

The Extraction Degree of Cale Monoids

Kimberly Cervello

*Department of Mathematics, State University of New York at Geneseo,
Geneseo, NY 14454*
E-mail: kacbambina@hotmail.com

Vadim Ponomarenko*

*Department of Mathematics, Trinity University,
San Antonio, TX 78212*
E-mail: vadim123@gmail.com

Denise Terry

*Department of Mathematics, University of Redlands,
Redlands, CA 92373*
E-mail: denise1501@hotmail.com

Liya Zhu

*Department of Mathematics, University of California at Berkeley,
Berkeley, CA 94720*
E-mail: liya.zhu@berkeley.edu

Communicated by L. Márki

The extraction degree measures commonality of factorization between any two elements in a commutative, cancellative monoid. Additional properties of the extraction degree are developed for monoids possessing a Cale basis. For block monoids, the complete set of extraction degrees is calculated between any two elements, between any two irreducible elements, and between any irreducible element and any general element.

Key Words: Cale monoid, extraction degree, Krull monoid, block monoid, minimal zero sequence

Research supported in part by NSF grant 0353488.

* Corresponding author.

1. INTRODUCTION

A powerful tool in studying nonunique factorization in integral domains or monoids is that of Cale representations, which capture internal features at a finer level than the original structure. Inspired by [7] and [8], Cale theory was first defined in [3]. See Chapter 7 of [1] for a full treatment, including examples in algebraic number rings, Diophantine monoids, Krull monoids, polynomial rings, coordinate rings, semigroup rings, and others.

We now recall the necessary properties of Cale monoids. Let M be a commutative and cancellative atomic monoid with units M^\times . We call $Q \subseteq M$ a *Cale basis* of M , if the monoid generated by Q (denoted by $[Q]$) is factorial and for every $x \in M$, there is some power $x^n \in M^\times [Q]$. If M possesses a Cale basis, we call M a *Cale monoid*. We note that Cale bases are not unique; however they are closely related. Because M is atomic, we may choose Q to have each of its elements irreducible in M ; this can be shown to determine Q uniquely. Suppose that q, r are both elements of a Cale basis, that differ by a unit. We can therefore express $q = \epsilon r$ for some unit ϵ . But this violates the unique Cale representation of q ; it is both $q^1 r^0$ and $\epsilon q^0 r^1$.

A key tool used with Cale bases is the *extraction degree* λ . For $x \in M$, write $x^n = \epsilon \prod_{q \in Q} q^{m_q}$, where $\epsilon \in M^\times$ and all but finitely many m_q are zero.

For $q \in Q$, we define $\lambda(q, x) = \frac{m_q}{n}$. Note that because $[Q]$ is factorial, this is well-defined, and independent of the choice of n . Let $Q_x = \{q \in Q : \lambda(q, x) > 0\}$ be the *span* of x .

For $x, y \in M$, we set $\lambda(x, y) = \min \left\{ \frac{\lambda(q, y)}{\lambda(q, x)} : q \in Q_x \right\}$, where we set $\lambda(x, y) = +\infty$ if $x \in M^\times$; equivalently, if $Q_x = \emptyset$. We set $Q_{x, y} \subseteq Q_x$ such that $\lambda(x, y) = \frac{\lambda(q, y)}{\lambda(q, x)}$ for all $q \in Q_{x, y}$.

The relevant properties of λ are summarized in the following.

THEOREM 1.1. *Let $x, y, z \in M$.*

1. *If $x, y \in Q$ with $x \neq y$, then $\lambda(x, y) = 0$ and $\lambda(x, x) = 1$.*
2. *$\lambda(x, y) = \sup \left\{ \frac{m}{n} : m \in \mathbb{Z}^{\geq 0}, n \in \mathbb{Z}^{> 0}, x^m | y^n \right\}$*
3. *Let $k, l \in \mathbb{Z}^{> 0}$; then $k\lambda(x^k, y^l) = l\lambda(x, y)$.*
4. *$\lambda(xy, z) \leq \min(\lambda(x, z), \lambda(y, z))$.*
5. *$\lambda(x, yz) \geq \lambda(x, y) + \lambda(x, z)$. If $x \in Q$, then equality holds.*

We recall several special types of Cale monoids. Let QM be the quotient group for monoid M . We call M *root-closed* if $M = \{x \in QM | x^n \in M \text{ for some } n \in \mathbb{Z}^{> 0}\}$. We call M *tame* if for every $q \in Q$ there exists some $t \in \mathbb{Z}^{> 0}$ such that $t\lambda(q, x) \in \mathbb{Z}^{\geq 0}$ for all $x \in M$. We set $t(q)$ to be the minimum such t .

These types of Cale monoids are quite common. All valuation monoids and generalized Krull monoids are root-closed. All outside factorial monoids are both root-closed and tame. All Krull monoids with torsion class groups are both root-closed and tame. See [1] for more examples; therein, all Cale monoids are assumed to be tame.

