Commutation Semigroups of Finite Metacyclic Groups with Trivial Centre

Darien DeWolf [1] and Charles C. Edmunds [2]

Abstract

We study the right and left commutation semigroups of finite metacyclic groups with trivial centre. These are presented

$$G(m,n,k) = \left\langle a, b; a^m = 1, b^n = 1, a^b = a^k \right\rangle \quad (m,n,k \in \mathbb{Z}^+)$$

with $(m, k-1) = 1$ and $n = ind_m(k)$, the smallest positive integer for which $k^n = 1 \pmod{m}$, with the conjugate of a by b written $a^b (= b^{-1}ab)$. The *right* and *left commutation semigroups of* G, denoted $\mathrm{P}(G)$ and $\Lambda(G)$, are the semigroups of mappings generated by $\rho(g) : G \to G$ and $\lambda(g) : G \to G$ defined by $(x)\rho(g) = [x, g]$ and $(x)\lambda(g) = [g, x]$, where the commutator of g and h is defined as $[g, h] = g^{-1}h^{-1}gh$. This paper builds on a previous study of commutation semigroups of dihedral groups conducted by the authors with C. Levy. Here we show that a similar approach can be applied to G, a metacyclic group with trivial centre. We give a construction of $\mathrm{P}(G)$ and $\Lambda(G)$ as unions of *containers*, an idea presented in the previous paper on dihedral groups. In the case that $\langle a \rangle$ is cyclic of order p or p^2 or its index is prime, we show that both $\mathrm{P}(G)$ and $\Lambda(G)$ are disjoint unions of maximal containers. In these cases, we give an explicit representation of the elements of each commutation semigroup as well as formulas for their exact orders. Finally, we extend a result of J. Countryman to show that, for $G(m, n, k)$ with m prime, the condition $|\mathrm{P}(G)| = |\Lambda(G)|$ is equivalent to $\mathrm{P}(G) = \Lambda(G)$.

Keywords: commutation semigroup, metacyclic group

1 Introduction

N.D. Gupta introduced the commutation semigroups of a group in [4]. Given a group G, the *right* and *left commutation maps* associated with an element $g \in G$ are the maps $\rho(g), \lambda(g) : G \to G$ defined by

$$(x)\rho(g) = [x, g] \text{ and } (x)\lambda(g) = [g, x],$$

where the commutator of x and y is denoted $[x, y] (= x^{-1}y^{-1}xy)$. Letting $\mathcal{M}(G)$ denote the semigroup, under composition, of all maps from G to G, we define the *right* and *left commutation semigroups*, denoted $\mathrm{P}(G)$ and $\Lambda(G)$, as the subsemigroups of $\mathcal{M}(G)$ generated by the sets $\mathrm{P}_1(G) = \{\rho(g) : g \in G\}$ and $\Lambda_1(G) = \{\lambda(g) : g \in G\}$. Note that if G is abelian, both commutation semigroups are trivial; thus for the remainder of this paper we will consider only the case where G is non-abelian.

[1]Department of Mathematics, Statistics and Computer Science, St. Francis Xavier University, 2323 Notre Dame Ave, Antigonish, NS B2G 2W5, ddewolf@stfx.ca

[2]Department of Mathematics and Statistics, Mount Saint Vincent University, 166 Bedford Highway, Halifax, NS B3M 2J6, cedmunds6868@gmail.com

It is interesting to note that when $G = S_3$, the symmetric group on three letters, $|\mathrm{P}(G)| = 6$ and $|\Lambda(G)| = 9$. One might have thought these two semigroups would be equal, or at least isomorphic. Thus the problem, originally asked by B.H. Neumann (oral communication to N.D. Gupta), was: for which groups are the left and right commutation semigroups (i) equal, (ii) isomorphic, or (iii) of equal order?

Gupta [4] solved the isomorphism problem for dihedral groups and showed that, for G nilpotent of class 2, 3, or 4, one has $\mathrm{P}(G) = \Lambda(G)$, $\mathrm{P}(G) \cong \Lambda(G)$, and $|\mathrm{P}(G)| = |\Lambda(G)|$, respectively. He also gave an example of a group nilpotent of class 5 for which the commutation semigroups are not isomorphic. In this context, since S_3 is not nilpotent, it is not surprising that its commutation semigroups are different.

Extending the work of Gupta [4], Countryman [1] studied the commutation semigroups of non-abelian pq-groups: pq-groups are extensions of a cycle of order p by a cycle of order q with both p and q prime. Since dihedral groups and pq-groups are metacyclic groups, the authors felt that the techniques of [2], [3], and [4] might extend to all metacyclic groups. We have chosen to restrict our discussion to metacyclic groups with trivial centre, where a number of fairly general results may be obtained. We will say more later about the decision to make this restriction. We continue, in the spirit of [2] and [3], to view the commutation semigroups in terms of containers. In [3], we were able to give formulas for the orders of the commutation semigroups of finite dihedral groups. For metacyclic groups, even those with trivial centre, we find that the situation is complex enough that such formulas are not likely obtainable. We will give examples illustrating how, even with trivial centre, the number-theoretic complexity of the parameter m makes the analysis more difficult. Despite this, we maintain that the method of containers is a powerful tool with which to study commutation semigroups of metacyclic groups in general.

In Section 2, we will show that the finite metacyclic groups with trivial centre have presentations

$$G(m, n, k) = \left\langle a, b; a^m = 1, b^n = 1, a^b = a^k \right\rangle,$$

where m, n, and k are positive integers, $(m, k-1) = 1$, and $n = ind_m(k)$, the smallest positive integer for which $k^n = 1 \pmod{m}$, where the conjugate of a by b is written $a^b (= b^{-1}ab)$. Each group $G(m, n, k)$ has $\langle a \rangle$ as a (cyclic) normal subgroup of order m and of index n. For different parameters, these presentations do not insure that the groups presented are non-isomorphic, but they do give exactly the finite metacyclic groups with trivial centre which we are studying. Thus these presentations are adequate for our purposes. It should be noted that, in [6], C.E. Hempel has classified the finite metacyclic groups up to isomorphism. $G(m, 2, m-1)$ is the dihedral group of order $2m$ and has trivial centre exactly when m is odd. Also, every pq-group can be presented as $G(p, q, k)$. Thus our results will apply to [1] on pq-groups as well as to [2], [3], and [7] on dihedral groups.

In [7], C. Levy obtained formulas for the orders of both left and right commutation semigroups for the dihedral groups $G(m, 2, m-1)$ with m odd. In [2], D. DeWolf gave formulas for $G(m, 2, m-1)$ with m even, and in [3], formulas were produced which covered both cases. For $G(m, 2, m-1)$ with m odd the container structure is less complex than when m is even. This is a consequence of the fact that when m is odd, the dihedral group $G(m, 2, m-1)$ has trivial centre. As our work with metacyclic groups proceeded, we saw that the assumption of trivial centre was a reasonable hypothesis to control some of the complexity. Thus, from Section 3 onward, we will assume our groups have trivial centre and can therefore be presented by some $G(m, n, k)$ as above. This hypothesis is equivalent to requiring that $k-1$ be coprime to m, as is shown in Section 2, and will force the value of m to be odd. Note, however, that $G(9, 3, 4)$ has odd m but also has trivial centre. Analogues of many of our results hold for metacyclic groups with centre, but we will leave them to a future study.

In Section 3, we introduce *mu-maps* and establish the fundamental information we will need about *containers*.

In Section 4, we move to a more general setting which will include both the left and the right commutation semigroups as particular cases of a more general construction. If G has trivial centre, then, based on any set $S \subseteq \mathbb{Z}_m$ which contains both zero and an invertible element, we will construct a semigroup $\Sigma_G(S)$, called the *G-semigroup based on S*. Under certain hypotheses, this will be *complete*, thereby allowing us to give a full characterization of the mappings in $\Sigma_G(S)$ as well as a formula for its exact order. Applying this result to $\mathrm{P}(G)$ and $\Lambda(G)$ will give us an explicit representation of the mappings they contain as well as formulas for their orders. This general approach may be of independent interest since it provides a construction of many different semigroups of mappings from G to G.

In Section 5, we will discuss non-basic orbits, the one difficulty that arises in the trivial centre case. For $\mathrm{P}(G)$ and $\Lambda(G)$, it appears that this difficulty is fairly rare. We will show in Section 6 that all orbits of $G(m,n,k)$ are basic when m is prime or the square of a prime or when n is prime. A computer search has determined that, for $\mathrm{P}(G)$ and $\Lambda(G)$ with $G = G(m,n,k)$, the first non-basic orbits appear when $m = 63 = 3^2 \cdot 7$. Further searching gives the next problematic values of m as $75 = 3 \cdot 5^2$, $81 = 3^4$, $99 = 3^2 \cdot 11$, $117 = 3^2 \cdot 13$, and $125 = 5^3$. We conjecture that there are infinitely many of these cases. The appearance of non-basic orbits appears to be correlated with the complexity of the factorization of m into primes. Thus, in place of formulas, we will give a procedure which deals with non-basic orbits and an example illustrating this procedure in action. In principle, our methods will determine the commutation semigroups of any metacyclic group with trivial centre, but our method is not uniform, depending very much on the number theory of each individual group.

In Section 6, we will give several applications of the general theory applied to $\mathrm{P}(G)$ and $\Lambda(G)$. We will show that for $G(m,n,k)$ with trivial centre, if m is prime or the square of a prime, or if n is prime, then $\mathrm{P}(G)$ and $\Lambda(G)$ are *complete* and can, therefore, be expressed as unions of maximal containers. Finally, we will re-state and extend the principle result of [1] showing that, for $G(m,n,k)$, if n is prime, then $\mathrm{P}(G)$ and $\Lambda(G)$ are complete.

2 Presenting finite metacyclic groups with trivial centre [1]

In Lemma 2.1 of [6], C.E. Hempel gives a presentation, which originated with Hölder, for finite metacyclic groups:

$$G = \left\langle a, b; a^m = 1, b^n = a^l, a^b = a^k \right\rangle \qquad (*)$$

where $k, l, m, n \in \mathbb{Z}^+$ with $k^n = 1 \pmod m$ and $l(k-1) = 0 \pmod m$. These have $\langle a \rangle$ as a (cyclic) normal subgroup of order m and index n.

Since we will be studying finite metacyclic groups with trivial centre, we will modify the presentation $(*)$ to produce a general presentation for all finite metacyclic groups *with trivial centre*. The derivation of the presentation given in Corollary 2.3 from $(*)$ is included since it is original and is not found in the literature. However, the details of this derivation can be skipped over without affecting understanding of the rest of the paper.

