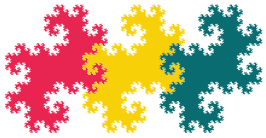
DOCTORAL PROGRAM
DISCRETE MATHEMATICS



TU & KFU GRAZ•MU LEOBEN
AUSTRIA

UNI GRAZ

Power monoids: A bridge between Factorization Theory and Arithmetic Combinatorics

Salvatore TRINGALI[(a),(b)]

University of Graz ∼ Heinrichstr. 36, 8010 Graz, AT

[(a)] Supported by FWF Project No. M1900-N39 — [(b)] Based on joint work with Yushuang FAN (Math. College, China Univ. of Geosciences ∼ Haidian Distr., Beijing, CN)

Combinatorics and Number Theory Meet ∼ HRI, Feb 22, 2017

Outline

Factorization Theory: What is it all about?

Factorization Theory (FT) investigates various phenomena arising from the non-uniqueness of factorizations in atomic monoids, and classify them by a variety of algebraic, arithmetic, or combinatorial invariants

It had its origins in algebraic NT, and was later extended to commutative (unital) rings and commutative monoids, with an emphasis on integral domains and cancellative, commutative monoids

- *D.D. Anderson & al.* (1980s): Integral domains and rings with zero-divisors
- *Chapman & Smith* (1993; 1998): Dedekind domains
- *Halter-Koch & Geroldinger* (1990s): Cancellative, commutative monoids
- *Halter-Koch* (1997): Transfer homomorphisms
- *100s of papers* (1990s-2016): In-depth study of several arithmetic invariants for various classes of monoids
- *Halter-Koch & Geroldinger* (2006): *Non-Unique Factorizations* is published
- *Geroldinger* (2016): "Sets of lengths" (AMM survey paper)

Why getting interested in power monoids?

Only in recent years, people have started considering more abstract settings, especially domains and (possibly) non-commutative, cancellative monoids (previous work didn't dig too deep into the subject)

A couple of reasons for this are, first, the many difficulties that one encounters when trying to extend the theory, *even in its most basic aspects*, to a non-commutative or non-cancellative setting, and secondly, the lack of sufficiently interesting examples

Things started changing a little bit with Smertnig's (J. Algebra, 2013) and Smertnig and Baeth's (J. Algebra, 2015) work on non-commutative, cancellative monoids (in fact, cancellative categories)

More recently, Fan, Geroldinger, Kainrath, and T. (J. Algebra Appl., 2017) have extended some aspects of FT to unit-cancellative, commutative monoids, and this paved the way to the generalization of FT to the non-commutative and non-cancellative setting, power monoids being one of the most significant examples (though not the only one) to motivate these further developments (arXiv:1701.09152)

Not enough?

Power monoids are, in disguise, one of the primary objects of study in Arithmetic Combinatorics (AC), a highly active area which has seen tremendous developments in recent years, expanding from the classical bases of additive number theory, where the focus is on the integers, to more abstract settings such as non-commutative groups and semigroups

There is actually more than a chance that AC can benefit from the interactions with FT offered by power monoids, much in the same way as the latter has, in its own right, drawn great benefits from the former

For one concrete example of the kind of interplay we are alluding to, let $(G, +)$ a finite group. A set $X \subseteq G$ is called primitive if $|X| \geq 2$ and there are not $A, B \subseteq G$ with $X = \{a + b : a \in A \text{ and } b \in B\}$ and $|A|, |B| \geq 2$. This is related to deep questions in AC (e.g., Ostmann's and Sárközy's conjectures, or work of Alon, Burgain, Gowers, Green, Tao, etc. on sum-product phenomena), and it turns out that X being primitive is the same as X being an atom in the power monoid of G

Another example comes from zero-sum theory (via the introduction of factorization systems and generalized Davenport constants...)

Outline

Basic notations and terminology

H: multiplicatively written monoid [= unital sgrp] with identity 1_H

$H^\times$: the set of units (or invertible elements) of H [$x \in H^\times$ iff $xy = yx = 1$ for some $y \in H$]

$x \simeq_H y$: x is associate to y (i.e., $x = uyv$ for some $u, v \in H^\times$)

$\mathcal{A}(H)$: the set of atoms (or irreducible elements) of H [$a \in \mathcal{A}(H)$ iff ($a \notin H^\times$ and $a = xy$ for some $x, y \in H \Rightarrow x \in H^\times$ or $y \in H^\times$)]

$\mathscr{F}^*(\mathscr{U})$: free monoid with basis $\mathscr{U}$ [whose operation we denote by $*$ and whose elements we call $\mathscr{U}$-words (or just words)]

$\|\mathfrak{z}\|_{\mathscr{U}}$: length of a word $\mathfrak{z} \in \mathscr{F}^*(\mathscr{U})$, given by $\sum_{z \in \mathscr{U}} \upsilon_z(\mathfrak{z})$, where $\upsilon_z(\mathfrak{z})$ is the number of z's appearing in $\mathfrak{z}$

π_H: unique homomorphism $\mathscr{F}^*(H) \to H$ s.t. $\pi_H(x) = x$ for all $x \in H$