We begin by developing additional properties of λ for Cale monoids in general, and other properties for root-closed and tame Cale monoids. Then, we turn our attention to a specific type of Cale monoid, namely the block monoid of a finite abelian group. For these monoids, consider the set of elements \mathfrak{B} and the set of irreducible elements \mathfrak{A} . We determine $\lambda(\mathfrak{B}, \mathfrak{B})$, $\lambda(\mathfrak{A}, \mathfrak{B})$, $\lambda(\mathfrak{B}, \mathfrak{A})$, and $\lambda(\mathfrak{A}, \mathfrak{A})$, where $\lambda(S, T) = \{\lambda(s, t) : s \in S, t \in T\}$ for sets S, T . Of these, the most interesting result is $\lambda(\mathfrak{A}, \mathfrak{A})$, which has three forms depending on whether G is cyclic, of the form $\mathbb{Z}_2 \oplus \mathbb{Z}_{2n}$, or otherwise. We use the notation (e, f) to denote the open interval between real numbers e and f .

2. EXTRACTION DEGREE IN CALE MONOIDS

We first develop some simple properties of the extraction degree. We assume henceforth that M is a Cale monoid (hence commutative, cancellative, and atomic).

THEOREM 2.1. *Let $x, y \in M$.*

1. *Suppose that $x = x_1 x_2 \cdots x_k$. Then $\frac{1}{\lambda(x, y)} \leq \frac{1}{\lambda(x_1, y)} + \cdots + \frac{1}{\lambda(x_k, y)}$.*
2. *$\lambda(x, y) = 0$ if and only if $Q_x \not\subseteq Q_y$.*
3. *$\lambda(x, y) \geq 1$ if and only if $\lambda(q, x) \leq \lambda(q, y)$ for all $q \in Q$.*

Proof.

1. Let $q \in Q_{x, y}$. Then $\frac{1}{\lambda(x, y)} = \frac{\lambda(q, x)}{\lambda(q, y)} = \frac{\sum_i \lambda(q, x_i)}{\lambda(q, y)} = \sum_i \frac{\lambda(q, x_i)}{\lambda(q, y)} \leq \sum_i \frac{1}{\lambda(x_i, y)}$, where the inequality follows from the definition of λ .

2. $\lambda(x, y) = 0$ if and only if there is some $q \in Q_x$ with $\lambda(q, y) = 0$, which is true if and only if there is some $q \in Q_x \setminus Q_y$.

3. $\lambda(q, x) \leq \lambda(q, y)$ for all $q \in Q$ if and only if $1 \leq \frac{\lambda(q, y)}{\lambda(q, x)}$ for all $x \in Q_x$, which in turn is true if and only if $1 \leq \lambda(x, y)$.

■

The following result is tight in the sense that examples can be constructed where $Q_x \subsetneq Q_y \subsetneq Q_z$ and $Q_{xz} \subsetneq Q_{x, y}$ and $Q_{xz} \subsetneq Q_{yz}$. It is, however, possible to extend it in trivial ways by considering various of x, y, z in M^\times .

THEOREM 2.2. *Let $x, y, z \in M \setminus M^\times$. Then $\lambda(x, y)\lambda(y, z) \leq \lambda(x, z)$, with equality if and only if either:*

1. $Q_x \not\subseteq Q_z$; or
2. $Q_x \subseteq Q_y \subseteq Q_z$ and $Q_{xz} = Q_{x,y} \cap Q_{yz} \neq \emptyset$.

Proof. If either $Q_x \not\subseteq Q_y$ or $Q_y \not\subseteq Q_z$, then the left side of the inequality is zero; hence the result holds. Otherwise, we have $Q_x \subseteq Q_y \subseteq Q_z$. Let $q \in Q_{xz} \subseteq Q_x \subseteq Q_y$. Then $\lambda(x, z) = \frac{\lambda(q, z)}{\lambda(q, x)} = \frac{\lambda(q, y)\lambda(q, z)}{\lambda(q, x)\lambda(q, y)} \geq \lambda(x, y)\lambda(y, z)$.

If both sides of the inequality are zero, then $Q_x \not\subseteq Q_z$. Conversely, if $Q_x \not\subseteq Q_z$, then either $Q_x \not\subseteq Q_y$ or $Q_y \not\subseteq Q_z$ (or both); hence both sides of the inequality are zero.

If nonzero equality holds, then $q \in Q_{xz} \cap Q_{yz} \cap Q_{x,y}$. Further, since both sides are nonzero, $Q_x \subseteq Q_y \subseteq Q_z$. The same equality holds for any other element besides q of Q_{xz} ; hence, $Q_{xz} \subseteq Q_{xz} \cap Q_{yz} \cap Q_{x,y}$ and consequently $Q_{xz} \subseteq Q_{yz} \cap Q_{x,y}$. Now, let $q' \in Q_{x,y} \cap Q_{yz}$. Then, since $q' \in Q_{x,y}$, we have $\lambda(x, y) = \frac{\lambda(q', y)}{\lambda(q', x)} = \frac{\lambda(q, y)}{\lambda(q, x)}$; hence $\frac{\lambda(q', x)}{\lambda(q, x)} = \frac{\lambda(q', y)}{\lambda(q, y)}$. But also, since $q' \in Q_{yz}$, we have $\frac{\lambda(q', y)}{\lambda(q, y)} = \frac{\lambda(q', z)}{\lambda(q, z)}$. Combining, we have $\frac{\lambda(q', x)}{\lambda(q, x)} = \frac{\lambda(q', z)}{\lambda(q, z)}$ and therefore $\lambda(x, z) = \frac{\lambda(q', z)}{\lambda(q', x)} = \frac{\lambda(q, z)}{\lambda(q, x)}$, so $q' \in Q_{xz}$ and hence $Q_{yz} \cap Q_{x,y} \subseteq Q_{xz}$.

