The Δ-set of a singular ACM

Trinity University REU in Algebra
George J. Schaeffer[1]
July 28th, 2006

We consider $\Delta(M)$ for M a singular arithmetic congruence monoid. This set is fully characterized when $a = 0$ and when $\gcd(a, b) = p^\alpha$ for p a rational prime and $\alpha > 0$. Finally, we show that the Δ-set of any singular ACM is finite and we develop theory towards the computation of $\Delta(M)$ in the nonprimary case.

$\mathbb{N}$ will denote the positive integers and $\mathbb{N}_0$ will denote the nonnegative integers. $\mathbb{P}$ will denote the set of (positive) rational primes, and for any $x \in \mathbb{N}$, $\mathbb{P}(x)$ will denote the set of rational primes which divide x. If $S \subseteq \mathbb{N}$, then $\overline{S}$ will denote the multiplicative closure of S in $(\mathbb{N}, \times)$. Intervals will be always be treated as subsets of $\mathbb{Z}$.

1 Introduction

For any $m > 0$ the set

$$H_m = \{x \in \mathbb{N} : x \equiv 1 \bmod m\} = 1 + m\mathbb{N}_0.$$

is a monoid under the usual multiplication operation. Monoids of this form are called *Hilbert monoids* after David Hilbert.

Hilbert monoids generalize to a broader class of submonoids of $(\mathbb{N}, \times)$: Let $b \in \mathbb{N}$ and choose a satisfying $0 < a \leq b$ and $a^2 \equiv a \bmod b$. The *arithmetic congruence monoid* (ACM) determined by the choice of a, b is defined as

$$M_{a,b} = \{x \in \mathbb{N} : x = 1 \text{ or } x \equiv a \bmod b\} = (a + b\mathbb{N}_0) \cup \{1\}$$

under multiplication. Essentially, an arithmetic congruence monoid is the smallest submonoid of $(\mathbb{N}, \times)$ which contains some arithmetic progression $\{a + kb : k \in \mathbb{N}\}$.

If M is any submonoid of $(\mathbb{N}, \times)$, 1 is the unique unit of M. Thus, we may call $x \in M$ *irreducible* iff $x = yz$ for $y, z \in M$ implies $y = 1$ or $z = 1$;

[1]Carnegie Mellon University, Dept. of Mathematical Sciences, Pittsburgh, PA 15213.
The author was supported by the National Science Foundation, Grant #DMS-0353488.

the set of all irreducible elements of M will be denoted $\mathcal{A}(M)$. Since $(\mathbb{N}, \times)$ is atomic, any such M is also atomic, in the sense that every $x \in M$ can be written as a product of finitely many elements of $\mathcal{A}(M)$. In $(\mathbb{N}, \times)$, such factorizations are of course unique, but this is not the case when dealing with ACMs:

Example 1.1 Consider $M_{2,2} = (2\mathbb{N}) \cup \{1\}$. A positive integer x is irreducible in M iff $2 \mid x$ but $4 \nmid x$; hence $6, 18, 54 \in \mathcal{A}(M_{2,2})$. Now

$$324 = (18)^2 = (6)(54)$$

so we see that a given element of $M_{2,2}$ need not have a unique factorization into irreducible elements. (We say in such a case that M is not *factorial*.)

In general the situation is even worse. For instance, it can be shown that $4, 10, 250 \in \mathcal{A}(M_{4,6})$, but $1000 = (4)(250) = (10)^3$. Thus, we are not even guaranteed that all factorizations of a given element are of the same length. (That is, $M_{4,6}$ is not *half-factorial*.)

Our purpose is to determine, to some extent, how badly unique factorization fails in $M_{a,b}$. If $x \in M$ where M is any monoid, we set

$$\mathcal{L}(x) = \{l \in \mathbb{N}_0 : \text{there exist } x_1, \ldots, x_l \in \mathcal{A}(M) \text{ such that } x = x_1 \cdots x_l\}.$$

Order $\mathcal{L}(x) = \{l_1 < \cdots < l_j\}$ and define

$$\Delta(x) = \{l_{i+1} - l_i : i \in [1, j)\}.$$

Finally, define $\Delta(M) = \bigcup_{x \in M} \Delta(x)$; this is the Δ-*set* of the monoid M. We wish to characterize $\Delta(M)$ when M is an arithmetic congruence monoid.

Determining the Δ-set of a given monoid is no simple task. For instance, the Hilbert monoid H_m (which is Krull) has the same factorization properties as the block monoid on $(\mathbb{Z}/m\mathbb{Z})^\times$ (see [5]); little can be said about the Δ-set of a block monoid on an arbitrary finite abelian group (unless it is cyclic, for example). It is known, however, that the Δ-set of a Hilbert monoid is always finite [3].

The Δ-set of a numerical monoid (an additive submonoid of $\mathbb{N}_0^k$) has been analyzed rigorously in [2]. We will show eventually that an arithmetic congruence monoid is a submonoid of a finite-dimensional numerical monoid. However, if $N \leq M$ there need not be any mathematical relationship between

$\Delta(M)$ and $\Delta(N)$: Of course, $\Delta(\mathbb{N}, \times) = \varnothing$, but there are submonoids M of $(\mathbb{N}, \times)$ which have $|\Delta(M)| = k$ for every $k \in \mathbb{N}_0$.

Many important factorization properties of ACMs have already been investigated: In particular, questions of factoriality, half-factoriality, and elasticity are covered extensively in [1]. Most relevant to our discussion will be the following result of Banister et al.:

Theorem 1.2 *Let $M_{a,b}$ be an arithmetic congruence monoid.*

1. *$\Delta(M_{a,b}) = \varnothing$ (that is, $M_{a,b}$ is half-factorial) iff either*
   a. *$M_{a,b} = H_m$ where $\varphi(m) \leq 2$, or*
   b. *$a \equiv p \bmod b$, where p is a rational prime dividing b.*
2. *If $\Delta(M_{a,b}) \neq \varnothing$, then $1 \in \Delta(M_{a,b})$.*

2 Basic structure theory of ACMs

Since an arithmetical congruence monoid is determined by the choice of a, b, it is logical to begin our discussion with a characterization of the idempotent residues modulo b. In particular, we will show that there is a bijection between the idempotents of $\mathbb{Z}/b\mathbb{Z}$ and the power set of $\mathbb{P}(b)$.

Lemma 2.1 *Factor $b = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ and let a be an integer, $0 < a \leq b$ and a idempotent modulo b. Then there exists $S \subseteq [1, n]$ such that*

$$\gcd(a, b) = \prod_{i \in S} p_i^{\alpha_i}.$$

Conversely, for any $S \subseteq [1, n]$ there exists a unique a, $0 < a \leq b$ and a idempotent modulo b, which satisfies the above.

Proof. Let $0 < a \leq b$ and $a^2 \equiv a \bmod b$ so that $b \mid a(a-1)$. Since a and $a-1$ are relatively prime we can write $a = ux$ and $a - 1 = vy$ where $b = uv$ and $\gcd(u, v) = 1$; we infer that $u = \prod_{i \in S} p_i^{\alpha_i}$ for some $S \subseteq [1, n]$. Moreover, $\gcd(x, v) = 1$, so $\gcd(a, b) = \gcd(ux, uv) = u$, as desired.

