involve
a journal of mathematics

Atoms of the relative block monoid

Nicholas Baeth and Justin Hoffmeier

mathematical sciences publishers

2009 Vol. 2, No. 1

INVOLVE 2:1(2009)

Atoms of the relative block monoid

Nicholas Baeth and Justin Hoffmeier

(Communicated by Scott Chapman)

Let G be a finite abelian group with subgroup H and let $\mathcal{F}(G)$ denote the free abelian monoid with basis G. The classical block monoid $\mathcal{B}(G)$ is the collection of sequences in $\mathcal{F}(G)$ whose elements sum to zero. The relative block monoid $\mathcal{B}_H(G)$, defined by Halter-Koch, is the collection of all sequences in $\mathcal{F}(G)$ whose elements sum to an element in H. We use a natural transfer homomorphism $\theta : \mathcal{B}_H(G) \to \mathcal{B}(G/H)$ to enumerate the irreducible elements of $\mathcal{B}_H(G)$ given an enumeration of the irreducible elements of $\mathcal{B}(G/H)$.

1. Introduction

In this paper we will study the so-called block monoid and a generalization called the relative block monoid. The block monoid has been ubiquitous in the literature over the past thirty years and has been used extensively as a tool to study nonunique factorization in certain commutative rings and monoids. The relative block monoid was introduced by Halter-Koch [1992]. Our main goal in this paper is to provide an enumeration of the irreducible elements of the relative block monoid given an enumeration of the irreducible elements of a related block monoid.

In this section we offer a brief description of some central ideas in factorization theory. The quintessential reference for the study of factorization in commutative monoids — in particular block monoids — is [Geroldinger and Halter-Koch 2006, Chapters 5, 6, 7]. In Section 2, we give notations and definitions relevant to studying the relative block monoid. We conclude Section 2 by stating several known results about the relative block monoid. Section 3 provides a means of enumerating the atoms of the relative block monoid $\mathcal{B}_H(G)$ by considering a natural transfer homomorphism $\theta : \mathcal{B}_H(G) \to \mathcal{B}(G/H)$.

For our purposes, a *monoid* is a commutative, cancellative semigroup with identity. We will restrict our attention to reduced monoids, that is, monoids whose set of

MSC2000: 11P70, 20M14.

Keywords: zero-sum sequences, block monoids, finite abelian groups.

This work consists of research done as part of Justin Hoffmeier's Master's thesis at the University of Central Missouri.

units, $H^\times$, contains only the identity element. An element h of a reduced monoid H is said to be *irreducible* or an *atom* if whenever $h = a \cdot b$ with $a, b \in H$, then either $a = 1$ or $b = 1$. We denote the set of atoms of a monoid H by $\mathcal{A}(H)$. If an element $\alpha \in H$ can be written as $\alpha = a_1 \cdots a_k$ with each $a_i \in \mathcal{A}(H)$, this factorization of α is said to have *length* k.

As it is often convenient to study factorization via a surjective map onto a smaller, simpler monoid, we now define transfer homomorphisms. Let H and D be reduced monoids and let $\pi : H \to D$ be a surjective monoid homomorphism. We say that π is a *transfer homomorphism* provided that $\pi^{-1}(1) = \{1\}$ and whenever $\pi(\alpha) = \beta_1\beta_2$ in D, there exist elements α_1 and $\alpha_2 \in H$ such that $\pi(\alpha_1) = \beta_1$, $\pi(\alpha_2) = \beta_2$, and $\alpha = \alpha_1\alpha_2$. It is known that transfer homomorphisms preserve length [Geroldinger and Halter-Koch 2006, Proposition 3.2.3]. That is, if $\pi : H \to D$ is a transfer homomorphism then all questions dealing with lengths of factorizations in H can be studied in D.