Conversely, if we let $q \in Q_{xz} \cap Q_{yz} \cap Q_{x,y}$, equality will hold in $\frac{\lambda(q, y)\lambda(q, z)}{\lambda(q, x)\lambda(q, y)} \geq \lambda(x, y)\lambda(y, z)$. \blacksquare

The following reciprocity theorem follows directly from Theorem 2.2.

THEOREM 2.3. *Suppose that $x, y \in M \setminus M^\times$. Then $\lambda(x, y)\lambda(y, x) \leq 1$, with equality if and only if $Q_x = Q_y = Q_{x,y} = Q_{yx} \neq \emptyset$.*

Proof. With the observation that $\lambda(x, x) = 1$ for any $x \notin M^\times$ the inequality follows. If equality holds, then $Q_x \subseteq Q_y \subseteq Q_x$ and hence $Q_x = Q_y$. Let $q \in Q_{x,y} \cap Q_{yx}$, and $q' \in Q_x = Q_y$. Compare $A = \frac{\lambda(q', y)}{\lambda(q', x)}$ to $B = \frac{\lambda(q, y)}{\lambda(q, x)}$. We must have $A \geq B$ since $q \in Q_{x,y}$. However, we take reciprocals and find that $1/A \geq 1/B$ since $q \in Q_{yx}$. Hence $A = B$ and $q' \in Q_{x,y} \cap Q_{yx}$. Therefore $Q_x \subseteq Q_{x,y} \cap Q_{yx} \subseteq Q_x$ and therefore $Q_x = Q_{x,y} \cap Q_{yx}$. Let $q \in Q_{x,y} \cap Q_{yx}$ and $q' \in Q_{x,y}$. We have $\frac{\lambda(q', y)}{\lambda(q', x)} = \frac{\lambda(q, y)}{\lambda(q, x)}$. We take reciprocals and find that $q' \in Q_{yx}$; hence $Q_{x,y} \subseteq Q_{x,y} \cap Q_{yx}$. Therefore $Q_{x,y} \subseteq Q_{yx}$; by symmetry $Q_{x,y} = Q_{yx}$. \blacksquare

We turn now to special Cale monoids. Recall that M is root-closed if $M = \{x \in QM \mid x^n \in M \text{ for some } n \in \mathbb{Z}^{>0}\}$. We have two results for Cale

monoids requiring this additional property; the first is rather specific but needed in the sequel; the second bounds $\lambda(x, y)$ if y is irreducible.

PROPOSITION 2.1. *Suppose that M is root-closed. Let $q \in Q$, and let $x \in M$ with $Q_x = \{q\}$. Then $x = \epsilon q^n$ for some $n \in \mathbb{Z}^{>0}$ and some $\epsilon \in M^\times$.*

Proof. It suffices to show that $q|x$, because then $\frac{x}{q}$ satisfies the same hypotheses and we proceed by induction. Write $x^n = \epsilon q^m$ for some $\epsilon \in M^\times$. If $m < n$, then in QM we write $\frac{1}{\epsilon}x^{n-m} = (\frac{q}{x})^m$. Since M is root-closed and $\frac{1}{\epsilon}x^{n-m} \in M$, we have $\frac{q}{x} \in M$, contradicting the irreducibility of q . Hence $m \geq n$. But now we write, in QM , $(\frac{x}{q})^n = \epsilon q^{m-n} \in M$. Since M is root-closed, $\frac{x}{q} \in M$ and thus $q|x$. \blacksquare

THEOREM 2.4. *Suppose that M is root-closed. Let $x, y \in M \setminus M^\times$ with y irreducible. Then $\lambda(x, y) \leq 1$. Further, equality holds if and only if $x = \epsilon y$, for some $\epsilon \in M^\times$.*

Proof. First, we note that if $x = \epsilon y$ for $\epsilon \in M^\times$, then $\lambda(x, y) = 1$. Conversely, if $\lambda(x, y) = 1$, then x, y have the same Cale representation (up to a unit).

Now, suppose that $1 < \lambda(x, y) = \frac{m}{n}$, where $x^m|y^n$. We can write $y^n = x^m z$, for some $z \in M$. Because $\frac{m}{n} > 1$, we have $m > n$. In QM , we can write $(\frac{y}{x})^n = x^{m-n} z$. But since $m > n$, $x^{m-n} z \in M$. Because M is root-closed, $\frac{y}{x} \in M$ and hence $x|y$. Since $x \notin M^\times$, y is reducible. \blacksquare

We now turn to root-closed tame Cale monoids. We recall that if M is tame then each $q \in Q$ has an associated integer $t(q)$, which is minimal such that $t(q)\lambda(q, x) \in \mathbb{Z}^{\geq 0}$ for all $x \in M$. For $x \in M$, let us define $t(x) = \text{lcm}\{t(q) : q \in Q_x\}$ and $t(M) = \text{lcm}\{t(q) : q \in Q\}$. These are chosen so that $t(x)\lambda(q, x) \in \mathbb{Z}^{\geq 0}$ for all $x \in M$ and $q \in Q$; also $t(M)\lambda(q, x) \in \mathbb{Z}^{\geq 0}$. Clearly $t(q) \leq t(x) \leq t(M)$ for all $x \in M$ and $q \in Q_x$.