For the converse take $S \subseteq [1, n]$, $u = \prod_{i \in S} p_i^{\alpha_i}$, and $v = b/u$. Then $\gcd(u, v) = 1$ so the Diophantine equation $ux - vy = 1$ has exactly one solution (x, y) modulo b. Observe that

$$(ux)^2 = ux(1 + vy) = ux + bxy \equiv ux \bmod b$$

so choosing a satisfying $0 < a \leq b$ and $a \equiv ux \bmod b$, we see that a is the unique such value which satisfies $a^2 \equiv a \bmod b$ and $\gcd(a, b) = u$. $\square$

Set $d = \gcd(a, b)$ and $m = b/d$. By arguments above,

$$\gcd(a, m) = \gcd(b, m) = \gcd(d, m) = 1.$$

We infer that a is an idempotent unit modulo m so $a \equiv 1 \bmod m$. This provides the following invaluable membership criterion for $M_{a,b}$:

Lemma 2.2 *$x \in M_{a,b}$ iff $x = 1$ or $d \mid_{\mathbb{N}} x$ and $x \equiv 1 \bmod m$. That is to say,*

$$M_{a,b} = (d\mathbb{N} \cap H_m) \cup \{1\}.$$

Proof. We will assume $x > 1$. Suppose that $d \mid_{\mathbb{N}} x$ and $x \equiv 1 \bmod m$. By the Chinese remainder theorem there exists a unique residue class modulo b which satisfies both these conditions. We infer that $x \equiv a \bmod b$ and so $x \in M_{a,b}$. The argument for the converse is similar. $\square$

The group $(\mathbb{Z}/m\mathbb{Z})^\times$ is actually the class group of $M_{a,b}$; we will often denote it by $\mathrm{Cl}(M_{a,b})$. Note also that if $x \in M_{a,b}$ is nonunit and $p \mid x$ is prime, $p \in \mathbb{P} \setminus \mathbb{P}(m)$, so $\mathbb{P}(d) \subseteq \mathbb{P}(x) \subset \mathbb{P} \setminus \mathbb{P}(m)$.

Corollary 2.3 *Let $x, y \in M_{a,b}$ be such that $x, y \neq 1$ and $y \mid_{\mathbb{N}} x$.*

- *If $d \mid_{\mathbb{N}} (x/y)$, then $x/y \in M_{a,b}$.*
- *If $x \in \mathcal{A}(M_{a,b})$, then $y \in \mathcal{A}(M_{a,b})$.*

Proof. For the first claim it is enough to note that $x \equiv y \equiv 1 \bmod m$ so that $x/y \equiv 1 \bmod m$.

For the second claim, suppose that y is reducible and z is an irreducible factor of y. We know that $y/z \in M_{a,b}$ and moreover $(x)(y/z) \in M_{a,b}$. Since $d \mid_{\mathbb{N}} (y/z)$ and $y \mid x$, $d \mid_{\mathbb{N}} (x/z)$. Observing that $(y)(x/z) \in M_{a,b}$ we infer by the first claim that $x/z \in M_{a,b}$, so x is reducible. $\square$

The value of d plays a rather important role in characterizing $\Delta(M)$ when M is an ACM. It is natural to deal with three separate cases:

- M is *regular*: $d = 1$.
- M is *primary*: $d = p^\alpha$ for p a rational prime and $\alpha > 0$.

- M is *nonprimary*: d has at least two distinct prime factors.

As M is a Krull monoid in the regular case and the factorization properties of Krull monoids have been extensively studied (see [3]), we will limit ourselves to the latter two cases wherein M is a *singular* ACM. The primary and nonprimary cases differ substantially: While we are able to obtain a bound on $\Delta(M)$ in the nonprimary case without much trouble, we can actually fully characterize the Δ-set of a primary ACM.

3 The Δ-set of a primary ACM

Throughout this section, M will denote a primary ACM with $d = p^\alpha$ for $p \in \mathbb{P}$ and $\alpha > 0$. By Lemma 2.1 $\gcd(p, m) = 1$ so in addition to fixing p, α we will let ω be the order of p modulo m. Take $\beta \geq \alpha$ to be least such that $p^\beta \equiv 1 \bmod m$. By the membership criterion, p^β is the smallest power of p which is an element of M, and of course, $p^\beta \in \mathcal{A}(M)$.

The main theorem of this section is the following:

Theorem 3.1 *Let M be a primary ACM.*

- *If $\alpha = \beta = 1$, $\Delta(M) = \varnothing$.*
- *If $\alpha = \beta > 1$, then $\Delta(M) = \{1\}$.*
- *If $\alpha < \beta$, then $\Delta(M) = [1, \beta/\alpha)$.*

The first of these results is an immediate consequence of Theorem 1.2: Observe that when $\alpha = \beta$, $p \in M_{a,b}$. Since a is minimal among the nonunits of M and $p \mid a$, it follows that $a = p$, so a is a prime divisor of b.

It is natural in the primary case to classify elements of the ACM by their p-adic values. We write $x \in \mathcal{H}_\gamma$ iff $x \in M$ and $v_p(x) = \gamma$; furthermore, we denote the intersection $\mathcal{H}_\gamma \cap \mathcal{A}(M)$ by $\mathcal{A}_\gamma$. Note that if $x \in M$ and $v_p(x) < 2\alpha$, x is irreducible. Similarly, if $v_p(x) \geq \alpha + \beta$, x is reducible:

$$x = p^{\alpha+\beta} y = (p^\beta)(p^\alpha y),$$

where $p^\beta \in M$ by hypothesis and $p^\alpha y \in M$ by Corollary 2.3. Hence, if $x \in \mathcal{A}(M)$, $v_p(x) \in [\alpha, \alpha + \beta)$.

Lemma 3.2 *The set $\mathcal{A}_\gamma$ is infinite if $\gamma \in [\alpha, \alpha+\beta)$ and is empty otherwise.*

Proof. The latter claim follows from the fact that $x \in M$ implies $v_p(x) \geq \alpha$ and the earlier argument that $v_p(x) \geq \alpha+\beta$ implies that x is a reducible element of M.

Suppose then that $\gamma \in [\alpha, \alpha+\beta)$ and let $q \neq p$ be a rational prime such that $q \equiv p^{-\gamma} \bmod m$ so that $p^\gamma q \in M$. We claim that $p^\gamma q \in \mathcal{A}(M)$: write $p^\gamma q = (p^s)(p^t q)$ where $s, t > 0$ and $s+t = \gamma$.

- If $p^s \not\equiv 1 \bmod m$, then $p^s \notin M$.
- Assume that $p^s \equiv 1 \bmod m$. Since $\beta \geq \alpha$ was chosen minimal such that $p^\beta \in M$, either $s < \alpha$ (and so $p^s \notin M$) or $s \geq \beta$. The latter implies $t < \alpha$ because $\gamma < \alpha+\beta$ and therefore $p^t q \notin M$.

We may therefore infer that $p^\gamma q$ is irreducible in M. The infinitude of such irreducibles now follows from Dirichlet's theorem. □

3.1 Bounding $\Delta(M)$ in the primary case

Let $\mathbf{F}$ be the set of all nonnegative integral vectors indexed by the interval $[\alpha, \alpha+\beta)$. For $\mathbf{f} \in \mathbf{F}$ write

$$x \in \mathcal{A}^{\mathbf{f}} = \mathcal{A}_\alpha^{f_\alpha} \cdots \mathcal{A}_{\alpha+\beta-1}^{f_{\alpha+\beta-1}}$$

iff x has a factorization into $|\mathbf{f}| = f_\alpha + \cdots + f_{\alpha+\beta-1}$ irreducibles of M such that f_γ of these factors have p-adic value γ. We say in this case that $\mathbf{f}$ is a *factorization scheme for* x; $\mathbf{F}(x)$ will denote the set of all such schemes. We will write $\mathbf{f}' \leq \mathbf{f}$ iff $f'_\gamma \leq f_\gamma$ for all $\gamma \in [\alpha, \alpha+\beta)$.

