Omega Primality and Elasticities of Arithmetic Congruence Monoids

Bruce Zheng

July 30, 2014

1 Introduction

Let $\mathbb{N}$ be the natural numbers $\{1, 2, \dots\}$ and $\mathbb{N}_0 = \{0\} \cup \mathbb{N}$.

A monoid M is a set paired with an associative binary operation and an identity element. One easy example of a monoid is the natural numbers with the binary operation of multiplication and the identity 1.

M is commutative if for every $x, y \in M$ we have $xy = yz$ and commutative if for every $x, y, z \in M$, $xy = xz$ is a necessary and sufficient condition for $y = z$.

In M, we write that x divides y or $x \mid y$ if there exists some $z \in M$ such that $xz = y$. An element u is a unit of M if u divides the identity element of M, usually denoted e. A nonunit x is irreducible, or an atom, if there exist no nonunits that divide x. The set of all atoms of M is denoted $\mathcal{A}(M)$.

If $x = a_1 \cdots a_n$ for $a_i \in \mathcal{A}(M)$, then $a_1 \cdots a_n$ is an atomic factorization of x. If every nonunit of M has an atomic factorization, then M is atomic. In this paper we only consider monoids which are commutative, cancellative, and atomic. Much is known about the atomic factorizations of natural numbers:

Theorem 1.1 (Fundamental Theorem of Arithmetic)**.** *$\mathbb{N}$ is atomic. If $x \in \mathbb{N}$ is greater than 1, then x has a unique atomic factorization up to ordering.*

The uniqueness property of factorizations in $\mathbb{N}$ is not shared in all atomic monoids nor even all submonoids of $\mathbb{N}$. For example, Hilbert famously used the set $\{1+4k : k \in \mathbb{N}_0\}$ as an example of a monoid without unique factorization. In this monoid, we have that 9, 21, 33, and 77 are all irreducible and $9 \cdot 77 = 21 \cdot 33$, so 693 has nonunique factorization.

Note that the Hilbert monoid is closed under multiplication as a consequence of the fact that $1^2 \equiv 1 \bmod 4$. We are interested in a generalization of the Hilbert monoid called arithmetic congruence monoids.

Given $a, b \in \mathbb{N}$ with $0 < a \leq b$ and $a^2 \equiv a \bmod b$, the arithmetic congruence monoid (or ACM) defined by a and b is

$$M(a, b) := \{1\} \cup \{x \in \mathbb{N} : x \equiv a \bmod b\}.$$

$\mathbb{N}$ itself is an ACM with $\mathbb{N} = M(1,1)$. Equivalence relations are often decomposable due to the chinese remainder therorem. For example, $x \equiv 4 \bmod 6$ if and only if $x \equiv 2 \bmod 2$ and $x \equiv 1 \bmod 3$. Hence, $M(4,6) = M(2,2) \cap M(1,3)$. Note here that $2 = \gcd(4,6)$ and $3 = 6/\gcd(4,6)$. This result generalizes to all ACM:

Theorem 1.2. [1, Lemma 4.1] *Let $M(a,b)$ be an ACM. Suppose $d = \gcd(a,b)$ and set $n = b/d$. Then $M(a,b) = M(d,d) \cap M(1,n)$.*

Given a set S with a commutative binary operation, we the free monoid defined on S, $\mathcal{F}(S)$, is the set of all finite unordered sequences of elements of S. Elements of free monoids we call free sequences, and a free sequence $W \in \mathcal{F}(S)$ is written as

$$W = x_1 x_2 \cdots x_n = \prod_{x \in S} x^{v_x(W)} \text{ where } v_x(W) \in \mathbb{N}_0$$

We say $x \in W$ or x is contained in W if $v_x(W) > 0$. The binary operation of $\mathcal{F}(S)$ is concatenation, where for $V = y_1 y_2 \cdots y_m$ we have that $WV = x_1 \cdots x_n y_1 \cdots y_m$. The identity element of $\mathcal{F}(S)$ is then the empty sequence, which we denote $(*)$. The length of W written $|W|$ is n. if V divides W, then V is known to be a subsequence of W, and furthermore a proper subsequence of W if we also have that $|V| < |W|$. We define the natural evaluation map θ from a free sequence W to the product of its elements $\theta(W) \in S$. The sumset of W written $\Sigma(W) \subseteq S$ is defined as

$$\Sigma(W) = \{\theta(V) : V \text{ is a subsequence of } W\}.$$

To make notation unambiguous, we have that the use of parenthesis denotes that the product of set elements is present in the free sequence, whereas a lack of parenthesis denotes each element being present in the free sequence. That is letting $W_1 = (ab)$ and $W_2 = ab$, we have that $|W_1| = 1$ with $ab \in W_1$, and $|W_2| = 2$ with $ab \notin W_2$.

2 Omega primality

A nonunit x of a monoid M is prime if whenever $x \mid yz$ for $y, z \in M$ either $x \mid y$ or $x \mid z$. By Euclid's lemma we have that all atoms of $\mathbb{N}$ are prime in $\mathbb{N}$.

Recall that in $M(1,4)$, we have that $9 \cdot 77 = 21 \cdot 33$. In this case we see that the atom 9, although irreducible, does not divide 21 or 33. This means that 9 is not prime in $M(1,4)$, and that Euclid's lemma does not hold in $M(1,4)$. Suppose however that in $M(1,4)$ we have $9 \mid xyz$. It turns out that either $9 \mid xy$, $9 \mid yz$, or $9 \mid xz$. In this sense 9 very close to being prime. Omega-primality is a way to measure this "closeness".

Let M be a commutative, cancellative, atomic monoid, x an element of M, and W be a free sequence over M. If x divides $\theta(W)$ but x does not divide the evaluation of any proper subsequence of W, then W is a bullet of x. We define the omega-primality of x over M, $\omega_M(x)$ as being the supremum of lengths of all bullets of x. Then, if there is a product with length greater than $\omega_M(x)$ that is divisible by x, there exists a subproduct of length at most $\omega_M(x)$ which is divisible by x.

An element of M is prime if and only if $\omega_M(x) = 1$, and in the case of $M = M(1,4)$ we have that $\omega_M(9) = 2$. In this section our goal is to classify the omega-primality of all ACM. We begin by classifying the omega-primality of the natural numbers:

Proposition 2.1. *Let $x \in N$ and $p_1 \cdots p_m$ be the prime factorization of x. Then $\omega_{\mathbb{N}}(x) = m$.*

Proof. The sequence $p_1 \cdots p_m$ is a bullet of length n for x.