2. The relative block monoid

Let G be a finite abelian group written additively and with identity 0. Let $\mathcal{F}(G)$ denote the free abelian monoid with basis G. That is, $\mathcal{F}(G)$ consists of all formal products $g_1^{n_1} \cdots g_k^{n_k}$ with $g_i \in G$ and $n_i \in \mathbb{N}$ with operation given by concatenation. When we write an element $g_1^{n_1} \cdots g_k^{n_k}$ of $\mathcal{B}(G)$ with exponents n_i larger than one, we generally assume that $g_i \neq g_j$ unless $i = j$. We define a monoid homomorphism $\sigma : \mathcal{F}(G) \to G$ by $\sigma(\alpha) = g_1 + \cdots + g_k$ where $\alpha = g_1 g_2 \cdots g_k$. We also use $|\alpha| = n_1 + n_2 + \cdots + n_t$ to denote the length of α in $\mathcal{F}(G)$. We call an element α in $\mathcal{F}(G)$ a *zero-sum sequence* if and only if $\sigma(\alpha) = 0$ in G. If α is a zero-sum sequence and if there does not exist a proper subsequence of α which is also a zero-sum sequence, then we call α a *minimal zero-sum sequence*. The collection of all zero-sum sequences in $\mathcal{F}(G)$, with operation given by concatenation, is called the *block monoid* of G and is denoted $\mathcal{B}(G)$. That is,

$$\mathcal{B}(G) = \{\alpha \in \mathcal{F}(G) \mid \sigma(\alpha) = 0\}.$$

Notice that $\mathcal{B}(G) = \ker(\sigma)$ and that the atoms of $\mathcal{B}(G)$ are simply the nonempty minimal zero-sum sequences. For more general groups, enumerating the atoms of the block monoid is a difficult task. In general, there is no known algorithm to enumerate all atoms of $\mathcal{B}(G)$, although there are some results for special cases of G; see [Geroldinger and Halter-Koch 2006; Ponomarenko 2004]. We will return to this question in Section 3.

When studying zero-sum sequences, the Davenport constant is an important invariant. The *Davenport constant* $\mathsf{D}(G)$ is defined to be the smallest positive integer d such that if $|\alpha| = d$ with $\alpha \in \mathcal{F}(G)$ then there must exist a nonempty subsequence α' of α such that $\sigma(\alpha') = 0$.

Over the past thirty years, several authors have attempted to calculate $\mathsf{D}(G)$ in certain cases, but no general formula is known. What is known about the Davenport constant we summarize in the following theorem [Geroldinger and Halter-Koch 2006]. First we need to define another invariant of a finite abelian group G. If

$$G \cong \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k},$$

with $n_i \mid n_{i+1}$ and $n_i > 1$ for each $1 \leq i < k$, we let

$$\mathsf{d}^*(G) = \sum_{i=1}^{k} (n_i - 1).$$

Theorem 2.1. Let G be a finite abelian group. Then:

(1) $\mathsf{d}^*(G) + 1 \leq \mathsf{D}(G) \leq |G|$;

(2) If G is a cyclic group of order n, then $\mathsf{D}(G) = n$.

We now introduce a somewhat larger submonoid of $\mathcal{F}(G)$, first defined by Halter-Koch [1992]. Let G be a finite abelian group and let H be a subgroup of G. We call an element $\alpha \in \mathcal{F}(G)$ an *H-sum sequence* if $\sigma(\alpha) \in H$. If α is an H-sum sequence and if there does not exist a proper subsequence of an α which is also an H-sum sequence, then α is said to be a *minimal H-sum sequence*. We call the collection of all H-sequences, the *block monoid of G relative to H* and denote it by $\mathcal{B}_H(G)$. Note that if $H = \{0\}$, the H-sum sequences are precisely the zero-sum sequences and hence $\mathcal{B}_H(G) = \mathcal{B}(G)$. In the other extreme case, if $H = G$, then $\mathcal{B}_H(G) = \mathcal{F}(G)$.

As we are now concerned with H-sum sequences, it is natural to define the H-Davenport constant. Let G be a finite abelian group and let H be a subgroup of G. The *H-Davenport constant*, denoted by $\mathsf{D}_H(G)$, is the smallest integer d such that every sequence $\alpha \in \mathcal{F}(G)$ with $|\alpha| \geq d$ has a subsequence $\alpha' \neq 1$ with $\sigma(\alpha') \in H$.

The following theorem [Halter-Koch 1992, Proposition 1] lists several known results about the relative block monoid. We are, in particular, interested in parts 2 and 3 of the theorem.