We define the index of k relative to m, denoted $ind_m(k)$, to be the smallest positive integer d for which $k^d = 1 \pmod m$. Note that this is the order of k in the group of invertible elements of $\mathbb{Z}_m$. If x is an element of a group G, we denote its order by $ord(x)$. Recall that the conjugate of a by b is $a^b = b^{-1}ab$, and the commutator of a and b is $[a,b] = a^{-1}b^{-1}ab$. The commutator identities $[xy,z] = [x,z]^y\,[y,z]$ and $[x,yz] = [x,z]\,[x,y]^z$ will be used in this section and the next without further comment.

We begin with an elementary observation.

Lemma 2.1. *For $k, m \in \mathbb{Z}^+$, if $k^n = 1 \pmod m$, then $(m,k) = 1$.*

Proof. Suppose $(m,k) = g > 1$, and $z \in \mathbb{Z}^+$ with $k^n = 1 + mz$. Then $k^n = 1 + mz$ and, since g divides k^n and m, g divides 1, a contradiction. □

[1]The authors express thanks to Prof. L.P. Comerford for his helpful comments on this section.

Lemma 2.2. *For $k, l, m, n \in \mathbb{Z}^+$ with $k^n = 1 \pmod{m}$ and $l(k-1) = 0 \pmod{m}$, the group*

$$G = \left\langle a, b; a^m = 1, b^n = a^l, a^b = a^k \right\rangle$$

has trivial centre if and only if $(m, k-1) = 1$ and $n = ind_m(k)$.

Proof. Suppose that there exists an $s \in \mathbb{Z}^+$ with $s < m$ and with s least so that $a^s = 1$ is a consequence of the relations given for G. Since $a^m = 1$, it follows that s divides m. We could apply Tietze transformations to the presentation to add the relation $a^s = 1$ and delete $a^m = 1$. Note that when we replace m by s, the congruences, since s divides m, still hold. We could then choose to replace the letter s by m throughout. Thus we may say $ord(a) = m$, without loss of generality. It follows that we may assume $k, l < m$. Note that

$$\left[a^i, b\right] = a^{-i}(a^i)^b = a^{-i}(a^i)^k = a^{i(k-1)}.$$

Thus

(i) $a^i \in Z(G)$ if and only if $i(k-1) = 0 \pmod{m}$.

(ii) Also since

$$\left[a, b^j\right] = a^{-1}a^{b^j} = a^{-1}a^{k^j} = a^{k^j - 1},$$

it follows that $b^j \in Z(G)$ if and only if $k^j - 1 = 0 \pmod{m}$.

(iii) Letting $d = ind_m(k)$ we claim that $b^d \in Z(G)$. To see this, note that $a^{b^d} = a^{k^d} = a$, since d is the least positive integer for which $k^d = 1 \pmod{m}$. Thus b^d commutes with both a and b and is, therefore, central in G.

($\Rightarrow$) Assuming G has trivial centre, we will first show that $(m, k-1) = 1$ by contradiction. Suppose that $(m, k-1) = g$ $(1 < g < m)$. Then there are positive integers m' and t such that $m = m'g$, $k - 1 = tg$, with $(m', t) = 1$. Since $0 < m' < m$ and $ord(a) = m$, we have $a^{m'} \neq 1$, but

$$m'(k-1) = m'tg = mt = 0 \pmod{m}.$$

Thus, by (i) above, we have $1 \neq a^{m'} \in Z(G) = \{1\}$, a contradiction. From the relation $b^n = a^l \in \langle a \rangle$, we have $a^{b^n} = a^{a^l} = a$; thus b^n is central in G and, therefore by assumption, is trivial. From this we see that $a^l = 1$ and, since $ord(a) = m$, we have $l = 0 \pmod{m}$. Since $b^n = 1 \in \langle a \rangle$, we know there are positive powers of b in $\langle a \rangle$. Suppose j is the least positive integer for which $b^j \in \langle a \rangle$ and let i be such that $b^j = a^i$. Note that $a = a^{a^i} = a^{b^j} = a^{k^j}$; therefore, $k^j = 1 \pmod{m}$, and since b^j is central, $b^j = 1$. Also note that, since j was selected minimally, we have $j = ind_m(k)$. Dividing n by j, we have a positive integer q and a non-negative integer r so that $n = qj + r$ $(0 \leq r < j)$, and hence $a^l = b^n = (b^j)^q b^r = b^r$. This contradicts the minimality of j unless $r = 0$. Therefore $n = jq$. Thus $a^l = b^n = (b^j)^q = (a^i)^q$, which shows that $b^j = a^i$ implies $b^n = a^l$. Since $b^j = a^i$ holds in G, it is a consequence of the relations of G; thus, by Tietze transformations, we can add $b^j = a^i$ to the relations of G, and remove its consequence $a^l = b^n$. As for the congruences on the parameters of the presentation, we have already noted that $j = ind_m(k)$. Thus, as j replaces n in the relations when removing $b^n = a^l$ and adding $b^j = a^i$, we drop the condition $k^n = 1 \pmod{m}$ and add $k^j = 1 \pmod{m}$. Also i replaces l in the deleting of $b^n = a^l$ and adding $b^j = a^i$. Thus we must see that $l(k-1) = 0 \pmod{m}$ can be replaced by $i(k-1) = 0 \pmod{m}$. This is the case because the relation $b^j = a^i$ implies that $b^j = 1$, since it is central, and therefore $a^i = 1$. This implies that $i = 0 \pmod{m}$ and therefore, $i(k-1) = 0 \pmod{m}$. Having applied these transformations, we may as well replace the letters i and j by l and n, respectively.

($\Leftarrow$) Suppose now that $(m, k-1) = 1$ and $n = ind_m(k)$. Since $\langle a \rangle \triangleleft G$ and $b^n = a^l \in \langle a \rangle$, the elements of the quotient group $G/\langle a \rangle$ are right cosets of $\langle a \rangle$, whose representatives are powers of b. G is the union of these cosets; therefore, each element of G can be written in the form $a^i b^j$ $(0 \le i < m,\ 0 \le j < n)$. Suppose then that some $a^i b^j \in G$is central. Note that

$$1 = \left[b, a^i b^j\right] = \left[b, b^j\right]\left[b, a^i\right]^{b^j} = \left[b, a^i\right]^{b^j} = \left(\left(a^{-i}\right)^b a^i\right)^{b^j} = \left(\left(a^{-i}\right)^k a^i\right)^{k^j} = a^{i(k-1)k^j}.$$

Thus $i(k-1)k^j = 0 \pmod m$. By Lemma 2.1, we know that k is invertible in and, by hypothesis, the same holds for $k-1$; therefore, we can reduce this congruence to $i = 0 \pmod m$. It follows that for any $a^i b^j \in Z(G)$, we have $a^i b^j = b^j \in Z(G)$. From (ii) above, b^j is central if and only if $k^j - 1 = 0 \pmod m$. If $j < n$, the statement $k^j - 1 = 0 \pmod m$ would contradict the minimality of $n(= ind_m(k))$ unless $j = 0$. Thus if $a^i b^j$ is central, it is trivial and, therefore, $Z(G) = \{1\}$, as required. □

Corollary 2.3. *For $m, n, k \in \mathbb{Z}^+$, every finite metacyclic group with trivial centre can be presented as*

$$G(m, n, k) = \left\langle a, b; a^m = 1, b^n = 1, a^b = a^k \right\rangle$$

where $(m, k-1) = 1$ and $n = ind_m(k)$.

Proof. We will begin with the presentation $(*)$, $G = \left\langle a, b; a^m = 1, b^n = a^l, a^b = a^k \right\rangle$, along with the conditions $k^n = 1 \pmod m$ and $l(k-1) = 0 \pmod m$. We know that every finite metacyclic group has this presentation for some $k, l, m, n \in \mathbb{Z}^+$. Lemma 2.2 says that the additional conditions, $(m, k-1) = 1$ and $n = ind_m(k)$, are necessary and sufficient to assure that the presentation gives a finite metacyclic group with trivial centre. Note that $n = ind_m(k)$ implies $k^n = 1 \pmod m$; thus the latter can be removed from the list as redundant. The condition $(m, k-1) = 1$ implies that $k-1$ is invertible in $\mathbb{Z}_m$. Multiplying both sides of the congruence $l(k-1) = 0 \pmod m$ by the inverse of $k-1$ yields $l = 0 \pmod m$. Therefore the relation $l = 0 \pmod m$ replaces $l(k-1) = 0 \pmod m$. Applying $l = 0 \pmod m$ to the only relation containing an l replaces $b^n = a^l$ with $b^n = 1$. Therefore, for $k, l, m, n \in \mathbb{Z}^+$ satisfying the conditions $(m, k-1) = 1$, $n = ind_m(k)$, and $l = 0 \pmod m$, the presentations $\left\langle a, b; a^m = 1, b^n = 1, a^b = a^k \right\rangle$ give exactly the finite metacyclic groups with trivial centre. Note that since the letter l does not occur in the presentation, we may omit the condition $l = 0 \pmod m$ without loss of generality. □

It will prove efficient to make the following notational conventions. If S is a subset of the multiplicative semigroup $\mathbb{Z}_m$, we denote the invertible elements of S by $I(S)$ and the non-invertible elements of S by $N(S)$. Recall that an element of is invertible if and only if it is coprime to m. For each t $(0 \le t \le n)$ we let $k_t = k^t - 1 \pmod m$. Thus $k_1 = k - 1 \pmod m$, $k_0 = 0 \pmod m$, and, since $k^n = 1 \pmod m$, we have $k_n = 0 \pmod m$.

Lemma 2.4. *If G is a finite metacyclic group presented by $(*)$ (possibly having a non-trivial centre) with $R = \{k_j \in \mathbb{Z}_m : j \in \mathbb{Z}_n\}$ and $L = \{-k_j \in \mathbb{Z}_m : j \in \mathbb{Z}_n\}$ then*

(i) $0 \in R$, $0 \in L$, *and*

(ii) *if $n = ind_m(k)$, the following conditions are equivalent:*

  (a) *the centre of G is trivial,*

  (b) $I(R) \neq \varnothing$,

  (c) $I(L) \neq \varnothing$.

Proof.

(i) Note that $0 = k_0 \in R$ and $0 = -k_0 \in L$.

(ii) ($a \Rightarrow b$) Suppose first that the centre of G is trivial and, hence, by Lemma 2.2, we have $(m, k_1) = 1$. It follows that $k_1 (\in R)$ is invertible in $\mathbb{Z}_m$.

($b \Rightarrow c$) If, for some $j \in \mathbb{Z}_n$, $k_j \in R$ is invertible in $\mathbb{Z}_m$, then $-k_j \in L$. Denoting the inverse of k_j in $\mathbb{Z}_m$ as k_j^{-1}, we see that $(-k_j)(-k_j^{-1}) = 1$; therefore, $-k_j$ is invertible. Hence $I(L) \neq \varnothing$.

