KYUNGPOOK Math. J. 54(2014), 607-617
http://dx.doi.org/10.5666/KMJ.2014.54.4.607

On the Subsemigroups of a Finite Cyclic Semigroup

David Earl Dobbs*
Department of Mathematics, University of Tennessee, Knoxville, Tennessee 37996-1320, USA
e-mail : dobbs@math.utk.edu

Brett Kathleen Latham
Squalicum High School, Bellingham, Washington 98226, USA
e-mail : BrettLatham@BellinghamSchools.org

Abstract. Let $S = C(r, m)$, the finite cyclic semigroup with index r and period m. Each subsemigroup of S is cyclic if and only if either $r = 1$; $r = 2$; or $r = 3$ with m odd. For $r \neq 1$, the maximum value of the minimum number of elements in a (minimal) generating set of a subsemigroup of S is 1 if $r = 3$ and m is odd; 2 if $r = 3$ and m is even; $(r-1)/2$ if r is odd and unequal to 3; and $r/2$ if r is even. The number of cyclic subsemigroups of S is $r-1+\tau(m)$. Formulas are also given for the number of 2-generated subsemigroups of S and the total number of subsemigroups of S. The minimal generating sets of subsemigroups of S are characterized, and the problem of counting them is analyzed.

1. Introduction

All semigroups considered in this note are written multiplicatively. If S is a semigroup and $x \in S$, then $\langle x \rangle$ denotes the subsemigroup of S that is generated by x; that is, $\langle x \rangle := \{x^n \mid n \in \mathbb{N}\}$ (where, as usual, $\mathbb{N}$ denotes the set of positive integers). A semigroup S is said to be *cyclic* if there exists $x \in S$ such that $S = \langle x \rangle$. Our main concern here is to study the extent to which the standard facts about finite cyclic groups extend to the context of semigroups, and so we will also assume that all semigroups considered below are finite. Given a (finite) cyclic semigroup, we will be especially interested in its subsemigroups and in the minimal generating sets of those subsemigroups.

Consider a (finite) cyclic semigroup $S = \langle x \rangle$ and the smallest possible positive integers r and m such that $x^{r+m} = x^r$. (Of course, such r and m exist because

* Corresponding Author.
Received August 4, 2012; accepted December 14, 2012.
2010 Mathematics Subject Classification: Primary 20M99; Secondary 20M14.
Key words and phrases: Finite cyclic semigroup, subsemigroup, minimal generating set, index, period, greatest common divisor, Frobenius number, $\tau(n)$, $\varphi(n)$.

S is finite.) We call r and m the *index* and the *period*, respectively, of x. In fact, these numbers can also be called the index and period, respectively, of S, since the following comments make clear that the values of r and m are each independent of the choice of the generator x of S. It will be convenient to call the set $\mathcal{S}(x) := \{x^i \mid 1 \leq i \leq r-1\}$ the *stem* of x (or of S) and the set $\mathcal{G}(x) := \{x^i \mid r \leq i \leq r+m-1\}$ the *group* of x (or of S). Note that S is the disjoint union of $\mathcal{S}(x)$ and $\mathcal{G}(x)$. Hence, the number of elements in S is $r+m-1$, which is called the *order* of x (or of S). In general, $\mathcal{G}(x)$ is a cyclic group of order m. The index and period of x determine $\langle x \rangle$ up to (semigroup) isomorphism. As in [1, page 10], if r and m are any positive integers, we let $C(r,m)$ denote a finite cyclic semigroup with (a generator x having) index r and period m. For two different constructions of $C(r,m)$, see [1, pages 10-11]. Note that if $n \in \mathbb{N}$, then $x^n \in \mathcal{G}(x)$ if and only if $n \geq r$. It follows that $C(r,m)$ is a group $\Leftrightarrow r = 1 \Leftrightarrow \mathcal{S}(x)$ is empty $\Leftrightarrow C(r,m)$ is a monoid.

Since finite cyclic groups (the case $r = 1$) are understood, we focus on the case $r > 1$. Although every subgroup of a cyclic group is cyclic, we prove in Proposition 2.1 that each subsemigroup of $C(r,m)$ is cyclic if and only if either $r = 1$; $r = 2$; or $r = 3$ with m odd. Thus, most finite cyclic semigroups contain non-cyclic subsemigroups. However, a subsemigroup of $C(r,m)$ never needs more than $(r+1)/2$ generators. More precisely, if $r \neq 1$, we prove in Theorem 2.2 that the maximum value of the minimum number of elements in a (minimal) generating set of a subsemigroup of $C(r,m)$ is 2 if $r = 3$ and m is even; $(r-1)/2$ if r is odd and unequal to 3; and $r/2$ if r is even.

The question of how many subsemigroups are contained in a given finite cyclic semigroup S is interesting because the answer to the corresponding question in group theory is straightforward: a finite cyclic group of order n has exactly $\tau(n)$ (cyclic) subgroups (where, as usual, $\tau(k)$ denotes the number of positive integral divisors of a positive integer k). More generally, we prove in Proposition 2.4 that $C(r,m)$ has exactly $r - 1 + \tau(m)$ cyclic subsemigroups. In addition, Corollary 2.8 gives a formula for the number of 2-generated subsemigroups of $C(r,m)$ for arbitrary r and m. Perhaps more interestingly, Corollary 2.11 (a) gives a formula for the number of subsemigroups of $C(r,m)$, while Remark 2.12 studies the asymptotics of a tractable upper bound for that formula.