Under these assumptions, we have two results. The first characterizes prime elements of such monoids, and the second produces gaps in the extraction degree (under certain irreducibility assumptions).

THEOREM 2.5. *Suppose that M is root-closed and tame. Let $x \in M$. x is prime if and only if there is some $\epsilon \in M^\times$, with $\epsilon x \in Q$ and with $t(\epsilon x) = 1$.*

Proof. Suppose that x is prime. Write $x^n = \epsilon \prod_{q \in Q} q^{m_q}$. x divides this expression; hence x divides some $q \in Q$. However, all elements of Q are irreducible; hence $\epsilon x = q$, for some $\epsilon \in M^\times$. It now suffices to show

that $\lambda(q, x) \in \mathbb{Z}$ for all $x \in M$. Let $x \in M$, and write $x^n = \epsilon \prod_{q \in Q} q^{m_q}$, where $\epsilon \in M^\times$. If $m_q = 0$, then $\lambda(q, x) = 0$. Otherwise, $q|x^n = xx \cdots x$. Since q is prime, $q|x$; hence $m_q \geq n$. But now we consider, in QM , that $(\frac{x}{q})^n = \frac{\epsilon}{q^n} \prod_{q \in Q} q^{m_q} \in M$. Hence $\frac{x}{q} \in M$ and we can continue to divide both sides by q^n ; at each step, either we have exhausted the q 's from both sides, or q divides both sides. The process must end since M is atomic. Hence, the original power of q (m_q) must have been an integral multiple of n , as desired.

Suppose now that $\lambda(q, x) \in \mathbb{Z}$ for all $x \in M$. Suppose that $q|xy$. Therefore, $\lambda(q, xy) \in \mathbb{Z}^{\geq 1}$. Write $\lambda(q, xy) = \lambda(q, x) + \lambda(q, y)$, a sum of two integers. Without loss of generality assume that $\lambda(q, x) \geq 1$. We write $x^n = \epsilon \prod_{q \in Q} q^{m_q}$, where $\epsilon \in M^\times$ and $m_q \geq n$. By dividing both sides by q^n (in QM) we find that $\frac{x}{q} \in M$ and hence $q|x$, as desired. \blacksquare

THEOREM 2.6. *Suppose that M is root-closed and tame. Let $x, y \in M$. If x is irreducible then $\lambda(x, y) \notin (0, \frac{1}{t(x)})$. If y is irreducible but not prime then $\lambda(x, y) \notin (1 - \frac{1}{t(y)}, 1)$.*

Proof. Suppose that x is irreducible. For some $q \in Q_{x,y}$, we have $\lambda(x, y) = \frac{\lambda(q,y)}{\lambda(q,x)} = \frac{t(q)\lambda(q,y)}{t(q)\lambda(q,x)}$. We have $t(q)\lambda(q, y) \in \mathbb{Z}$; in particular, either $\lambda(q, y) = 0$ (in which case $\lambda(x, y) = 0$), or $t(q)\lambda(q, y) \geq 1$. By the previous theorem, $\lambda(q, x) \leq 1$. By definition of $t(x)$ we have $t(q) \leq t(x)$. Hence, $t(q)\lambda(q, x) \leq t(x)$, and hence $\lambda(x, y) \geq \frac{1}{t(x)}$.

Suppose now that y is irreducible. Again we have $\lambda(x, y) = \frac{\lambda(q,y)}{\lambda(q,x)} = \frac{t(q)\lambda(q,y)}{t(q)\lambda(q,x)}$. We have $t(q)\lambda(q, x) \in \mathbb{Z}$. Further, by the previous theorem, we have $\lambda(q, y) \leq 1$. If $\lambda(q, y) < 1$, then $t(q)\lambda(q, y) \leq t(q) - 1$. Hence, either $\lambda(x, y) \geq 1$ or (for some integer $\alpha \leq t(q)$), $\lambda(x, y) \leq \frac{\alpha-1}{\alpha} = 1 - \frac{1}{\alpha} \leq 1 - \frac{1}{t(q)} \leq 1 - \frac{1}{t(y)}$, as desired. Otherwise we have $\lambda(q, y) = 1$, and we have $y = \epsilon q$ for some $\epsilon \in M^\times$ and hence $\lambda(x, y) = \lambda(x, q)$. Either $\lambda(x, y) = 0$ or $Q_x = \{q\}$; in the latter case, by Proposition 2.1, $\lambda(x, y) = \lambda(q^n, q) = \frac{1}{n} \notin (1 - \frac{1}{t(y)}, 1)$, apart from the special case $t(y) = 1$, which is excluded by assumption and Theorem 2.5. \blacksquare

3. BLOCK MONOIDS

We turn now to the important special case of block monoids. Consider a fixed finite abelian group G , written additively, with the set of nonzero elements denoted by G^* . For $g \in G$, let $|g|$ denote the order of g in

G , and let $\langle g \rangle$ be the subgroup of G generated by g . Consider $\mathfrak{B}(G)$, the collection of all multisets of elements of G^* that have sum zero in G . Write $x \in \mathfrak{B}(G)$ as $x = g_1^{m_{g_1}} g_2^{m_{g_2}} \cdots g_k^{m_{g_k}}$; by definition we have $m_{g_1} g_1 + m_{g_2} g_2 + \cdots + m_{g_k} g_k = 0$. $\mathfrak{B}(G)$ forms a monoid under the operation of multiset union (with the empty multiset serving for identity). $\mathfrak{B}(G)$ is a Krull monoid, as shown in [6], and is therefore root-closed and tame.