For $\mathbf{f} \in \mathbf{F}(x)$ define $r(\mathbf{f}) = \beta|\mathbf{f}| - v_p(x)$. Note that

$$r(\mathbf{f}) = \sum_{i=1-\alpha}^{\beta-\alpha} i f_{\beta-i}.$$

Since r can be expressed in this way, we immediately derive the following:

Lemma 3.3 *Let $\mathbf{f} \in \mathbf{F}(x)$.*

- *If $r(\mathbf{f}) \leq R \leq 0$ there is $\mathbf{f}' \leq \mathbf{f}$ such that $r(\mathbf{f}') \in [R-\alpha+1, R]$.*
- *Similarly, if $r(\mathbf{f}) \geq R \geq 0$ there is $\mathbf{f}' \leq \mathbf{f}$ such that $r(\mathbf{f}') \in [R, R-\alpha+\beta]$.*

The above lemma is crucial in that it affords us very tight bounds on the values taken by r.

Lemma 3.4 *Fix $x \in M$, $\mathbf{f} \in \mathbf{F}(x)$, and suppose that $r(\mathbf{f}) \leq -\alpha$. Then $|\mathbf{f}| + 1 \in \mathcal{L}(x)$.*

Proof. By Lemma 3.3, there exists $\mathbf{f}' \leq \mathbf{f}$ such that $r(\mathbf{f}) \in [1 - 2\alpha, -\alpha]$. Since $-r(\mathbf{f}') \geq \alpha$, there is a factorization rule

$$\mathcal{A}^{\mathbf{f}'} \subseteq (p^{\beta})^{|\mathbf{f}'|}\mathcal{H}_{-r(\mathbf{f}')}$$

which is obtained by extracting $|\mathbf{f}'|$ copies of p^{β}. As $-r(\mathbf{f}') < 2\alpha$, we know that $\mathcal{H}_{-r(\mathbf{f}')} = \mathcal{A}_{-r(\mathbf{f}')}$, so the right factorization has exactly $|\mathbf{f}'| + 1$ factors. This suffices to prove the claim because $\mathcal{A}^{\mathbf{f}} \subseteq \mathcal{A}^{\mathbf{f}'}\mathcal{A}^{\mathbf{f}-\mathbf{f}'}$. $\square$

Corollary 3.5 *If $\alpha = \beta > 1$, then $\Delta(M) = \{1\}$.*

Proof. Let $x \in M$ be a nonunit; since M is not half-factorial, we may take x such that $\Delta(x) \neq \varnothing$. Suppose that $\mathbf{f} \in \mathbf{F}(x)$ with $r(\mathbf{f}) > -\alpha$. By the definition of r and the fact that $\alpha = \beta$ we see that $r(\mathbf{f})$ satisfies

$$\frac{v_p(x)}{\alpha} < |\mathbf{f}| + 1.$$

Since $l \leq v_p(x)/\alpha$ for all $l \in \mathcal{L}(x)$, it follows that $|\mathbf{f}| = \max \mathcal{L}(x)$. Let $\mathbf{g} \in \mathbf{F}(x)$ such that $|\mathbf{g}| = \min \mathcal{L}(x)$. Since $\min \mathcal{L}(x) \neq \max \mathcal{L}(x)$, $r(\mathbf{g}) \leq -\alpha$, so applying Lemma 3.4 iteratively to $\mathbf{g}$, we find

$$\mathcal{L}(x) = \{\min \mathcal{L}(x), \min \mathcal{L}(x) + 1, \min \mathcal{L}(x) + 2, \ldots, \max \mathcal{L}(x)\}$$

whence $\Delta(x) = \{1\}$. As x was arbitrary among elements with nonempty Δ-set, $\Delta(M) = \{1\}$. $\square$

Lemma 3.6 *Let M be a primary ACM with $\alpha < \beta$. Fix $x \in M$, $\mathbf{f} \in \mathbf{F}(x)$, and suppose that*

$$r(\mathbf{f}) \geq K = \frac{2\alpha + \beta(\beta - \alpha) - 1}{\alpha}.$$

Then $|\mathbf{f}| - k \in \mathcal{L}(x)$ where $0 < k < \beta/\alpha$.

Proof. Note that $K \geq 1$. By Lemma 3.3 there exists $\mathbf{f}' \leq \mathbf{f}$ with $r(\mathbf{f}') \in [K, K-\alpha+\beta]$. For the remainder of the proof we will abbreviate $r = r(\mathbf{f}')$.

Fix bounds $J_1 = (\alpha + r)/\beta$ and $J_2 = r/(\beta - \alpha)$. We have

$$J_2 - J_1 = \frac{\alpha r}{\beta(\beta-\alpha)} - \frac{\alpha}{\beta} \geq K \geq 1.$$

so $[J_1, J_2)$ is nonempty; let $q \in [J_1, J_2)$. Note that

$$0 < q < J_2 = \frac{r}{\beta - \alpha} \leq |\mathbf{f}'|.$$

and because $q \geq J_1$, $q\beta - r \geq \alpha$. Thus, we have a factorization rule

$$\mathcal{A}^{\mathbf{f}'} \subseteq (p^\beta)^{|\mathbf{f}'|-q}\mathcal{H}_{q\beta-r}.$$

A factorization scheme on the right has at most

$$|\mathbf{f}'| - q + \frac{q\beta - r}{\alpha} < |\mathbf{f}'| + \frac{\beta-\alpha}{\alpha}J_2 - \frac{r}{\alpha} = |\mathbf{f}'|.$$

terms, so for $k > 0$, let $|\mathbf{f}'| - k$ be the length of some factorization in $(p^\beta)^{|\mathbf{f}'|-q}\mathcal{H}_{q\beta-r}$. We have

$$\begin{aligned} k \leq q - \frac{q\beta - r}{\alpha+\beta-1} &\leq \left(\frac{r}{\beta-\alpha}\right)\left(\frac{\alpha-1}{\alpha+\beta-1}\right) + \frac{r}{\alpha+\beta-1} \\ &= \frac{(\beta-1)}{\beta(\beta-1)-\alpha(\alpha-1)}r. \end{aligned}$$

Since $r \leq K - \alpha + \beta$,

$$k \leq \frac{(\beta-1)(\beta-\alpha+1)}{\alpha(\beta-\alpha)} < \beta/\alpha$$

So $|\mathbf{f}| - k \in \mathcal{L}(x)$ with $0 < k < \beta/\alpha$, as claimed. □

Theorem 3.7 *If M is a primary ACM and $\alpha < \beta$, $\Delta(M)$ is nonempty and finite with $\max \Delta(M) < \beta/\alpha$.*

Proof. $\Delta(M)$ is nonempty since $\beta > 1$. Let K be defined as in Lemma 3.6 and fix $x \in M$. Since the values of r on $\mathbf{F}(x)$ depend only on $v_p(x)$ and

the length of a given factorization, we will treat r as a function on $\mathcal{L}(x)$. Partition $\mathcal{L}(x) = \mathcal{L}_+(x) \cup \mathcal{L}_0(x) \cup \mathcal{L}_-(x)$ where

$$\mathcal{L}_+(x) = \{l \in \mathcal{L}(x) : r(l) \geq K\} = \left\{ l \in \mathcal{L}(x) : l \geq \frac{v_p(x) + K}{\beta} \right\}, \text{ and}$$
$$\mathcal{L}_-(x) = \{l \in \mathcal{L}(x) : r(l) \leq -\alpha\} = \left\{ l \in \mathcal{L}(x) : l \leq \frac{v_p(x) - \alpha}{\beta} \right\}.$$

This partition is monotonic in the sense that if $\mathcal{L}(x) = \{l_1 < \cdots < l_n\}$, and $l_i \in \mathcal{L}_-(x)$ then $l_j \in \mathcal{L}_-(x)$ for all $j \leq i$; similarly if $l_i \in \mathcal{L}_+(x)$ then $l_j \in \mathcal{L}_+(x)$ for all $j \geq i$.

Let $\Delta_-(x) = \{l_{j+1} - l_j : l_j \in \mathcal{L}_-(x)\}$; by Lemma 3.4 $\Delta_-(x)$ is either empty or equal to $\{1\}$. Similarly, let $\Delta_+(x) = \{l_{j+1} - l_j : l_{j+1} \in \mathcal{L}_+(x)\}$ and note that by Lemma 3.6 $\Delta_+(x)$ is either empty or $\max \Delta_+(x) < \beta/\alpha$.