The above counting results on the subsemigroups of $C(r,m)$ are due, in part, to a useful technical result in Lemma 2.6 (a). Rather than state Lemma 2.6 here, we will state another of its consequences, namely, Theorem 2.7 (b): given positive integers $n_1 < \ldots < n_k \leq r-1$, with $d := \gcd(n_1, \ldots, n_k, m)$, then the number of subsemigroups of $C(r,m)$ that can be generated by the union of $\{x^{n_1}, \ldots, x^{n_k}\}$ with a (possibly empty) subset of $\mathcal{G}(x)$ is $\tau(d)$. This leads, in turn, to the characterization in Corollary 2.9 of the minimal generating sets of subsemigroups of a given $C(r,m)$. (That result ignores the sub(semi)groups that are contained in $\mathcal{G}(x)$ since it is well known that any subgroup of a cyclic group is cyclic.) Finally, we note that Remark 2.10 discusses the problem of counting the minimal generating sets of subsemigroups of a given $C(r,m)$.

2. Results

It seems appropriate to begin by noting two ways in which the subsemigroups of a finite cyclic semigroup do not behave analogously to the subgroups of a finite cyclic group. First, the analogue of Lagrange's Theorem fails: for instance, $C(4,3) = \{x, x^2, x^3, x^4, x^5, x^6\}$ has order $r + m - 1 = 4 + 3 - 1 = 6$, which is not divisible by the order, 4, of its subsemigroup $\langle x^2\rangle = \{x^2, x^4, x^5, x^6\}$. Second, a finite cyclic semigroup can have distinct cyclic subsemigroups that have the same order: for instance, in $C(4,1) = \{x, x^2, x^3, x^4\}$, consider the subsemigroups $\langle x^2\rangle = \{x^2, x^4\}$ and $\langle x^3\rangle = \{x^3, x^4\}$. We turn next to conclusions of a more positive nature.

The most basic fact about cyclic groups is surely that each of their subgroups is also cyclic. We will next determine the analogous fact about finite cyclic semigroups $S = \langle x\rangle$. First, we recall two useful facts that are used in the proof of Proposition 2.1 (and elsewhere). For integers $u \geq v \geq r$ (where $x^{r+m} = x^r$), we have $x^u = x^v$ if and only if $m|(u - v)$ [1, Theorem 2.1 (1)]. Also, any finite subsemigroup T of $\mathcal{G}(x)$ is a cyclic (semi)group (since it is a finite cancellative semigroup).

Proposition 2.1. Let $r, m \in \mathbb{N}$ and put $S := C(r,m)$. Then each subsemigroup of S is cyclic if and only if (exactly) one of the following three conditions holds: (i) $r = 1$; (ii) $r = 2$; (iii) $r = 3$ with m odd.

Proof. As observed above, $r = 1 \Leftrightarrow S$ is a group. As the situation for groups is understood, we can suppose that $r > 1$; that is, S is not a group, and so $\mathcal{S}(x)$ is nonempty. We seek to determine necessary and sufficient conditions that each subsemigroup T of S is cyclic. By the above comment, the cyclicity of such a T holds if $T \subseteq \mathcal{G}(x)$, and so we need only consider T such that $T \cap \mathcal{S}(x)$ is nonempty. If $r = 2$, then $T \cap \mathcal{S}(x) = \{x\}$, and so $T = \{x^n \mid n \in \mathbb{N}\} = \langle x\rangle$ $(= S)$, which is cyclic. On the other hand, if $r > 3$, then the semigroup $T := \langle x^2, x^3\rangle = \{x^n \mid n \geq 2\}$ is not cyclic, since each minimal generating set of T must contain both x^2 and x^3. It remains only to consider the case $r = 3$.

Since $r = 3$, $\mathcal{S}(x) = \{x, x^2\}$. By reasoning as above, we need only consider the semigroups T of S such that $x \notin T$ and $x^2 \in T$. These T are the sets of the form $T = \{x^2\} \cup T'$ as T' ranges over the sub(semi)groups of $\mathcal{G}(x)$ such that $x^4 \in T'$ and $x^2T' \subseteq T'$. It suffices to prove that each such T' is a subset of $\langle x^2\rangle$ if and only if m is odd.

Suppose that m is even. Taking $T' := \mathcal{G}(x)$ leads to $T = \{x^2\} \cup T' = \{x^n \mid n \geq 2\}$. However, this T is not cyclic, since $x^3 \notin \langle x^2\rangle$; that is, there does not exist $n \geq 2$ such that $x^3 = (x^2)^n$ $(= x^{2n})$. To see this, it suffices to note that m being even (together with 3 being odd) implies that $2n - 3$ is not divisible by m (for any $n \geq 2$).