We obtain an upper bound by induction. Since p_1 is prime, $\omega_{\mathbb{N}}(p_1) = 1$. Assume that $\omega_{\mathbb{N}}(p_1 \cdots p_k) \leq k$ for some positive integer $k < m$. We claim that $\omega_{\mathbb{N}}(p_1 \cdots p_{k+1}) \leq k+1$. Let W be a sequence of length greater than $k+1$ whose evaluation is divisible by $p_1 \cdots p_{k+1}$. Then $\theta(W)$ is divisible by $p_1 \cdots p_k$, so there exists a subproduct W_1 of length at most k whose evaluation is divisible by $p_1 \cdots p_k$. Set $W_2 = W/W_1$ so that $W = W_1 W_2$. Since $\theta(W_1)\theta(W_2)$ is divisible by $p_1 \cdots p_{k+1}$, either $p_1 \cdots p_{k+1} \mid \theta(W_1)$ or $p_{k+1} \mid \theta(W_2)$. In the second case, there must exist a subproduct V of W_2 with length 1 and $\theta(V)$ divisible by p_{k+1}. Then $W_1 V$ is a proper subproduct of W with $p_1 \cdots p_{k+1} \mid \theta(W_1 V)$. In both cases, W is not a bullet for $p_1 \cdots p_{k+1}$. Thus any bullet for $p_1 \cdots p_{k+1}$ has a length of at most $k+1$ so $\omega_{\mathbb{N}}(p_1 \cdots p_{k+1}) \leq k+1$, and our claim is satisfied. Therefore $\omega_{\mathbb{N}}(x) \leq m$, and we are done. $\square$

Corollary 2.2. *Let x be a positive integer with prime factorization $p_1 \cdots p_m$ and W be a free sequence over $\mathbb{N}$ with length $r \geq m$ and evaluation divisible by x. For all integers t, $m \leq t \leq r$, there exists a subsequence of W with length t whose evaluation is divisible by x.*

Proof. Since the length of W is greater than $m = \omega_{\mathbb{N}}(x)$, there exists a proper subsequence V_0 of W where $p_1 \cdots p_n \mid \theta(V)$. Furthermore, let $|V_0|$ be minimal. Then V_0 is a bullet for W, meaning that $|V_0| \leq n \leq t$. Now let $V = W/V_0$. V has length $m - |V_0|$, and therefore set $V = V_1 V_2$ for some V_1, V_2, $|V_1| = t - |V_0|$ and $|V_2| = m - t$. $V_0 V_1$ is a subsequence of W of length t. Moreover, $\theta(V_0 V_1) = \theta(V_0)\theta(V_1)$ is divisible by $p_1 \cdots p_m$, so we are done. $\square$

Proposition 2.3. *Let $M = M(d,d) \cap M(1,n)$ be an ACM and $x, y \in M$. Then $x \mid y$ if and only if $dx \mid_{\mathbb{N}} y$.*

Proof. If $x \mid y$, then $y/x \in M$. Then y/x is divisible by d in $\mathbb{N}$, so $y/(dx)$ is a positive integer. Therefore, $dx \mid_{\mathbb{N}} y$. If $dx \mid_{\mathbb{N}} y$, then $y/(dx)$ is a positive integer, and y/x is a positive integer divisible by d. Furthermore, $(x/y) \equiv y(x/y) \equiv x \equiv 1 \bmod n$, so $x/y \in M$. $\square$

As a result of this proposition, division in an ACM is easy in the case where $d = 1$, since it behaves exactly the same as divisibility in $\mathbb{N}$.

For an ACM $M = M(d,d) \cap M(1,n)$ and nonunit $x \in M$ define $r_x \in \mathbb{N}$ as the largest integer divisor of x relatively prime to d and define $s_x = x/r_x$. Furthermore, write $\delta(x)$ as the infimum of all nonnegative integers δ such that $s_x \mid_{\mathbb{N}} d^{\delta(x)}$ and $\gamma(x)$ as the supremum of all integers γ such that $d^{\gamma} \mid_{\mathbb{N}} s_x$.

Lemma 2.4. *Let $M = M(d,d) \cap M(1,n)$ be an ACM with $d > 1$ and x, y be nonunit elements of M.*

1. *$\delta(x)$ and $\gamma(x)$ are positive integers.*
2. *$\delta(dx) = \delta(x) + 1$ and $\gamma(dx) = \gamma(x) + 1$.*
3. *If $\gamma(y) > \delta(x)$ and $r_x \mid_{\mathbb{N}} y$ then $x \mid y$.*
4. *If $\delta(x) > \delta(y) = \gamma(y)$, then $x \nmid y$.*

Proof. (1) Since $d > 1$, and $d \mid_{\mathbb{N}} x$, we have that $s_x \geq d$ and hence $\delta(x) > 0$. 1 divides s_x, so $\gamma(x)$ is also greater than 0. Finally, because s_x is finite there exists some $N \in \mathbb{N}$ such that if $k > N$, $d^k > s_x$, so $\gamma(x) < N < \infty$.

(2) We have that $s_{dx} = ds_x$. Note that for any $k \in \mathbb{N}$ we have that if $ds_x \mid_{\mathbb{N}} d^{k+1}$ then $s_x \mid_{\mathbb{N}} d^k$ and if $d^{k+1} \mid_{\mathbb{N}} ds_x$ then $d^k \mid_{\mathbb{N}} s_x$. Thus $\delta(dx) \geq \delta(x)+1$ and $\gamma(dx) \leq \gamma(x) + 1$. Furthermore $ds_x \mid_{\mathbb{N}} d^{\delta(x)+1}$ and $d^{\gamma(x)+1} \mid_{\mathbb{N}} ds_x$ so $\delta(dx) \leq \delta(x) + 1$ and $\gamma(dx) \geq \gamma(x) + 1$.

(3) Because $\delta(x)$ is less than $\gamma(y)$, s_y/s_x is an integer divisible by d. Furthermore, r_x is relatively prime to s_y so that $r_x \mid_{\mathbb{N}} r_y$. Hence $ds_x r_x \mid_{\mathbb{N}} (s_y/s_x)s_x r_y \mid_{\mathbb{N}} y$, and by Proposition 2.3 $x \mid y$.

(4) Because $\delta(y) = \gamma(y)$, s_y must be a power of d. Therefore $s_x \nmid_{\mathbb{N}} s_y$ and s_x is relatively prime to r_y, so $s_x \nmid_{\mathbb{N}} y$. Thus $x \nmid y$. $\square$

Theorem 2.5. *Let $M = M(d,d) \cap M(1,n)$ be an ACM, $x \in M$, and $x = s_x p_1 \cdots p_m$ where $p_1 \cdots p_m$ is the prime factorization of r_x. Then $\omega(x) = \max(\delta(x) + 1, m)$.*

Proof. Let $\delta = \delta(x)$ and $\mu = \max(\delta + 1, m)$.

Either $\delta = 0$ or $\delta > 0$. If $\delta = 0$, then clearly $\omega(x) \geq 1$. Otherwise suppose that $\delta > 0$. Then $d \neq 1$. Since $dp_1 \cdots p_m$ and d are relatively prime to n, by Dirchlet's Theorem we may choose primes q_1 and q_2 such that $dq_1 p_1 \cdots p_n$ and dq_2 are equivalent to 1 modulo n and q_1, q_2 are relatively prime to x. Note that $dq_1 p_1 \cdots p_n$ and dq_2 are elements of M, and set $W_1 = (dq_1 p_1 \cdots p_m)(dq_2)^{\delta}$. $p_1 \cdots p_m$ divides $\theta(W_1)$ in $\mathbb{N}$, and $\gamma(\theta(W_1)) = \delta + 1 > \delta$, so x divides $\theta(W_1)$ in M by Lemma 2.4 (3).