It remains only to bound $\Delta_0(x) = \{l_{j+1} - l_j : l_j, l_{j+1} \in \mathcal{L}_-(x)\}$ since

$$\Delta(x) = \Delta_-(x) \cup \Delta_0(x) \cup \Delta_+(x).$$

Let $l, l' \in \mathcal{L}_0(x)$ and observe that

$$|l - l'| = \frac{|r(l) - r(l)'|}{\beta} \leq \frac{(K - 1/\alpha) + (\alpha - 1)}{\beta} = \frac{\alpha^2 - \alpha\beta + \beta^2 - 2}{\alpha\beta} < \beta/\alpha$$

and thus we may infer that $\max \Delta(M) < \beta/\alpha$. $\square$

3.2 Identity of $\Delta(M)$ in the primary case

In the previous section we proved that if M is a primary ACM with $\alpha = \beta$ then $\Delta(M) = \varnothing$ or $\Delta(M) = \{1\}$ (depending on whether $\alpha = \beta = 1$ or $\alpha = \beta > 1$, respectively). Moreover, we showed that $\Delta(M)$ is finite where M is a primary ACM. It remains then to prove only the last claim of Theorem 3.1, which we will now attempt. Throughout this section we will assume that $\alpha < \beta$.

Lemma 3.8 *If $\beta = \omega$ then $[1, \delta] \subseteq \Delta(M)$ where $\delta = \lceil \beta/\alpha \rceil - 1$.*

Proof. Let $\gamma \in [\alpha, \beta)$ and choose rational primes q, r such that $q \equiv p^{-\alpha} \mod m$ and $r \equiv p^{-\gamma} \mod m$. Set

$$t = \left\lceil \frac{\beta - \gamma}{\alpha} \right\rceil + 1,$$

so that $\alpha t - \beta + \gamma \in [\alpha, 2\alpha)$. Consider $x = p^{\alpha t+\gamma} q^t r$ and note that $x \in M$. Furthermore, we have irreducible factorizations

$$x = (p^\alpha q)^t (p^\gamma r) = (p^\beta)(p^{\alpha t-\beta+\gamma} q^t r)$$

which are of lenghts $t+1$ and 2, respectively.

Suppose that y is an irreducible factor of x in M and write $y = p^v q^i r^j$ where $i \in [0, t]$ and $j \in [0, 1]$. Since $y \equiv 1 \bmod m$ and β is the order of p modulo m by hypothesis we must also have $v \equiv i\alpha + j\gamma \bmod \beta$. From this we infer the following:

- If $i = j = 0$, then $v = \beta$ and $y = p^\beta$.
- If $i = 0$ and $j = 1$, then $v = \gamma$ and $y = p^\gamma r$.
- If $i > 0$ then $v < 2\alpha$; otherwise $p^\alpha q$ is an irreducible factor of y in M.

Assume that $i > 0$ so that $v \in [\alpha, 2\alpha)$. Let S be the set of residue classes $[\alpha, 2\alpha) + \beta\mathbb{Z}$ and note that we must have $\alpha i + \gamma j + \beta\mathbb{Z} \in S$. We have two cases:

- If $j = 0$, then $\alpha i + \beta\mathbb{Z} \in S$, so either $i = 1$ or $\alpha i \geq \alpha + \beta$. In the latter case, we see that since $i \leq t$, $\alpha t \geq \alpha + \beta$, but this contradicts the choice of t, as then $\alpha t - \beta + \gamma \geq 2\alpha$.
- If on the other hand $j = 1$, then $\alpha i + \gamma + \beta\mathbb{Z} \in S$. Since $\gamma \geq \alpha$, we have $\alpha i + \gamma \geq \alpha + \beta$, and it follows that $i \geq \frac{1}{\alpha}(\beta - \gamma) + 1$, whence $i = t$ by the choice of t.

Combining all of these arguments the irreducible divisors of x in M are precisely p^β, $p^\gamma r$, $p^\alpha q$, and $p^{\alpha t-\beta+\gamma} q^t r$. Since $v_q(x) = t$ and $v_r(x) = 1$, the last of these irreducibles can only appear with p^β. Hence $(p^\alpha q)^t (p^\gamma r)$ and $(p^\beta)(p^{\alpha t-\beta+\gamma} q^t r)$ are the only factorizations of x in M and so $\Delta(x) = \{t-1\}$.

We conclude that

$$\left\{ \left\lceil \frac{\beta - \gamma}{\alpha} \right\rceil : \gamma \in [\alpha, \beta) \right\} \subseteq \Delta(M),$$

but the set on the left-hand side is exactly $[1, \delta]$, as desired. $\square$

Lemma 3.9 *If $\beta \geq 2\alpha - 1$ then $\beta = \omega$.*

Proof. Set $\beta = k\omega$. By the minimality of $\beta \geq \alpha$, $(k-1)\omega \leq \alpha - 1$. Combining this with the assumed bound on β,

$$\omega = k\omega - (k-1)\omega \geq (2\alpha - 1) - (\alpha - 1) = \alpha$$

so that $\beta = \omega$. $\square$

Theorem 3.10 *If $\alpha < \beta$ then $\Delta(M) = [1, \beta/\alpha)$.*

Proof. Let $\delta = \lceil \beta/\alpha \rceil - 1$ so that $[1, \delta] = [1, \beta/\alpha)$. By Theorem 3.7, $\Delta(M) \subseteq [1, \delta]$. If $\beta = \omega$, then $[1, \delta] \subseteq \Delta(M)$ by Lemma 3.8.

If on the other hand $\beta \neq \omega$, we see that $\beta \leq 2(\alpha - 1)$ by Lemma 3.9, so $\delta = 1$. Because $\Delta(M)$ is nonempty (as $1 \leq \alpha < \beta$), equality must hold in the inclusion $\Delta(M) \subseteq [1, \delta] = \{1\}$. $\square$

4 The Δ-set of a nonprimary ACM

Throughout this section, we will assume that $d = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ where $p_i \in \mathbb{P}$ and $\alpha_i > 0$ for each i. As before, we note that p_i is relatively prime with m, so for each i we will fix ω_i to be the order of p_i modulo m; $\beta_i \geq \alpha_i$ will again be minimal such that $\omega_i \mid \beta_i$.

We will digress a moment to acknowledge a possible strategy. Oftentimes in number theory one needs only to prove the primary case and then the general case follows by some property of the objects in question. For example, any singular ACM can be decomposed as an intersection of primary ACMs:

$$M_{a,b} = \bigcap_{i=1}^{n} M_{a_i, b/q_i}$$

where $q_i = \prod_{j \neq i} p_j^{\alpha_j}$, and a_i is the reduced residue congruent to a modulo b/q_i. Each of the terms in this intersection is easily seen to be primary by results in Section 2. Furthermore, this primary decomposition is unique by the Chinese remainder theorem. Though this decomposition always exists, a mathematical relationship between $\Delta(M \cap N)$ and $\Delta(M), \Delta(N)$ may not exist. If N is a general submonoid of M, the factorization properties of M and N might be substantially different, since it is not always the case, for example, that $\mathcal{A}(N) = \mathcal{A}(M) \cap N$ (see Section 5).

Moving on, we recall that in Section 3 we often made use of the fact that p^β is irreducible in the primary ACM M. In the nonprimary case we will employ a similar strategy. Let $\mathfrak{V}_M = \overline{\mathbb{P}(d)} \cap M$ and note that in fact, $\mathcal{A}(\mathfrak{V}_M) = \mathcal{A}(M) \cap \mathfrak{V}_M$ (this will be discussed with more depth in Section 5). Since $x = p_1^{\beta_1} \cdots p_n^{\beta_n} \in \mathfrak{V}_M$ by the membership criterion, we see that $\mathcal{A}(\mathfrak{V}_M)$ is nonempty as either x or some irreducible $y \mid_M x$ is an element of this set.