Lastly, suppose that m is odd. It suffices to prove that for any integer $i \geq r = 3$, there exists $n \geq 2$ such that $x^i = x^{2n}$. Since m is odd, m is relatively prime to 2, and so there exist integers λ and μ such that $\lambda m + \mu 2 = 1$. By the Archimedean principle, there exists a positive integer ν such that $n := i\mu + \nu m \geq 2$. As

$$2n - i = 2(i\mu + \nu m) - i = i(2\mu - 1) + 2\nu m = (-\lambda i + 2\nu)m$$

is divisible by m, the proof is complete. □

Proposition 2.1 leads naturally to the following question: what is the maximum value of the minimum cardinality of a generating set of a subsemigroup of a given $C(r,m)$? Theorem 2.2 gives the answer to this question. Of course, we ignore the case $r = 1$ there, since every sub(semi)group of a finite cyclic group is cyclic.

Theorem 2.2. *Let $r, m \in \mathbb{N}$ with $r \neq 1$, and put $S := C(r,m)$. Then the maximum value of the minimum number of elements in a (minimal) generating set of a subsemigroup of $C(r,m)$ is 1 if $r = 3$ and m is odd; 2 if $r = 3$ and m is even; $(r-1)/2$ if r is odd and unequal to 3; and $r/2$ if r is even.*

Proof. As usual, let x be a generator of S. Fix a subsemigroup T of S. Let n be the smallest positive integer such that $t := x^n \in T$. If $t \in \mathcal{G}(x)$, then T is a subgroup of $\mathcal{G}(x)$ and, hence, can be generated by one element. Thus, without loss of generality, $t \in \mathcal{S}(x)$, and so $n \leq r-1$. Since the case $n = 1$ would force $T = \langle x \rangle$, which is cyclic, we can assume henceforth that $n > 1$.

If $r = 3$, then it follows from the proof of Proposition 2.1 that there is a (necessarily cyclic) subgroup T' of $\mathcal{G}(x)$ such that $T = \{x^2\} \cup T'$, and so T can be generated by $\{x^2, y\}$ where y is any generator of T'. In view of Proposition 2.1, the assertions for $r = 3$ now follow. The assertion for $r = 2$ also follows from Proposition 2.1.

We may assume henceforth that $r \geq 4$. We claim that T can be generated by a set of cardinality at most $n+1$. To see this, we begin to build a generating set W for T by letting $t\ (= x^n)$ be an element of W. The next element that we adjoin to W is x^{n_1} where n_1 (if it exists) is minimal such that $x^{n_1} \in T$, $n < n_1 \leq r-1$, and n does not divide n_1. Note that if $x^d \in T$ with $n < d < n_1$, then $n|d$ and so $x^d \in \langle x^n \rangle \subseteq \langle W \rangle$. The next element that we adjoin to W is x^{n_2} where n_2 (if it exists) is minimal such that $x^{n_2} \in T$, $n_1 < n_2 \leq r-1$, and n_2 is not congruent to either of 0 or n_1 modulo n. Note that if $x^d \in T$ with $n_1 < d < n_2$, then either d is congruent modulo n to 0 (in which case, x^d is an integral power of x^n and hence is in $\langle W \rangle$) or d is congruent modulo n to n_1 (in which case, $d - n_1 = kn$ for some $k \in \mathbb{N}$ and $x^d = x^{n_1}(x^n)^k \in \langle W \rangle$). Iterate. The process terminates in finitely many steps. Let the subset of W that has been built so far be denoted by $W' := \{x^n, x^{n_1}, \ldots, x^{n_e}\}$. By construction, $W' \subseteq T \cap \mathcal{S}(x) \subseteq \langle W' \rangle$. Moreover, the cardinality of W' is at most n since $n, n_1, \ldots, n_e$ represent $e+1$ different residue classes modulo n. Choosing a generator z for the cyclic group $T \cap \mathcal{G}(x)$, we see that $W := W' \cup \{z\}$ is a generating set for T of cardinality at most $n+1$, thus proving the above claim.

Suppose first that r is even, say with $r = 2s$ and $2 \leq s \in \mathbb{N}$. We consider first the subcase where $n < r/2\ (= s)$. (Note that $s \leq r-1$ since $r \geq 2$.) Then $n \leq s-1$ and the preceding paragraph has constructed a generating set of T that has cardinality at most $n+1 \leq s = r/2$, as asserted. Next, consider the subcase where $n > s$. Then, in the above construction, W' is a subset of $\{x^i \mid s+1 \leq i \leq r-1\}$, and so the cardinality of the generating set W is at most $(r-1-s)+1 = r/2$, as asserted. Finally, we consider the subcase where $n = s$. If we cannot argue essentially as in

the previous subcase, it must be that in the above construction, $W' = \{x^j \mid s \leq j \leq r-1\}$, which has cardinality $r/2$. However, in this situation, the s integers $s, s+1, \ldots, r-1$ represent all of the residue classes modulo $n = s$. It follows that for any integer $d \geq r$, there exists an integer j such that $s \leq j \leq r-1$ and d is congruent to j modulo n, say $d - j = kn$ with $k \in \mathbb{N}$. Then $x^d = x^j(x^n)^k \in \langle W' \rangle$, and so W' generates T in this subcase. This completes the proof that if r is even, then T has a generating set of cardinality at most $r/2$.

The reasoning in the last subcase that was considered above can be used to show that our result for even r is sharp. To wit, if $r = 2s$ is even, then every generating set of the semigroup $\langle \{x^j \mid s \leq j \leq r-1\} \rangle$ must contain $\{x^j \mid s \leq j \leq r-1\}$.