Theorem 2.2. Let G be an abelian group and let H be a subgroup of G.

(1) The embedding $\mathcal{B}_H(G) \hookrightarrow \mathcal{F}(G)$ is a divisor theory with class group (isomorphic to) G/H and every class contains $|H|$ primes, unless $|G| = 2$ and $H = \{0\}$. If $|G| = 2$ and $H = \{0\}$, then obviously $\mathcal{B}_H(G) = \mathcal{B}(G) \cong (\mathbb{N}_0^2, +)$.

(2) The monoid homomorphism $\theta : \mathcal{B}_H(G) \to \mathcal{B}(G/H)$, defined by

$$\theta(g_1 \cdots g_k) = (g_1 + H) \cdots (g_k + H)$$

is a transfer homomorphism.

(3) $\mathsf{D}_H(G) = \sup\{|\alpha| \mid \alpha \text{ is an atoms of } \mathcal{B}_H(G)\} = \mathsf{D}(G/H)$.

Note that in Theorem 2.2, $|H|$ denotes the cardinality of H while $|\sigma|$ denotes the length of σ. The transfer homomorphism θ from Theorem 2.2 will be heavily used in Section 3 to enumerate the atoms of the relative block monoid.

3. Enumerating the atoms of $\mathcal{B}_H(G)$

Define $N(H)$ to be the number of atoms of a monoid H. In this section we investigate $N(\mathcal{B}_H(G))$. Let G be a finite abelian group and let H be a subgroup. Since $\theta : \mathcal{B}_H(G) \to \mathcal{B}(G/H)$, as defined in Theorem 2.2, is a transfer homomorphism, lengths of factorizations of sequences in $\mathcal{B}_H(G)$ can be studied in the somewhat simpler structure $\mathcal{B}(G/H)$. When G is cyclic of order $n \geq 10$, the number of minimal zero-sum sequences in $\mathcal{B}(G)$ of length $k \geq 2n/3$ is $\phi(n)p_k(n)$ where ϕ is Euler's totient function and where $p_k(n)$ denotes the number of partitions of n into k parts [Ponomarenko 2004, Theorem 8]. Note that by recent work of Yuan [2007, Theorem 3.1] and Savchev and Chen [2007, Proposition 10], the inequality $k \geq 2n/3$ can be replaced by $k \geq \lfloor n/2 \rfloor + 2$ (see also [Geroldinger 2009, Corollary 7.9]). In general, there is no known formula for the number of atoms of $\mathcal{B}(G)$. However, given an enumeration of the atoms of $\mathcal{B}(G/H)$ we can calculate $N(\mathcal{B}_H(G))$ exactly, as the following example illustrates.

Example 1. Let G be a finite abelian group with a subgroup H of index 2. We will calculate $N(\mathcal{B}_H(G))$ as a function of $|H|$, the order of H. Write

$$G/H = \{H, g + H\}, \qquad \text{for some } g \in G \backslash H.$$

It is clear that

$$\mathcal{A}(\mathcal{B}(G/H)) = \{H, (g + H)^2\}.$$

From Theorem 2.2 we know that for each atom $\alpha \in \mathcal{B}_H(G)$, either $\alpha \in \theta^{-1}(H)$ or $\alpha \in \theta^{-1}\left((g + H)^2\right)$. In the first case $|\alpha| = 1$ and so $\alpha \in H$. In the second case, $\alpha = xy$ where $x, y \in g + H$, not necessarily distinct. To count the number of elements of this form, note that we are choosing two elements from the $|H|$ elements of the coset $g + H$. That is, there are $\binom{|H|+1}{2}$ elements in the preimage of $(g_1 + H)^2$. Therefore,

$$N(\mathcal{B}_H(G)) = |H| + \binom{|H| + 1}{2} = \frac{1}{2}|H|^2 + \frac{3}{2}|H|.$$

In the previous example, $N(\mathcal{B}_H(G))$ is a polynomial in $|H|$ with rational coefficients. We now give a series of results to establish this fact in general.