Call $y \in \mathcal{A}(\mathfrak{V}_M)$ a *p_i-amenable* irreducible iff $p_i^{k\omega_i} y \in \mathcal{A}(\mathfrak{V}_M)$ for each $k \in \mathbb{N}_0$. It is actually relatively easy to demonstrate the existence of such irreducibles: Choose $y \in \mathcal{A}(\mathfrak{V}_M)$ and $j \in [1, n]$ such that y is of minimal p_j-adic value among elements of $\mathcal{A}(\mathfrak{V}_M)$. If $i \neq j$, then y is p_i-amenable. Thus p_i-amenable irreducibles exist and, as a corollary, $\mathcal{A}(\mathfrak{V}_M)$ is infinite. This is precisely the feature of the nonprimary case which we will use to our advantage.

We are ready to prove that $\Delta(M)$ is finite in the nonprimary case. However, what we will prove is actually a good deal stronger. Say that $\lambda \in \mathbb{N}_0$ is a *critical length* for a monoid M iff for all $x \in M$, $\min \mathcal{L}(x) < \lambda$.

Lemma 4.1 *Let M be a monoid which is not a group. If there is λ such that λ is a critical length for M, then $\Delta(M)$ is nonempty and finite with $\max \Delta(M) \leq \lambda - 2$.*

Proof. Let $x \in M$ be arbitrary. The result is obviously true if $\max \mathcal{L}(x) \leq \lambda$, so suppose that $\max \mathcal{L}(x) > \lambda$. Factor $x = x_1 \cdots x_\lambda \cdots x_\mu$ where $x_i \in \mathcal{A}(M)$ for each i and $\mu > \lambda$. By earlier arguments, there is $l \in \mathcal{L}(x_1 \cdots x_\lambda)$ such that $1 < l < \lambda$ and thus $x_1 \cdots x_\lambda = y_1 \cdots y_l$. Thus, $x = y_1 \cdots y_l x_{\lambda+1} \cdots x_\mu$ and so $\mu, \mu - (\lambda - l) \in \mathcal{L}(x)$. The claim now follows, since $\lambda - l \geq \lambda - 2$. □

Theorem 4.2 *Let M be a nonprimary ACM, $j \in [1, n]$, and y a p_j-amenable irreducible. Choose λ satisfying*

$$\lambda \geq \max_i \left(1 + \frac{v_{p_i}(y)}{\alpha_i}\right), \quad \textit{and} \quad \lambda \geq \frac{2\alpha_j + \omega_j}{\alpha_j}.$$

Then λ is a critical length for M.

Proof. Let $x \in M$ such that $l \in \mathcal{L}(x)$ for $l \geq \lambda$. Of course $v_{p_i}(x) \geq \lambda \alpha_i$ for each i. By the first bound on λ, $v_{p_i}(x) \geq \alpha_i + v_{p_i}(y)$ for each i and therefore $v_{p_i}(x/y) \geq \alpha_i$. We infer that $x/y \in M$ by the membership criterion.

Now find k such that $\alpha_j \leq v_{p_j}(x/y) - k\omega_j \leq \alpha_j + \omega_j - 1$. By the usual arguments, $x/p_j^{k\omega_j} y \in M$ and since

$$v_p\left(\frac{x}{p_j^{k\omega_j} y}\right) \leq \alpha_j + \omega_j - 1,$$

a factorization of $x/p_j^{k\omega_j} y$ has at most k irreducible factors where

$$k \leq \frac{\alpha_j + \omega_j - 1}{\alpha_j}.$$

Moreover, $k+1 \in \mathcal{L}(x)$ since $p_j^{k\omega_j} y$ is irreducible in M (as y was chosen to be p_j-amenable). By the second bound on λ, $\lambda > k+1$, so $\min \mathcal{L}(x) < \lambda$. By definition, λ is a critical length for M. $\square$

The above theorem does not apply to the primary case because in the primary case $\mathcal{A}(\mathfrak{V}_M)$ is finite and thus there are no p-amenable irreducibles. Combining Theorems 3.7 and 4.2, we infer the following:

Theorem 4.3 *If M is a singular ACM, then $\Delta(M)$ is finite.*

We will now demonstrate the usefulness of Theorem 4.2 in formulating bounds for $\Delta(M)$ where M is nonprimary and singular. For instance, we can derive the following two corollaries:

Corollary 4.4 *Let M be a nonprimary ACM. Furthermore, assume that $p_1^{\gamma_1} \cdots p_n^{\gamma_n} \in M$ where $\gamma_i \in [\alpha_i, 2\alpha_i)$ for each i and that for some j we have $\omega_j \leq \alpha_j$. Then $\Delta(M) = \{1\}$*

Proof. Set $y = p_1^{\gamma_1} \cdots p_n^{\gamma_n}$ and note that since $\gamma_i < 2\alpha_i$, y is a p_i-amenable irreducible for all $i \in [1, n]$. Applying Theorem 4.2 we see that $\lambda = 3$ is a critical length for M. Since the Δ-set of a nonprimary ACM is nonempty and $\lambda = 3$ is a critical length for M, $\Delta(M) = \{1\}$. $\square$

Corollary 4.5 *Let M be a singular ACM with $a = b$. Then*

$$\Delta(M) = \begin{cases} \varnothing & \text{if } b \text{ is prime,} \\ \{1\} & \text{if } b \text{ is composite.} \end{cases}$$

Proof. This is simply a combination of results; specifically Theorem 3.1 and Corollary 4.4. $\square$

Example 4.6 Consider $M = M_{6,30}$. Here $d = 6$ and $m = 5$; $\boldsymbol{p} = (2, 3)$, $\boldsymbol{\alpha} = (1, 1)$, and $\boldsymbol{\omega} = (4, 4)$. Note that 6 is a 2-amenable irreducible of M (it is of course also 3-amenable). Since 2 has order 4 modulo 5, we may apply Theorem 4.2 to see that $\lambda = 6$ is a critical length of $M_{6,30}$. By Lemma 4.1, $\max \Delta(M) \leq 4$. This is actually the best bound because

$$6^6 = (96)(486),$$

$6, 96, 486 \in \mathcal{A}(M)$, and there are no other factorizations of 6^6 in M. Without much trouble we can find witnesses to $1, 2, 3 \in \Delta(M)$, so $\Delta(M) = [1, 4]$. We also note that $M_{6,30} = M_{6,10} \cap M_{6,15}$, and $\Delta(M_{6,10}) = \Delta(M_{6,15}) = [1, 3]$ by Theorem 3.1.

Example 4.7 Let $M = M_{96,480}$. We have $d = 96$, $m = 5$, $\boldsymbol{p} = (2, 3)$, $\boldsymbol{\alpha} = (5, 1)$, and $\boldsymbol{\omega} = (4, 4)$. Since $d = 96 \in M$ and $4 = \omega_1 \leq \alpha_1 = 5$, we can conclude by Corollary 4.4 that $\Delta(M) = \{1\}$. Again, we decompose M into primary ACMs: $M_{96,480} = M_{96,160} \cap M_{6,15}$. Applying Theorem 3.1, $\Delta(M_{96,160}) = \{1\}$ and $\Delta(M_{6,15}) = [1, 3]$.