The Cale basis of $\mathfrak{B}(G)$ is easily seen to be $Q = \{g^{|g|} : g \in G^*\}$. Let $x \in \mathfrak{B}(G)$; we see that $\lambda(g^{|g|}, x) = \frac{m_g}{|g|}$. Apart from the trivial case of $G = \mathbb{Z}_2$ (which we will ignore henceforth), we can always construct some $x \in \mathfrak{B}(G)$ that has $m_g = 1$; hence $t(g^{|g|}) = |g|$. Consequently, $t(\mathfrak{B}(G))$ is the exponent of G , $\exp(G)$. Let $x \in \mathfrak{B}(G)$; we see that $Q_x = \{g^{|g|} : m_g > 0\}$. Let $x, y \in \mathfrak{B}(G)$, where $x = \prod g^{m_g}, y = \prod g^{n_g}$. We then see that $\lambda(x, y) = \min\{\frac{n_g}{m_g} : m_g > 0\}$.

All of these characterizations make block monoids particularly appealing for study. Let $\mathfrak{A}(G)$ be the atoms of $\mathfrak{B}(G)$. In this section, we determine $\lambda(\mathfrak{B}(G), \mathfrak{B}(G))$, $\lambda(\mathfrak{A}(G), \mathfrak{A}(G))$, $\lambda(\mathfrak{A}(G), \mathfrak{B}(G))$, and $\lambda(\mathfrak{B}(G), \mathfrak{A}(G))$, where $\lambda(S, T) = \{\lambda(s, t) : s \in S, t \in T\}$. We do not know which of these results, if any, have analogues for general Cale monoids; this is a topic for further study.

THEOREM 3.1. $\lambda(\mathfrak{B}(G), \mathfrak{B}(G)) = \mathbb{Q}^{\geq 0}$

Proof. It suffices to show that $\mathbb{Q}^{\geq 0} \subseteq \lambda(\mathfrak{B}(G), \mathfrak{B}(G))$. Let $\frac{n}{m} \in \mathbb{Q}^{\geq 0}$. Let $g \in G^*$, and set $x = g^{|g|m}, y = g^{|g|n}$. Evidently $x, y \in \mathfrak{B}(G)$, and $\lambda(x, y) = \frac{n}{m}$, as desired. \blacksquare

An interesting phenomenon occurs in cyclic groups that does not occur in higher-rank groups.

THEOREM 3.2. *Suppose that $|G| > 2$. Let $g \in G^*$. Then:*

1. $|g|\lambda(g^{|g|}, \mathfrak{B}(G)) = \mathbb{Z}^{\geq 0}$.
2. If $\langle g \rangle \neq G$, then $|g|\lambda(g^{|g|}, \mathfrak{A}(G)) = \{0, 1, \dots, |g|\}$.
3. If $\langle g \rangle = G$, then $|g|\lambda(g^{|g|}, \mathfrak{A}(G)) = \{0, 1, \dots, |g| - 2, |g|\}$.

Proof. First, let $m \in \mathbb{Z}^{\geq 0}$, and let $h \in G^* \setminus \{g\}$. Set $x = g^m(g - h)^{m+|G|-|g|} h^{m+|G|-|g|}$; this is in the block monoid though is not necessarily irreducible. Because neither $g - h$ nor h are equal to 0 or g , we have $\lambda(g^{|g|}, x) = \frac{m}{|g|}$.

Let $m \in \{0, 1, \dots, |g|\}$; it suffices to construct $x \in \mathfrak{A}(G)$ with $m_g = m$. If $m = 0$, let $x = h^{|h|}$ for some $h \neq g$. If $m = |g|$, let $x = g^{|g|}$. For all other m besides $|g| - 1$, set $h = (|g| - m)g$, and set $x = g^m h^1$. x has sum zero,

and no proper submultiset has sum zero. Because $0 < m < |g| - 1$, $h \neq 0$ and $h \neq g$. For all of these cases $\lambda(g^{|g|}, x) = \frac{m}{|g|}$.

It remains to consider $m = |g| - 1$. If $\langle g \rangle \neq G$, choose $h \in G^* \setminus \langle g \rangle$. Set $x = g^{|g|-1}(g+h)^1(-h)^1$. By choice of h , no proper submultiset of x has sum zero; further, neither $g+h$ nor $-h$ are equal to 0 or g . Hence, $\lambda(g^{|g|}, x) = \frac{|g|-1}{|g|}$.

If, however, $\langle g \rangle = G$, then it is not possible to have $x \in \mathfrak{A}(G)$ with $m_g = |g| - 1 = |G| - 1$. The reason is that $g^{|g|-1}$ does not have sum zero; however its submultisets make all other elements of G . Therefore, for any $h \in G^*$ with $h \neq g$, $g^{|g|-1}h$ will have a proper submultiset with zero sum. \blacksquare

This allows us to compute $\lambda(\mathfrak{A}(G), \mathfrak{B}(G))$, as follows. For sets A, B , let $\frac{A}{B} = \{\frac{a}{b} : a \in A, b \in B\}$.