($c \Rightarrow a$) Now suppose that there is a $j \in \mathbb{Z}_n$ for which $-k_j$ is invertible. Note that if $j = 0$, then $-k_0 = 0 \notin I(L)$. Therefore, we may assume that $0 < j < n$. If $j = 1$, we have k_1 invertible in $\mathbb{Z}_m$ and, hence, coprime to m. Thus, along with the hypothesis $n = ind_m(k)$, Lemma 2.2 implies that G has trivial centre. If $1 < j < n$, then

$$-k_j = -k_1(1 + k + \ldots + k^{j-1}) = k_1(-(1 + k + \ldots + k^{j-1})).$$

Since $-k_j$ is invertible, so are both factors; therefore, k_1 is invertible. It follows, by Lemma 2.2, that G has trivial centre. □

In Section 4, we will use the sets R and L to construct right and left commutation semigroups. The previous lemma illustrates how the triviality of the centre of G splits the number theory associated with the commutation semigroups into two distinct cases: R and L will each contain 0, a non-invertible element, but they will contain an invertible element exactly when the centre of G is trivial. The existence of invertible elements in R (and hence in L) will allow us to proceed with the arguments given below (see the definitions of *G-semigroup* and *orbit*). We will not give a complete description of the commutation semigroups in the case that the centre of G is trivial, but we will be able to obtain some useful and rather general results with this assumption. We will also show that our method will allow the calculation of the elements of the commutation semigroups and their orders provided the reader is willing to take on some cumbersome modular arithmetic calculations. A theory for metacyclic groups with non-trivial centre could still be approached using containers, but it would have to take a different form from what we do below.

From this point onward, $G(m, n, k)$, abbreviated as G, will be a finite metacyclic group with trivial centre as described in Corollary 2.3.

3 Commutation mappings, mu-maps, and containers

We begin to study commutation mappings on G with a general result about commutators.

Lemma 3.1. *If $G = G(m, n, k)$, $i, r \in \mathbb{Z}_m$ and $j, s \in \mathbb{Z}_n$, then $\left[a^i b^j, a^r b^s\right] = a^N$ where $N = ik^j k_s - rk^s k_j$* (mod m).

Proof.

$$\begin{aligned}\left[a^i b^j, a^r b^s\right] &= \left[a^i, a^r b^s\right]^{b^j} \left[b^j, a^r b^s\right] = \left[a^i, b^s\right]^{b^j} \left[b^j, a^r\right]^{b^s} \\ &= \left(a^{-i}(a^i)^{b^s}\right)^{b^j} \left(b^{-j} a^{-r} b^j a^r\right)^{b^s} = \left(a^{-i}(a^i)^{k^s}\right)^{k^j} \left(a^{-rb^j} a^r\right)^{k^s} = \left(a^{i(k^s-1)}\right)^{k^j} \left(a^{r(1-k^j)}\right)^{k^s} \\ &= a^{i(k^s-1)k^j + r(1-k^j)k^s} = a^{ik^j k_s + rk^s k_j}.\end{aligned}$$ □

The following concept was introduced by N.D. Gupta in [4].

Definition 3.2. For $G = G(m, n, k)$, and (x, y) a pair of elements, of a *mu-map* is a mapping $\mu(x, y) : G \to G$ defined by $\left(a^i b^j\right) \mu(x, y) = a^N$, where $N = xik^j - yk_j$ (mod m).

Lemma 3.3. *For each $g \in G$ the mappings $\rho(g)$ and $\lambda(g)$ are mu-maps. In particular if $g = a^r b^s$, then $\rho(a^r b^s) = \mu(k_s, rk^s)$ and $\lambda(a^r b^s) = \mu(-k_s, -rk^s)$.*

Proof. Note that, by Lemma 3.1,

$$(a^i b^j)\rho(a^r b^s) = \left[a^i b^j, a^r b^s\right] = a^N,$$

with $N = ik^j k_s - rk^s k_j \pmod m$. By the definition of mu-map, $(a^i b^j)\mu(k_s, rk^s) = a^{N'}$ with $N' = k_s ik^j - rk^s k_j$; thus $\rho(a^r b^s) = \mu(k_s, rk^s)$. Similarly

$$(a^i b^j)\lambda(a^r b^s) = \left[a^r b^s, a^i b^j\right] = a^N,$$

with $N = rk^s k_j - ik^j k_s \pmod m$, while $(a^i b^j)\mu(-k_s, -rk^s) = a^{N'}$ with $N' = -k_s ik^j - (-rk^s)k_j = -ik^j k_s + rk^s k_j$. Therefore $\lambda(a^r b^s) = \mu(-k_s, -rk^s)$. □

The fundamental problem in constructing the commutation semigroups is that, when taking products of rho-maps and lambda-maps, their products, in general, are not rho-maps and lambda-maps. Identifying the generating maps as mu-maps allows us a clearer view of how these products are formed since products of mu-maps are mu-maps.

Lemma 3.4. *If $\mu(x_1, y_1)$ and $\mu(x_2, y_2)$ are mu-maps, then their composition is a mu-map with*

$$\mu(x_1, y_1) \circ \mu(x_2, y_2) = \mu(x_1 x_2, y_1 x_2).$$

Proof.

$$\begin{aligned}
(a^i b^j)\mu(x_1, y_1) \circ \mu(x_2, y_2) &= (a^{x_1 ik^j - y_1 k_j} b^0)\mu(x_2, y_2) \\
&= a^{x_2(x_1 ik^j - y_1 k_j)k^0 - y_2 k_0} \\
&= a^{x_2(x_1 ik^j - y_1 k_j)} \\
&= a^{x_1 x_2 ik^j - y_1 x_2 k_j} \\
&= (a^i b^j)\mu(x_1 x_2, y_1 x_2).
\end{aligned}$$

□

In light of this result we make the following definition.

Definition 3.5. The set $\mathrm{M}(G) = \{\mu(x, y) : x, y \in \mathbb{Z}_m\}$ of all mu-maps forms a semigroup under composition of mappings. We will refer to $\mathrm{M}(G)$ as the *μ-semigroup associated with G*.

To obtain the commutation semigroups $\mathrm{P}(G)$ and $\Lambda(G)$, we will use Lemma 3.3 to rewrite the generating sets $\mathrm{P}_1(G)$ and $\Lambda_1(G)$ as mu-maps and form their closures in $\mathrm{M}(G)$ under composition. We can simplify this process further by grouping these mappings together into sets called *containers*.

Definition 3.6. For any pair $(x, y) \in \mathbb{Z}_m \times \mathbb{Z}_m$, the *$(x, y)$-container with respect to G* is the set $C_G(x, y) = \{\mu(x, yz) : z \in \mathbb{Z}_m\}$.

When no confusion will arises, we abbreviate $C_G(x, y)$ as $C(x, y)$. We denote the order of the container by $|C(x, y)|$. Note that by letting $z = 1$ in $\mu(x, yz)$ we see that $\mu(x, y) \in C(x, y)$. Containers may intersect, but only in a limited way.

Lemma 3.7. *For $G = G(m, n, k)$ and $x_1, x_2, y_1, y_2 \in \mathbb{Z}_m$, $C(x_1, y_1) \cap C(x_2, y_2) \neq \varnothing$ if and only if $x_1 = x_2 \pmod m$.*

Proof. ($\Rightarrow$) If $\mu \in C(x_1, y_1) \cap C(x_2, y_2)$, then there exist $z_1, z_2 \in \mathbb{Z}_m$ such that $\mu = \mu(x_1, y_1 z_1) = \mu(x_2, y_2 z_2)$. Applying both maps to $a \in G$, we have $(a)\mu(x_1, y_1 z_1) = a^{N_1}$ with $N_1 = x_1 \cdot 1 \cdot k^0 - y_1 z_1 k_0 = x_1 \pmod m$, while $(a)\mu(x_2, y_2 z_2) = a^{N_2}$ with $N_2 = x_2 \cdot 1 \cdot k^0 - y_2 z_2 k_0 = x_2 \pmod m$. It follows that $x_1 = x_2 \pmod m$.

($\Leftarrow$) Note that $\mu(x_1, 0) = \mu(x_1, y_1 \cdot 0) \in C(x_1, y_1)$ while $\mu(x_2, 0) = \mu(x_2, y_2 \cdot 0) \in C(x_2, y_2)$. But, since $x_1 = x_2 \pmod m$, we have $\mu(x_1, 0) = \mu(x_2, 0) \in C(x_1, y_1) \cap C(x_2, y_2)$. Thus $C(x_1, y_1) \cap C(x_2, y_2) \neq \varnothing$. □

We need a preliminary lemma to calculate the orders of containers.

Lemma 3.8. *Let $G = G(m, n, k)$ and $x, y \in \mathbb{Z}_m$. Then, for all $z_1, z_2 \in \mathbb{Z}_m$, $\mu(x, yz_1) = \mu(x, yz_2)$ if and only if $z_1 = z_2 \pmod{m'}$, where $m' = \frac{m}{(m,y)}$.*

Proof. Letting $(m, y) = g$, with $m = m'g$ and $y = y'g$, it follows that $(m', y') = 1$. Notice that $\frac{m}{(m,y)} = \frac{m'g}{g} = m'$.

($\Rightarrow$) Supposing that $\mu(x, yz_1) = \mu(x, yz_2)$, we will apply both mappings to $b \in G$. This gives $(b)\mu(x, yz_1) = a^{N_1}$ with $N_1 = x \cdot 0 \cdot k^1 - yz_1k_1$ and $(b)\mu(x, yz_2) = a^{N_2}$ with $N_2 = x \cdot 0 \cdot k^1 - yz_2k_1$. It follows that $yz_1k_1 = yz_2k_1 \pmod m$. One of the conditions on the presentation of G is that $(m, k_1) = 1$; therefore k_1 is invertible in $\mathbb{Z}_m$ and, multiplying both sides of the congruence by k_1^{-1}, we have $yz_1 = yz_2 \pmod m$. This can be rewritten $y'gz_1 = y'gz_2 \pmod{m'g}$. Thus we have $y'z_1 = y'z_2 \pmod{m'}$. Since $(m', y') = 1$, y' is invertible in $\mathbb{Z}_m$. Thus we can multiply both sides of the congruence by the inverse of y' in $\mathbb{Z}_m$ to obtain $z_1 = z_2 \pmod{m'}$.