In the primary case, $\Delta(M)$ the values α and ω are sufficient to retrieve $\Delta(M)$. Thus, it may seem intuitive that $\Delta(M)$ is determined by $\boldsymbol{\alpha}, \boldsymbol{\omega}$ in the general case. However, even if we know the values of $\boldsymbol{\alpha}, \boldsymbol{\omega}, m$ and even the structure of the subgroup of $\mathrm{Cl}(M)$ generated by $\tilde{p}_1, \ldots \tilde{p}_n$, we still cannot describe $\Delta(M)$ precisely all the time:

Example 4.8 Consider $M = M_{56,70}$. Making the usual preliminary calculations, we see that $(\boldsymbol{\alpha}_M, \boldsymbol{\omega}_M, m_M) = (\boldsymbol{\alpha}_N, \boldsymbol{\omega}_N, m_N)$, where $N = M_{6,30}$. Though $\boldsymbol{p}_M = (2, 7)$ and $\boldsymbol{p}_N = (2, 3)$, both sets of primes generate the whole class group $\mathrm{Cl}(M) = \mathrm{Cl}(N) = (\mathbb{Z}/5\mathbb{Z})^\times$.

Despite these similarities, we claim that

$$\max \Delta(M) \leq 3 < 4 = \max \Delta(N).$$

Proof. Using Theorem 4.2 with $y = 56 = 2^3 7$ (which is 2-amenable), we see that $\lambda = 6$ is a critical length for M. Suppose that $6 \in \mathcal{L}(x)$ and that $x = y_1 y_2$ is a factorization of x into 2 irreducibles.

Of course, $v(x) = v_2(y_1) + v_2(y_2) \geq 6$ and $v(x) = v_7(y_1) + v_7(y_2) \geq 6$. By the pigeonhole principle there exist i, j with $v_2(y_i) \geq 3$ and $v_7(y_j) \geq 3$. We must have $i \neq j$, for if $i = j$ then 14^2 is a nontrivial irreducible factor of y_i in M which contradicts the hypotheses. Thus, without loss of generality we take

$v_2(y_1) \geq 3$, $v_7(y_2) \geq 3$, and write $y_1 = 2^2 z_1$ and $y_2 = 7^2 z_2$. We know that $z_1, z_2 \in M$ by the membership criterion, and since they divide irreducible elements of M in $\mathbb{N}$, $z_1, z_2 \in \mathcal{A}(M)$ by Corollary 2.3. Thus, $x = (14^2) z_1 z_2$ is a factorization of x into 3 irreducibles of M, whence the claim. $\square$

In all three of the preceding examples we considered nonprimary ACMs with two primary factors: $M = M_1 \cap M_2$ for M_1, M_2 primary. Note that there are instances of $M_1 = M_2 \subsetneq M$, $M = M_1 \subsetneq M_2$, and $M = M_1 = M_2$. This suggests that the connection between $\Delta(M)$ and the Δ-sets of the terms in the primary decomposition of M is tenuous at best.

5 Higher structure theory of ACMs

Example 4.8 illustrates that characterizing the full Δ-set of an ACM in the nonprimary case is somewhat more complicated than in the primary case. In particular even if we know $\boldsymbol{\alpha}, \boldsymbol{\omega}, m$ and the structure of the subgroup of $\mathrm{Cl}(M)$ generated by $\boldsymbol{p}$, we still cannot determine $\Delta(M)$ exactly.

In the example, $\boldsymbol{p}_M = (2, 7)$ and $\boldsymbol{p}_N = (2, 3)$. While it is true that $2, 3, 7$ all have order 4 modulo 5, $2 \equiv 7 \bmod 5$ but $2 \equiv 3^{-1} \bmod 5$. As a result, $d_N \in N$ but $d_M \notin M$.

This suggests that in order to precisely describe $\Delta(M)$ in the nonprimary case, we need some adequate characterization of $\mathfrak{V}_M = \overline{\mathbb{P}(d)} \cap M$. We will begin by generalizing this object for any monoid.

5.1 Saturated submonoids and the vinculum

Let M be any monoid. A submonoid $S \leq M$ is called *saturated* iff $xy \in S$ implies $x, y \in S$. That is, whenever S is a saturated submonoid,

$$xy \in S \iff x \in S \text{ and } y \in S.$$

Lemma 5.1 *We characterize the saturated submonoids of an ACM. Namely, if M is an ACM and $S \leq M$ is saturated, then either $S = \{1\}$ or $S = \overline{P} \cap M$ where $\mathbb{P}(d) \subseteq P \subseteq \mathbb{P} \setminus \mathbb{P}(m)$.*

Furthermore, suppose $S \leq T \leq M$ with S saturated in T and T saturated in M and write $T = \overline{P} \cap M$. Then we may conclude that $S = \overline{P'} \cap M$ for $P' \subseteq P$.

Proof. The set $\{1\}$ is a saturated submonoid of M, since it is the group of units. So suppose that $S = \overline{P} \cap M$ where P satisfies the required inclusions. S is certainly a submonoid of M, so let $x \in S$, $x \neq 1$, and factor $x = yz$. But then y, z are products of primes in $\mathbb{P}(x) \subseteq P$, whence $y, z \in \overline{P}$.

Conversely, let M be an ACM and S a saturated submonoid of M. Suppose that S contains some $x \neq 1$ and let $y \in M$ be such that $\mathbb{P}(y) \subseteq \mathbb{P}(x)$. Choose $k \in \mathbb{N}$ such that $y \mid_{\mathbb{N}} x^k$ and note that $y \mid_M x^{k+1}$ since x^{k+1}/y satisfies the membership criterion. Thus $x^{k+1} = yz$ for some $z \in M$; since $x^{k+1} \in S$ (as S is a submonoid), $y, z \in S$. Thus $\overline{\mathbb{P}(x)} \cap M \subseteq S$ for each $x \in S$.

Since S is a submonoid of M, if $x, y \in S$ then $xy \in S$ so $\overline{\mathbb{P}(xy)} \cap M = \overline{\mathbb{P}(x) \cup \mathbb{P}(y)} \cap M$ and thus we conclude that $S = \overline{\mathbb{P}(S)} \cap M$. The second claim is a simple corollary. $\square$

Lemma 5.2 *If S is a saturated submonoid of T and T is a saturated submonoid of M, then S is a saturated submonoid of M.*

Moreover, if $\mathcal{F}$ is a family of saturated submonoids of M, then $\bigcap_{S \in \mathcal{F}} S$ is a saturated submonoid of M.

Proof. A routine application of the definitions. $\square$

Saturated submonoids interest us especially for the following reason:

Lemma 5.3 *If $S \leq M$ is saturated, then $\Delta(S) \subseteq \Delta(M)$.*

Proof. It is clear from the definitions that $\mathcal{A}(S) = \mathcal{A}(M) \cap S$ (as long as S is saturated; this is certainly false for a general submonoid). Let $x \in S$; by the preceding statement and the fact that S is closed under factorization, $\mathcal{L}(x)$ is the same regardless of whether we view x as an element of S or an element of M. Hence $\Delta(S) \subseteq \Delta(M)$. $\square$

Every monoid which is not a group has at least two saturated submonoids, namely M and $M^\times$ (the group of units). Since $M^\times \leq S$ for every saturated submonoid $S \leq M$, $M^\times$ is the minimal saturated submonoid of M. Since the structure of $M^\times$ is rather irrelevant to concerns of monoid theory (as it can always be collapsed to $\{1\}$ by reducing M), we wish to define a saturated submonoid $\mathfrak{V}_M \leq M$ such that whenever S is also saturated and $M^\times \leq S \leq \mathfrak{V}_M$, then either $S = \mathfrak{V}_M$ or $S = M^\times$. The *vinculum of M* is defined as the saturated submonoid

$$\mathfrak{V}_M = \bigcap_{\substack{S \leq M \\ S \text{ saturated} \\ S \neq M^\times}} S.$$

Given $x \in M$, the smallest saturated submonoid $S(x)$ of M containing x is the multiplicative closure of

$$\{y \in M : (\exists k \in \mathbb{N})\ y \mid_M x^k\}$$

$S(x) = M^\times$ iff x is a unit, so

$$\mathfrak{V}_M = \bigcap_{x \in M \setminus M^\times} S(x).$$

Therefore $y \in \mathfrak{V}_M$ iff for all $x \in M \setminus M^\times$, y divides some power of x (in M). We infer that

$$\mathfrak{V}_M = \{y \in M : \sqrt{y} \cup M^\times = M\}$$

where $\sqrt{y}$ is the radical of the principal ideal generated by y. So we may think of the vinculum as the set of elements of M whose radical contains $M \setminus M^\times$.