COROLLARY 3.1. *Let $S = \{1, 2, \dots, \exp(G)\}$, $S' = S \setminus \{\exp(G) - 1\}$.*

If G is not cyclic, then $\lambda(\mathfrak{A}(G), \mathfrak{B}(G)) = \frac{\mathbb{Z}^{\geq 0}}{S}$.

If G is cyclic, then $\lambda(\mathfrak{A}(G), \mathfrak{B}(G)) = \frac{\mathbb{Z}^{\geq 0}}{S'}$.

Proof. The only difficulty in applying Theorem 3.2 is that since $\lambda(x, y) = \min\{\frac{\lambda(q, y)}{\lambda(q, x)} : q \in Q_x\}$, the desired $q \in Q_x$ might not be in $Q_{x, y}$. However, since y need not be irreducible, we may simply add copies of the undesirable q' to y ; this increases $\frac{\lambda(q', y)}{\lambda(q', x)}$ by one. By adding sufficiently many such copies, we can force the desired q to be minimal. \blacksquare

We next have a number-theoretic lemma, necessary in the sequel.

LEMMA 3.1. *Let a, b, n be positive integers. Suppose that $a \leq n - 2$ and that $a < b$. Then $\frac{a}{b} > \frac{n-2}{n}$ if and only if $a = b - 1$ and $\frac{n}{2} < b < n$.*

Proof. First, some algebra shows that $\frac{n}{2} < b$ if and only if $\frac{b-1}{b} > \frac{n-2}{n}$. This establishes one direction. If $b \geq n$, then $\frac{a}{b} \leq \frac{n-2}{n}$, a contradiction. Similarly, if $\frac{n}{2} \geq b$, then we have $\frac{a}{b} \leq \frac{b-1}{b} \leq \frac{n-2}{n}$, another contradiction. Hence $\frac{n}{2} < b < n$; a bit of algebra now shows that $\frac{b-2}{b} < \frac{n-2}{n}$. If $a \leq b - 2$, then again we have the contradiction $\frac{a}{b} \leq \frac{b-2}{b} < \frac{n-2}{n}$; thus $a = b - 1$. \blacksquare

Note that for cyclic G , $t(\mathfrak{B}(G)) = |G|$. Therefore, one of the bounds of Theorem 2.6 is $\lambda(\mathfrak{B}(G), \mathfrak{A}(G)) \cap (1 - \frac{1}{|G|}, 1) = \emptyset$. The following sharpens this bound. In fact, this is best possible, as will be shown in Theorem 3.4.

LEMMA 3.2. *Let G be cyclic with $|G| > 2$. Then*

$$\lambda(\mathfrak{B}(G), \mathfrak{A}(G)) \cap (1 - \frac{2}{|G|}, 1) = \emptyset.$$

Proof. Let $x \in \mathfrak{B}(G), y \in \mathfrak{A}(G)$, and let $g^{|g|} \in Q_{x,y}$. Note that if $|g| < |G|$ then the desired result follows from Theorem 2.6 and Lagrange's theorem. Hence we assume $|g| = |G|$; furthermore, we may apply an automorphism to G and assume that $g = 1$. For convenience, write $q = 1^{|G|}$. By Theorem 3.2, $|G|\lambda(q, y) \in \{0, 1, \dots, |G| - 2, |G|\}$. By Theorem 2.4, $\lambda(q, x) \geq \lambda(q, y)$. We now argue by way of contradiction; we assume that $\lambda(x, y) \in (1 - \frac{2}{|G|}, 1)$. Since $\lambda(x, y) < 1$ we may apply Lemma 3.1 to get $\lambda(q, y) = \lambda(q, x) - 1$ and $\frac{|G|}{2} < \lambda(q, x) < |G|$.

Write $y = 1^m g_1^{m_1} g_2^{m_2} \cdots g_k^{m_k}$. Note that $m = \lambda(q, y) \geq \frac{|G|-1}{2}$. We claim now that $m1 + m_1 g_1 + m_2 g_2 + \cdots + m_k g_k = |G|$, where the terms are treated as integers¹. Consider $g_1, 2g_1, \dots, m_1 g_1, m_1 g_1 + g_2, m_1 g_1 + 2g_2, \dots, m_1 g_1 + m_2 g_2 + \cdots + m_k g_k$. These terms are monotonically increasing (in \mathbb{Z}), and the last term is $\alpha|G| - m$, for some integer α . If $\alpha \neq 1$, then there must be two consecutive terms (say a, b) where $a < |G|$, and $b \geq |G| + 1$ (neither can equal $|G|$ since y is irreducible). Further, since y is irreducible, we must have $a \leq |G| - m - 1$. Now, $b - a = g_i$ for some $i \in [1, k]$; hence $g_i \geq m + 2$. But also, since y is irreducible, $g_i \leq |G| - m - 1$. Hence $|G| - m - 1 \geq m + 2$. Hence $m \leq \frac{|G|-3}{2}$, which contradicts $m \geq \frac{|G|-1}{2}$; therefore $\alpha = 1$ and y sums to $|G|$ in \mathbb{Z} .