Let V_1 be a proper subproduct of W_1: then $\gamma(\theta(V_1)) = \delta(\theta(V_1)) \leq \delta$ and $x \neq \theta(V_1)$. Then by Lemma 2.4 (4) x does not divide the evaluation of V_1. Then W_1 is a bullet for x of length $\delta+1$ in the case that $\delta > 0$. Therefore $\omega(x) \geq \delta+1$ always.

Set the integer $y = d^2 p_1 \cdots p_m$. Then y is relatively prime to n, so let z be the smallest positive integer such that $yz \equiv 1 \bmod n$. Then $yz \in M$. For each p_i, set the integer q_i as

$$q_i = \frac{yz}{dp_i} + n = dp_1 \cdots p_{i-1} p_{i+1} \cdots p_n z + n.$$

$dp_i q_i = yz + dnp_i \equiv 1 \bmod n$, so $dp_i q_i \in M$. Then set $W_2 = \prod_{i=1}^{m} (dp_i q_i)$ as a free sequence over M. The evaluation of W_2 is divisible by $p_1 \cdots p_m$ in $\mathbb{N}$. Suppose $m > \delta$. Either $d = 1$ or $\delta(\theta(W_2)) = m > \delta$ so W_2 is divisible by x.

We claim that if $1 \le j \le m$ and $j \ne i$ then p_j does not divide q_i in $\mathbb{N}$. Suppose not: because $p_j \mid_{\mathbb{N}} (yz)/(dp_i)$ then $p_j \mid_{\mathbb{N}} n$, so $\gcd(x, n) > p_j > 1$, a contradiction because $x \in M(1, n)$. Our claim holds. Let V_2 be a proper subproduct of W_2. Then for some $I \subset \{1, \ldots, m\}$, we have that $V_2 = \prod_{i \in I} (dp_i q_i)$. Let j be an element of $\{1, \ldots, m\} \backslash I$: clearly $p_j \nmid_{\mathbb{N}} \prod_{i \in I} (dq_i)$, so $p_1 \cdots p_n \nmid \theta(V_2)$. Then W_2 is a bullet for x of length m when $m > \delta$, so if $m > \delta$, $\omega(x) \ge m$.

Thus far, we have established that $\omega(x) \ge \delta(x) + 1$ and $\omega(x) \ge m$ when $m > \delta$. Thus, $\omega(x) \ge \mu$.

Let U be a free sequence over M with $x \mid \theta(U)$ and $|U| > \mu$. Because $\mu \ge m$, and U is also a free sequence over $\mathbb{N}$, using Corollary 2.2 there exists a subsequence T of U with length μ which is divisible by $p_1 \cdots p_m$ over $\mathbb{N}$. If $d = 1$ then $x \mid \theta(T)$. Otherwise we have that since each element in U is divisible by d, $\gamma(\theta(T)) \ge \mu > \delta$ so $x \mid \theta(T)$. U is not a bullet for x. Therefore $\omega(x) \le \mu$. □

3 Elasticities

3.1 Preliminary Results

We now investigate the lengths of atomic factorizations of ACM. Many results in this subsection are stated without proof; a friendly introduction to factorization lengths in ACM may be found in [3]. [1] and [2] contain a more careful exposition of preliminary results.

In Hilbert's monoid $M(1, 4)$, it is clear that factorization is nonunique. However, factorizations for a fixed element in Hilbert's monoid are always the same length: for example the nonunique factorzations of $693 = 9 \cdot 77 = 21 \cdot 33$ are both products of length 2.

On the other hand in $M(4, 6)$ we have factorizations that do differ in length. For example, we have that $10000 = 10^4 = 250 \cdot 10 \cdot 4$. There does exist a bound on the possible ratio between lengths of factorizations: given a fixed element x, if there exists a factorization of length k for x, then there does not exist a factorization of length $2k$ or greater for x.

We may also consider the case of $M(6, 6)$ which has even more wild behavior than $M(4, 6)$. In $M(6, 6)$, for any $k > 2$ we have that $6^k = (2^{k-1} \cdot 3) \cdot (2 \cdot 3^{k-1})$, so there exists no bound on the ratio of lengths of factorizations.

Let M be an atomic monoid and let x be a nonunit of M. The set of lengths of x is

$$\mathcal{L}(x) = \{k \in \mathbb{N} : x = a_1 \cdots a_k \text{ where } a_i \in \mathcal{A}(M)\}.$$

Then let $L(x) = \sup(\mathcal{L}(x))$ and $l(x) = \min(\mathcal{L}(x))$. We define $\rho(x)$ to be $L(x)/l(x)$ to be elasticity of x. Furthermore $\rho(M) = \sup\{\rho(x) : x \in M, x \nmid e\}$ is the elasticity of M.

It turns out that $\rho(M(1,4)) = 1$, $\rho(M(4,6)) = 2$, and $\rho(M(6,6)) = \infty$. This variance of behavior in elasticities of ACM is largely determined by the greatest common divisor of the two integers a and b of $M(a,b)$.

Let $M = M(a,b)$ be an ACM and let $d = \gcd(a,b)$. If $d = 1$, then $a = 1$ (by Theorem 1.2) and M is called regular. If M is not regular, then M is singular. We classify singular ACM further based on the prime factorization of d. If d is a power of a prime, then M is local. Otherwise, M is global. $M(1,4)$ is regular, $M(4,6)$ is local, and $M(6,6)$ is global.

Theorem 3.1. *Let $M = M(a,b)$ be an ACM.*

1. *If M is regular, then $\rho(M) = 1$.*
2. *If M is local, then with $\gcd(a,b) = p^\alpha$ for a prime p and $p^\beta \in M$ for minimal β, we have that $\rho(M) = (\alpha + \beta - 1)/\alpha$.*
3. *If M is global, then $\rho(M) = \infty$.*

The elasticity of M is accepted if there exists an x such that $\rho(x) = \rho(M)$. We see that if M is a regular ACM, the elasticity of M is always accepted. On the other hand, if M is a global ACM the elasticity is never accepted: the length of the factorization of x in M cannot be infinite since its factorization in $\mathbb{N}$ is finite.

However, if M is a local ACM in general we do not really know when the elasticity of M is accepted or not. Some partial results for this problem are found in [4] and [5].

3.2 ρ_k of Local ACM

We may consider accepted elasticities in the larger context of unions of length sets: define $\rho_k(M) = \sup\{L(x) : k \in \mathcal{L}(x)\}$. $\rho(M)$ is accepted if and only if $\rho_k(M) = k\rho(M)$ for some k. Our goal for the rest of this section is to investigate the behavior of ρ_k in local ACM and find cases where the elasticity of a local ACM is not accepted.

Let M be a local ACM, so that $\gcd(a,b) = p^\alpha$ for a prime p. Then, $a = p^\alpha \xi$ and $b = p^\alpha n$ for some integers ξ and n, and ξ is uniquely determined by n. Then we may write $M(a,b) = M(p,\alpha,n)$.