Example 5.4 Let M be an ACM. By Lemma 5.1 we have $\mathfrak{V}_M = \overline{P} \cap M$ where $P = \bigcap_{x \in M, x \neq 1} \mathbb{P}(x)$ whence we conclude that $\mathfrak{V}_M = \overline{\mathbb{P}(d)} \cap M$, which is exactly how we defined it earlier in Section 4.

By the above example, the vinculum actually helps us generalize the notions of regular and singular for any monoid. In particular we say that M is *regular* iff $\mathfrak{V}_M = M^\times$, and that M is *singular* otherwise. In particular, all groups are regular.

Furthermore we call a singular monoid M *primary* iff $\mathfrak{V}_M$ is finitely generated. This is consistent with the definition of a primary ACM because if M is a primary ACM then $\mathcal{A}(\mathfrak{V}_M) = \{p^{\beta + k\omega} : 0 \leq k < \alpha/\omega\}$ and we know that if M is a nonprimary ACM then $\mathcal{A}(\mathfrak{V}_M)$ is infinite.

5.2 $\mathcal{L}$-collapses and the Δ-set of an ACM

For any $Q \subseteq \mathbb{P}$, set

$$\mathfrak{V}_M[Q] = \overline{\mathbb{P}(d) \cup Q} \cap M.$$

Implicitly, 3.8 characterizes the Δ-set of a primary ACM M by describing factorizations in the saturated submonoids $\mathfrak{V}_M[q, r]$ where $q \equiv p^{-\alpha} \bmod m$ and $r \equiv p^{-\gamma} \bmod m$ with $\gamma \in [\alpha, \beta)$. We will show that a similar method works in the nonprimary case.

Lemma 5.5 *Let M, N be monoids. An* $\mathcal{L}$-collapse *is a surjective homomorphism $\theta : M \to N$ such that $\mathcal{L}(\theta x) = \mathcal{L}(x)$. If such a map exists, $\Delta(M) = \Delta(N)$.*

Proof. Since θ preserves $\mathcal{L}$-sets, for every $x \in M$, $\Delta(x) = \Delta(\theta x)$ and so $\Delta(M) \subseteq \Delta(N)$. The argument for the reverse inclusion simply requires that θ be surjective, which is true by definition. □

Lemma 5.6 *Let M be an ACM, $x \in M \setminus \overline{\mathbb{P}(d)}$, and let $q = 1$ or $q \in \mathbb{P}(x) \setminus \mathbb{P}(d)$. Then if $q' \in \mathbb{P} \setminus \mathbb{P}(d)$ and $q \equiv q' \bmod m$, $x' = (x/q)q' \in M$. Furthermore, x is irreducible iff x' is irreducible.*

Proof. The former claim is true by the membership criterion.

For the latter claim, suppose x is irreducible and factor $x' = y'z'$. Without loss of generality, let $q' \mid y'$. By the first part, $y = (y'/q')q \in M$, and since $x = yz'$ and y is not a unit, $z' = 1$, whence x' is irreducible. The proof of the converse is identical. □

Theorem 5.7 *Let $Q \subseteq \mathbb{P} \setminus \mathbb{P}(m)$ such that $\tilde{Q} = \mathrm{Cl}(M) \setminus \{\tilde{1}\}$ and the reduction map $Q \to \mathrm{Cl}(M)$ is injective. There is an $\mathcal{L}$-collapse $\theta : M \to \mathfrak{V}_M[Q]$.*

Proof. For each $\tilde{r} \in \mathrm{Cl}(M) \setminus \{\tilde{1}\}$, let $q(\tilde{r})$ be the unique element of Q' such that $q(\tilde{r}) \equiv r \bmod m$. Define a map $\theta : \mathbb{P} \to \mathbb{P} \cup \{1\}$ by

$$\theta p = \begin{cases} p & \text{if } p \in \mathbb{P}(d), \\ 1 & \text{if } p \notin \mathbb{P}(d) \text{ and } p \equiv 1 \bmod m, \\ q(\tilde{r}) & \text{if } p \notin \mathbb{P}(d) \text{ and } p \equiv r \bmod m, \end{cases}$$

θ certainly preserves divisibility by d and residues modulo m, so it is easy to see that $\theta : M \to \mathfrak{V}_M[Q]$. Since $\mathfrak{V}_M[Q]$ is a saturated submonoid of M (Lemma 5.1), $\mathcal{A}(\mathfrak{V}_M[Q]) = \mathcal{A}(M) \cap \mathfrak{V}_M[Q]$ and moreover, θ fixes $\mathfrak{V}_M[Q]$, so θ is surjective. Applying Lemma 5.6 iteratively, θ preserves $\mathcal{L}$-sets, and thus θ is an $\mathcal{L}$-collapse. □

Theorem 5.8 *Let M be a singular ACM. Up to $\mathcal{L}$-collapse and isomorphism, M has at most $2^{\varphi(m)-1}$ saturated submonoids.*

Proof. Let Q satisfy the assumptions of Theorem 5.7. If $S \leq M$ is saturated and nontrivial we have $\mathfrak{V}_M \leq \theta S \leq \theta M = \mathfrak{V}_M[Q]$. By Lemma 5.1 there are at most $2^{\varphi(m)-1}$ submonoids θS (up to isomorphism) which satisfy these inclusions, corresponding to the subsets of Q. □

The above shows that we need only work in finitely many saturated submonoids of M in order to completely determine $\Delta(M)$. Though this Theorem was a generalization formulated in the same spirit as Lemma 3.8, it is comparably imprecise, owing to the structural complexity and diversity of nonprimary ACMs.

5.3 Further structural results

Lemma 5.9 *Let M be a singular ACM and let Q satisfy the assumptions of Theorem 5.7. The monoid $\mathfrak{V}_M[Q]$ can be embedded in a finite-dimensional numerical monoid.*

Proof. Enumerate $\mathrm{Cl}(M) \setminus \{\tilde{1}\} = \{\tilde{r}_1, \ldots, \tilde{r}_{\varphi(m)-1}\}$ and define a homomorphism $\eta : \mathbb{N}_0^n \times \mathbb{N}_0^{\varphi(m)-1} \to \mathrm{Cl}(M)$ by

$$\eta(x_1, \ldots, x_n, y_1, \ldots, y_{\varphi(m)-1}) = \tilde{p}_1^{x_1} \cdots \tilde{p}_n^{x_n} \tilde{r}_1^{y_1} \cdots \tilde{r}_{\varphi(m)-1}^{y_{\varphi(m)-1}}$$

then we clearly have

$$\mathfrak{V}_M[Q] \cong \ker \eta \cap \prod_{i=1}^{n} [\alpha_i, \infty) \times \mathbb{N}_0^{\varphi(m)-1}. \ \square$$

Unfortunately, the right-hand submonoid of $\mathbb{N}_0^n \times \mathbb{N}_0^{\varphi(m)-1}$ is not saturated, so we cannot immediately make use of extensive results concerning the Δ-set of numerical monoids [2].