$\mathscr{C}_H$: smallest congruence on $\mathscr{F}^*(\mathcal{A}(H))$ s.t. if $\mathfrak{a} = a_1 * \cdots * a_m$ and $\mathfrak{b} = b_1 * \cdots * b_n$, then $(\mathfrak{a}, \mathfrak{b}) \in \mathscr{C}_H$ iff $\pi_H(\mathfrak{a}) = \pi_H(\mathfrak{b})$, $m = n$, and there is a permutation $\sigma \in \mathfrak{S}_n$ s.t. $b_{\sigma(i)} \simeq_H a_i$ for each i

Factorizations and sets of lengths

We call $\mathsf{Z}(H) := \mathscr{F}^*(\mathcal{A}(H))/\mathscr{C}_H$ the factorization monoid of H and set

$$\mathsf{Z}_H(x) := \left\{ [\![\mathfrak{a}]\!]_{\mathscr{C}_H} : \mathfrak{a} \in \mathscr{F}^*(\mathcal{A}(H)) \text{ and } \pi_H(\mathfrak{a}) = x \right\} \subseteq \mathsf{Z}(H)$$

(we use $[\![\cdot]\!]_{\mathscr{C}_H}$ to denote a congruence class) and

$$\mathscr{Z}_H(x) := \pi_H^{-1}(x) = \bigcup \mathsf{Z}_H(x) \subseteq \mathscr{F}^*(\mathcal{A}(H))$$

We refer to the elements of $\mathscr{Z}_H(x)$ as the factorizations of x and to the elements of $\mathsf{Z}_H(x)$ as the factorization classes of x, and we let

$$\mathsf{L}_H(x) = \left\{ \|\mathfrak{a}\|_H : \mathfrak{a} \in \mathscr{Z}_H(x) \right\} \subseteq \mathbf{N},$$

which we call the set of lengths of x (relative to H)

It is not difficult to show that $\mathsf{L}_H(1_H) = \{0\}$ and $\mathsf{L}_H(u) = \emptyset$ for every $u \in H^\times \setminus \{1_H\}$ [differently from the classical approach...]

H is said to be atomic iff $\mathsf{L}_H(x) \neq \emptyset$ for every $x \in H \setminus H^\times$, and BF iff it is atomic and $|\mathsf{L}_H(x)| < \infty$ for all $x \in H$

Unions of sets of lengths and distances

We define the system of sets of lengths of H by

$$\mathscr{L}(H) := \{\mathsf{L}_H(x) : x \in H\} \subseteq \mathcal{P}(\mathbf{N}),$$

and for every $k \in \mathbf{N}$ we let

$$\mathscr{U}_k(H) := \bigcup_{L \in \mathscr{L}(H) : k \in L} L \subseteq \mathbf{N}$$

Given $L \subseteq \mathbf{Z}$ and $d \in \mathbf{N}^+$, we say that d is a distance of L if

$$L \cap [\![\ell, \ell + d]\!] = \{\ell, \ell + d\} \quad \text{for some } \ell \in \mathbf{Z},$$

and we denote by $\Delta(L)$ the set of distances of (the set) L. Accordingly,

$$\Delta(H) := \bigcup_{L \in \mathscr{L}(H)} \Delta(L) \subseteq \mathbf{N}^+$$

is called the delta set of (the monoid) H

The distance function

Set $\mathcal{A}^*(H) := \big\{[\![a]\!]_{\mathscr{C}_H} : a \in \mathcal{A}(H)\big\}$. Given $\mathfrak{A} \in \mathcal{A}^*(H)$ and $\mathfrak{z} \in \mathscr{F}^*(H)$, we let

$$\mathsf{v}_H(\mathfrak{z};\mathfrak{A}) := \begin{cases} \big|\{i \in [\![1,n]\!] : z_i \in \mathfrak{A}\}\big| & \text{if } n := \|\mathfrak{z}\|_H \geq 1 \text{ and } \mathfrak{z} = z_1 * \cdots * z_n \\ 0 & \text{otherwise} \end{cases}$$

It is not difficult to see that

$$\|\mathfrak{z}\|_H = \sum\nolimits_{\mathfrak{A} \in \mathcal{A}^*(H)} \mathsf{v}_H(\mathfrak{z};\mathfrak{A}), \quad \text{for every } \mathfrak{z} \in \mathscr{F}^*(\mathcal{A}(H)) \tag{1}$$

Then, for all $\mathfrak{a}, \mathfrak{b} \in \mathscr{F}^*(\mathcal{A}(H))$ we take

$$\delta_H(\mathfrak{a},\mathfrak{b}) := \begin{cases} 0 & \text{if } \pi_H(\mathfrak{a}) = \pi_H(\mathfrak{b}) \\ \frac{1}{2} & \text{otherwise} \end{cases}$$

and

$$\mathfrak{a} \wedge_H \mathfrak{b} := \max\big(\|\mathfrak{a}\|_H, \|\mathfrak{b}\|_H\big) - \sum\nolimits_{\mathfrak{A} \in \mathcal{A}^*(H)} \min(\mathsf{v}_H(\mathfrak{a};\mathfrak{A}), \mathsf{v}_H(\mathfrak{b};\mathfrak{A}))$$