We begin with some observations on the structure of atoms:

Proposition 3.2. *Let $M = M(p, \alpha, n)$ and set β to be the order of p modulo n. Let q be a prime distinct from p and m be a positive integer not divisible by p. Then*

1. *If $p^t m$ is reducible, then $t \geq 2\alpha$.*
2. *If $\alpha \leq t < 2\alpha$ and $p^t m \equiv 1 \bmod n$, then $p^t m$ is an atom of M.*
3. *p^β is the smallest power of p found in M, and an atom.*
4. *If $\beta < t < \beta + \alpha$ and $p^t q \equiv 1 \bmod n$, then $p^t q$ is an atom of M.*
5. *If $\beta + \alpha \leq t$, then $p^t m$ is not an atom of M.*

Proof. p^α divides any element of M over the natural numbers, thus any reducible element must be divisible by $p^{2\alpha}$ over the natural numbers. Hence (1) and (2) follow.

Because β is the order of p modulo n, we must have that $p^\beta \equiv 1 \bmod M$. Then p^β is the smallest power of p found in M, and irreducibility immediately follows, giving us (3).

We prove (4) by contradiction. Suppose that $p^t q$ is not an atom, so there is a nonunit divisor of $p^t q$. Since q is a prime, any factorization of $p^t q$ into two nonunits will be of the form $p^r \cdot p^{t-r} q$ for $r \leq t$. Since $p^r \in M$, we must have by (3) that $r \geq \beta$. But the $t - r < \alpha$, so $p^\alpha \nmid_{\mathbb{N}} p^{t-r} q$. Hence $p^{t-r} q \notin M$, giving us the contradiction.

Finally we have that $p^\beta p^\alpha \mid_{\mathbb{N}} p^t m$, so by Proposition 2.3 $p^\beta \mid p^t m$, from which (5) follows. □

We introduce our first result, which gives us a lower bound on ρ_k:

Theorem 3.3. *Let $M = M(p, \alpha, n)$ be a local ACM and k be an integer greater than 1. Set β to be the order of p modulo n. Then*

$$\rho_k(M) \geq \left\lfloor \frac{(k-1)(\beta-1)-1}{\alpha} \right\rfloor + k + 1.$$

Proof. Using the division algorithm, let m and r be positive integers such that $m\alpha + r = (k-1)\beta + 2\alpha - 1$ where r is at most α. Then, by Dirchlet's Theorem, there exist primes q_1, q_2, q_3, q_4 distinct from p such that

$$q_1 \equiv p^{-\beta-\alpha+1} \quad q_2 \equiv p^{\beta-1} \quad q_3 \equiv p^{-\alpha} \quad q_4 \equiv p^{-\alpha-r} \bmod n.$$

We immediately see that $u_1 = p^{\beta+\alpha-1} q_1$, $v_1 = p^\alpha q_1 q_2$, $v_2 = p^\alpha q_3$, and $v_3 = p^{\alpha+r} q_4$ are atoms of M. We also claim that the integer $u_2 = p^{2\alpha-1} q_2^{k-1} q_3^{m-1} q_4$ is also an atom in M. It suffices to show that $u_2 \equiv 1 \bmod n$. Note that

$$(2\alpha-1) + (k-1)(\beta-1) + (m-1)(-\alpha) + (-\alpha-r) =$$
$$(2\alpha-1) + (k-1)(\beta-1) - (k-1)(\beta-1) - (2\alpha-1) = 0$$

hence

$$u_2 \equiv p^{2\alpha-1}q_2^{k-1}q_3^{m-1}q_4 \equiv p^{2\alpha-1}p^{(k-1)(\beta-1)}p^{(m-1)(-\alpha)}p^{-\alpha-r} \equiv p^0 \equiv 1 \bmod n$$

so $u_2 \in \mathcal{A}(M)$. Then set

$$x = u_1^{k-1}u_2 = p^{(k-1)(\beta+\alpha-1)+(2\alpha-1)}q_1^{k-1}q_2^{k-1}q_3^{m-1}q_4 = v_1^{k-1}v_2^{m-1}v_3.$$

Therefore $x \in M$, and $k, m+k-1 \in \mathcal{L}(x)$. Thus, $\rho_k(M) \geq \max(\mathcal{L}(x)) \geq m+k-1$. Moreover, we have that

$$m+k-1 = \left\lfloor \frac{(k-1)\beta + 2\alpha - 1}{\alpha} \right\rfloor + k - 1 = \left\lfloor \frac{(k-1)\beta - 1}{\alpha} \right\rfloor + k + 1,$$

from which we immediately obtain our result. □

3.3 $M(p,1,n)$

We now shift our focus to ACM of the form $M = M(p,1,n)$, which greatly simplifies the structure of factorizations of M. First, letting β be defined as in the previous Theorem, we now have that $\rho(M) = \beta$. Furthermore if the elasticity of M is accepted, we must have some $x \in M$ such that

$$x = p^\beta w_1 \cdots p^\beta w_k = pv_1 \cdots pv_{k\beta}.$$

Additionally, for any atom of the form $p^\beta m$ we must have that $m \equiv 1 \bmod n$.

Let M and N be commutative, cancellative, atomic monoids. A map $\sigma : M \to N$ is a transfer homomorphism if:

1. For $x \in M$, $\sigma(x)$ is a unit of N if and only if x is a unit of M.
2. For every $a \in N$, there exists a unit u of N and $x \in M$ such that $\sigma(x) = au$.
3. Whenever $x \in M$ and $a, b \in N$ such that $\sigma(x) = ab$, there exist some $y, z \in M$ and units $u, v \in N$ such that $x = yz$, $\sigma(y) = ua$, and $\sigma(z) = vb$.

If a $\sigma : M \to N$ is a transfer homomorphism, then for any $x \in M$ we have that $\mathcal{L}(x) = \mathcal{L}(\sigma(x))$. Thus, instead of $\rho(M)$ or $\rho_k(M)$ we may equivalently consider $\rho(N)$ and $\rho_k(N)$.

Let G be a finite abelian group with element g. The submonoid $T(g,G)$ of $(\mathbb{N},+) \times \mathcal{F}(G)$ is defined to be

$$T(g,G) = \{(0,*)\} \cup \{(t,W) \in \mathbb{N} \times \mathcal{F}(G) : t > 1 \text{ and } \theta(W) = g^t\}.$$

Proposition 3.4. *Let $M(p,1,n)$ be a local ACM. The map*

$$\sigma : M(p,1,n) \to T([p], \mathbb{Z}_n^\times)$$

defined by

$$\sigma(1) = (0,*), \quad \sigma(x) = (t, [q_1]^{-1} \cdots [q_m]^{-1})$$

where $x = p^t q_1 \cdots q_m$ for $q_i \neq p$, is a transfer homomorphism.

Proof. We have that 1 is the only unit of $M(p,1,n)$ and $(0,*)$ is the only unit of $T([p],\mathbb{Z}_n^\times)$. We have by definition that $\sigma(1)=(0,*)$. If x is not a unit, then $t>0$ and $\sigma(x)$ is not a unit. Then σ satisfies conditions (1) and (2) of the definition of a transfer homomorphism.