($\Leftarrow$) Conversely, we will assume that $z_1 = z_2 \pmod{m'}$ and show that when the mappings $\mu(x, yz_1)$ and $\mu(x, yz_2)$ are applied to any $a^ib^j \in G$ the images are equal. We begin with $(a^ib^j)\mu(x, yz_1) = a^{N_1}$ and $(a^ib^j)\mu(x, yz_2) = a^{N_2}$ with $N_1 = xik^j - yz_1k_j$ and $N_2 = xik^j - yz_2k_j$. Therefore, $N_2 - N_1 = y(z_1 - z_2)k_j \pmod m$. Our hypothesis is equivalent to $z_1 - z_2 = 0 \pmod{m'}$. Multiplying both sides of the congruence by $y'k_j$ yields $y'(z_1 - z_2)k_j = 0 \pmod{m'}$. This can then can be transformed to $y'g(z_1 - z_2)k_j = g \cdot 0 \pmod{m'g}$, or $y(z_1 - z_2)k_j = 0 \pmod m$. Thus $N_2 - N_1 = 0 \pmod m$ and our conclusion follows. □

Corollary 3.9. *If $G = G(m, n, k)$ and $x \in \mathbb{Z}_m$ then, for all $y_1, y_2 \in \mathbb{Z}_m$, $\mu(x, y_1) = \mu(x, y_2)$ if and only if $y_1 = y_2 \pmod m$.*

Proof. In Lemma 3.8, replace y by 1, z_1 by y_1, and z_2 by y_2. Note that $(m, y) = (m, 1) = 1$; thus $m' = m$. □

Corollary 3.10. *If $G = G(m, n, k)$ and $x, y \in \mathbb{Z}_m$, then $|C(x, y)| = \frac{m}{(m,y)}$.*

Proof. From Lemma 3.8, there are exactly $\frac{m}{(m,y)}$ distinct mappings in the container $C(x, y)$. □

We will use the following lemmas in several of our examples.

Lemma 3.11. *If $G = G(m, n, k)$, for each $x, y \in \mathbb{Z}_m$,*

(i) $C(x, yz) \subseteq C(x, y)$,

(ii) $C(x, y) \subseteq C(x, 1)$,

(iii) *if $u \in I(\mathbb{Z}_m)$, then $C(x, y) = C(x, yu)$, and*

(iv) $C(x, y) = C(x, 1)$ *if and only if $y \in I(\mathbb{Z}_m)$.*

Proof.

(i) Let $\mu(x, (yz)w)$ be an arbitrary element of $C(x, yz)$ for some $w \in \mathbb{Z}_m$. Since $wz \in \mathbb{Z}_m$, we have $\mu(x, y(zw)) \in C(x, y)$ and our result follows.

(ii) In part (i), let $y = 1$ and change z to y.

(iii) ($\subseteq$) Let $\mu(x, y)$ $(z \in \mathbb{Z}_m)$ be an arbitrary element of $C(x, y)$. Since $zu^{-1} \in \mathbb{Z}_m$, it follows that $\mu(x, yu(zu^{-1})) \in C(x, yu)$. But $\mu(x, yu(zu^{-1})) = \mu(x, yz)$. Thus we have shown that $\mu(x, yz) \in C(x, yu)$.

($\supseteq$) This is immediate from part (i).

(iv) ($\Rightarrow$) Since $\mu(x,1) \in C(x,1) = C(x,y)$, there is a $z \in \mathbb{Z}_m$ so that $\mu(x,yz) = \mu(x,1)$. By Corollary 3.9, we have $yz = 1 \pmod{m}$, from which it follows that $y \in U(\mathbb{Z}_m)$.

($\Leftarrow$) This follows directly from part (iii) by letting $y = 1$. □

Lemma 3.12. *If $G = G(m,n,k)$ and $x, y_1, y_2 \in \mathbb{Z}_m$, then $C(x,y_1) \subseteq C(x,y_2)$ if and only if there exists $z \in \mathbb{Z}_m$ such that $y_1 = y_2 z \pmod{m}$.*

Proof. ($\Rightarrow$) We have $\mu(x,y_1) \in C(x,y_1) \subseteq C(x,y_2)$; therefore, there exists $z \in \mathbb{Z}_m$ such that $\mu(x,y_1) = \mu(x,y_2 z)$. Applying these mappings to b, we obtain $(b)\mu(x,y_1) = a^{N_1}$ where $N_1 = -y_1 k_1 \pmod{m}$ and $(b)\mu(x,y_2 z) = a^{N_2}$ where $N_2 = -y_1 z k_1 \pmod{m}$. Thus $y_1 k_1 = y_2 z k_1 \pmod{m}$ and, since $k_1$is invertible, we have $y_1 = y_2 z \pmod{m}$.

($\Leftarrow$) The fact that $C(x,y_1) = C(x,y_2 z) \subseteq C(x,y_2)$ follows immediately from Lemma 3.11(i). □

4 A generalized approach

Recall that if $\varnothing \neq S \subseteq \mathbb{Z}_m$, S^* denotes the subsemigroup of Z_m generated by S, and the invertibles $I(S^*)$ form a subgroup of $\mathbb{Z}_m$. It follows that $1 \in I(S^*)$ and, since $I(S^*)$ is a finite group, for each $x \in I(S^*)$, there is a least non-negative integer u for which $x^u = 1$. Thus $x^{-1} = x^{u-1} \in I(S^*)$.

Definition 4.1. A non-empty subset S of $\mathbb{Z}_m$ is a *base* if $0 \in S$ and $I(S)$ is non-empty.

Definition 4.2. For $G = G(m,n,k)$ and S a base, the *G-semigroup based on S*, denoted $\Sigma_G(S)$, is the subsemigroup of $\mathrm{M}(G)$ generated by $\Gamma_\mu(S) = \{\mu(s,z) : s \in S, z \in \mathbb{Z}_m\}$. We call the set $\Gamma_\mu(S)$ the set of *μ-generators associated with* S and the set $\Pi_\mu(S) = \{\mu(ss^*, s^* z) : s \in S, s^* \in S^*, z \in \mathbb{Z}_m\}$ the set of *μ-products associated with S.*

Lemma 4.3. *For $G = G(m,n,k)$ and S a base, $\Sigma_G(S) = \Gamma_\mu(S) \cup \Pi_\mu(S)$.*

Proof. We first show that $\Pi_\mu(S)$ is the set of products of two or more μ-generators. Suppose we form the product of two or more generators $\mu(s_1,z_1)\mu(s_2,z_2)\cdots\mu(s_t,z_t)$. By repeated use of Lemma 3.4, the product can be written $\mu(s_1 s_2 \cdots s_t, z_1 s_2 \cdots s_t)$. Note then that s_1 could be any element of S and $s_2 \cdots s_t$ represents an arbitrary element of S^*; therefore, each $\mu(ss^*, zs^*) \in \Pi_\mu(S)$ is such a product and each product is an element of $\Pi_\mu(S)$. Since we have included the generating set $\Gamma_\mu(S)$ and all products of generators, it is clear that $\Sigma_G(S) = \Gamma_\mu(S) \cup \Pi_\mu(S)$. □

By proper selection of S, we will be able to produce both the left and right commutation semigroups as particular instances of $\Sigma_G(S)$. The theorems we want to exhibit for $\mathrm{P}(G)$ and $\Lambda(G)$ will follow immediately from the same results for $\Sigma_G(S)$. In addition to representing the commutation semigroups, the construction of $\Sigma_G(S)$ produces a subsemigroup of $\mathrm{M}(G)$ for each choice of a base S and therefore may be worthy of further study on its own.

First we will establish that the commutation semigroups are, indeed, instances of $\Sigma_G(S)$.

Lemma 4.4. *If $G = G(m,n,k)$, $R = \{k_j \pmod{m} : j \in \mathbb{Z}_n\}$, and $L = \{-k_j \pmod{m} : j \in \mathbb{Z}_n\}$ then R and L are bases with $\mathrm{P}(G) = \Sigma_G(R)$ and $\Lambda(G) = \Sigma_G(L)$.*

Proof. Before we can form $\Sigma_G(S)$, we must confirm that S is a base; in particular, we must show that R and L are bases. By Lemma 2.4, we have zero in both $N(R)$ and $N(L)$, and since G has trivial centre, $I(R)$ and $I(L)$ are non-empty. Therefore R and L are bases. We will prove $\mathrm{P}(G) = \Sigma_G(R)$ and note that a similar argument can be given to prove $\Lambda(G) = \Sigma_G(L)$. By Lemma 3.3, we have $\rho(a^r b^s) = \mu(k_s, rk^s)$ for each $r \in \mathbb{Z}_m, s \in \mathbb{Z}_n$. Since $k_s \in R$ and $rk^s \in \mathbb{Z}_m$, $\mu(k_s, rk^s) \in \Gamma_\mu(R)$. Since k, and thus k^s, is invertible in $\mathbb{Z}_m$, it follows that $\{rk^s : r \in \mathbb{Z}_m\} = \mathbb{Z}_m$. Every element of $\Gamma_\mu(R)$ occurs in the form

$\mu(k_s, rk^s)$; therefore, $\{\rho(a^i b^j) : i \in \mathbb{Z}_m, j \in \mathbb{Z}_n\} = \Gamma_\mu(R)$. Since $\mathrm{P}(G)$ and $\Sigma_G(R)$ are generated by the same mappings, they are equal. $\square$

Lemma 4.5. *Suppose $G = G(m,n,k)$ and S is a base. For each $x, y \in \mathbb{Z}_m$, $\mu(x,y) \in \Sigma_G(S)$ if and only if $C(x,y) \subseteq \Sigma_G(S)$.*

Proof. $(\Rightarrow)$ Given any $z \in \mathbb{Z}_m$ we wish to show that if $\mu(x,y) \in \Sigma_G(S)$, then $\mu(x,yz) \in \Sigma_G(S)$. Suppose that $\mu(x,y) \in \Gamma_\mu(S)$; then $x \in S$ and $y \in \mathbb{Z}_m$. Thus $yz \in \mathbb{Z}_m$ and clearly $\mu(x,zy) \in \Gamma_\mu(S) \subseteq \Sigma_G(S)$. If $\mu(x,y) \in \Pi_\mu(S)$, then we know there are $s \in S$, $s^* \in S^*$, and $z' \in \mathbb{Z}_m$ so that $x = ss^* \pmod m$ and $y = s^*z' \pmod m$. Therefore, $yz = s^*z'z \pmod m$. Thus $\mu(x,yz) = \mu(ss^*, s^*z'z) \in \Pi_\mu(S) \subseteq \Sigma_G(S)$. In each case, $\mu(x,yz) \in \Sigma_G(S)$.

$(\Leftarrow)$ We know that $\mu(x,y) \in C(x,y)$. Thus, assuming $C(x,y) \subseteq \Sigma_G(S)$, it is immediate that $\mu(x,y) \in \Sigma_G(S)$. $\square$

The following lemma shows that each x in S^* produces at least one container in $\Sigma_G(S)$.