It remains to prove that if $r \geq 5$ is odd, then the maximum value of the minimum number of elements in a generating set of some subsemigroup T of $C(r, m)$ is $(r-1)/2$. The above analysis for the case of even r can be somewhat adapted to the present case. We have $r = 2s + 1$ and $2 \leq s \in \mathbb{N}$. (Also, $s < r - 1$ since $r > 1$.) If $n < s$, then T has a generating set of cardinality at most $n + 1 \leq s = (r-1)/2$. Next, suppose that $n = s$. The above construction gives that W' is a subset of $\{x^i \mid s \leq i \leq r-1\}$, which is a set of cardinality $r - 1 - (s-1) = s + 1$. Since $x^s = x^n \in W'$, it cannot be the case that $r - 1 = 2s \in W'$, and so the cardinality of W' is at most s. Adjoining a generator of $T \cap \mathcal{G}(x)$ to W' produces a generating set of T. The only possible difficulty with its cardinality would arise if $W' = \{x^i \mid s \leq i \leq r-2\}$. However, in this situation, the s integers $s, s+1, \ldots, r-2$ represent all of the residue classes modulo $n = s$. As above, one can then show that if d is any integer such that $d \geq r - 1$, then $x^d \in \langle W' \rangle$, and so W' is a generating set of T with cardinality s in this subcase.

In the remaining subcase, $n > s$ (and $r = 2s + 1 \geq 5$ is odd). The analysis of this subcase will present a novelty that did not arise when r was even. The above construction gives that W' is a subset of $\{x^i \mid s + 1 \leq i \leq r - 1\}$, which is a set of cardinality $r - 1 - s = s$. Once again, adjoining a generator of $T \cap \mathcal{G}(x)$ to W' produces a generating set of T. The only possible difficulty with its cardinality would arise if $W' = \{x^i \mid s + 1 \leq i \leq r - 1\}$. However, in this situation, we will show that W' is a generating set of T (with cardinality s). To that end, it suffices to show that if d is an integer such that $d \geq r$, then there exist non-negative integers λ and μ and a positive integer ν such that $d + \nu m = \lambda(s+1) + \mu(s+2)$, for then $x^d = x^{d+\nu m} = (x^{s+1})^\lambda (x^{s+2})^\mu \in \langle W' \rangle$. Consider the additive submonoid V of $\mathbb{N} \cup \{0\}$ that is generated by $\{s+1, s+2\}$. Since $s+1$ and $s+2$ are relatively prime, V is a numerical semigroup (or "numerical monoid" in the terminology of [1]). Therefore, by a classic result of Sylvester and A. Brauer (cf. [1, Theorem 2.2]), V has Frobenius number $g = s(s+1) - 1$, in the sense that if h is any integer such that $h > g$, then $h \in V$. Accordingly, given an integer $d \geq r$, we use the Archimedean principle to find a positive integer ν such that $h := d + \nu m > h$, so that $h \in V$. By the definition of V, there exist non-negative integers λ and μ such that $h = \lambda(s+1) + \mu(s+2)$; that is, $d + \nu m = \lambda(s+1) + \mu(s+2)$, as desired. This completes the proof that if $r \geq 5$ is odd, then T has a generating set of cardinality at most $(r-1)/2$.

Lastly, we show that our result for odd r is sharp. To wit, if $r = 2s + 1 \geq 5$ is odd, then every generating set of the semigroup $\langle \{x^j \mid s+1 \leq j \leq r-1\} \rangle$ must contain $\{x^j \mid s+1 \leq j \leq r-1\}$, a set whose cardinality is $r-1-s = s = (r-1)/2$. The proof is complete. □

Remark 2.3. In the statement of Theorem 2.2, the value given for $r = 3$ when m is even does not follow the pattern that holds for odd $r = 2s + 1 \geq 5$. This raises the question of where one used the condition $r = 2s+1 \geq 5$ in the proof of Theorem 2.2. This condition was used implicitly in constructing the numerical semigroup V, where it was important to know that $s+2 \leq r-1$ (so that in the relevant subcase, x^{s+2} is then an element of W'). However, $s+2 \leq (2s+1)-1$ is equivalent to $2 \leq s$; that is, to $r\ (= 2s+1) \geq 5$.

The next corollary is an immediate consequence of Theorem 2.2.

Corollary 2.4. Let $r, m \in \mathbb{N}$ and put $S := C(r, m)$. Then each subsemigroup of S has a generating set of cardinality at most $(r+1)/2$.

We turn next to questions about the total number of subsemigroups of various kinds that are contained in a given $C(r, m)$. It is particularly easy to count the cyclic subsemigroups of $C(r, m)$.

Proposition 2.5. Let $r, m \in \mathbb{N}$ and put $S := C(r, m)$. Then the number of cyclic subsemigroups of S is $r - 1 + \tau(m)$.