Suppose that $(t,[a_1]\cdots[a_m])\in T([p],\mathbb{Z}_n^\times)$. Then by Dirchlet's Theorem there exist primes $q_1,\dots,q_m$ not equal to p such that $[q_1]=[a_1]^{-1}$. Furthermore we must have $[q_1]\cdots[q_m]=[p]^{-t}$ so that $p^tq_1\cdots q_m\in M(p,1,n)$. Furthermore, $\sigma(p^tq_1\cdots q_m)=(t,[a_1]\cdots[a_m])$, so σ satsifies (3).

Finally, suppose that $x\in M(1,p,n)$ and that a,$b\in T([p],\mathbb{Z}_n^\times)$. Write x as $p^tq_1\cdots q_m$. Then $\sigma(x)=(t,[q_1]^{-1}\cdots[q_m]^{-1})$. Without loss of generality we have that $a=(r,[q_1]^{-1}\cdots[q_k]^{-1})$ and that $b=(t-r,[q_{k+1}]^{-1}\cdots[q_m]^{-1})$ for some integers r and k. Then setting $y=p^rq_1\cdots q_k$ and $z=p^{t-r}q_{k+1}\cdots q_m$ we have that $y,z\in M(1,p,n)$ and that $x=yz$. Therefore σ satisfies (4). $\square$

It is not surprising that $T(g,G)$ have many of the same properties as ACM of the form $M(p,1,n)$. Notably, $\rho(T(g,G))=o(g)$. It is then appropriate to focus on accepted elasticities of $T(g,G)$ and $\rho_k(T(g,G))$ even though it is easy to construct some $T(g,G)$ for which there is not a transfer homomorphism from some $M(p,1,n)$ to $T(g,G)$.

We summarize the remainder of the section. First, we present a closed form solution for $\rho_k(T(g,G))$ when $\langle g\rangle=G$. Next, we give several positive conditions for when $\rho_k(T(g,G))=ko(g)$. Finally, we obtain a lower bound for the size of $G/\langle g\rangle$ for $\rho(T(g,G))$ to not be accepted.

Lemma 3.5. *Let g be an element of a finite abelian group G, (t,W) be an element of $T(g,G)$.*

1. *If $t>o(g)$, then (t,W) is not irreducible.*
2. *If $t\le o(g)$, then (t,W) is irreducible if and only if*

$$\Sigma(W)\cap\{g,g^2,\dots,g^{t-1}\}=\varnothing.$$

Proof. (1) The empty sequence $*$ evaluates to $e=g^{o(g)}$. Then $(o(g),*)$ is a nontrivial divisor of (t,W).

(2) Suppose that (t,W) is not an atom. Then there exists a nontrivial divisor (r,V) of (t,W). Furthermore, $r<t$ and V is a subsequence of W with $\theta(V)$ is g^r. Then $g^r\in\{g,g^2,\dots,g^{t-1}\}$ and $g^r\in\Sigma(W)$.

Suppose that $g^r\in\Sigma(W)\cap\{g,g^2,\dots,g^{t-1}\}$. Then there exists a subsequence V of W with $\theta(V)=g^r$. Then (r,V) is a nontrivial divisor of (t,W). $\square$

Lemma 3.6. *Let V_1 and V_2 be elements of $\mathcal{F}(G)$ and $U_1\cdots U_k\mid V_1V_2$ with $U_i\neq *$. If $\theta(U_i)$ is not in the sumset of V_2 for all i, then $k\le|V_1|$.*

Proof. Suppose that $k>|V_1|$. Since $U_1\cdots U_k\mid V_1V_2$, we have that $U_1\cdots U_k=A_1B_1\cdots A_kB_k$ where $U_i=A_iB_i$, $A_i\mid V_1$, and $B_i\mid V_2$ for all i. Then, $A_1\cdots A_k\mid$

V_1. However, $k > |V_1|$, so for some j, $A_j = *$. Then $B_j = U_j$ and $U_j \mid V_2$, so $\theta(U_j)$ is found in the sumset of V_2, and we have a contradiction. $\square$

The following theorem applies for $T([p], \mathbb{Z}_n^\times)$ when p is a primitive root modulo n.

Theorem 3.7. *Let $G = \langle g \rangle$ be a finite abelian group and k be an integer greater than 1. Then $\rho_k(T(g, G)) = (k-1)o(g) + 1$.*

Proof. The elements $(o(g), *)$, $(1, (g)^{(k-1)o(g)+1})$ are irreducible, with

$$(o(g), *)^{k-1}(1, (g)^{(k-1)o(g)+1}) = (1, g)^{(k-1)o(g)+1}.$$

Hence $\rho_k(T(g, G)) \geq (k-1)o(g) + 1$. We introduce a claim to aid construction of an upper bound on ρ_k.

Claim. If (t, W) is an atom in $T(g, G)$ with $t > o(g)/2$, the number of nonidentity group elements in W is at most $o(g) - t$.

Proof of claim. Suppose not. Let V be the largest subsequence of W that does not contain e. Then $V = (g^{n_1})(g^{n_2}) \cdots (g^{n_l})$ with $0 < n_i < o(g)$ and $l > o(g) - t$. Since (t, W) is irreducible, by Lemma 3.5 (2) each n_i is at least t and any subsequence of V cannot have an evaluation of $g_1, \ldots, g_{t-1}$. Now consider the set

$$\{\theta(g^{n_1}), \theta(g^{n_1}g^{n_2}), \ldots, \theta(g^{n_1} \cdots g^{n_l})\} \subseteq \{g^t, \ldots, g^{o(g)}\},$$

and note that $|\{g^t, \ldots, g^{o(g)}\}| = o(g) - t + 1$. $l \geq o(g) - t + 1$ hence there exists some j and i between 1 and l where $\theta([g^{n_1}] \cdots [g^{n_i}]) = \theta([g^{n_1}] \cdots [g^{n_j}])$. Then the sequence $[g^{n_{i+1}}][g^{n_{i+1}}] \cdots [g^{n_j}]$ is zero-sum. The evaluation of $[g^{n_{i+2}}] \cdots [g^{n_j}]$ is $g^{o(g)-n_{i+1}}$, and $t > o(g)/2$ so $0 < o(g) - n_{i+1} < t$. This is also a subsequence of W, meaning (t, W) is not irreducible. Contradiction, therefore $|W| < o(g) - t$.

We now show that $\rho_k(T(g, G)) \leq (k-1)o(g) + 1$ by contradiction. Suppose that there exists an element $(t, W) \in T(g, G)$ which has an atomic factorization of length k and an atomic factorization of length $m > (k-1)o(g) + 1$. t is at most $ko(g)$, and m must be at most t. Then $(t, W) = (t_1, W_1) \cdots (t_k, W_k) = (r_1, V_1) \cdots (r_m, V_m)$ for atoms (t_i, W_i) and (r_m, V_m). Without loss of generality, we may assume that $[e]$ is not a subsequence of W and that t_i, r_j are ordered in descending order.