Lastly, we take the matching distance of H to be the function

$$\mathsf{d}_H : \mathscr{F}^*(\mathcal{A}(H)) \times \mathscr{F}^*(\mathcal{A}(H)) \to \mathbf{R} : (\mathfrak{a},\mathfrak{b}) \mapsto \max(\delta_H(\mathfrak{a},\mathfrak{b}), \mathfrak{a} \wedge_H \mathfrak{b})$$

The catenary set

We let the catenary degree of an element $x \in H$, which we denote by $\mathsf{c}_H(x)$, be the infimum of the set of integers $d \in \mathbf{N}$ s.t.:

- For all $\mathfrak{a}, \mathfrak{b} \in \mathscr{Z}_H(x)$ there are determined $\mathfrak{c}_0, \dots, \mathfrak{c}_n \in \mathscr{Z}_H(x)$ with $\mathfrak{c}_0 = \mathfrak{a}$ and $\mathfrak{c}_n = \mathfrak{b}$ s.t. $\mathsf{d}_H(\mathfrak{c}_{i-1}, \mathfrak{c}_i) \le d$ for every $i \in [\![1, n]\!]$

It is seen that $\mathsf{c}_H(x) = 0$, for a given $x \in H$, iff $|\mathsf{Z}_H(x)| \le 1$. Thus, we let

$$\mathsf{Ca}(H) := \{\mathsf{c}_H(x) : x \in H\} \setminus \{0\} \subseteq \mathbf{N}^+ \cup \{\infty\}$$

(We assume $\inf \emptyset := \infty$.) We call $\mathsf{Ca}(H)$ the catenary set of H. It is clear that $\mathsf{Ca}(H) \subseteq \mathbf{N}^+$ if H is a BF-monoid, but this is not true in general

It can be shown that if H is commutative and cancellative, then $\mathsf{c}_H(x) = \mathsf{c}_{\mathrm{GeH}}(x)$ for every $x \in H$, where $\mathsf{c}_{\mathrm{GeH}}(x)$ denotes the "classical" catenary degree (Definition 1.6.1.2 in Geroldinger & Halter-Koch's book)

Transfer principles

The kind of arithmetic properties in which we are interested are often proved by reduction to suitable families of (atomic) monoids

This is achieved by means of *transfer techniques*, as per Halter-Koch's notion of transfer hom (commutative & cancellative monoids) or Baeth and Smertnig's notion of weak transfer hom (cancellative monoids)

Specifically, let H and K be multiplicatively written monoids, and let φ a hom $H \to K$. We denote by φ^* the unique hom $\mathscr{F}^*(H) \to \mathscr{F}^*(K)$ s.t. $\varphi^*(x) = \varphi(x)$ for all $x \in H$, and we refer to φ as an equimorphism if:

(E1) $\varphi(x) = 1_{\boldsymbol{K}}$ for some $x \in H$ only if $x \in H^\times$, that is, $\varphi^{-1}(1_{\boldsymbol{K}}) \subseteq H^\times$

(E2) φ is atom-preserving, i.e., $\varphi(a) \in \mathcal{A}(K)$ for all $a \in \mathcal{A}(H)$

(E3) If $x \in H \setminus \{1_{\boldsymbol{H}}\}$ and $\mathfrak{b} \in \mathscr{Z}_{\boldsymbol{K}}(\varphi(x)) \neq \emptyset$, then $\varphi^*(\mathfrak{a}) \in [\![\mathfrak{b}]\!]_{\mathscr{C}_{\boldsymbol{K}}}$ for some $\mathfrak{a} \in \mathscr{Z}_{\boldsymbol{H}}(x)$

We call φ a weak transfer homomorphism (WTH) if (a) it satisfies (E2) and (E3) and (b) $K = K^\times \varphi(H) K^\times$ and $\varphi^{-1}(K^\times) = H^\times$

H is equimorphic to K if there is an equimorphism $H \to K$, and is a transfer Krull monoid if there is a WTH from H to a monoid of zero-sum sequences over an abelian group G with support in $G_0 \subseteq G$

Outline

A couple of transfer results

A submonoid M of H is said to be *divisor-closed* if $x \in M$ whenever $x \mid_H y$ (i.e., $y = uxv$ for some $u, v \in H$) and $y \in M$. Divisor-closed embeddings preserve lengths, factorizations, and the catenary degree

Proposition 1

Let H be a monoid, and assume M is a divisor-closed submonoid of H. Then $M^\times = H^\times$ and $\mathcal{A}(M) = \mathcal{A}(H) \cap M$. In addition, $\mathsf{L}_M(x) = \mathsf{L}_H(x)$, $\mathsf{Z}_M(x) = \mathsf{Z}_H(x)$, and $\mathsf{c}_M(x) = \mathsf{c}_H(x)$ for all $x \in M$, and consequently $\mathscr{L}(M) \subseteq \mathscr{L}(H)$, $\Delta(M) \subseteq \Delta(H)$, and $\mathrm{Ca}(M) \subseteq \mathrm{Ca}(H)$.

In turn, equimorphisms preserve lengths and decrease the catenary degree

Proposition 2

Let H and K be monoids, and $\varphi : H \to K$ an equimorphism. Then:

(i) $\mathsf{L}_H(x) = \mathsf{L}_K(\varphi(x))$ *for every* $x \in H \setminus H^\times$.

(ii) $\mathsf{c}_K(\varphi(x)) \le \mathsf{c}_H(x)$ *for all* $x \in H$.