Proof. As usual, let x be a generator of S. A cyclic subsemigroup of S is generated either by an element of $\mathcal{S}(x)$ or by an element of $\mathcal{G}(x)$ (but not both). In the former case, there are $r-1$ distinct such subsemigroups, namely, $\langle x^i \rangle$ for $i = 1, \ldots, r-1$. In the latter case, the number of such sub(semi)groups is the number of positive integral divisors of the order m of $\mathcal{G}(x)$, namely, $\tau(m)$. The proof is complete. □

In Corollary 2.8, we will give a formula for the number of non-cyclic subsemigroups of a given $C(r, m)$ that can be generated by a set of two elements. It will be convenient to say that such a (sub)semigroup is 2-*generated*. The next lemma collects some facts that will be useful in developing the desired formula. Some of these facts are couched in terms of subsemigroups of $C(r, m)$ that may have more than two generators. This additional generality will lead to a formula for the number of subsemigroups of $C(r, m)$.

Lemma 2.6. Let $r, m \in \mathbb{N}$ with $r \neq 1$. Consider $S := C(r, m)$, with generator x as usual. Then:

(a) Consider positive integers $n_1 < \ldots < n_k \leq r-1$ and $z \geq r$. Put $d := \gcd(n_1, \ldots, n_k, m)$. Then $x^z \in \langle x^{n_1}, \ldots, x^{n_k} \rangle$ if and only if $d | z$. Consequently, the cardinality of $\langle x^{n_1}, \ldots, x^{n_k} \rangle \cap \mathcal{G}(x)$ is m/d.

(b) The number of non-cyclic subsemigroups of S that can be generated by a

set consisting of two elements of $\mathcal{S}(x)$ is

$$\frac{(r-2)(r-3)}{2} + \left\lfloor \frac{r-1}{2} \right\rfloor - 1 - \sum_{k=2}^{\lfloor \frac{r-1}{2} \rfloor} \left\lfloor \frac{r-1}{k} \right\rfloor .$$

Proof. (a) Suppose that $x^z \in \langle x^{n_1}, \ldots, x^{n_k} \rangle$. Then there exist non-negative integers $a_1, \ldots, a_k$ with $x^z = x^{\sum_{i=1}^k a_i n_i}$. It follows that $m|(z - \sum_{i=1}^k a_i n_i)$ and, hence, that $d|z$.

Conversely, suppose $d|z$. By the definition of d, there exist integers $u_1, \ldots, u_k$ and v such that $d = \sum_{i=1}^k u_i n_i + vm$. Choose e to be a positive integer that is so large that $u_i + em \prod_{j \neq i} n_j \geq r$ for all $i = 1, \ldots, k$ and $v - ke \prod_{j=1}^k n_j < 0$. Since

$$(u_1 + em \prod_{j \neq 1} n_j)n_1 + \cdots + (u_k + em \prod_{j \neq k} n_j)n_k + (v - ke \prod_{j=1}^k n_j)m = d,$$

we can assume, without loss of generality, that each of $u_1, \ldots, u_k$ is greater than $r-1$ and that $v < 0$. By hypothesis, $z = \zeta d$ for some $\zeta \in \mathbb{N}$. Next, choose $f \in \mathbb{N}$ such that $f + \zeta v > 0$. Then

$$x^z = x^z x^{fm} = x^{\zeta(u_1 n_1 + \cdots + u_k n_k)} x^{(f+\zeta v)m} = x^{\zeta(u_1 n_1 + \cdots + u_k n_k)} =$$

$(x^{n_1})^{\zeta u_1} \cdot \ldots \cdot (x^{n_k})^{\zeta u_k} \in \langle x^{n_1}, \ldots, x^{n_k} \rangle$.

For the "Consequently" assertion, the above work shows that it suffices to prove that the number of integers z such that $r \leq z \leq r + m - 1$ and $d|z$ is m/d. To see this, let i be minimal such that $0 \leq i \leq d-1$ $(\leq m-1)$ and $d|(r+i)$. Then d also divides $r+i+d, r+i+2d, \ldots$, and $r+i+(m/d-1)d$, but $r+i+(m/d)d > r+m-1$.

(b) An overcount for the desired number is provided by the number of two-element subsets of $\mathcal{S}(x)$, namely, $(r-1)(r-2)/2$. Because of various redundancies, several terms must be subtracted from this overcount. One such term counts the number of two-element subsets of $\mathcal{S}(x)$ that contain the element x. There are $r-2$ such subsets. Notice that $(r-1)(r-2)/2-(r-2) = (r-2)(r-3)/2$, which is one of the terms in the asserted answer. Next, for each integer k such that $2 \leq k \leq r-1$, we must subtract the number of subsets of $\mathcal{S}(x)$ that consist of x^k and x^{ek} where $e \geq 2$ is an integer such that $ek \leq r-1$. For a given value of k, the number of such subsets (equivalently, the number of such e) is $\lfloor \frac{r-1}{k} \rfloor - 1$. After all the subtractions have been made, algebraic simplification produces the asserted formula. □

Theorem 2.7. *Let $r, m \in \mathbb{N}$ with $r \neq 1$. Consider $S := C(r, m)$, with generator x as usual. Consider positive integers $n_1 < \ldots < n_k \leq r-1$. Put $H := \langle x^{n_1}, \ldots, x^{n_k} \rangle$ and $d := \gcd(n_1, \ldots, n_k, m)$. Then:*

(a) *The number of sub(semi)groups V of $\mathcal{G}(x)$ such that $H \cap \mathcal{G}(x) \subseteq V$ is $\tau(d)$.*