Because $m \leq ko(g) - r_j$, $r_j < o(g)$. Since $\sum_{i=1}^k t_i = t > (k-1)o(g) + 1$, all t_i for $i \neq k$ must be greater than $o(g)/2$ and $t_k > 1$. Suppose that $t_k > o(g)/2$. Then by our claim we have that $|W| = |W_1 \cdots W_k| < \sum_i^k (o(g) - t_i) < o(g) - 1$. Furthermore, $|V_1 \cdots V_m| = |W|$, so for some j we have that $V_j = *$. But $(r_j, *)$ is not an atom, so we must have that $t_k \leq o(g)/2$.

Let n be some positive integer such that $r_j \geq t_k$ for all $j \leq n$. Then g^{r_j} is not in the sumset of W_k for $j > n$, and

$$(k-1)o(g) + 1 < m \leq t_k n + (m - n) \leq \sum_{i=1}^m r_i \leq t \leq ko(g),$$

so $(t_k - 1)n < o(g) - 1$, and

$$m - n > (k-1)o(g) + 1 - (o(g)-1)/(t_k - 1) > o(g) + 1 - \frac{o(g)-1}{t_k - 1} \geq 2.$$

$V_{n+1} \cdots V_m$ divides W. Furthermore, no V_j can be the empty sequence since (r_j, V_j) is an atom, and all $\theta(V_j)$ are not found in the sumset of W_k for $n+1 \leq j \leq m$. From our claim, $|W_1 \cdots W_{k-1}| < \sum_i^{k-1}(o(g)-t_i) = (k-1)o(g)-t+t_k \leq t_k - 2$. Hence, $m - n < t_k$. If $t_k < 3$ then $2 < m - n < t_k - 2 < 1$, which is a contradiction. On the other hand, if $t_k \geq 3$,

$$m - n > o(g) + 1 - \frac{o(g)-1}{2} > \frac{o(g)}{2} > \frac{o(g)}{2} - 2 \geq t_k - 2 > m - n$$

which creates another contradiction. Hence, we always arrive at a contradiction if we let $\rho_k(T(g,G)) > (k-1)o(g) + 1$, so $\rho_k(T(g,G)) \leq (k-1)o(g) + 1$. □

When g does not generate G, the elasticities of $\rho_k(T(g,G))$ are not nearly as well known. To aid in our investigation we introduce the concept of H-sum subsequences:

Suppose that H is a subgroup of G. Then, since H is closed over its subgroup elements, free sequences which evaluate to members of H will naturally form a submonoid of $\mathcal{F}(G)$. These free sequences are known as H-sum sequences. An H-sum sequence is a minimal it has no proper H-sum subsequences. In the case where H is the trivial group, we may instead use the term zero-sum sequence instead.

There is a relationship between minimal H-sum sequences of $\mathcal{F}(G)$ and minimal zero-sum sequences of $\mathcal{F}(G/H)$. Namely, if $(a_1H)\cdots(a_mH)$ is a minimal zero-sum sequence if and only if for any $h_1, \ldots, h_m \in H$ we have that $(h_1a_1)\cdots(h_ma_m)$ is a minimal H-sum sequence. The proof of this property may be found in [5, Propositions 5.2, 5.3].

Before continuing, we introduce three invariants. Let G be a finite abelian group. We may rewrite $G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_m}$. Let $d^*(G)$ be defined as $\sum_{i=1}^m (n_i - 1)$. We define the Davenport constant $D(G)$ to be the length of the longest minimal zero-sum sequence of $\mathcal{F}(G)$. Finally define the exponent of G written $\exp(G) = n_m$, which is also the largest possible order of an element of G.

The following result is a corollary of [5, Theorem 4.5]. The original Theorem applies to local ACM, not necessarily of the form $M(p,1,n)$, but we have adapted the construction of atomic factorizations to that of $T(g,G)$:

Proposition 3.8. *Let G be a finite abelian group where $G \cong \langle g \rangle \times H$ for an element g and subgroup H of G, and k be an integer greater than 1. If $(k-1)d^*(H) \geq k(o(g)-1)$, then $\rho_k(T(g,G)) = ko(g)$.*

Proof. Let $d = d^*(H)$. Since H is finite and abelian, we have that $H \simeq \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_m}$ for some $n_1 \mid n_2 \mid \cdots \mid n_m$. Thus, $H = \langle h_1 \rangle \times \cdots \times \langle h_n \rangle$ for some $h_1, \ldots, h_n \in H$ with $o(h_i) = n_i$.

Let $W_1 = \prod_{i=1}^m (gh_i)^{n_i-1}(g^{-1}h_i^{-1})^{n_i-1}$ and $W_2 = \prod_{i=1}^m (h_i^{-1})^{(2k-2)n_i}$ be zero-sum sequences of G. Then $\Sigma(W_1) \cap \langle g \rangle = \Sigma(W_2) \cap \langle g \rangle = \{e\}$, so $(o(g), W_1)$ and $(o(g), W_2)$ are atoms of $T(g, G)$. Furthermore, let $kd - d = q(o(g) - 1) + r$ with $0 \leq r \leq o(g) - 1$ by the division algorithm.

If $1 \leq i \leq kd - d$, define t_i to be the unique integer such that

$$(k-1)\sum_{j=1}^{t_i-1}(n_j - 1) < i \leq (k-1)\sum_{s=1}^{t_i}(n_j - 1)$$

. If $1 \leq i \leq q$, define s_i to be equal to $(i-1)(o(g)-1)$. Now define sequences $U_1, \ldots, U_{kd-d}$ and $V_1, \ldots, V_q$ where

$$U_i = (gh_{t_i})h_{t_i}^{-1}, \quad V_i = \prod_{j=s_i+1}^{s_{i+1}} (g^{-1}h_{t_j})h_{t_j}^{-1} \text{ for } i < q, \quad V_q = \prod_{j=s_q+1}^{kd-d} (g^{-1}h_{t_j})h_{t_j}^{-1}$$

Now define $U_{kd-d+1}, \ldots, U_{kd-d+q}$ as $U_{kd-d+i} = V_i$ for $1 \leq i \leq q$. Then we have that

$$W_1^{k-1}W_2 = U_1 \cdots U_{kd-d+q} \prod_{i=1}^m (h_i^{-1})^{2k-2}.$$

We have that $\theta(U_i) = g$ for $1 \leq i \leq kd - d$ and $\theta(U_j) = g^{-o(g)+1} = g$ for $kd - d + 1 \leq j \leq kd - d + q$. Suppose that $kd - d + q \geq ko(g)$. Then let $U = U_{ko(g)} \cdots \prod_{i=1}^m (h_i^{-1})^{2k-2}$, so $W_1^{k-1}W_2 = U_1 \cdots U_{ko(g)-1}U$. Since W_1 and W_2 are zero-sum sequences,

$$e = \theta(W_1^{k-1}W_2) = \theta(U_1)\cdots\theta(U_{ko(g)-1})\theta(U) = g^{ko(g)-1}\theta(U) = g^{-1}\theta(U)$$

from which $\theta(U) = g$ follows. Therefore, $(1, U_1), \ldots, (1, U_{ko(g)-1}), (1, U)$ are all atoms in $T(g, G)$. Then consider the element $x = (ko(g), W_1^{k-1}W_2)$ with atomic factorizations

$$x = (o(g), W_1)^{k-1}(o(g), W_2),$$
$$x = (1, U_1)\cdots(1, U_{ko(g)-1})(1, U),$$

which are of length k and $ko(g)$ respectively.