In particular, $\mathscr{L}(H) \subseteq \mathscr{L}(K)$ and $\Delta(H) \subseteq \Delta(K)$.

A pseudo-philosophical remark

The *use* we are going to make of transfer techniques is a little bit unconventional, which could result into confusion. So it is perhaps worth trying to put things in perspective

Roughly, the idea behind the introduction of transfer techniques in factorization theory can be outlined as follows: We have a monoid hom $\varphi : H \to K$ of some special kind, and we want to investigate certain properties of one of H or K by looking at corresponding properties of the other. To this end, we use φ to shift information from H to K, which is what we do here with equimorphisms, if H is, in a sense, easier to understand than K, or pull it back from K to H, as is normally the case with weak transfer homomorphisms, if it is the other way around

But the "change of philosophy" stemming from the *use* we are making of transfer techniques has little or nothing to do with their deep meaning or, for example, with the definitions of equimorphism and weak transfer homomorphism we are giving

Seeking a criterion for atomicity and BF-ness, I

We call H unit-cancellative (resp., strongly unit-cancellative) provided that $xy = x$ or $yx = x$ for some $x, y \in H$ only if $y \in H^\times$ (resp., $y = 1_H$)

We say that H satisfies:

- the ascending chain condition (shortly, ACC) on principal right (resp., left) ideals if, for every sequence $(a_n)_{n\geq 1}$ of elements of H s.t. $a_nH \subseteq a_{n+1}H$ (resp., $Ha_n \subseteq Ha_{n+1}$) for all $n \in \mathbf{N}^+$, there exists an index $\nu \in \mathbf{N}^+$ with the property that $a_nH = a_\nu H$ (resp., $Ha_n = Ha_\nu$) for every $n \geq \nu$;
- the ascending chain condition on principal ideals (shortly, ACCP) if it satisfies the ACC on both principal right and principal left ideals.

Lastly, we let a fnc $\lambda : H \to \mathbf{N}$ be a length function on H if $\lambda(x) < \lambda(y)$ for all $x, y \in H$ s.t. $y = uxv$ for some $u, v \in H$ with $u \notin H^\times$ or $v \notin H^\times$

E.g., an order in an algebraic number field (in particular, the ring of integers of an algebraic number field) has a length fnc

Seeking a criterion for atomicity and BF-ness, II

The ACCP implies atomicity in various classes of *cancellative* monoids. This carries over to unit-cancellative monoids

Theorem 1

Let M be a submonoid of H with $M^\times = M \cap H^\times$. The following hold:

(i) *If H is unit-cancellative and satisfies the* ACCP*, then it is atomic*

(ii) *If H is unit-cancellative, then so is M*

(iii) *If H has a length function, then H satisfies the* ACCP

(iv) *If H has a length function and is unit-cancellative, then M is a* BF*-monoid*

Corollary

Let H be unit-cancellative. Then H is a BF*-monoid iff has a length fnc*

Outline

Introducing power monoids

Let H be a multiplicatively written monoid and $\mathcal{P}_{\text{fin}}(H)$ the set of all *non-empty* finite subsets of H. We denote by $\cdot$ the binary operation

$$\mathcal{P}_{\text{fin}}(H) \times \mathcal{P}_{\text{fin}}(H) \to \mathcal{P}_{\text{fin}}(H) : (X, Y) \mapsto XY,$$

where $XY := X \cdot Y := \{xy : (x, y) \in X \times Y\}$, and we define

$$\mathcal{P}_{\text{fin},1}(H) := \{X \in \mathcal{P}_{\text{fin}}(H) : X \cap H^\times \neq \emptyset\}.$$

It is trivial that $\mathcal{P}_{\text{fin}}(H)$, endowed with the above operation, forms a monoid with identity $\{1_H\}$, and $\mathcal{P}_{\text{fin},1}(H)$ is a submonoid of $\mathcal{P}_{\text{fin}}(H)$

Accordingly, we call $\mathcal{P}_{\text{fin}}(H)$ and $\mathcal{P}_{\text{fin},1}(H)$, respectively, the power monoid and restricted power monoid of H

Proposition

$\mathcal{P}_{\text{fin}}(H)$ [*respectively,* $\mathcal{P}_{\text{fin},1}(H)$] *is cancellative iff* $H = \{1_H\}$

So, the study of power monoids is, except for trivial cases, entirely beyond the scope of the factorization theory of *cancellative* monoids

Making it smoother

The next result suggests that the arithmetic of $\mathcal{P}_{\text{fin}}(H)$ and $\mathcal{P}_{\text{fin},1}(H)$ is "smoother" when H is Dedekind-finite (i.e., $xy = 1_H$ iff $yx = 1_H$)

Proposition 3

(i) *Every unit-cancellative monoid is Dedekind-finite.*

(ii) $\big\{\{u\} : u \in H^\times\big\} \subseteq \mathcal{P}_{\text{fin}}(H)^\times$, *and the inclusion is an equality if H is Dedekind-finite.*

(iii) *Assume that H is Dedekind-finite (respectively, strongly unit-cancellative) and fix $a \in H$. Then $\{a\} \in \mathcal{A}(\mathcal{P}_{\text{fin}}(H))$ only if (respectively, iff) $a \in \mathcal{A}(H)$.*