Lemma 4.6. *If $G = G(m,n,k)$ and S is a base, then for each $x \in S^*$, there exists $y \in S^*$ so that $C(x,y) \subseteq \Sigma_G(S)$.*

Proof. If $x \in S^*$, then $x \in S$ or x is a product of elements of S. If $x \in S$ then, selecting $y = 1$, we obtain $\mu(x,1) \in \Gamma_\mu(G) \subseteq \Sigma_G(S)$. Therefore, by Lemma 4.5, we have $C(x,1) \subseteq \Sigma_G(S)$, as required. If $x = s_1 s_2 \dots s_t$ ($s_i \in S, t > 1$), let $x' = s_2 \dots s_t$. Since $x' \in S^*$, we see that $\mu(s_1 x', x') \in \Pi_\mu(S) \subseteq \Sigma_G(S)$. Since $x = s_1 x'$, if we select $y = x'$, Lemma 4.5 implies that $C(x,y) \subseteq \Sigma_G(S)$. $\square$

We now introduce a set $Y(x)$ associated with each x in S^*. The following lemma characterizes exactly those y-values for which $C(x,y) \subseteq \Sigma_G(S)$.

Lemma 4.7. *If $G = G(m,n,k)$, S is a base, $x \in S^*$, and*

$$Y(x) = \{s^*z : s^* \in S^*, z \in \mathbb{Z}_m, \exists s \in S \text{ so that } x = ss^* \pmod m\},$$

then $y \in Y(x)$ if and only if $C(x,y) \subseteq \Sigma_G(S)$.

Proof. It will be convenient to suppress mention of the modulus m.

$(\Rightarrow)$ If $y \in Y(x)$ then, there exist $s^* \in S^*$, $z \in \mathbb{Z}_m$, and $s \in S$ with $x = ss^*$ and $y = s^*z$. By Lemma 4.6, we know there exists $y' \in S^*$ such that $\mu(s^*, y') \in \Sigma_G(S)$. Also, we have $\mu(s,z) \in \Gamma_\mu(S) \subseteq \Sigma_G(S)$. Therefore, $\mu(s,z)\mu(s^*,y') \in \Sigma_G(S)$. Note that $\mu(s,z)\mu(s^*,y') = \mu(ss^*, s^*z) = \mu(x,y)$. And, since $\mu(x,y) \in \Sigma_G(S)$, Lemma 4.5 implies that $C(x,y) \subseteq \Sigma_G(S)$.

$(\Leftarrow)$ Suppose now that $C(x,y) \subseteq \Sigma_G(S)$. By Lemma 4.5, we have $\mu(x,y) \in \Sigma_G(S)$. By Lemma 4.3, $\mu(x,y) \in \Gamma_\mu(S)$ or $\Pi_\mu(S)$. In the first case, we have $x \in S$. Since $I(S^*)$ is a group, we know $1 \in I(S^*) \subseteq S^*$; therefore, we let $s = x$, $s^* = 1$, and $z = y$ to obtain $x = ss^* = x \cdot 1$, with $y = s^*z = 1 \cdot y$. Therefore, $y \in Y(x)$. In the second case, $\mu(x,y) \in \Pi_\mu(S)$. Thus we have $s \in S, s^* \in S^*$ and $z \in \mathbb{Z}_m$, with $x = ss^*$ and $y = s^*z$. It follows that $y \in Y(x)$. $\square$

Note that by Lemma 4.6, given any $x \in S^*$ there is a $y \in S^*$ for which $C(x,y) \subseteq \Sigma_G(S)$; furthermore, Lemma 4.7 determines exactly those values of y for which $C(x,y) \subseteq \Sigma_G(S)$. We will refer to these containers as a *family*.

Definition 4.8. Suppose $G = G(m,n,k)$ and S is a base. For each $x \in S^*$, the *x-family of containers (with respect to G and S)* is the set $\mathcal{F}_G(x,S) = \{C(x,y) : y \in Y(x)\}$. We denote the union of the x-family by $\cup\mathcal{F}_G(x,S) = \bigcup_{y \in Y(x)} C(x,y)$.

Theorem 4.9. *If $G = G(m, n, k)$ and S is a base, then*

$$\Sigma_G(S) = \dot{\bigcup}_{x \in S^*} \left(\cup \mathcal{F}_G(x, S) \right).$$

Proof. Note that the union is disjoint by Lemma 3.7.

($\subseteq$) If $\mu(x_0, y_0) \in \Sigma_G(S)$, then, by Lemma 4.5, $C(x_0, y_0) \subseteq \Sigma_G(S)$. Thus, by Lemma 4.7, $y_0 \in Y(x_0)$. Therefore $C(x_0, y_0) \in \mathcal{F}_G(x_0, S)$, which implies that $\mu(x_0, y_0) \in C(x_0, y_0) \subseteq \cup \mathcal{F}_G(x_0, S)$. Therefore

$$\mu(x_0, y_0) \in \dot{\bigcup}_{x \in S^*} \left(\cup \mathcal{F}_G(x, S) \right).$$

($\supseteq$) If

$$\mu(x_0, y_0) \in \dot{\bigcup}_{x \in S^*} \left(\cup \mathcal{F}_G(x, S) \right),$$

it follows, by Lemma 3.7, that

$$\mu(x_0, y_0) \in \cup \mathcal{F}_G(x_0, S) = \bigcup_{y \in Y(x_0)} C(x_0, y).$$

Therefore $y_0 \in Y(x_0)$ and thus, by Lemma 4.7, $C(x_0, y_0) \subseteq \Sigma_G(S)$. By Lemma 4.5, $\mu(x_0, y_0) \in \Sigma_G(S)$. □

Theorem 4.9 states that $\Sigma_G(S)$ is the disjoint union of all the x-families. Since distinct families are disjoint, the complexity involved in representing $\Sigma_G(S)$ as a union of containers occurs entirely within each x-family. In this section, we will determine conditions that assure a minimal amount of complexity, so that this union is easily determined. In Section 5, we will study the more involved situation.

Definition 4.10. If $G = G(m, n, k)$ and S is a base, for each $x \in S^*$, we say the x-family $\mathcal{F}(x, S)$ is *complete* if $C(x, 1) \in \mathcal{F}(x, S)$. The G-semigroup $\Sigma_G(S)$ is *complete* if each x-family is complete .

Not all x-families are complete. In Section 5, Example 5.1 will show, for $G = G(63, 6, 2)$, that $\mathcal{F}(21, \{0, 1, 3, 7, 15, 31\})$ is not complete.

Lemma 4.11. *For $x \in S^*$, if $\mathcal{F}(x, S)$ is complete, then $\cup \mathcal{F}(x, S) = C(x, 1)$.*

Proof. ($\subseteq$) By Lemma 3.11(ii), we have $C(x, y) \subseteq C(x, 1)$ for each $y \in \mathbb{Z}_m$. Therefore,

$$\cup \mathcal{F}_G(x, S) = \bigcup_{y \in Y(x)} C(x, y) \subseteq C(x, 1).$$

($\supseteq$) Since $\mathcal{F}(x, S)$ is complete, we know that $C(x, 1) \in \mathcal{F}(x, S)$; therefore, $C(x, 1) \subseteq \cup \mathcal{F}(x, S)$. □

Theorem 4.12. *If $G = G(m, n, k)$, S is a base, and $\Sigma_G(S)$ is complete, then $\Sigma_G(S) = \dot{\bigcup}_{x \in S^*} C(x, 1)$ and $|\Sigma_G(S)| = m\,|S^*|$.*

Proof. By Theorem 4.9,

$$\Sigma_G(S) = \dot{\bigcup}_{x \in S^*} \left(\cup \mathcal{F}_G(x, S) \right).$$

Since each x-family is complete, Lemma 4.11 implies that

$$\Sigma_G(S) = \dot{\bigcup}_{x \in S^*} C(x, 1).$$

By Corollary 3.10, $|C(x, 1)| = \frac{m}{(m,1)} = m$. Therefore $|\Sigma_G(S)| = m\,|S^*|$. □

Thus, if $\Sigma_G(S)$ is complete, we have the simplest situation. $\Sigma_G(S)$ is a disjoint union of maximal containers and its order is easily calculated. At this point we turn our attention to incomplete x-families.

Definition 4.13. If $G = G(m, n, k)$, S is a base, and $x \in S^*$, then *the orbit of* x in S^* is the set $orb(x, S^*) = \{xy : y \in I(S^*)\}$.

Since S is a base, there are invertibles in S^*. As noted earlier, $I(S^*)$ forms a group, thus $1 \in I(S^*)$ and it follows that $x \in orb(x, S^*)$. If G had non-trivial centre, there will be no invertibles with which to create an orbit and a different approach will be required.

Lemma 4.14. *If $G = G(m, n, k)$ and S is a base, then, for each $x_1, x_2 \in S^*$, either $orb(x_1, S^*) = orb(x_2, S^*)$ or $orb(x_1, S^*) \cap orb(x_2, S^*) = \varnothing$.*

Proof. Suppose that $orb(x_1, S^*) \cap orb(x_2, S^*) \neq \varnothing$ and that $z \in orb(x_1, S^*) \cap orb(x_2, S^*)$. Thus there are $y_1, y_2 \in I(S^*)$ so that $x_1y_1 = z = x_2y_2$. It follows that $x_1 = x_2y_2y_1^{-1}$. An arbitrary element of $orb(x_1, S^*)$ is of the form x_1u ($u \in I(S^*)$, thus $x_1u = x_2(y_2y_1^{-1}u) \in orb(x_2, S^*)$. It follows that $orb(x_1, S^*) \subseteq orb(x_2, S^*)$. The other containment is shown similarly and our result follows. □

The fact that S^* is the union of its orbits together with Lemma 4.14 imply that the orbits of S^* partition it into equivalence classes with respect to the relation defined as $x \sim y$ if and only if there exists a $z \in I(S^*)$ for which $x = yz$. In fact $\sim$ is a congruence; thus the quotient semigroup $S/\sim$ can be formed. The number of distinct orbits in S^* is the order of the quotient semigroup. We will next show how these orbits are involved in the search for the containers within $\Sigma_G(S)$.

Definition 4.15. If $G = G(m, n, k)$, S is a base, and $x \in S^*$, the orbit, $orb(x, S^*)$ is called *basic* if $orb(x, S^*) \cap S \neq \varnothing$.