Theorem 3.1. Let G be a finite abelian group and let H be a subgroup of G. If $\alpha = \alpha_1^{t_1}\alpha_2^{t_2}\cdots\alpha_n^{t_n} \in \mathscr{B}(G/H)$ where $\alpha_i \neq \alpha_j$ whenever $i \neq j$ then

$$\left|\theta^{-1}(\alpha)\right| = \prod_{i=1}^{n}\binom{|H|+t_i-1}{t_i}.$$

Proof. Let

$$\alpha = (x_1+H)^{t_1}(x_2+H)^{t_2}\cdots(x_n+H)^{t_n}$$

be a sequence in $\mathscr{B}(G/H)$ where $x_i+H \neq x_j+H$ unless $i \neq j$. Each element of $\theta^{-1}(x_i+H)^{t_i}$ looks like $y_1y_2\cdots y_{t_i}$ where each $y_j \in x_i+H$. We wish to count the number of such elements in $\mathscr{F}(G)$. Since $\left|\theta^{-1}(x_i+H)\right| = |H|$, we have $|H|$ elements from which to choose. Then to find $\left|\theta^{-1}((x_i+H)^{t_i})\right|$, we choose t_i not necessarily distinct elements from x_i+H. Thus,

$$\left|\theta^{-1}((x_i+H)^{t_i})\right| = \binom{|H|+t_i-1}{t_i}.$$

Since each x_i+H is a distinct coset representative, the elements in the preimage of x_i+H are not in the preimage of any other coset. That is,

$$\theta^{-1}(x_i+H)\cap\theta^{-1}(x_j+H) = \varnothing,$$

whenever $i \neq j$. To find $\left|\theta^{-1}(\alpha)\right|$, we simply multiply, which yields

$$\left|\theta^{-1}(\alpha)\right| = \prod_{i=1}^{n}\binom{|H|+t_i-1}{t_i}. \qquad \square$$

Let $\alpha = \alpha_1^{t_1}\alpha_2^{t_2}\cdots\alpha_n^{t_n} \in \beta(G/H)$. We say that two sequences $\alpha_1^{t_1}\alpha_2^{t_2}\cdots\alpha_n^{t_n}$ and $\beta_1^{r_1}\beta_2^{r_2}\cdots\beta_n^{r_n} \in \mathscr{F}(G/H)$ are of *similar form* if

(1) $\alpha_i \neq \alpha_j$ when $i \neq j$,
(2) $\beta_k \neq \beta_l$ when $k \neq l$, and
(3) there exists some $\tau \in S_n$ such that $t_i = r_{\tau(i)}$ for all i.

As we see in the following corollary if α and β are sequences of similar form, then

$$\left|\theta^{-1}(\alpha)\right| = \left|\theta^{-1}(\beta)\right|.$$

Corollary 3.2. Let $\alpha = \alpha_1^{t_1}\alpha_2^{t_2}\cdots\alpha_n^{t_n}$ and $\beta = \beta_1^{r_1}\beta_2^{r_2}\cdots\beta_n^{r_n} \in \mathscr{F}(G/H)$ be of similar form. Then

$$\left|\theta^{-1}(\alpha)\right| = \left|\theta^{-1}(\beta)\right|.$$

Proof. By Theorem 3.1,

$$\left|\theta^{-1}(\alpha)\right| = \prod_{i=1}^{n}\binom{|H|+t_i-1}{t_i} \qquad \text{and} \qquad \left|\theta^{-1}(\beta)\right| = \prod_{i=1}^{n}\binom{|H|+r_i-1}{r_i}.$$

By assumption, there exists a $\tau \in S_n$ such that $t_i = r_{\tau(i)}$ for all i. Thus, after an appropriate reordering, $t_i = r_i$ for all i. Hence,

$$\left|\theta^{-1}(\alpha)\right| = \prod_{i=1}^{n} \binom{|H| + t_i - 1}{t_i} = \prod_{i=1}^{n} \binom{|H| + r_i - 1}{r_i} = \left|\theta^{-1}(\beta)\right|. \qquad \square$$

In Example 2, we will categorize the atoms of $\mathcal{B}(G/H)$ to make use of this corollary. We now give our main result. A polynomial $f \in \mathbb{Q}[X]$ is called *integer-valued* if $f(\mathbb{Z}) \subseteq \mathbb{Z}$, and we denote $\operatorname{Int}(\mathbb{Z}) \subset \mathbb{Q}[X]$ the set of integer-valued polynomials on $\mathbb{Z}$. It is well-known that the polynomials $\binom{X}{n}$ form a basis of the $\mathbb{Z}$-module $\operatorname{Int}(\mathbb{Z})$ (see [Cahen and Chabert 1997, Proposition I.1.1]).