(iv) *If H is Dedekind-finite, then $\mathcal{P}_{\text{fin},1}(H)$ is a divisor-closed submonoid of $\mathcal{P}_{\text{fin}}(H)$. In particular, $\mathcal{P}_{\text{fin},1}(H)^\times = \big\{\{u\} : u \in H^\times\big\}$, $\mathscr{L}(\mathcal{P}_{\text{fin},1}(H)) \subseteq \mathscr{L}(\mathcal{P}_{\text{fin}}(H))$, and $\mathsf{Ca}(\mathcal{P}_{\text{fin},1}(H)) \subseteq \mathsf{Ca}(\mathcal{P}_{\text{fin}}(H))$.*

Keeping the above in mind, we look for (natural) sufficient conditions to guarantee that $\mathcal{P}_{\text{fin}}(H)$ [respectively, $\mathcal{P}_{\text{fin},1}(H)$] is a BF-monoid

BF-ness of power monoids

$\mathcal{P}_{\text{fin}}(H)$ and $\mathcal{P}_{\text{fin},1}(H)$ need not be unit-cancellative or atomic. However:

Proposition

Suppose there exists a total order $\preceq$ on H s.t. $xz \prec yz$ and $zx \prec zy$ for all $x, y, z \in H$ with $x \prec y$ [we say that H is a linearly orderable monoid (LOM) and $(H, \preceq)$ is a linearly ordered monoid]. Then $\mathcal{P}(H)$ is strongly unit-cancellative

This result, together with Theorem 1 and Proposition 1, yields:

Proposition 4

Let H be a linearly orderable monoid. The following hold:

(i) *$\mathcal{P}_{\text{fin},1}(H)$ is a* BF*-monoid*

(ii) *$\mathcal{P}_{\text{fin}}(H)$ is a* BF*-monoid iff so is H*

Proof. As for (i) and the "if" part of (ii), show that $\mathcal{P}_{\text{fin},\mathbf{1}}(H) \to \mathbf{N} : X \mapsto |X| - 1$ and $\mathcal{P}_{\text{fin}}(H) \to \mathbf{N} : X \mapsto |X| + \sup \mathsf{L}_{\boldsymbol{H}}(X^\circ) - 1$ are length fncs, where $X^\circ \in H$ is the max of the (finite) set X wrt an order $\preceq$ s.t. $(H, \preceq)$ is a lin. ordered monoid [we assume $\sup \emptyset := 0$] ■

Linearly orderable monoids: Examples

Trivial examples:

- The additive group of the real field is a linearly orderable group (LOG)
- Every submonoid of an LOM is still a LOM, and the same is true of any direct product (either finite or infinite) of LOMs

Non-trivial examples:

- abelian torsion-free groups are LOGS [F.W. Levi, Rend. Circ. Mat. Palermo 1913]
- torsion-free nilpotent groups are LOGs, see [Iwasawa, J. Math. Soc. Japan 1948], [Mal'tsev, Izv. Akad. Nauk. SSSR Ser. Mat. 1948], and [B.H. Neumann, Amer. J. Math. 1949]
- *Pure* braid groups are LOGs [Rolfsen & Zhu, J. Knot Theory Ramifications 1998]
- Free groups are LOGs [Iwasawa, J. Math. Soc. Japan 1948]
- Matrix monoids, multiplicative monoids of semigroup rings, and semi-direct products of groups are *sometimes* LOMs [T., Sgrp Forum 2015] and [Plagne & T., Comm. Algebra 2016]

Shifting to $(\mathbf{N}, +)$

Let $\mathcal{P}_{\text{fin},0}(\mathbf{N})$ denote the restricted power monoid of $(\mathbf{N}, +)$

Because $(\mathbf{N}, +)$ is a linearly orderable, reduced, commutative monoid, we have by Proposition 4 that $\mathcal{P}_{\text{fin},0}(\mathbf{N})$ is a strongly unit-cancellative, reduced, commutative BF-monoid, where the identity is $\{0\} \subseteq \mathbf{N}$

With this in mind, we show how to shift the arithmetic of $\mathcal{P}_{\text{fin},1}(H)$, under suitable assumptions on H, to $\mathcal{P}_{\text{fin},0}(\mathbf{N})$

Theorem 2

Assume H is a Dedekind-finite, aperiodic monoid. Then there exists a (monoid) monomorphism $\Phi : \mathcal{P}_{\text{fin},0}(\mathbf{N}) \to \mathcal{P}_{\text{fin},1}(H)$ for which:

(C) *Given $X \in \mathcal{P}_{\text{fin},0}(\mathbf{N})$ and $Y_1, \dots, Y_n \in \mathcal{P}_{\text{fin},1}(H)$ such that $\Phi(X) = Y_1 \cdots Y_n$, there are determined $X_1, \dots, X_n \in \mathcal{P}_{\text{fin},0}(\mathbf{N})$ with $\Phi(X_i) \simeq_{\mathcal{P}_{\text{fin},\mathbf{1}}(H)} Y_i$ for every $i \in [\![1, n]\!]$ and $X = X_1 + \cdots + X_n$*