(b) *The number of subsemigroups of S that can be generated by the union of H with a (possibly empty) subset of $\mathcal{G}(x)$ is $\tau(d)$.*

Proof. (a) By Lemma 2.6 (a), $\mathfrak{H} := H \cap \mathcal{G}(x)$ is a subsemigroup, hence a subgroup, of $\mathcal{G}(x)$ of order m/d. Let V be a sub(semi)group of $\mathcal{G}(x)$ such that $\mathfrak{H} \subseteq V$. Let c be the order of V. By Lagrange's Theorem, $\frac{m}{d} | c$ and $c | m$. Thus, there exist $p, q \in \mathbb{N}$ such that $c = p(m/d)$ and $m = qc$. It follows easily that $d = pq$. On the other hand, if $p^\star$ is a positive integral divisor of d and $V^\star$ is the unique subgroup of $\mathcal{G}(x)$ of order $p^\star(m/d)$, then it follows from the well known theory of finite cyclic groups that $\mathfrak{H} \subseteq V^\star$ (since $V^\star$ has to contain a subgroup of order m/d and $\mathfrak{H}$ is the only subgroup of $\mathcal{G}(x)$ of order m/d). Thus, there is a one-to-one correspondence between the set of sub(semi)groups of $\mathcal{G}(x)$ that contain $\mathfrak{H}$ and the set of positive integral divisors of d.

(b) Suppose a subsemigroup T of S is generated by $H \cup \{x^{z_1}, \ldots, x^{z_s}\}$, where each $z_i \geq r$. (We do not rule out the possibility that each $x^{z_i} \in H$, in which case T is also generated by $H \cup \emptyset$.) Since $\{x^{z_1}, \ldots, x^{z_s}\}$ generates a cyclic subgroup of $\mathcal{G}(x)$, there exists $z^\star \geq r$ such that $x^{z^\star}$ generates this same cyclic subgroup. It follows that $T = \langle x^{n_1}, \ldots, x^{n_k}, x^{z^\star} \rangle$. Note that $V := T \cap \mathcal{G}(x)$ is a finite nonempty cancellative subsemigroup of $\mathcal{G}(x)$ and, hence, a cyclic subgroup of $\mathcal{G}(x)$. Thus, $V = \langle x^z \rangle$ for some integer $z \geq r$. We have $\mathfrak{H} := H \cap \mathcal{G}(x) \subseteq V$ and $T = (H \cap \mathcal{S}(x)) \cup V = \langle H \cup V \rangle$.

On the other hand, suppose that W is a subgroup of $\mathcal{G}(x)$ such that $\mathfrak{H} \subseteq W$. We claim that $U := \langle H \cup W \rangle$ can be expressed as $U = (H \cap \mathcal{S}(x)) \cup W$. Of course, $U = (H \cap \mathcal{S}(x)) \cup (U \cap \mathcal{G}(x))$, and so to prove the claim, it will suffice to show that $U \cap \mathcal{G}(x) = W$. As one inclusion is clear, we need only show that if $u \in U \cap \mathcal{G}(x)$, then $u \in W$. Since $\mathfrak{H} \subseteq W$, it follows from the definition of U that we can assume, without loss of generality, that there exist $h \in H$ and $w \in W$ such that $u = hw$. Then, working in the group $\mathcal{G}(x)$, we have $h = uw^{-1} \in H \cap \mathcal{G}(x) = \mathfrak{H} \subseteq W$. Thus, u is a product of two elements of W, and so the claim has been proved.

The upshot is that T is a subsemigroup of S that can be generated by the union of H with a subset of $\mathcal{G}(x)$ if and only if $T = (H \cap \mathcal{S}(x)) \cup V$ for some subgroup V of $\mathcal{G}(x)$ such that $\mathfrak{H} \subseteq V$. While it is clear that such a V determines T, the converse is also true, since $V = T \setminus (H \cap \mathcal{S}(x))$. Thus, the set of subsemigroups T of S with the property in question is in one-to-one correspondence with the set of subgroups V of $\mathcal{G}(x)$ such that $\mathfrak{H} \subseteq V$. Therefore, the assertion follows from (a). □

We next give the promised formula for the number of 2-generated subgroups of $C(r, m)$. Since every subgroup of a cyclic group is cyclic, it is natural to restrict to the case $r \neq 1$.

Corollary 2.8. Let $r, m \in \mathbb{N}$ with $r \neq 1$. Consider $S := C(r, m)$, with generator x as usual. Then the number of 2-generated subsemigroups of S is

$$\frac{(r-2)(r-3)}{2} + \left\lfloor \frac{r-1}{2} \right\rfloor - 1 - \sum_{k=2}^{\lfloor \frac{r-1}{2} \rfloor} \left\lfloor \frac{r-1}{k} \right\rfloor + \sum_{n=1}^{r-1} (\tau(\gcd(n, m)) - 1) \, .$$