Theorem 3.3. Let K be a finite abelian group. There exists an integer-valued polynomial $f \in \operatorname{Int}(\mathbb{Z})$ of degree $\deg(f) = \mathsf{D}(K)$ with the following property: if G is a finite abelian group and $H \subseteq G$ a subgroup with $G/H \cong K$, then

$$N(\mathcal{B}_H(G)) = f(|H|).$$

Proof. From Theorem 2.2 every atom of $\mathcal{B}_H(G)$ is in the preimage of an atom from $\mathcal{B}(G/H)$ under the transfer homomorphism $\theta : \mathcal{B}_H(G) \to \mathcal{B}(G/H)$. Let $A_1, A_2, \dots, A_m$ denote the atoms of $\mathcal{B}(G/H)$. Then

$$N(\mathcal{B}_H(G)) = \left|\theta^{-1}(A_1)\right| + \left|\theta^{-1}(A_2)\right| + \cdots + \left|\theta^{-1}(A_m)\right|$$

since the preimages $\theta^{-1}(A_i)$ are pairwise disjoint. From Theorem 3.1,

$$\left|\theta^{-1}(A_i)\right| = \prod_{i=1}^{n} \binom{|H| + t_i - 1}{t_i}$$

where $A_i = \alpha_1^{t_1}\alpha_2^{t_2}\cdots\alpha_n^{t_n}$. Since $\binom{|H|+t_i-1}{t_i}$ is a polynomial in terms of $|H|$, we know that $\prod_{i=1}^{n}\binom{|H|+t_i-1}{t_i}$ is a polynomial in terms of $|H|$. Thus,

$$N(\mathcal{B}_H(G)) = \left|\theta^{-1}(A_1)\right| + \left|\theta^{-1}(A_2)\right| + \cdots + \left|\theta^{-1}(A_m)\right|$$

is also a polynomial in terms of $|H|$. The definition of the Davenport constant implies that there exists an atom in $\mathcal{B}(G/H)$ with length $\mathsf{D}(G/H) = \mathsf{D}_H(G)$ and that no longer atom exists. Let $A_i = \alpha_1^{t_1}\alpha_2^{t_2}\cdots\alpha_n^{t_n} \in \mathcal{B}(G/H)$ such that $|A| = \mathsf{D}(G/H) = \mathsf{D}_H(G)$. Then

$$t_1 + t_2 + \cdots + t_n = \mathsf{D}_H(G).$$

Since

$$\binom{|H| + t_i - 1}{t_i} = \frac{(|H| + t_i - 1)(|H| + t_i - 2)\cdots|H|}{t_i}$$

is a polynomial in terms of $|H|$ of degree t_i, $\prod_{i=1}^{n} \binom{|H|+t_i-1}{t_i}$ has degree $\mathsf{D}_H(G)$. Since $\left|A_j\right| \leq \mathsf{D}_H(G)$ for all j, we have that

$$N(\mathcal{B}_H(G)) = \left|\theta^{-1}(A_1)\right| + \left|\theta^{-1}(A_2)\right| + \cdots + \left|\theta^{-1}(A_m)\right|,$$

which also has degree $\mathsf{D}_H(G)$. □

Remark 1. If $|H| = 1$, then $H = \{0\}$ and so $\mathcal{B}_H(G) = \mathcal{B}(G)$. In this case, $\left|\theta^{-1}(A_i)\right| = 1$ for all i and thus $N(\mathcal{B}_H(G)) = N(\mathcal{B}(G))$.

We conclude with a final example, which illustrates how much larger $\mathcal{A}(\mathcal{B}_H(G))$ is than $\mathcal{A}(\mathcal{B}(G/H))$.