In particular, Φ is an injective equimorphism, and hence we have that $\mathsf{L}_{\mathcal{P}_{\text{fin},\mathbf{0}}(\mathbf{N})}(X) = \mathsf{L}_{\mathcal{P}_{\text{fin},\mathbf{1}}(H)}(\Phi(X))$ and $\mathsf{c}_{\mathcal{P}_{\text{fin},\mathbf{1}}(H)}(\Phi(X)) \le \mathsf{c}_{\mathcal{P}_{\text{fin},\mathbf{0}}(\mathbf{N})}(X)$ for every $X \in \mathcal{P}_{\text{fin},0}(\mathbf{N})$

Proof of Theorem 3 (sketch)

Using that H is aperiodic, fix $x_0 \in H$ with $\mathrm{ord}(x_0) = \infty$, and denote by ϕ the unique hom $(\mathbf{N}, +) \to H$ for which $\phi(1) = x_0$. Of course, ϕ is a mono, and lifts to a mono $\Phi : \mathcal{P}_{\mathrm{fin},\mathbf{0}}(\mathbf{N}) \to \mathcal{P}_{\mathrm{fin},\mathbf{1}}(H)$ by taking $\Phi(X) := \{\phi(x) : x \in X\}$ for every $X \in \mathcal{P}_{\mathrm{fin},\mathbf{0}}(\mathbf{N})$

As for condition (**C**), let $X \in \mathcal{P}_{\mathrm{fin},\mathbf{0}}(\mathbf{N})$ and $Y_1, \ldots, Y_n \in \mathcal{P}_{\mathrm{fin},\mathbf{1}}(H)$ s.t. $\Phi(X) = Y_1 \cdots Y_n$. Since $0 \in X$ and ϕ is a hom, there exist $u_1 \in Y_1, \ldots, u_n \in Y_n$ with $u_1 \cdots u_n = \phi(0) = 1_H$, and Dedekind-finiteness implies that $u_1, \ldots, u_n \in H^\times$. For every $i \in [\![1, n]\!]$ set

$$Y_i' := u_0 \cdots u_{i-1} Y_i u_i^{-1} \cdots u_1^{-1},$$

where $u_0 := 1_H$. Then

$$\Phi(X) = Y_1' \cdots Y_n' \quad \text{and} \quad Y_1' \simeq_{\mathcal{P}_{\mathrm{fin},\mathbf{1}}(H)} Y_1, \ldots, Y_n' \simeq_{\mathcal{P}_{\mathrm{fin},\mathbf{1}}(H)} Y_n$$

Moreover, $1_H \in \bigcap_{i=1}^n Y_i'$, with the result that $Y_1', \ldots, Y_n' \subseteq \Phi(X)$. But this means, by the injectivity of Φ, that there exist $X_1, \ldots, X_n \in \mathcal{P}(X)$ with $\Phi(X_i) = Y_i' \simeq_{\mathcal{P}_{\mathrm{fin},\mathbf{1}}(H)} Y_i$ and $0 \in X_i$ for all $i \in [\![1, n]\!]$. Since Φ is a mono, it follows that $\Phi(X) = \Phi(X_1 + \cdots + X_n)$, and hence $X = X_1 + \cdots + X_n$, which proves that Φ satisfies condition (**C**)

We are left to show that Φ is an equimorphism, as all the rest will follow from Proposition 2. Actually, it is clear from the above that Φ satisfies conditions (E1) and (E3). Therefore, it will be enough to prove that Φ is atom-preserving. To this end, let $A \in \mathcal{A}(\mathcal{P}_{\mathrm{fin},\mathbf{0}}(\mathbf{N}))$.

The proof that $\Phi(A) = X'Y'$ for some $X', Y' \in \mathcal{P}_{\mathrm{fin},\mathbf{1}}(H)$ only if X' and Y' belongs to $\mathcal{P}_{\mathrm{fin},\mathbf{1}}(H)^\times$ is a consequence of condition (**C**) (we skip details). On the other hand, suppose for a contradiction that $\Phi(A) \in \mathcal{P}_{\mathrm{fin},\mathbf{1}}(H)^\times$. Then, we have by Proposition 3(iii) and the Dedekind-finiteness of H that $|\Phi(A)| = 1$. So $|A| = 1$, and hence $A = \{0\}$. A contradiction. ∎

Main result

Theorem 3

Let H be a Dedekind-finite, aperiodic monoid. We have that:

(i) $\mathscr{L}(\mathcal{P}_{\text{fin}}(H)) \supseteq \mathscr{L}(\mathcal{P}_{\text{fin},1}(H)) \supseteq \mathscr{L}(\mathcal{P}_{\text{fin},0}(\mathbf{N}))$

(ii) $\mathscr{U}_k(\mathcal{P}_{\text{fin}}(H)) = \mathscr{U}_k(\mathcal{P}_{\text{fin},1}(H)) = \mathscr{U}_k(\mathcal{P}_{\text{fin},0}(\mathbf{N})) = \mathbf{N}_{\ge 2}$ *for* $k \ge 2$

(iii) $\Delta(\mathcal{P}_{\text{fin}}(H)) = \Delta(\mathcal{P}_{\text{fin},1}(H)) = \Delta(\mathcal{P}_{\text{fin},0}(\mathbf{N})) = \mathbf{N}^+$