Proof. There are two kinds of 2-generated subsemigroups of S, namely, those that can be generated (non-redundantly) by a pair of elements of $\mathcal{S}(x)$ and those

that can be generated (non-redundantly) by an element of $\mathcal{S}(x)$ and an element of $\mathcal{G}(x)$. The semigroups of the former type have been counted in Lemma 2.6 (b). It therefore suffices to show that the number of semigroups of the latter type is $\sum_{n=1}^{r-1}(\tau(\gcd(n,m))-1)$. In fact, a semigroup T is of the latter type if and only if $T=\langle x^n, x^z\rangle$ where n and z are positive integers such that $n \leq r-1$, $r \leq z \leq r+m-1$ and $x^z \notin \langle x^n\rangle$. Given n, the number of distinct such T is, by Theorem 2.7 (b), exactly $\tau(\gcd(n,m))-1$. (Notice that the subtraction of 1 is due to the fact that the set that was counted in Theorem 2.7 (b) included the semigroup $\langle x^n\rangle$, which should not be counted here because it is cyclic.) By adding these values as n goes from 1 to $r-1$, we complete the proof. □

In part of the literature, a semigroup is said to be k-generated if it has a generating set of cardinality at most k. If one wishes to determine the number of 2-generated subsemigroups of $C(r,m)$ in *this* sense (with $r,m \in \mathbb{N}$ and $r \neq 1$), one need only add the answers that were given in Proposition 2.5 and Corollary 2.8.

Suppose, as usual, that $r,m \in \mathbb{N}$ and $r \neq 1$. The proof of Theorem 2.7 (a), together with Lemma 2.6 (a), makes clear that a subsemigroup T of $C(r,m)$ contains at least one element from $\mathcal{S}(x)$ but is not generated by a subset of $\mathcal{S}(x)$ if and only if $T=\langle x^{n_1}, \ldots, x^{n_k}, x^z\rangle$ for some nonempty list of positive integers $n_1 < \ldots < n_k \leq r-1$ and an integer $z \geq r$ such that z is not divisible by $\gcd(n_1, \ldots, n_k, m)$. One now easily infers the necessary and sufficient condition in Corollary 2.9 (b) for such a generating set to be minimal.

Corollary 2.9. Let $r,m \in \mathbb{N}$ with $r \neq 1$. Let $S := C(r,m)$, with generator x as usual. Consider positive integers $n_1, \ldots, n_k \leq r-1$ and $z \geq r$ Then:

(a) $\{x^{n_1}, \ldots, x^{n_k}\}$ is a minimal generating set of a subsemigroup of S if and only if $x^{n_{i+1}} \notin \langle x^{n_1}, \ldots, x^{n_i}\rangle$ for each $i = 1, \ldots, k-1$.

(b) $\{x^{n_1}, \ldots, x^{n_k}, x^z\}$ is a minimal generating set of a subsemigroup of S if and only if $x^{n_{i+1}} \notin \langle x^{n_1}, \ldots, x^{n_i}\rangle$ for each $i = 1, \ldots, k-1$ and $\gcd(n_1, \ldots, n_k, m)$ is not an integral divisor of z.

Remark 2.10. Let $r,m \in \mathbb{N}$ with $r \neq 1$. Consider $S := C(r,m)$, with generator x as usual. We can now explain how, in principle, to determine the number, say M, of subsets of S which are minimal generating sets of a subsemigroup of S. In fact, we will write $M = M_1 + M_2 + M_3$, where M_1, M_2, M_3 are integers that are described below. Let N be the number of nonempty sets of positive integers $n_1 < \ldots < n_k$ ($\leq r-1$) which are "non-redundant" in the sense of satisfying the condition in Corollary 2.9 (a). Then $M_1 := N$ is the number of minimal generating sets $\mathfrak{S}$ of a subsemigroup of S such that $\mathfrak{S} \subseteq \mathcal{S}(x)$.

Next, we claim that that $M_2 := \sum_{1 \leq d \mid m} \varphi(d)$ is the number of minimal generating sets $\mathfrak{S}$ of a sub(semi)group of S such that $\mathfrak{S} \subseteq \mathcal{G}(x)$. To prove this claim, note that $\mathcal{G}(x)$ is a cyclic group of order m and hence has $\tau(m)$ (necessarily cyclic) subgroups, one for each positive integral divisor d of m; and for each such d, the corresponding subgroup of $\mathcal{G}(x)$ of order d has exactly $\varphi(d)$ minimal (that is, singleton) generating sets.

Finally, if we let M_3 denote the number of minimal generating sets $\mathfrak{S}$ of a subsemigroup of S such that $\mathfrak{S}$ is the union of a nonempty subset of $\mathcal{S}(x)$ with a singleton subset of $\mathcal{G}(x)$, it is clear that $M = M_1 + M_2 + M_3$, and so it remains only to explain how to calculate M_3. (Such sets $\mathfrak{S}$ were characterized in Corollary 2.9 (b).) Let $\mathfrak{S}_1, \ldots, \mathfrak{S}_N$ be the N minimal generating sets that are each subsets of $\mathcal{S}(x)$. For each $i = 1, \ldots, N$, let d_i be the greatest common divisor of m and the exponents of the elements of $\mathfrak{S}_i$. Then, by Theorem 2.7 (b), $M_3 = \sum_{i=1}^{N}(\tau(d_i) - 1)$.

Thus, the calculation of M has been reduced to the calculation of N. In principle (cf. Corollary 2.9 (a)), one could determine N in finitely many steps that involve inspecting the part of the multiplication table of S that is restricted to data from $\mathcal{S}(x)$. On the other hand, without the above analysis, the determination of M from first principles would have involved the inspection of the entire multiplication table of S.