Now, write $x = 1^{m+1} g_1^{n_1} g_2^{n_2} \cdots g_k^{n_k}$. Note that the group elements in x must be some subset of those in y , by Theorem 2.1. Because $\lambda(x, y) > 1 - \frac{2}{|G|}$, we must have $\frac{m_i}{n_i} > 1 - \frac{2}{|G|}$ for each $i \in [1, k]$. However, if any of these fractions were less than 1, we could again apply Lemma 3.1 to get $m_i \geq \frac{|G|-1}{2}$; this is impossible, as then the sum of y (as integers) would be at least $1m + 2m_i > |G|$. Hence, each $\frac{m_i}{n_i} = 1$, and therefore $x = y \cup \{1\}$. But, the sum (in \mathbb{Z}) of x is $|G| + 1$, which is not a multiple of $|G|$; hence x is not in $\mathfrak{B}(G)$, which is violative of hypothesis. ■

We next have what appears to be an obscure lemma; however it is critical in the classification of $\lambda(\mathfrak{A}(G), \mathfrak{A}(G))$ which follows.

LEMMA 3.3. *Suppose that $G = \mathbb{Z}_2 \oplus \mathbb{Z}_{2n}$. Then $\frac{2n-2}{2n-1} \notin \lambda(\mathfrak{A}(G), \mathfrak{A}(G))$.*

Proof. By way of contradiction, suppose that $x, y \in \mathfrak{A}(G), g^{|g|} \in Q_{x,y}$, $\lambda(g^{|g|}, x) = 2n - 1, \lambda(g^{|g|}, y) = 2n - 2$. However, the largest atom² in G is of cardinality $2n + 1$. Hence $x = g^{|g|-1} e f$, for some $e, f \in G^*$. Both are necessary, since x has sum 0 in G . They must be distinct, since otherwise $e + e = g$, which is not possible because $|g| = 2n$ and $|2e| \leq n$.

¹Atoms with this property are called *basic*; this notion was defined in [2] and explored in [10].

²This cardinality is known as the Davenport constant, and has been thoroughly studied. For an introduction, see [9] or [4].

Applying Theorem 2.1, we see that $y = g^{|g|-2}efd$, for some $d \in G^* \setminus \{g\}$ (d is necessary since otherwise $g = \sum x - \sum y = 0 - 0 = 0$). However, have $d + \sum x = g + \sum y$; hence $d = g$, which establishes a contradiction. \blacksquare

We are now ready for the $\lambda(\mathfrak{A}(G), \mathfrak{A}(G))$ classification theorem.

THEOREM 3.3. *Let $|G| > 2$. Set $S = \{1, 2, \dots, \exp(G)\}$, $S_0 = S \cup \{0\}$, $S' = S \setminus \{\exp(G) - 1\}$, $S'_0 = S' \cup \{0\}$. Then $\lambda(\mathfrak{A}(G), \mathfrak{A}(G))$ is:*

1. $\left\{ \frac{a}{b} : a \in S'_0, b \in S', \frac{a}{b} \leq 1 - \frac{2}{\exp(G)} \right\} \cup \{1\}$; for G cyclic.
2. $\left\{ \frac{a}{b} : a \in S_0, b \in S, \frac{a}{b} \leq 1 \right\} \setminus \left\{ \frac{2n-2}{2n-1} \right\}$; for $G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{2n}$.
3. $\left\{ \frac{a}{b} : a \in S_0, b \in S, \frac{a}{b} \leq 1 \right\}$; for all other G .

Proof. One direction follows from Theorem 3.2, Lemma 3.2, and Lemma 3.3; it remains to exhibit $x, y \in \mathfrak{A}(G)$ with $\lambda(x, y) = \frac{a}{b}$, for each of the above a, b . For $x = y = g^{|g|}$, $\lambda(x, y) = 1$; for $x = g^{|g|}, y = h^{|h|}$, $\lambda(x, y) = 0$. We turn now to $\lambda \in (0, 1)$.

Let $g \in G$ have $|g| = \exp(G)$. We will construct $x, y \in \mathfrak{A}(G)$, where $x = g^b \prod h^{m_h}, y = g^a \prod h^{n_h} \prod f^{n_f}$, where $\frac{a}{b} \leq \frac{n_h}{m_h}$ for $h \in x$.

If $b \leq |g| - 2$ and $a \leq b - 2$, then set $h = (|g| - b)g, f = (b - a)g$. The conditions imposed on a, b imply that $h \neq g$ and $f \neq g$ ($f = h$ is possible, but irrelevant). Now, set $x = g^b h, y = g^a h f$.

If $b = |g|$ and $a \leq b - 2$, then set $f = (b - a)g$. We have $f \neq g$. Now, set $x = g^b, y = g^a f$.

If $b = |g|$ and $a = |g| - 1$, then G is not cyclic; take $f \in G^* \setminus \langle g \rangle$. Set $x = g^b, y = g^a(g + f)(-f)$. Neither $g + f$ nor $-f$ are equal to 0 or g .

If $b = |g| - 1$ and $a \leq b - 2$, then G is not cyclic; take $h \in G^* \setminus \langle g \rangle$. Set $f = (b - a)g$, and $x = g^b(g + h)(-h), y = g^a(g + h)(-h)f$. By construction, none of $g + h, -h, f$ are equal to g .

If $b = |g| - 1$ and $a = b - 1$, then G is not cyclic. If $G / \langle g \rangle$ is not an elementary 2-group, then take some $h \in G^*$ with $h \notin \langle g \rangle$ and $2h \notin \langle g \rangle$. Now, set $x = g^b(g + h)(-h), y = g^a(g + h)^2(-h)^2$.