Thus, if $kd - d + q \geq ko(g)$, then $\rho_k(T(g, G)) = ko(g)$. Moreover, we have that $kd - d + q = \lfloor (k-1)o(g)d/(o(g)-1) \rfloor$. $ko(g)$ is an integer hence $kd - d + q \geq ko(g)$ if and only if $(k-1)o(g)d/(o(g)-1) \geq ko(g)$, which occurs if and only if $(k-1)d \geq k(o(g)-1)$. Then if $(k-1)d \geq k(o(g)-1)$, we have $\rho_k(T(g, G)) = ko(g)$. □

This proposition is also a corollary of a previous result, specifically that of [5, Proposition 4.10].

Proposition 3.9. *Let $\langle g \rangle \times H \cong G$ for $g \in G$ and $H \leq G$ and let k be an integer greater than 1. If $o(g) \mid \exp(H)$, then $\rho_k(M) = ko(g)$.*

Proof. Let $h \in H$ such that $o(h) = \exp(H)$. $(gh)^{k\exp(H)}$ and $(h^{-1})^{k\exp(H)}$ are zero-sum sequences; we claim that both sequences have no nonidentity powers of g in their sumsets. All subsequences of $(gh)^{k\exp(H)}$ are of the form $(gh)^n$ for some integer n between 0 and $k\exp(h)$. Suppose that $(gh)^n$ is a $\langle g\rangle$-sum subsequence. Then, since $\langle g\rangle \cap H = \{e\}$ and $g^n h^n \in \langle g\rangle$, $h^n = e$. Hence n is divisible by $\exp(H)$ and therefore divisible by the order of g. Then $g^n h^n = e$ hence $\Sigma((gn)^{k\exp(H)}) \cap \langle g\rangle = \{e\}$. Since sumset of $(h^{-1})^{k\exp(H)}$ is a subset of H, $\Sigma((h^{-1})^{k\exp(H)}) \cap \langle g\rangle = \{e\}$. Our claim holds thus $(\exp(g), (gh)^{k\exp(H)})$ and $(\exp(g), (h^{-1})^{k\exp(H)})$ are atoms of $T(g, G)$.

Set $x = (ko(g), (gh)^{k\exp(H)}(h^{-1})^{k\exp(H)})$:

$$x = (o(g), *)^{k-2}(o(g), (gh)^{k\exp(H)})(o(g), (h^{-1})^{k\exp(H)}),$$
$$x = (1, (gh)h^{-1})^{ko(g)-1}\big(1, (gh)^{k(\exp(H)-o(g))+1}(h^{-1})^{k(\exp(H)-o(g))+1}\big)$$

are two atomic factorizations of x with lengths k and $ko(g)$ respectively. Then $\rho_k(T(g, G)) \geq ko(g)$ and $\rho_k(T(g, G)) = ko(g)$. □

Proposition 3.10. *Let g be an element of a finite abelian group G and let $D(G/\langle g\rangle) \geq ko(g)$. Then $\rho_k(T(g, G)) = ko(g)$.*

Proof. Let $ko(g) = m$, $d = D(G/\langle g\rangle)$, and $h_1\langle g\rangle \cdots h_d\langle g\rangle$ be a minimal zero-sum sequence of $\mathcal{F}(G/\langle g\rangle)$. Then $h_1 \cdots h_d$ is a minimal $\langle g\rangle$-sum sequence with evaluation g^n for some integer n.

Let $U_1 = h_1 \cdots h_m$, $U_2 = h_{m+1} \cdots h_{d-1}(g^{-n}h_d)$, $V_1 = (gh_1^{-1}) \cdots (gh_m^{-1})$ and $V_2 = h_{m+1}^{-1} \cdots h_{d-1}^{-1}(g^n h_d^{-1})$; we see that U_1U_2 and V_1V_2 are minimal $\langle g\rangle$-sum sequences with $\theta(U_1U_2) = \theta(V_1V_2) = \theta(U_2V_2) = e$. Let $x = (m, U_1U_2V_1V_2)$. Then

$$x = (o(g), *)^{k-2}(o(g), U_1U_2)(o(g), V_1V_2)$$
$$x = (1, h_1(gh_1^{-1})) \cdots (1, h_{m-1}(gh_{m-1}^{-1}))(1, h_m(gh_m^{-1})U_2V_2)$$

are two atomic factorizations of x of length k and length m respectively. Then $\rho_k(T(g, G)) = ko(g)$. □

Lemma 3.11. *Let g be an element of a finite abelian group G, and k be a positive integer. If $\rho_k(T(g, G)) = ko(g)$, then there exist $a_{i,j} \in G$ for $1 \leq i \leq k$ and $1 \leq j \leq ko(g)$ such that for each i, $(o(g), a_{i,1} \cdots a_{i,ko(g)})$ is an atom of $T(g, G)$ and for each j, $a_{1,j} \cdots a_{k,j} = e$.*

Proof. If $\rho_k(T(g, G)) = ko(g)$, then there exist free sequences $W_1, \ldots, W_k$ and $V_1, \ldots, V_{ko(g)}$ such that

$$(o(g), W_1) \cdots (o(g), W_k) = (1, V_1) \cdots (1, V_{ko(G)})$$

with each $(o(g), W_i)$ and $(1, V_j)$ atoms of $T(g, G)$. Then each W_i is a minimal zero-sum sequence and each V_j evaluates to g. Furthermore, we have that there exist $A_{i,j}$ for $1 \leq i \leq k$ and $1 \leq j \leq ko(g)$. □

The main result of [4] gives us an exact condition for when the elasticity of $M = M(p, \alpha, n)$ is accepted for p primitve modulo n, but if p is not primitive very little is known about when the elasticity is not accepted. Our last result shows that given a fixed order of g, there is a bound on the cardinality of G such that below that bound the elasticity of $T(g, G)$ cannot be accepted. This sheds some light on the conditions for having $\rho(M(p, 1, n))$ not be accepted.

First we make some observations on the structure of W for atoms of the form $(o(g), W) \in T(g, G)$.

Lemma 3.12. *Let G be a finite abelian group with subgroup H, and W a zero-sum sequence of G such that $\Sigma(W) \cap H = e$. Set ψ as the natural homomorphism G to G/H and the map $\phi : \mathcal{F}(G) \to \mathcal{F}(G/H)$ given by $\phi(g_1 \cdots g_m) = \psi(g_1) \cdots \psi(g_m)$.*

1. *ϕ forms a bijection between zero-sum subsequences of W and zero-sum subsequences of $\phi(W)$.*
2. *Let $aH \in \phi(W)$. If there exists a zero-sum subsequence V of $\phi(W)$ where $0 < v_{aH}(V) < v_{aH}(\phi(W))$, then there is a unique $h \in H$ where (ah) is contained in W.*

Proof. Let $\phi(W) = a_1H \cdots a_mH$ and $W = (a_1h_1) \cdots (a_mh_m)$.