Having characterized and (in principle) counted the minimal generating sets of subsemigroups of $C(r, m)$, we turn now to the question of counting those semigroups and finding a tractable upper bound for their number.

Corollary 2.11. Let $r, m \in \mathbb{N}$ with $r \neq 1$. Then:

(a) The number of subsemigroups of $C(r, m)$ is

$$\tau(m) + \sum_{\substack{1 \leq n_1 < \ldots < n_k \leq r-1 \\ x^{n_{i+1}} \notin \langle x^{n_1}, \ldots, x^{n_i} \rangle \text{ for each } i}} \tau(\gcd(n_1, \ldots, n_k, m)) .$$

(b) An upper bound for the number of subsemigroups of $C(r, m)$ is

$$\tau(m) + \sum_{1 \leq n_1 < \ldots < n_k \leq r-1} \tau(\gcd(n_1, \ldots, n_k, m)) .$$

Proof. It suffices to prove (a). The subsemigroups of $C(r, m)$ are of the following non-overlapping kinds: those that can be generated by non-redundant (that is, singleton) subsets of $\mathcal{G}(x)$; those that can be generated by non-redundant (and nonempty) subsets of $\mathcal{S}(x)$; and those containing at least one element of $\mathcal{S}(x)$ but not generated by a subset of $\mathcal{S}(x)$. Since $\mathcal{G}(x)$ is a cyclic group of order m, there are exactly $\tau(m)$ sub(semi)groups of the first kind. By Corollary 2.9 (a), the number of subsemigroups of the second kind is the number of indexes for the summation in the asserted formula. Finally, by combining Corollary 2.9 (b) and Theorem 2,7 (b), we see that the number of subsemigroups of the third kind is the indexed sum of the corresponding terms $\tau(\gcd(n_1, \ldots, n_k, m)) - 1$. The proof is complete. □

Note that the formula in Corollary 2.11 (b) is an upper bound, not an exact count, for only one reason, namely, that there may be some redundancy in the indexes $1 \leq n_1 < \ldots < n_k \leq r - 1$ for the summation in that formula. For instance, if $n_1 \leq (r - 1)/2$, then the index "$1 \leq n_1 < 2n_1 \leq r - 1$" is redundant

because $\langle n_1, 2n_1\rangle = \langle n_1\rangle$. One may conclude that the upper bound in Corollary 2.11 (b) is reasonably good for "small" values of r (as the number of such redundancies increases as r increases). We close by producing a weaker, but more tractable, upper bound and examining its asymptotics.

Remark 2.12. (a) The conclusions in Corollary 2.11 also hold if $r = 1$ (because empty sums are 0), but our emphasis here will continue to be on those $C(r, m)$ which are not groups. Thus, we assume throughout the rest of this remark that $r, m \in \mathbb{N}$ with $r \neq 1$.

(b) The upper bound in Corollary 2.11 (b) is somewhat intractable for at least the following two reasons. It is not clear how many indexes arise in the summation that appears as a term in that upper bound; and it is also not clear how many of those indexes give rise to the same value of $\gcd(n_1, \ldots, n_k, m)$. In any case, that upper bound leads easily to a weaker but more tractable upper bound, namely, $2^{r-1}\tau(m)$. To see this, observe that there are at most $2^{r-1} - 1$ indexes $1 \leq n_1 < \ldots < n_k \leq r - 1$; and for any such index, $\tau(\gcd(n_1, \ldots, n_k, m)) \leq \tau(m)$. Thus, we get the upper bound $B := \tau(m) + (2^{r-1} - 1)\tau(m) = 2^{r-1}\tau(m)$.

(c) It is well known that if $\delta > 0$, then $\lim_{m\to\infty} \tau(m)/m^\delta = 0$ (cf. [2, Theorem 6.25 (b)]). It follows that for bounded (for instance, fixed) r, the upper bound B that was given in (b) for the number of subsemigroups of $C(r, m)$ is small relative to m^δ, in the sense that $\lim_{m\to\infty} B/m^\delta = \lim_{m\to\infty} 2^{r-1}\tau(m)/m^\delta = 0$. It follows that $\lim_{m\to\infty} 2^{r-1}\tau(m)/(r + m - 1) = 0$. Intuitively, this means that if r is bounded and m is "large", then the number of subsemigroups of $C(r, m)$ is insignificant with respect to the cardinality of $C(r, m)$.

(d) It is natural to ask if it is "rare" for a nonempty subset of $C(r, m)$ to be a subsemigroup of $C(r, m)$. For the limit context from (b), where r is bounded and $m \to \infty$, we can intuitively confirm "rarity", since the ratio of the upper bound B to the number of nonempty subsets of $C(r, m)$, $2^{r-1}\tau(m)/2^{r+m-1} = \tau(m)/2^m$, has limit 0 as $m \to \infty$. However, the upper bound B does not lead to an intuitive answer to this question for the limit process where m is fixed and $r \to \infty$, since $\tau(m)/2^m$ is constant during that limit process (and, in particular, does not approach 0).

References

[1] R. Gilmer, Commutative Semigroup Rings, Univ. Chicago Press, Chicago, 1984.

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