Theorem 4.16. *If $G = G(m, n, k)$, S a base, and $x \in S^*$, then $orb(x, S^*)$ is basic if and only if $\mathcal{F}(x, S)$ is complete.*

Proof. ($\Rightarrow$) Since $orb(x, S^*)$ is basic, we know there is an $s \in S$ and an invertible $y \in I(S^*)$ for which $xy = s$. Thus, representing the inverse of y (mod m) as y^{-1}, we have $x = sy^{-1}$. Since $I(S^*)$ forms a group, $y^{-1} \in I(S^*) \subseteq S^*$; therefore,

$$\mu(x, y^{-1}) = \mu(sy^{-1}, y^{-1}) \in \Pi_\mu(S) \subseteq \Sigma_G(S).$$

Thus $C(x, y^{-1}) \subseteq \Sigma_G(S)$, by Lemma 4.5. Since y^{-1} is invertible, Lemma 3.11(iv) implies that $C(x, y^{-1}) = C(x, 1)$; therefore, $C(x, 1) \subseteq \Sigma_G(S)$ and $\mathcal{F}(x, S)$ is complete.

($\Leftarrow$) If $\mathcal{F}(x, S)$ is complete, then $C(x, 1) \subseteq \Sigma_G(S)$. Thus $\mu(x, 1) \in \Sigma_G(S)$, by Lemma 4.5. If $\mu(x, 1) \in \Gamma_\mu(S)$, then $x \in S$ and, since $x \in orb(x, S^*) \cap S$,$orb(x, S^*)$ is basic. If $\mu(x, 1) \in \Pi_\mu(S)$, then $x = ss^*, 1 = s^*z$ and, since $s^*z = 1$, s^* is invertible. Therefore, $x(s^*)^{-1} \in orb(x, S^*)$, and $x(s^*)^{-1} = ss^*(s^*)^{-1} = s \in S$. Thus $x(s^*)^{-1} \in orb(x, S^*) \cap S$, and it follows that $orb(x, S^*)$ is basic. □

Theorem 4.17. *If $G = G(m, n, k)$ and S is a base, then $orb(x, S^*)$ is basic, for each $x \in S^*$, if and only if $\Sigma_G(S)$ is complete. In this case we have $\Sigma_G(S) = \dot{\bigcup}_{x \in S^*} C(x, 1)$ and $|\Sigma_G(S)| = m\,|S^*|$.*

Proof. By Theorem 4.16, each orbit is basic if and only if each x-family $\mathcal{F}(x, S)$ is complete. This is the case if and only if $\Sigma_G(S)$ is complete. The second sentence follows by Theorem 4.12. □

Corollary 4.18. *If $G = G(m, n, k)$, $R = \{k_j : j \in \mathbb{Z}_n\}$ and $L = \{-k_j : j \in \mathbb{Z}_n\}$, then*

(i) If, for each $x \in R^*$, $orb(x, R)$ is basic, then $\Sigma_G(S) = \dot{\bigcup}_{x \in R^*} C(x, 1)$ and $|\mathrm{P}(G)| = |R^*|\,m$, and

(ii) If, for each $x \in L^*$, $orb(x, L)$ is basic, then $\Sigma_G(S) = \dot{\bigcup}_{x \in L^*} C(x, 1)$ and $|\Lambda(G)| = |L^*|\,m$.

Proof. By Lemma 4.4, we know that $\mathrm{P}(G) = \Sigma_G(R)$ and $\Lambda(G) = \Sigma_G(L)$. The result then follows immediately from Theorem 4.17. □

If the orbit of x is basic, then $\cup\mathcal{F}(x,S) = C(x,1)$. However if the orbit of x is non-basic, the containers in $\mathcal{F}(x,S)$ have a more complex interrelationship. We now give examples to illustrate that, for $G(m,n,k)$ with trivial centre, it is possible for each orbit to be basic in R^* but not in L^* and vice versa. Thus the completeness of $\mathrm{P}(G)$ and $\Lambda(G)$ are independent.

Example 4.19. We leave the modular arithmetic calculations to the reader. Note that $G(315,12,272)$ has trivial centre and that $orb(x,R^*)$ is basic for each $x \in R^*$, but $orb(225,L^*)$ is not basic. Also $G(135,12,62)$ has trivial centre and $orb(x,L^*)$ is basic for each $x \in L^*$, but $orb(130,R^*)$ is not basic. In each case there is just one orbit which is not basic though, in general, this is not the case. A computer search shows that 63 is the smallest value of m for which non-basic orbits exist in metacyclic groups with trivial centre for $\mathrm{P}(G)$ or $\Lambda(G)$.

We will apply the following Lemma and Corollary to narrow the search for non-basic orbits.

Lemma 4.20. *If $G = G(m,n,k)$, S is a base, and $x \in I(S^*)$, then $orb(x,S^*)$ is basic.*

Proof. Since $x \in I(S^*)$, it is invertible. Let us call the inverse x^{-1} and note that, by Lemma 4.7, $x^{-1} \in I(S^*)$. Since S is a base, we know that there is some $y \in I(S)$. Then

$$y = 1\,(y) = (xx^{-1})y = x(x^{-1}y) \in orb(x,S^*).$$

Thus $y \in orb(x,S^*) \cap S$ and it follows that $orb(x,S^*)$ is basic. □

Corollary 4.21. *Let $G = G(m,n,k)$ and let S be a base. If, for each $x \in N(S^*) - N(S)$, $orb(x,S)$ is basic, then all orbits are basic.*

Proof. Let $x \in S^*$. It is clear that if $x \in S$, then $x \in S \cap orb(x,S)$, thus $orb(x,S)$ is basic. By Lemma 4.20, if $x \in I(S^*)$, then $orb(x,S^*)$ is basic. Therefore, if $orb(x,S)$ is non-basic, $x \in N(S^*)$ and $x \notin S$. □

Example 4.22. Let us return to the smallest non-abelian (metacyclic) group, $S_3 = G(3,2,2)$. Since $(k_1,m) = (1,3) = 1$, we know that S_3 has trivial centre. We calculate the sets R^* and L^* as the multiplicative closures, modulo 3, of

$$R = \{k^j - 1 : j \in \mathbb{Z}_2\} = \{2^0 - 1, 2^1 - 1\} = \{0,1\}$$

and

$$L = \{1 - k^j : j \in \mathbb{Z}_2\} = \{1 - 2^0, 1 - 2^1\} = \{0,2\}$$

(Note that $L = -R$.) Thus $R^* = \{0,1\}$ and $L^* = \{0,1,2\}$. We must next verify that each orbit is basic. By Corollary 4.21, we need only check those $x \in N(S^* - S)$. Since $R^* = R$, this case requires no checking. For L^*, we need only check to see if $orb(1,L^*)$ intersects L. This is true since

$$orb(1,L^*) = \{1 \cdot y : y \in (L^*)\} = \{1,2\}$$

and

$$orb(1,L^*) \cap L = \{2\} \neq \varnothing.$$

Thus Corollary 4.18 applies and we conclude that $|\mathrm{P}(S_3)| = |R^*|\,m = 2 \cdot 3 = 6$ and $|\Lambda(S_3)| = |L^*|\,m = 3 \cdot 3 = 9$, as previously stated. This is a kind of "solution" to the mystery of how these orders can be different in the face of so much symmetry. In fact we can identify the exact mappings contained in both $\mathrm{P}(G)$ and $\Lambda(G)$ using containers. Theorem 4.17 implies that

$$\mathrm{P}(S_3) = C(0,1) \cup C(1,1) = \{\mu(0,0), \mu(0,1), \mu(0,2), \mu(1,0), \mu(1,1), \mu(1,2)\}$$

and

$$\Lambda(S_3) = C(0,1) \cup C(1,1) \cup C(2,1)$$
$$= \{\mu(0,0), \mu(0,1), \mu(0,2), \mu(1,0), \mu(1,1), \mu(1,2), \mu(2,0), \mu(2,1), \mu(2,2)\}.$$

Example 4.23. Since the construction of $\Sigma_G(S)$ may be of independent interest, we will select a small m for G, with trivial centre, and choose a base S which will generate in "interesting" example of $\Sigma_G(S)$. Let $G = G(5,4,3)$ and let $S = \{0,4\}$. Since $(k-1,m) = (2,5) = 1$, it follows that G has trivial centre. S is a base since $0 \in N(S)$ and $4 \in I(S)$. We compute that $S^* = \{0,1,4\}$. To see that each orbit is basic, we need only check $x \in S^* - S = \{1\}$. Since $orb(1,S^*) = \{1,4\}$, we have $orb(1,S^*) \cap S = \{4\} \neq \varnothing$. It follows that Theorem 4.17 and Corollary 4.18 hold in this case. Thus we see that $\Sigma_G(S)$ is a union of the maximal containers $C(x,1)$ for $x \in S^*$. It follows from our theorems, since $|C(x,1)| = 5$ and $|S^*| = 3$, that $|\Sigma_G(S)| = 15$. In this case we may also compute that $R^* = L^* = \{0,1,2,3,4\}$ and $|\mathrm{P}(G)| = |\Lambda(G)| = 25$; thus it is clear that $\Sigma_G(S)$ is a semigroup distinct from the commutation semigroups.

5 Non-basic orbits

In the previous section we have seen that, given $G(m,n,k)$ and a base S, if each orbit is basic, $\Sigma_G(S)$ is complete. Theorem 4.12 then gives us a description of the mu-maps in $\Sigma_G(S)$ in terms of containers as well as an easily calculated formula for its order. The other case to consider is the occurrence of non-basic orbits in S^*. Here we have a more complex situation for which a uniform description of the mu-maps in $\Sigma_G(S)$ is more difficult to obtain. Thus we will provide a procedure which lists the x's with non-basic orbits. In each case we will then apply Lemma 4.7 to generate $\mathcal{F}_G(x,S)$. Having done this for each non-basic x, we can then find exactly those containers which constitute $\Sigma_G(S)$. When $orb(x,S^*)$ is non-basic, we may need to include more than one x-container in the union. Some x-families have one container which is a superset of all other members of the family, and this can be used as the only x-container in the union. However, some x-families require the union of several containers. These containers will not be disjoint; thus, to determine the order of the x-family portion of the union forming $\Sigma_G(S)$, we may have to use the principle of inclusion and exclusion. We will then work through an example to illustrate the procedure in action.

Procedure. We assume we are given $G = G(m,n,k)$, a metacyclic group with trivial centre, and a base $S \subseteq \mathbb{Z}_m$. We generate S^* by closing S under multiplication and then write $S^* = I(S^*)\dot{\bigcup}N(S^*)$.

Next, we calculate the orbits, for each $x \in S^*$, by forming the sets $orb(x,S^*) = \{xy : y \in I(S^*)\}$.

By Corollary 4.21, we need only check the orbits for $x \in N(S^*) - N(S)$ to see if $orb(x,S^*) \cap S = \varnothing$. If each orbit intersects S, then Theorem 4.17 tells us that $\Sigma_G(S)$ is complete, how to write it as a union of containers, and its order.