(iv) $\mathsf{Ca}(\mathcal{P}_{\text{fin}}(H)) \supseteq \mathsf{Ca}(\mathcal{P}_{\text{fin},1}(H)) \supseteq \mathsf{Ca}(\mathcal{P}_{\text{fin},0}(\mathbf{N})) = \mathbf{N}^+$

In particular, if H is a linearly orderable BF-monoid, then the inclusions of point (iv) *are equalities*

Note that (ii)-(iv) in Theorem 3 are *independent* results, and none of them can be derived by means of "standard transfer techniques":

Proposition

Let H be a Dedekind-finite, aperiodic monoid. Then neither $\mathcal{P}_{\text{fin}}(H)$ nor $\mathcal{P}_{\text{fin},1}(H)$ is equimorphic to a cancellative monoid (in particular, neither is a transfer Krull monoid)

Outline

Seeking atoms

Theorem 3 depends on Theorem 2 and the fact that it is actually possible to determine the $\mathscr{U}_k$'s, the delta set, and the catenary set of $\mathcal{P}_{\text{fin},0}(\mathbf{N})$. For this, we first need to prove that suitable $X \in \mathcal{P}_{\text{fin},0}(\mathbf{N})$ are atoms

Proposition 5

Assume H is a LOM*, and let $X \in \mathcal{P}_{\text{fin},1}(H)$ s.t. $2 \le |X| \le 3$. Then $X \notin \mathcal{A}(\mathcal{P}_{\text{fin},1}(H))$ iff there exist $x, z \in H^\times$ and $y \in H \setminus \{1_H\}$ with $xy = yx$ s.t. $z^{-1}X = \{x, xy, xy^2\}$ or $Xz^{-1} = \{x, xy, xy^2\}$*

Proposition 6

Let $d, n, q \in \mathbf{N}^+$ with $d \ge nq + 1$, and let A be a non-empty finite set of integers $\ge nq + 1$ s.t. $a \equiv b \bmod d$ for all $a, b \in A$. Then $\left(q \cdot [\![0, n]\!]\right) \cup A$ is not an atom of $\mathcal{P}_{\text{fin},0}(\mathbf{N})$ iff $A = \{(n + k)q\}$ for some $k \in [\![1, \lceil n/2 \rceil]\!]$

Proposition 7

Let $A \in \mathcal{P}_{\text{fin},0}(\mathbf{N})$ and $b, q \in \mathbf{N}^+$ be such that $A \subseteq q \cdot \mathbf{N}$, but $q \nmid b$. Then $A \cup \{b\} \notin \mathcal{A}(\mathcal{P}_{\text{fin},0}(\mathbf{N}))$ if and only if $A = \{0, 2b\}$

Unions of sets of lengths

Proposition 8

$\mathsf{L}(\llbracket 0, n \rrbracket) = \llbracket 2, n \rrbracket$ *for every* $n \ge 2$

Proof. We have already observed that $\mathcal{P}_{\text{fin},\mathbf{0}}(\mathbf{N})$ is a reduced BF-monoid. So the claim is trivial if $n = 2$, because $\llbracket 0, 2 \rrbracket = X + Y$ for some $X, Y \subseteq \mathcal{P}_{\text{fin},\mathbf{0}}(\mathbf{N}) \setminus \{\{0\}\}$ only if $X = Y = \{0, 1\}$, and $\{0, 1\}$ is an atom (e.g., by Proposition 5)

Accordingly, suppose the claim is true for a fixed $n \ge 2$. Since $\llbracket 0, n+1 \rrbracket = \llbracket 0, 1 \rrbracket + \llbracket 0, n \rrbracket$ and $\mathsf{L}(X) + \mathsf{L}(Y) \subseteq \mathsf{L}(X + Y)$ for all $X, Y \in \mathcal{P}_{\text{fin},\mathbf{0}}(\mathbf{N})$, it follows that

$$\mathsf{L}(\llbracket 0, n+1 \rrbracket) \supseteq 1 + \mathsf{L}(\llbracket 0, n \rrbracket) = \llbracket 3, n+1 \rrbracket \tag{2}$$

On the other hand, let $A := \{k \in \llbracket 2, n \rrbracket : k \equiv n \bmod 2\}$, and set $B := \{0, 2\}$ if $n = 2$ and $B := \{0, 1\} \cup A$ otherwise. Then B is an atom by Propositions 5 and 6 (apply the latter with $d = 2$ and $\ell = q = 1$), and we have $\llbracket 0, n+1 \rrbracket = \{0, 1\} + B$, which implies, together with (2), that $\llbracket 2, n+1 \rrbracket \subseteq \mathsf{L}(\llbracket 0, n+1 \rrbracket)$

We are left to show that $\max \mathsf{L}(\llbracket 0, n+1 \rrbracket) \le n+1$. But this is simple, since if

$$\llbracket 0, n+1 \rrbracket = X_{\mathbf{1}} + \cdots + X_{\boldsymbol{k}}$$

for some $X_{\mathbf{1}}, \ldots, X_{\boldsymbol{k}} \in \mathcal{P}_{\text{fin},\mathbf{0}}(\mathbf{N}) \setminus \{\{0\}\}$, then $n + 1 = \max X_{\mathbf{1}} + \cdots + \max X_{\boldsymbol{k}} \ge k$ ∎

Corollary

$\mathscr{U}_k(\mathcal{P}_{\text{fin},0}(\mathbf{N})) = \mathbf{N}_{\ge 2}$ *for every integer* $k \ge 2$

The key lemma

Lemma

Let $u_1, \dots, u_{n+1} \in \mathbf{N}^+$ *be given so that*

(a) $u_1 + \cdots + u_n \leq u_{n+1} - u_n$,

(b) $2u_n \neq u_{n+1}$, *and*

(c) $u_1 + \cdots + u_i < \frac{1}{2} u_{i+1}$ *for all* $i \in [\![1, n-1]\!]$.