Corollary 5.10 *Let M, N be singular ACMs and let Q_M, Q_N satisfy the assumptions of 5.7. Suppose that $n_M = n_N$, $\boldsymbol{\alpha}_M = \boldsymbol{\alpha}_N$, and $\mathrm{Cl}(M) \cong \mathrm{Cl}(N)$. By Lemma 5.9, $\mathfrak{V}_M[Q_M], \mathfrak{V}_N[Q_N]$ may be embedded as submonoids of $\mathbb{N}_0^n \times \mathbb{N}_0^{\varphi(m)-1}$. If the resulting homomorphisms η_M, η_N have the same kernel, then $\mathfrak{V}_M[Q_M] \cong \mathfrak{V}_N[Q_N]$ and so $\Delta(M) = \Delta(N)$.*

Example 5.11 We briefly revisit Example 4.8. Both ACMs $M = M_{56,70}$ and $N = M_{6,30}$ may be embedded as submonoids of $\mathbb{N}_0^2 \times \mathbb{N}_0^3$. In the standard embedding given by Lemma 5.9 we see that $\eta_M(\mathbf{v}, \mathbf{w}) = \tilde{2}^{v_1+v_2+w_1} \tilde{3}^{w_2} \tilde{4}^{w_3}$, and $\eta_N(\mathbf{v}, \mathbf{w}) = \tilde{2}^{v_1+w_1} \tilde{3}^{v_2+w_2} \tilde{4}^{w_3}$.

Identifying $\mathrm{Cl}(M) = \mathrm{Cl}(N) = \mathbb{Z}/4\mathbb{Z}$ with 2 as our primitive root, these homomorphisms are determined by

$$\eta_M : (\mathbf{v}, \mathbf{w}) \mapsto v_1 + v_2 + w_1 - w_2 + 2w_3 + 4\mathbb{Z}$$
$$\eta_N : (\mathbf{v}, \mathbf{w}) \mapsto v_1 - v_2 + w_1 - w_2 + 2w_3 + 4\mathbb{Z}$$

so $\ker \eta_M \neq \ker \eta_N$.

We conclude with a (very hopeful) conjecture suggested by Theorem 5.7:

Conjecture 5.12 *Let M, N be singular ACMs and let Q_M, Q_N satisfy the assumptions of 5.7. Then we have $\mathfrak{V}_M[Q_M] \cong \mathfrak{V}_N[Q_N]$ iff $\mathfrak{V}_M \cong \mathfrak{V}_N$ and $\mathrm{Cl}(M) \cong \mathrm{Cl}(N)$.*

6 The asymptotic density of irreducible elements in a singular ACM

This section is not tangibly related to a description of $\Delta(M)$ for M a singular ACM, as it mainly concerns questions of analytic number theory.

Theorem 6.1 *If M is a singular ACM and $x \in M$ is reducible, $x+b \in \mathcal{A}(M)$.*

Proof. Suppose otherwise and write $x = (a + bh)(a + bk)$ and $x + b = (a + bi)(a + bj)$. Substituting and expanding gives

$$x + b = a^2 + ab(i + j) + b^2ij = a^2 + ab(k + h) + b^2kh + b$$

and canceling terms,

$$\begin{aligned} a(i + j) + bij &= a(k + h) + bkh + 1 \\ a(i + j - k - h) + b(ij - kh) &= 1 \end{aligned}$$

so $d = 1$ which contradicts the singularity of M. $\square$

This suggests that if the limit exists and M is a singular ACM,

$$\varsigma(M) = \lim_{k\to\infty} \frac{|\mathcal{A}(M) \cap [1, k]|}{|M \cap [1, k]|} \geq \frac{1}{2}.$$

Example 6.2 For any b, $\varsigma(M_{b,b}) = 1/2$ (immediate by the characterization of irreducibles in this case, see Example 1.1).

If p is an odd prime, $\varsigma(M_{p,2p}) = (p-1)/p$. In this case $x \in M$ is irreducible iff $p \mid x$ but $p^2 \nmid x$. Thus, dividing through by p we see that $\varsigma(M)$ is equal to the density of odd numbers which are not divisible by p, which is as claimed. This example shows that $\varsigma(M)$ for M an ACM can be made arbitrarily close to 1.

$\varsigma(M_{4,6}) = 1/2$: This argument is largely heuristic. Let $x \in \mathcal{A}(M_{4,6})$; then

- $v_2(x) \in [1, 2]$.
- $\mathcal{A}_1 = \mathcal{H}_1$ (that is, $y \in M_{4,6}$ is irreducible whenever $v_2(y) = 1$).
- $x \in \mathcal{A}_2$ iff $v_2(x) = 2$ and x has no odd prime factors congruent to 2 modulo 3. (Otherwise x has an irreducible factor in $\mathcal{A}_1$.)

The asymptotic density of $\mathcal{A}_1$ in $M_{4,6}$ is clearly $1/2$ so we need only compute the asymptotic density of $\mathcal{A}_2$ in $M_{4,6}$. Of course, the density of all elements $x \in M_{4,6}$ with 2-adic value 2 is $1/4$. By the above, an irreducible in $\mathcal{A}_2$ is of the form $4y$ where y is a (possibly empty) product of primes congruent to 1 modulo 3. As the limiting variable k grows, we observe that there are many more reducible elements in $\mathcal{H}_2$ than irreducible elements and that the density of $\mathcal{A}_2$ in $\mathcal{H}_2$ must tend towards 0 (essentially, the probability a number congruent to 1 modulo 3 has a divisor congruent to 2 modulo 3 tends towards 1 as $k \to \infty$).

7 Further questions

- Suppose we are given a critical length λ for M via Theorem 4.2. This gives us the estimate $\max \Delta(M) \leq \lambda - 2$, and this bound can be verified or improved by computing $\Delta(x)$ where $x \in \mathcal{A}(M)^l$, $l \in [2, \lambda)$ (we used a similar strategy in Example 4.8 to show that $\max \Delta(M_{56,70}) \leq 3$). By Theorem 5.7 we actually need only check $x \in \mathcal{A}(\mathfrak{V}_M[Q])^l$.

  Is there a finite (or relatively sparse) subset $A \subseteq \mathcal{A}(\mathfrak{V}_M[Q])$ such that it suffices to compute $\Delta(x)$ for $x \in A^l$?

- Let Q satisfy the assumptions of Theorem 5.7. By Theorem 5.8 choose j_M to be minimal such that

$$\Delta(M) = \bigcup_{\substack{Q' \subseteq Q \\ |Q'| \leq j_M}} \Delta(\mathfrak{V}_M[Q']).$$

  If M is primary, then by Lemma 3.8 $j_M \leq 2$. Can we say anymore about j_M? When (if ever) is j_M pessimal: $j_M = \varphi(m) - 1$?

- Compute $\varsigma(M)$ for any singular ACM. Is there a singular ACM M such that $\varsigma(M)$ is irrational? Is there any connection between the rationality of $\varsigma(M)$ and $\Delta(M)$ or between $\varsigma(M)$ and the structure of $\mathfrak{V}_M$?

- Let M be any monoid, $S \leq M$ a saturated submonoid. For $x, y \in M$ say that $x \sim_S y$ iff there exist $u, v \in S$ with $ux = vy$. This is an equivalence relation and the resulting quotient M/S is a monoid. Just as S preserves some of the factorization properties of M, is the same true of M/S? Does the structure of $M/\mathfrak{V}_M$ tell us anything interesting about M?

References

[1] M. Banister, S. T. Chapman, J. Chaika, and W. Meyerson. *On the arithmetic of arithmetical congruence monoids*. Submitted for publication.

[2] C. Bowles, N. Kaplan, and D. Reiser. *Δ-sets of numerical monoids*. Trinity University, Mathematics Technical Report #S35, San Antonio, TX 2004.

[3] S. T. Chapman and A. Geroldinger. *Krull domains and their monoids, their sets of lengths, and associated combinatorial problems*. *Lecture Notes in Pure and Applied Mathematics* **189** (1997), 73–112.

[4] A. Geroldinger and F. Halter-Koch. *Non-Unique Factorizations*. Chapman & Hall, 2006.

[5] F. Halter-Koch. *Arithmetical semigroups defined by congruences*. Semigroup Forum **42** (1991), 59–62.

[6] R. D. James and I. Niven. *Unique factorization in multiplicative systems*. Proc. Amer. Math. Soc. **5** (1954), 834–838.