When an orbit does not intersect S, we add $orb(x,S^*)$ to the list of non-basic orbits. Assuming there are non-basic orbits, write $S^* = B \cup N$, with $B = \{x \in S^* : orb(x,S^*) \text{isbasic}\}$ and $N = \{x \in S^* : orb(x,S^*) \text{isnotbasic}\}$. By Theorem 4.16, we can write the portion of $\Sigma_G(S)$ covered by families of containers associated with basic orbits, as with size $m\,|B|$. The remaining portion of $\Sigma_G(S)$ is $\dot{\bigcup}_{x \in N} \cup \mathcal{F}(x,S)$. We know that, for each $x \in N$, $\cup\mathcal{F}(x,S) = \bigcup_{y \in Y(x)} C(x,y)$. The first step in determining these unions is to calculate the set $Y(x)$ for a particular $x \in N$. Since $N \cap S = \varnothing$, we know that $\mu(x,y) \in \Pi_\mu(S)$. Therefore, there exist $s \in S$ and $s^* \in S^*$ such that $x = ss^*$ and $y = s^*z$. We find all such pairs (s^*, z) and write the list of containers $C(x, s^*z)$ that the pairs yield. This set is the x-family. The union of these containers is the portion of $\Sigma_G(S)$ contributed to the union by $\cup\mathcal{F}(x,S)$. Looking at a list of such containers, we need to determine the containment relationships among them. We can make use of Lemma 3.11 and the principle of inclusion and exclusion to calculate the size of this union.

At this point an example will be useful.

Example 5.1. Taking $G = G(63, 6, 2)$, we see that since $k - 1 = 1$, it is coprime to 63 and, therefore, G has trivial centre. We will construct $\mathrm{P}(G)$ and determine its order. Here a calculation gives

$$R = \{0, \underline{1}, 3, 7, 15, \underline{31}\}$$

and, closing this under multiplication, we have

$$R^* = \{0, \underline{1}, 3, \underline{4}, 6, 7, 9, 12, 15, \underline{16}, 18, 21, 24, 27, 28, 30, \underline{31}, 33, 36, 39, 42, 45, 48, 49, 51, 54, \underline{55}, 57, 60, \underline{61}\},$$

where the invertible elements in R and R^* have been underlined. The values of x for which we wish to check the orbits are in

$$N(R^*) - N(R) = \{6, 9, 12, 18, 21, 24, 27, 28, 30, 33, 36, 39, 42, 45, 48, 49, 51, 54, 57, 60\}.$$

Note that 31 generates the group of invertibles $I(R^*)$; therefore we can multiply repeatedly by 31 to produce each orbit. When we do this, we find three non-basic orbits: $orb_R(9)$, $orb_R(21)$, and $orb_R(42)$. So for each value of $x \in R^* - \{9, 21, 42\}$, the x-family is complete and its contribution to $\mathrm{P}(G)$ is $C(x, 1)$. Each of these maximal containers has order 63.

Next consider the 9-family. Here we wish to find all solutions of the congruence $uv = 9 \pmod{63}$ for $u \in R$ and $v \in N(R^*)$. The modular arithmetic here may be simplified by noting that if we write uv as $9u'v'$, we can reduce $9u'v' = 9 \pmod{9 \cdot 7}$ to $u'v' = 1 \pmod{7}$, yielding

$$\{u', v'\} \in \{\{1, 1\}\, \{2, 4\}, \{3, 5\}, \{6, 6\}\},$$

using multisets, since we can ignore order temporarily, for these pairs. Thus, depending on how the two factors of 3 are distributed between u and v,

$$\{u, v\} \in \{\{1, 9\}, \{3, 3\}, \{18, 4\}, \{6, 12\}, \{2, 36\}, \{27, 5\}, \{9, 15\}, \{3, 45\}, \{54, 6\}, \{18, 18\}\}.$$

Since $u \in R$, we can remove any doubleton with no coordinate in R. This leaves us with

$$\{\{1, 9\}, \{3, 3\}, \{9, 15\}, \{3, 45\}\}.$$

Checking that $v \in N(R^*)$, we see that all four doubletons are solutions. Thus we have

$$(u, v) \in \{(1, 9), (3, 3), (3, 45), (15, 9)\};$$

hence,

$$\mathcal{F}_G(9, R) = \{C(9, 9), C(9, 3), C(9, 45)\}.$$

By Lemma 3.11 and 3.12, we have $C(9, 45) = C(9, 9) \subseteq C(9, 3)$ and therefore, $\cup\mathcal{F}_G(9, R) = C(9, 3)$ and $|\cup\mathcal{F}_G(9, R)| = |C(9, 3)| = 21$.

To find $\cup\mathcal{F}_G(21, R)$, we solve the congruence $uv = 21 \pmod{63}$ $(u \in R, v \in N(R^*))$ by removing 21 to obtain $u'v' = 1 \pmod{3}$. The two solutions, $(1, 1)$ and $(2, 2)$, yield the doubletons $\{\{1, 21\}, \{3, 7\}, \{2, 42\}, \{6, 14\}\}$. Checking the domains, we obtain the solutions of the original congruence, $\{(1, 21), (3, 7), (7, 3)\}$. Thus $\mathcal{F}_G(21, R) = \{C(21, 21), C(21, 7), C(21, 3)\}$. Note, by Lemma 3.12, that $C(21, 21) \subseteq C(21, 3)$ and $C(21, 21) \subseteq C(21, 7)$, but $C(21, 3)$ and $C(21, 7)$ are incomparable. Also $C(21, 21) = C(21, 3) \cap C(21, 7)$; therefore, by the law of inclusion and exclusion,

$$|\mathcal{F}_G(21, R)| = |C(21, 3)| + |C(21, 7)| - |C(21, 21)| = 21 + 9 - 3 = 27.$$

Similarly, we find that $\cup\mathcal{F}_G(42,R) = C(42,3)$ with $|\cup\mathcal{F}_G(42,R)| = 21$. In summary, there are 27 elements of R^* with basic orbits, therefore that portion of $\mathrm{P}(G)$ is $\left(\bigcup_{orb(x,R^*)basic} C(x,1)\right)$ having order $27 \cdot 63 = 1701$. The remainder of $\mathrm{P}(G)$ consists of the unions of the three families calculated. Thus

$$\begin{aligned}\mathrm{P}(G) &= \left(\bigcup_{orb(x,R^*)basic} C(x,1)\right) \cup (\cup\mathcal{F}_G(9,R)) \cup (\cup\mathcal{F}_G(21,R)) \cup (\cup\mathcal{F}_G(42,R))\\ &= \left(\bigcup_{orb(x,R^*)basic} C(x,1)\right) \cup C(9,3) \cup ((C(21,3) \cup C(21,7)) - C(21,21)) \cup C(42,3)\end{aligned}$$

with $|\mathrm{P}(G)| = 1701 + 21 + 27 + 21 = 1770$.

6 Application of the general theory to the commutation semigroups

In this section we will apply the general results obtained in Section 4 to the commutation semigroups $\mathrm{P}(G)$ and $\Lambda(G)$ for $G = G(m,n,k)$ a metacyclic group with trivial centre. Specifically we will investigate situations in which m and n are of, number theoretically, simple form. As mentioned earlier, $m = 63$ is the first value for which non-basic orbits exist. Note that $63 (= 3^2 \cdot 7)$ is of the form $p^2 q$. We will show, in this section, that if m is of the form p or p^2 or if n is prime, then there are no non-basic orbits and the commutation semigroups are complete. Since this can fail when $m = p^2 q$, it would be interesting to study the situation for $m = pq$ and p^3.

Theorem 6.1. *If $G = G(p,n,k)$ with p prime and S is a base, then $\Sigma_G(S)$ is complete.*

Proof. Since p is prime, all non-zero elements of $\mathbb{Z}_p$ are invertible. Thus $N(S^*) = \{0\}$. Since $0 \in S$, we have $N(S^*) - N(S) = \varnothing$, and thus, by Corollary 4.21, it follows that $orb(x,R)$ is basic for each $x \in S^*$. The result follows by Theorem 4.17. □

Theorem 6.1 with Lemma 4.4 imply the following.

Corollary 6.2. *If $G = G(p,n,k)$ with p prime, then $\mathrm{P}(G)$ and $\Lambda(G)$ are complete.* □

Theorem 6.3. *If $G = G(p^2,n,k)$ with p prime, then $\mathrm{P}(G)$ and $\Lambda(G)$ are complete.*

Proof. We will prove the result for $\mathrm{P}(G)$ and comment that the proof for $\Lambda(G)$ is similar. Given $m = p^2$, for some prime p, we claim that either $N(R) = \{0\}$ or $N(R) = \{0, p, 2p, \ldots, (p-1)p\}$. Assuming this has been shown, Corollary 4.21 says it is enough to check that the elements of $N(R^*) - N(R)$ generate basic orbits. If $N(R) = \{0\}$, it is clear that the only non-invertible in the closure of R would be 0 itself. In this case, $N(R^* - R) = \varnothing$, and Corollary 4.21 implies that all orbits are basic. Hence, by Theorem 4.17, $\mathrm{P}(G)$ is complete. If $N(R) = \{0, p, 2p, \ldots, (p-1)p\}$, this is the complete set of non-invertibles in $\mathbb{Z}_{p^2}$ and therefore no new non-invertibles could be generated in R^* when forming their products. Again, Corollary 4.21 assures us that all orbits are basic and Theorem 4.17 yields our conclusion.

It remains to prove the following:

Claim. Either $N(R) = \{0\}$ or $N(R) = \{0, p, 2p, \ldots, (p-1)p\}$.