Finally, we consider the case of $b = |g| - 1, a = b - 1$, and $H = G / \langle g \rangle$ an elementary 2-group. H cannot be cyclic, otherwise we have the excluded case $G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{2n}$. Hence there are h, f with $h \notin \langle f, g \rangle, f \notin \langle h, g \rangle$, and $\langle f, h \rangle \cap \langle g \rangle = \{0\}$. We set $x = g^b(g + h)(-h), y = g^a(g + h)(-h)(g + f)(-f)$. \blacksquare

Here are several examples illustrating this theorem.

EXAMPLE 3.1.

1. $G = \mathbb{Z}_4$. We have $S'_0 = \{0, 1, 2, 4\}$ and $S' = \{1, 2, 4\}$. Theorem 3.3 gives $\lambda(\mathfrak{A}(G), \mathfrak{A}(G)) = \{0, \frac{1}{4}, \frac{1}{2}, 1\}$.

2. $G = \mathbb{Z}_2 \oplus \mathbb{Z}_4$. We have $S_0 = \{0, 1, 2, 3, 4\}$ and $S = \{1, 2, 3, 4\}$. Theorem 3.3 gives $\lambda(\mathfrak{A}(G), \mathfrak{A}(G)) = \{0, \frac{1}{4}, \frac{1}{3}, \frac{1}{2}, \frac{3}{4}, 1\}$.

3. $G = \mathbb{Z}_4 \oplus \mathbb{Z}_4$. We have $S_0 = \{0, 1, 2, 3, 4\}$ and $S = \{1, 2, 3, 4\}$. Theorem 3.3 gives $\lambda(\mathfrak{A}(G), \mathfrak{A}(G)) = \{0, \frac{1}{4}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, 1\}$.

As a consequence, we are now able to compute $\lambda(\mathfrak{B}(G), \mathfrak{A}(G))$.

THEOREM 3.4. *Let $|G| > 2$. Set $T' = \frac{\{0, 1, 2, \dots, \exp(G) - 2, \exp(G)\}}{\mathbb{Z}_{>0}}$, and $T = \frac{\{0, 1, 2, \dots, \exp(G)\}}{\mathbb{Z}_{>0}}$.*

If G is cyclic, then $\lambda(\mathfrak{B}(G), \mathfrak{A}(G)) = (T' \cap [0, 1]) \setminus (1 - \frac{2}{\exp(G)}, 1)$.

If G is not cyclic, then $\lambda(\mathfrak{B}(G), \mathfrak{A}(G)) = T \cap [0, 1]$.

Proof. One direction follows from Theorem 3.2 and Lemma 3.2; it remains to exhibit $x \in \mathfrak{B}(G), y \in \mathfrak{A}(G)$ with $\lambda(x, y) = \frac{a}{b}$, for each of the above a, b .

Apply Theorem 3.3 to find $x, y \in \mathfrak{A}(G)$ with $\lambda(q, x) = 1, \lambda(q, y) = a$, for some $q \in Q_{x, y}$. Now, $x^b \in \mathfrak{B}(G)$, and $\lambda(q, x^b) = b$ by Theorem 1.1. We have $q \in Q_{x^b, y}$; hence, $\lambda(x, y) = \frac{a}{b}$, as desired. ■

REFERENCES

1. Scott T. Chapman, editor. *Arithmetical Properties of Commutative Rings and Monoids*, volume 241 of *Lecture Notes in Pure and Applied Mathematics*. Chapman & Hall/CRC, Boca Raton, FL, New York, 2005. Including papers from a conference held in Chapel Hill, NC, October 2003.
2. Scott T. Chapman, Michael Freeze, and William W. Smith. Equivalence classes of minimal zero-sequences modulo a prime. In *Ideal theoretic methods in commutative algebra (Columbia, MO, 1999)*, volume 220 of *Lecture Notes in Pure and Appl. Math.*, pages 133–145. Dekker, New York, 2001.
3. Scott T. Chapman, Franz Halter-Koch, and Ulrich Krause. Inside factorial monoids and integral domains. *J. Algebra*, 252(2):350–375, 2002.
4. W. D. Gao. Zero sums in finite cyclic groups. *Integers*, pages A12, 7 pp. (electronic), 2000.
5. A. Geroldinger and F. Halter-Koch. Nonunique factorizations in block semigroups and arithmetical applications. *Math. Slovaca*, 42(5):641–661, 1992.
6. Franz Halter-Koch. Halbgruppen mit Divisorentheorie. *Exposition. Math.*, 8(1):27–66, 1990.
7. Ulrich Krause. Eindeutige Faktorisierung ohne ideale Elemente. *Abh. Braunschweig. Wiss. Ges.*, 33:169–177, 1982.
8. Ulrich Krause. Semigroups that are factorial from inside or from outside. In *Lattices, semigroups, and universal algebra (Lisbon, 1988)*, pages 147–161. Plenum, New York, 1990.

9. Marcin Mazur. A note on the growth of Davenport's constant. *Manuscripta Math.*, 74(3):229–235, 1992.
10. Vadim Ponomarenko. Minimal zero sequences of finite cyclic groups. *Integers*, 4:A24, 6 pp. (electronic), 2004.

Received August 26, 2005; in final form October 13, 2005.