(1) Note that $\psi(\theta(X)) = \theta(\phi(X))$. Then X is a zero-sum subsequence if of W and only if $\phi(X)$ is zero-sum subsequence of $\phi(W)$.

We show that ϕ is surjective: Let V be a zero-sum subsequence of $\phi(W)$. Because free sequences are invariant under arrangement of terms, without loss of generality we may assume $V = a_1H \cdots a_nH$ for $n \leq m$. Then $(a_1h_1) \cdots (a_nh_n)$ is a subsequence of W with $\phi((a_1h_1) \cdots (a_nh_n)) = V$.

We show that ϕ is injective: Let X_1, X_2 be zero-sum subsequences of W such that $\phi(X_1) = \phi(X_2) = V$, a subsequence of $\phi(W)$. Without loss of generality let $V = a_1H \cdots a_nH$. Then for $b_1, \ldots, b_n, c_1, \ldots, c_n \in H$ we may write $X_1 = (a_1b_1) \cdots (a_nb_n)$ and $X_2 = (a_1c_1) \cdots (a_nc_n)$. Suppose that $X_1 \neq X_2$, seeking a contradiction: $b_j \neq c_j$ for some positive $j \leq n$, thus

$$\theta((a_1b_1) \cdots (a_{j-1}b_{j-1})(a_jc_j)(a_{j+1}b_{j+1}) \cdots (a_nb_n)) = c_jb_j^{-1} \in \Sigma(W) \cap H.$$

However $c_jb_j^{-1} \neq e$ which is the contradiction. Therefore $X_1 = X_2$.

(2) Let $t = v_{aH}(V)$ and $n = v_{aH}(\phi(W))$. Then without loss of generality we may assume that $a_1H, a_2H, \ldots, a_nH$ are all equal to aH. Then we may rewrite $W = (ah_1) \cdots (ah_n)(a_{n+1}h_{n+1}) \cdots (a_mh_m)$. For some $I \subseteq \{n+1, \ldots, m\}$ we have that $\phi\left((ah_1) \cdots (ah_t) \prod_{i \in I}(a_ih_i)\right) = V$. Let $X = \prod_{i \in I}(a_ih_i)$.

To complete the proof it suffices to show that for $i, j \in \{1, \ldots, n\}$, $h_i = h_j$. Without loss of generality we may assume $j \geq i$. If $1 \leq i \leq t$ and $t + 1 \leq j \leq n$ then

$$\phi((ah_1) \cdots (ah_r)X) = \sigma((ah_1) \cdots (ah_{i-1})(ah_j)(ah_{i+1}) \cdots (ah_r)X) = V,$$

and because V is a zero-sum sequence, from (1) $h_i = h_j$. If i and j are both at most t, then we have that $g_i = g_n = g_j$. If i and j both greater than t, then $g_i = g_1 = g_j$. Therefore $g_i = g_j$. $\square$

Theorem 3.13. *Let G be a finite abelian group and g an element of G. If $o(g) > \sum_{a\in G} o(a\langle g\rangle)$, then the elasticity of $T(g,G)$ is not accepted.*

Proof. For a free sequence $W = g_1 \cdots g_m$ over G, we introduce the function $f(W,n)$ where $f(W,n) = |\{i : 1 \leq i \leq m, g_i^n \neq e\}|$. That is, $f(W,n)$ counts the elements in W which have orders that do not divide n.

Claim. If the elasticity of $T(g,G)$ is accepted and $n < o(g)$, then there exists an irreducible $(o(g),W)$ such that $f(W,n) \geq o(g)$.

Proof of claim. Recall that for $g_1, g_2 \in G$, $\mathrm{lcm}(o(g_1), o(g_2)) \geq o(g_1 g_2)$. Thus if U is a free sequence with evaluation g then $f(U,n) \geq 1$. Furthermore, for free sequences U_1 and U_2, clearly $f(U_1U_2,n) = f(U_1,n) + f(U_2,n)$. Because the elasticity of $T(g,G)$ is accepted, there exist atoms $(o(g),W_1),\ldots,(o(g),W_k)$ and $(1,V_1),\ldots,(1,V_{ko(g)})$ where

$$(o(g),W_1)\cdots(o(g),W_k) = (1,V_1)\cdots(1,V_{ko(g)}).$$

Since $\theta(V_j) = g$, we infer that $u(V_j,n) \geq 1$. Then

$$\sum_{i=1}^{k} f(W_i,n) = \sum_{j=1}^{ko(g)} f(V_j,n) \geq ko(g).$$

By the pigeonhole principle there must exist some W_i such that $f(W_i,n) \geq o(g)$. The claim holds.

Now we continue on to the main statement, which we approach by a proof by contradiction. Suppose that the elasticity of $T(g,G)$ is accepted. Then let $\epsilon = \exp(G/\langle g\rangle)$. From our claim there exists an atom $(o(g),W)$ such that $f(W,\epsilon) \geq o(g)$. Then $\Sigma(W) \cap \langle g\rangle = \{e\}$, so we may define ϕ and ψ as in Lemma 3.12 letting $H = \langle g\rangle$.

Let S be the set of all $g \in G$ where $g^\epsilon \neq e$.

$$\sum_{g\in S} v_{\psi(g)}(\phi(W)) \geq \sum_{g\in S} v_g(W) = f(W,\epsilon) > \sum_{a\in G} o(a\langle g\rangle)$$

hence by a pigeonhole argument there exists some $a\langle g\rangle \in \psi(S)$ such that $v_{a\langle g\rangle}(\phi(W)) > o(a\langle g\rangle)$. Moreover $(a\langle g\rangle)^{o(a\langle g\rangle)}$ is a zero-sum sequence, so by Lemma 3.12 (2) there exists a unique $g_0 \in \langle g\rangle$ such that (ag_0) is contained in W. Then $(ag_0)^{o(a\langle g\rangle)}$ is a zero-sum subsequence of W, and so $(ag_0)^\epsilon = e$. However, $a\langle g\rangle \in \psi(S)$ so $ag_0 \in S$, meaning that $(ag_0)^\epsilon \neq e$, thus creating the contradiction. $\square$

References

[1] P. Baginski and S. T. Chapman, *Arithmetic Congruence Monoids: A Survey.*

[2] M. Banister, J. Chaika, S. T. Chapman, and W. Meyerson, *On the Arithmetic of Arithmetical Congruence Monoids.*

[3] S. T. Chapman, *A Tale of Two Monoids: A Friendly Introduction to Nonunique Factorizations*, Mathematics Magazine **87:3** (June 2014).

[4] M. Banister, J. Chaika, S. T. Chapman, and W. Meyerson, *A theorem on accepted elasticity in certain local arithmetical congruence monoids.*

[5] L. Crawford, V. Ponomarenko, J. Steinberg, and M. Williams, *Accepted Elasticity in Local Arithmetic Congruence Monoids.*