Example 2. We calculate $N(\mathcal{B}_H(G))$ where $G/H \cong \mathbb{Z}/6\mathbb{Z} = \{0, 1, 2, 3, 4, 5\}$. Note that $\mathcal{A}(\mathcal{B}(\mathbb{Z}/6\mathbb{Z}))$ consists of the following twenty elements:

0	1^6	$1^4 2$	$1^3 3$	$1^2 2^2$	$1^2 4$	123
134^2	15	2^3	$2^2 35$	24	25^2	3^2
345	35^3	4^3	$4^2 5^2$	45^4	5^6	

For each sequence $\alpha \in \mathcal{A}(\mathcal{B}(G/H))$, we compute $\left|\theta^{-1}(\alpha)\right|$. Several pairs of atoms have similar forms and thus we can reduce the number of calculations by using Corollary 3.2. By applying Theorem 3.1 we obtain, for example:

$$\left|\theta^{-1}(3^2)\right| = \binom{|H|+1}{2} = \frac{1}{2}|H|^2 + \frac{1}{2}|H|,$$

$$\left|\theta^{-1}(123, 345)\right| = 2\binom{|H|}{1}^3 = 2|H|^3,$$

and

$$\left|\theta^{-1}(1^4 2, 5^4 4)\right| = 2\binom{|H|+3}{4}\binom{|H|}{1} = \frac{1}{12}|H|^5 + \frac{1}{2}|H|^4 + \frac{11}{12}|H|^3 + \frac{1}{2}|H|^2.$$

These and several similar calculations yield

$$N(\mathcal{B}_H(G)) = \frac{1}{360}|H|^6 + \frac{1}{8}|H|^5 + \frac{185}{72}|H|^4 + \frac{63}{8}|H|^3 + \frac{1247}{180}|H|^2 + \frac{5}{2}|H|.$$

Applying this formula to the case when $|H| = 1$, we find $N(\mathcal{B}_H(G)) = 20$. If $|H| = 10$, then $N(\mathcal{B}_H(G)) = 49,565$, illustrating how quickly $\mathcal{A}(\mathcal{B}_H(G))$ grows as a function of $|H|$.

Acknowledgement

The authors wish to thank the anonymous referee for many insightful comments that greatly improved this paper.

References

[Cahen and Chabert 1997] P.-J. Cahen and J.-L. Chabert, *Integer-valued polynomials*, vol. 48, Mathematical Surveys and Monographs, Am. Math. Soc., Providence, RI, 1997. MR 98a:13002

[Geroldinger 2009] A. Geroldinger, "Additive group theory and non-unique factorizations", in *Combinatorial Number Theory and Additive Group Theory*, edited by A. Geroldinger and I. Ruzsa, Birkhäuser, 2009.

[Geroldinger and Halter-Koch 2006] A. Geroldinger and F. Halter-Koch, *Non-unique factorizations*, vol. 278, Pure and Applied Mathematics (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2006. Algebraic, combinatorial and analytic theory. MR 2006k:20001 Zbl 1113.11002

[Halter-Koch 1992] F. Halter-Koch, "Relative block semigroups and their arithmetical applications", *Comment. Math. Univ. Carolin.* **33**:3 (1992), 373–381. MR 94a:11168 Zbl 0769.11038

[Ponomarenko 2004] V. Ponomarenko, "Minimal zero sequences of finite cyclic groups", *Integers* **4** (2004), A24, 6 pp. (electronic). MR 2005m:11024 Zbl 1083.11015

[Savchev and Chen 2007] S. Savchev and F. Chen, "Long zero-free sequences in finite cyclic groups", *Discrete Math.* **307**:22 (2007), 2671–2679. MR 2008m:11050

[Yuan 2007] P. Yuan, "On the index of minimal zero-sum sequences over finite cyclic groups", *J. Combin. Theory Ser. A* **114**:8 (2007), 1545–1551. MR 2008j:11147 Zbl 1128.11011

Received: 2008-09-15 Revised: 2008-11-10 Accepted: 2008-11-12

baeth@ucmo.edu *Mathematics and Computer Science, University of Central Missouri, Warrensburg, MO 64093, United States*

hoffmeier@ucmo.edu *Mathematics and Computer Science, University of Central Missouri, Warrensburg, MO 64093, United States*