frac{2}{3}$.) Thus, one cannot, in general, view a minimal generating set (if it exists) of a finite semigroup S as constituting a negligible subset of S.

In referring to "negligible" subsets above, we were implicitly using a notion of "probability" that is couched in terms of the natural density of subsets of $\mathbb{N}$ (in the sense of [9]). Such a view of probability has occurred often in the literature on number theory, polynomial rings, and linear

algebra: cf. [6, pp. 268-269 and Theorems 332 and 333] and, more recently, [3, Theorems 4.1 and 5.1], [4, Corollary 4], [2, Remark 4.1(b)], [1, p. 749 and Theorems 4.1 and 4.2(b)], and [7, p. 491 and Remark 3.4].

(b) It seems natural to ask if there are any ring-theoretic analogues of the above results. To be brief, we shall focus here on such analogues of Proposition 2.3. Since $\mathbb{Z}$ is a unique factorization domain (UFD), one is led to investigate what can be said in the above spirit if $\mathbb{Z}$ is replaced by a UFD, R. In doing so, one must decide which subset of R should play the earlier role of $\mathbb{N}$. The discussion of the sets $S(1, \mathcal{P})$ and $S(1, \widetilde{\mathcal{P}})$ below reveals that one has choices in this regard.

To avoid trivialities, assume that R is not a field. Let u be a unit of R (that is, an element of R having a multiplicative inverse in R). Let $\mathcal{T}$ be any set of associate class representatives for the irreducible elements (also known as the "atoms") of R. Since R is not a field, $\mathcal{T}$ is nonempty. We next introduce what we view as one of the desired analogues of $\mathbb{N}$. Let $S(u, \mathcal{T})$ be the set of elements of T that are expressible as the product of u^i, where $i \in \mathbb{N} \cup \{0\}$, and $a_1^{j_1}, ..., a_k^{j_k}$, where $k \in \mathbb{N} \cup \{0\}, a_1, ..., a_k \in \mathcal{T}$, $j_1, ..., j_k \in \mathbb{N}$, and $i + k > 0$. Since R is a UFD, it follows that if $r, s \in S(u, \mathcal{T})$, then there is a unique way to express some least common multiple of r and s (in the sense of ring theory) as a product (ignoring order of factors and allowing repetition of factors) of the above form

$$u^i a_1^{j_1} . \ ... \ . \ a_k^{j_k} .$$

(As usual in ring theory, "unique" means apart from the order of factors and allows repetition of factors; while the exponents $j_1, ..., j_k$ are uniquely determined by the list $a_1, ..., a_k$, the "uniqueness" that applies to the factor u^i refers to this factor itself and not necessarily to the exponent i.) Define a binary operation $\circ$ on $S(u, \mathcal{T})$ by taking $r \circ s$ to be the aforementioned least common multiple. The above "unique way" observation shows that $\circ$ is associative and, thus, equips $S(u, \mathcal{T})$ with the structure of a semigroup. Since the multiplication in any UFD satisfies an analogue of the Fundamental Theorem of Arithmetic, we can

show, by reasoning as in the proof of Proposition 2.3, that $\{u\} \cup \{p^j \mid p \in \mathcal{T} \text{ and } j \in \mathbb{N}\}$ is a minimal generating set for the above semigroup structure on $S(u, \mathcal{T})$.

The following example should clarify matters. Let $R := \mathbb{Z}$, let $\mathcal{P}$ denote the set of prime numbers, and let $\widetilde{\mathcal{P}} := \{q \mid -q \in \mathcal{P}\}$. It is straightforward to check that $S(1, \mathcal{P}) = \mathbb{N}$. Moreover, $S(-1, \mathcal{P}) = \mathbb{Z} \setminus \{0\} = S(-1, \widetilde{\mathcal{P}})$. Therefore, as a special case of the final comment in the preceding paragraph, we see that $\{-1\} \cup \{p^j \mid p \in \mathcal{P} \text{ and } j \in \mathbb{N}\}$ and $\{-1\} \cup \{p^j \mid p \in \widetilde{\mathcal{P}} \text{ and } j \in \mathbb{N}\}$ are distinct minimal generating sets of $\mathbb{Z} \setminus \{0\}$ with respect to the above semigroup structure that was induced by least common multiple.

Finally, we make explicit, in a self-contained way, how the above construction produces a semigroup structure having a unique minimal generating set when working with a UFD of the form $R = F[X]$, the ring of polynomials in one variable over any field F. (This paragraph could fit into any beginning ring theory course, as $\mathbb{Z}$ and rings of the form $F[X]$ are the types of UFDs that are typically studied first in such a course.) Let S be the set of monic polynomials in R (resp., the set of monic polynomials in R of degree at least 1). Note that if $f, g \in R \setminus \{0\}$, then R contains a unique monic polynomial that is a least common multiple (in the sense of ring theory) of f and g. It follows that least common multiple induces a binary operation on S. As this operation is associative, S thereby has the structure of a semigroup. Moreover, this semigroup has a unique minimal generating set, namely, $\{1\} \cup \{p^j \mid p$ is a monic irreducible element of $F[X]$ and $j \in \mathbb{N}\}$ (resp., $\{p^j \mid p$ is a monic irreducible element of $F[X]$ and $j \in \mathbb{N}\}$).

References

[1] D. E. Dobbs and A. J. Hetzel, Ahmes expansions of rational numbers of length two, Int. J. Math. Educ. Sci. Technol. 34 (2003), 742-751.

[2] D. E. Dobbs and L. E. Johnson, On the probability that Eisenstein's criterion applies to an arbitrary irreducible polynomial, pp. 241-256, Lecture Notes Pure Appl. Math. 205, Dekker, New York, 1999.

[3] D. E. Dobbs and M. J. Lancaster, The expected dimension of a sum of vector subspaces, Bull. Austral. Math. Soc. 45 (1992), 467-477.

[4] D. E. Dobbs, M. J. Lancaster and R. M. McConnel, The probability of maximal rank for a matrix over a finite commutative ring, C. R. Math. Rep. Acad. Sci. Canada 15 (1993), 207-212.

[5] R. Gilmer, Commutative Semigroup Rings, Univ. Chicago Press, Chicago / London, 1984.

[6] G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, 5th ed., Clarendon Press, Oxford, 1979.

[7] A. J. Hetzel, J. S. Liew and K. E. Morrison, The probability that a matrix of integers is diagonalizable, Amer. Math. Monthly 114 (2007), 491-499.

[8] W. J. LeVeque, Fundamentals of Number Theory, Addison-Wesley, Reading, Mass., 1977.

[9] I. Niven, H. S. Zuckerman and H. L. Montgomery, An Introduction to the Theory of Numbers, 5th ed., Wiley, New York, 1991.