Next, let $X, Y \in \mathcal{P}_{\mathrm{fin},0}(\mathbf{N})$ *s.t.* $\{0, u_1\} + \cdots + \{0, u_{n+1}\} = X + Y$, *and set* $I_X := \{i \in [\![1, n+1]\!] : u_i \in X\}$ *and* $I_Y := \{i \in [\![1, n+1]\!] : u_i \in Y\}$

The following hold:

(i) $[\![1, n+1]\!] = I_X \uplus I_Y$

(ii) $X \setminus \sum_{i \in I_X} \{0, u_i\}, Y \setminus \sum_{i \in I_Y} \{0, u_i\} \subseteq \{u_1 + \cdots + u_n\}$

(iii) *if* $X \neq \sum_{i \in I_X} \{0, u_i\}$ *or* $Y \neq \sum_{i \in I_Y} \{0, u_i\}$, *then* $n \geq 2$, $u_1 + \cdots + u_n = u_{n+1} - u_n$, *and one of* X *and* Y *is equal to* $\{0, u_n\}$

Proof. Completely elementary, but quite intricate ■

The final step (modulo a couple more lemmas)

Proposition 9

Let $n \in \mathbf{N}_{\ge 2}$, *and let* $u_1, \dots, u_{n+1} \in \mathbf{N}^+$ *such that*

(a) $u_1 \equiv \cdots \equiv u_{n-1} \equiv 0 \bmod 2$ *and* $u_n \equiv 1 \bmod 2$,

(b) $u_1 + \cdots + u_n = u_{n+1} - u_n$, *and*

(c) $u_1 + \cdots + u_i < \frac{1}{2} u_{i+1}$ *for every* $i \in [\![1, n-1]\!]$

Set $V := \{0, u_1\} + \cdots + \{0, u_{n+1}\}$ *and*

$$A' := \left\{ \sum_{i \in I} u_i : I \subseteq [\![1, n+1]\!] \smallsetminus \{n\} \right\}$$

Then the following hold:

(i) $A'' := \{u_1 + \cdots + u_n\} \cup A' \in \mathcal{A}(\mathcal{P}_{\mathrm{fin},0}(\mathbf{N}))$ *and* $A'' \neq \{0, u_i\}$ *for every* $i \in [\![1, n+1]\!]$

(ii) $\mathsf{Z}(V) = \{\{0, u_n\} * A'', \{0, u_1\} * \cdots * \{0, u_{n+1}\}\}$

In particular, $\mathsf{L}(V) = \{2, n+1\}$, $\Delta(V) = \{n-1\}$, *and* $\mathsf{c}(V) = \{n\}$

Outline

Some open questions

(1) Let $X \in \mathcal{P}_{\text{fin},0}(\mathbf{N})$. Prove or disprove that there are determined $A, B \in \mathcal{A}(\mathcal{P}_{\text{fin},0}(\mathbf{N}))$ s.t. $A \neq B$ and $X + A = X + B$ (resp., $X \neq A$ and $X + B = A + B$)

(2) Prove that $\mathscr{L}(\mathcal{P}_{\text{fin},0}(\mathbf{N})) = \big\{\{0\}, \{1\}\big\} \cup \mathcal{P}_{\text{fin}}(\mathbf{N}_{\ge 2})$

(3) Given $n \in \mathbf{N}_{\ge 2}$ and an n-element subset $L = \{\ell_1, \dots, \ell_n\}$ of $\mathbf{N}_{\ge 2}$, what about the set of n-tuple $(m_1, \dots, m_n)$ of positive integers for which there exists $X \in \mathcal{P}_{\text{fin},0}(\mathbf{N})$ s.t., for each $i \in [\![1, n]\!]$, there are precisely m_i factorizations of X of length ℓ_i that are pairwise different modulo the congruence $\mathscr{C}_{\mathcal{P}_{\text{fin},\mathbf{0}}(\mathbf{N})}$?

(4) Given $d \in \mathbf{N}^+$, let $\Delta_d(\mathcal{P}_{\text{fin},0}(\mathbf{N}))$ be the union of all $\Delta(L)$ for which $L \in \mathscr{L}(\mathcal{P}_{\text{fin},0}(\mathbf{N}))$ and $d \in \Delta(L)$. Prove that $\Delta_d(\mathcal{P}_{\text{fin},0}(\mathbf{N})) = \mathbf{N}^+$ (this would follow from (2), but is much weaker)

(5) What about extensions of (parts of) Theorem 1 to more abstract classes of monoids? E.g., the power monoid of a finite field of prime order $p \ge 3$ is *not* unit-cancellative, but is atomic