Proof of Claim. We will suppose that $N(R) \neq \{0\}$ and show that $N(R) = \{0, p, 2p, \ldots, (p-1)p\}$. Note that each of the elements of the form ap $(0 \leq a \leq p-1)$ has a common factor of p with $m (= p^2)$ and, hence, is non-invertible in $\mathbb{Z}_{p^2}$. We are assuming there is a non-zero, non-invertible in R, thus there exists an a $(0 < a \leq p-1)$ and a t $(1 \leq t \leq n-1)$ so that $k^t - 1 = ap \pmod{p^2}$. Note that a is invertible modulo p; thus there is an s $(1 \leq s \leq p-1)$ so that $as = 1 (\mathrm{mod} p)$. Thus there is u $(1 \leq u \leq p-1)$ for which $sa = 1 + up$. If a, s, and u are interpreted as integers modulo p^2, we have $sa = 1 + up \pmod{p^2}$. Since $k^t - 1 = ap \pmod{p^2}$, we have $k^t = ap + 1 \pmod{p^2}$, and thus, $k^{st} = (ap+1)^s \pmod{p^2}$. By the binomial theorem,

$$k^{st} = (ap+1)^s \pmod{p^2} = \begin{pmatrix} s \\ 0 \end{pmatrix} a^s p^s + \begin{pmatrix} s \\ 1 \end{pmatrix} a^{s-1} p^{s-1} + \cdots + \begin{pmatrix} s \\ s-1 \end{pmatrix} ap + 1 \pmod{p^2}.$$

Reducing these terms modulo p^2, we obtain

$$k^{st} = sap + 1 \pmod{p^2} = (1 + up)p + 1 \pmod{p^2} = p + 1 \pmod{p^2}.$$

Therefore, $k^{st} - 1 = p$, and it follows that $p \in R$. If $b \in \mathbb{Z}_{p^2} \cap \{1, 2, \ldots, p-1\}$, we note that $k^{bst} = (p+1)^b \pmod{p^2}$. Again, by the binomial theorem we have

$$k^{bst} = (p+1)^b \pmod{p^2} = bp + 1 \pmod{p^2}$$

and, hence, $bp \in N(R)$. This establishes our claim. □

Next we introduce a technical lemma. Recall that $k_t = k^t - 1$, that k and k_1 are both coprime to m, that $n = ind_m(k)$ and, hence, that $k_n = 0 \pmod{m}$.

Lemma 6.4. *Let $G = G(m, n, k)$ and let p be a prime which divides m. Let s $(1 < s \leq n)$ be minimal so that p divides k_s. Then, for each t $(1 < t \leq n)$, p divides k_t if and only if s divides t.*

Proof. We will first justify the existence of the number s in the statement of the Lemma. Note that since $k_n = 0 \pmod{m}$, we know that p divides k_n. Thus there is a minimal s $(s \leq n)$ for which p divides k_s. Since $(m, k_1) = 1$, p does not divide k_1 and, therefore, $1 < s \leq n$.

($\Rightarrow$) Since $k_s = k_1(1 + k + \ldots + k^{s-1})$ and $k_t = k_1(1 + k + \ldots + k^{t-1})$, and since p does not divide k_1, it divides both $(1 + k + \ldots + k^{s-1})$ and $(1 + k + \ldots + k^{t-1})$. Let q and r be the non-negative integers so that $t = qs + r$ with $0 \leq r < s$. If $r = 0$, then s divides t and we are done. Suppose then that $r > 0$. Then

$$\begin{aligned}
(1 + k + \ldots + k^{t-1}) &= (1 + k + \ldots + k^{s-1}) + (k^s + k^{s+1} + \ldots + \\
&\qquad k^{2s-1}) + (k^{2s} + k^{2s+1} + \ldots + k^{3s-1}) + \ldots + \\
&\qquad (k^{(q-1)s} + k^{(q-1)s+1} + \ldots + k^{qs-1}) + (k^{qs} + k^{qs+1} + \ldots + k^{qs+r-1}) \\
&= (1 + k + \ldots + k^{s-1}) + k^s(1 + k + \ldots + k^{s-1}) + \ldots + \\
&\qquad k^{(q-1)s}(1 + k + \ldots + k^{s-1}) + k^{qs}(1 + k + \ldots + k^{r-1}) \\
&= (1 + k^s + k^{2s} + \ldots + k^{(q-1)s})(1 + k + \ldots + k^{s-1}) + k^{qs}(1 + k + \ldots + k^{r-1}).
\end{aligned}$$

Since p divides $(1 + k + \ldots + k^{s-1})$ and $(1 + k + \ldots + k^{t-1})$, it follows that p must also divide $k^{qs}(1 + k + \ldots + k^{r-1})$. By Lemma 2.1, p does not divide k; therefore it must divide $(1 + k + \ldots + k^{r-1})$ and, hence, p divides $k_r = (k-1)(1 + k + \ldots + k^{r-1})$. But since $r < s$, this contradicts the minimality of s. Thus $r = 0$, and our result follows.

($\Leftarrow$) Now suppose that s divides t $(1 < t \leq n)$ with $t = qs$ for some positive integer q. From a calculation similar to the one above, we derive

$$(1 + k + \ldots + k^{t-1}) = (1 + k + \ldots + k^{qs-1}) = (1 + k^s + k^{2s} + \ldots + k^{(q-1)s})(1 + k + \ldots + k^{s-1}).$$

We next multiply both sides by k_1 :

$$k_1(1+k+\ldots+k^{t-1}) = (1+k^s+k^{2s}+\ldots+k^{(q-1)s})k_1(1+k+\ldots+k^{s-1}).$$

Therefore, $k_t = (1+k^s+k^{2s}+\ldots+k^{(q-1)s})k_s$, and since p divides k_s, it follows that p divides k_i. □

Theorem 6.5. *If $G = G(m,p,k)$ with p prime, then $R^* - \{0\}, L^* - \{0\} \subseteq I(\mathbb{Z}_m)$ and both $\mathrm{P}(G)$ and $\Lambda(G)$ are complete.*

Proof. Suppose p is a prime which divides m. Since $k_n = 0 \pmod m$, we know that k_n must have p as a divisor. Select s minimal so that p divides k_s. We know that $k_1 = k-1$ is coprime to m, thus p does not divide k_1. So $1 < s \leq n$. By Lemma 6.4, it follows that s divides n, but, since n is prime, we have $s = n$. It follows that p is not a divisor of any k_i with $i < n$. This argument applies to each prime dividing m; therefore we can conclude that no prime divisor of m divides k_i with $i < n$. Thus all such k_i are coprime to m and, hence they, and their products, are invertible in $\mathbb{Z}_m$. By Lemma 2.4(i), $0 \in R$, thus 0 is the only non-invertible in R^*, and it follows that $N(R^*) - N(R) = \varnothing$. Then, by Corollary 4.21, all orbits are basic and our result for $\mathrm{P}(G)$ follows from Theorem 4.17. Note that if x is invertible in $\mathbb{Z}_m$ with inverse x^{-1}, then $(-x)(-x^{-1}) = xx^{-1} = 1$. Thus all non-zero elements of L^* are also invertible. So both the left are right commutation semigroups are complete. □

Theorem 6.6. *Any non-abelian pq-group is a metacyclic group with trivial centre and its commutation semigroups are complete.*

Proof. We assume, without loss of generality, that $p > q$. It is easily seen that a non-abelian group of order pq has presentation $G(p,q,k)$. Since p is prime, $(p, k-1) = 1$; thus G has trivial centre. Since $m = p$ is prime, Theorem 6.1 gives our result. □

This result applies to the pq-groups studied by Countryman in [1]. Thus each of the commutation semigroups of a non-abelian pq-group is simply a disjoint union of maximal containers. Each maximal container is of order p and the order of the two commutation semigroups are determined by the sizes of the multiplicative closures of R and L in $\mathbb{Z}_p$. For example, in the pq-group $G(7,2,6)$ we have $R = \{0,5\}$, $R^* = \{0,1,2,3,4,5,6\}$, $L = \{0,2\}$, and $L^* = \{0,1,2,4,\}$. Thus, by Corollary 4.18, we have $\mathrm{P}(G) = \bigcup_{x\in R^*} C(x,1)$ and $\Lambda(G) = \bigcup_{x\in L^*} C(x,1)$ with $|\mathrm{P}(G)| = |R^*|\,7 = 49$, and $|\Lambda(G)| = |L^*|\,7 = 28$.

In [1] (Theorem 2.1) Countryman proves: If G is a non-abelian pq-group (p, q primes), then $\mathrm{P}(G) = \Lambda(G)$ if and only if $|\mathrm{P}(G)| = |\Lambda(G)|$. He also notes that these two conditions are equivalent to $\mathrm{P}(G) \cong \Lambda(G)$. Having developed the theory to this point, we are now able to extend his result.

Theorem 6.7. *If $G = G(p,n,k)$ with p a prime, then the following are equivalent:*

(i) $\mathrm{P}(G) = \Lambda(G)$,

(ii) $\mathrm{P}(G) \cong \Lambda(G)$,

(iii) $|\mathrm{P}(G)| = |\Lambda(G)|$,

(iv) $|R^*| = |L^*|$.

Proof. First note that, by Theorem 6.5, all non-zero elements of R^* and L^* are invertible.

(i) ⇒ *(ii)* and *(ii)* ⇒ *(iii)* are clear.

(iii) ⇒ *(iv)* : By Corollary 6.2, we know that $\mathrm{P}(G)$ and $\Lambda(G)$ are complete. Thus, Corollary 4.18(i) and (ii) imply that $|\mathrm{P}(G)| = |R^*|\,p$ and $|\Lambda(G)| = |L^*|\,p$. By hypothesis (iii), this yields $|R^*| = |L^*|$.

(iv) ⇒ *(i)* : Note that $R^* - \{0\}$ and $L^* - \{0\}$ are subgroups of $\mathbb{Z}_p - \{0\}$ of the same order. Since $\mathbb{Z}_p - \{0\}$ is the multiplicative group of a finite field, it is cyclic, and since both $R^* - \{0\}$ and $L^* - \{0\}$ are subgroups of a cyclic group, they are cyclic. Since cyclic groups have only one subgroup of each possible

order, we conclude that $R^* - \{0\} \overset{\cdot}{=} L^* - \{0\}$. Thus $R^* = L^*$. By Corollary 4.18(i) and (ii) we have $\mathrm{P}(G) = \dot{\bigcup}_{x \in R^*} C(x,1)$ and $\Lambda(G) = \dot{\bigcup}_{x \in L^*} C(x,1)$; therefore, $\mathrm{P}(G) = \Lambda(G)$. □

References

[1] Countryman, James J., *On commutation semigroups of pq groups*, Ph.D. Thesis, University of Notre Dame (1970) pp. 58.

[2] DeWolf, Darien, *Commutation semigroups of dihedral groups of order* $2n$ *where* n *is even*, Honours Thesis, Mount Saint Vincent University (2012) pp. 20.

[3] DeWolf, Darien, Edmunds, Charles C., Levy, Christopher D., *On commutation semigroups of dihedral groups*, Semigroup Forum 87, (2013) pp. 467–488.

[4] Gupta, N.D., *On commutation semigroups of a group*, J. Australian Math. Soc. 6, (1966) pp. 36–45.

[5] Gupta, N.D., *Commutation near-rings of a group*, J. Australian Math. Soc. 7, (1967) pp. 135–140.

[6] Hempel, C.E., *Metacyclic groups*, Communications in Algebra 28 (8), (2000) pp. 3865–3897.

[7] Levy, Christopher D., *Investigation of commutation semigroups of dihedral groups*, Honours Thesis, Mount Saint Vincent University (2009) pp. 26.