Power monoids and a conjecture by Bienvenu and Geroldinger

Salvatore Tringali
School of Mathematical Sciences, Hebei Normal University

based on joint work with Weihao Yan(1)

Conference on Rings and Factorizations 2023
DMSC, University of Graz (AT), July 12, 2023

(1)Weihao defended his bachelor's thesis in mathematics on May 18, 2023.

Outline

What is... a power monoid?

Throughout, M is a multiplicative[ly written] monoid and we denote by $M^\times$ its group of units (note that M need not be commutative, cancellative, etc.)

The large power monoid (LPM) of M is the (multiplicative) monoid $\mathcal{P}(M)$ obtained by endowing the *non-empty* subsets of M with the setwise product

$$(X, Y) \mapsto XY := \{xy \colon x \in X,\, y \in Y\}.$$

Each of the following is a submonoid of $\mathcal{P}(M)$:

- $\mathcal{P}_\times(M) := \{X \in \mathcal{P}(M) \colon X \cap M^\times \neq \varnothing\}$, the restricted LPM of M.
- $\mathcal{P}_1(M) := \{X \in \mathcal{P}(M) \colon 1_M \in X\}$, the reduced LPM of M.
- $\mathcal{P}_{\rm fin}(M) := \{X \in \mathcal{P}(M) \colon |X| < \infty\}$, the finitary power monoid (FPM) of M.
- $\mathcal{P}_{{\rm fin},\times}(M) := \mathcal{P}_{\rm fin}(M) \cap \mathcal{P}_\times(M)$, the restricted FPM of M.
- $\mathcal{P}_{{\rm fin},1}(M) := \mathcal{P}_{\rm fin}(M) \cap \mathcal{P}_1(M)$, the reduced FPM of M.

Altogether, these structures will be referred to as power monoids[2] (PMs).

[2] The definition of $\mathcal{P}(\cdot)$ and $\mathcal{P}_{\rm fin}(\cdot)$ does even make sense for semigroups (see Slide 4).

Older literature and origins

$\mathcal{P}(M)$ and $\mathcal{P}_{\mathrm{fin}}(M)$ have been considered by semigroup theorists and computer scientists since the late 1960s and quite intensively in the 1980s-1990s[(3)].

They were first *explicitly* studied by T. Tamura & J. Shafer[(4)] (in the more general context of *semigroups*) in 1967, though the definition of these structures is already *implicit* to the early work on additive combinatorics[(5)].

Since then, there has been continuous interest in properties of M that [do not] ascend to $\mathcal{P}(M)$ or $\mathcal{P}_{\mathrm{fin}}(M)$. Tamura & Shafer were especially interested in:

The Isomorphism Problem (for Power Semigroups)

Assume the large power semigroup of a semigroup S is (semigroup-)isomorphic to the one of a semigroup T. Is it true that S is isomorphic to T?

For *infinite* semigroups, the problem was quickly answered in the negative[(6)], but remains open for *finite* semigroups.

---

(3) See J. Almeida, Semigroup Forum **64** (2002), 159–179 (a must-read survey).

(4) See *Power semigroups*, Mathematica Japonicae **12** (1967), 25–32.

(5) At least starting with the work of A.L. Cauchy in his famous 1813 paper containing a proof of what is now known as the Cauchy-Davenport inequality.

(6) See E. M. Mogiljanskaja, Semigroup Forum **6** (1973), 330–333.

Recent literature and popularization

$\mathcal{P}_{\mathrm{fin}}(M)$, $\mathcal{P}_{\mathrm{fin},\times}(M)$, and $\mathcal{P}_{\mathrm{fin},1}(M)$ were rediscovered by Y. Fan and T. in 2018 and further studied in a series of subsequent papers:

- Fan & T., J. Algebra **512** (2018), 252–294.
- Antoniou & T., Pacific J. Math. **312** (2021), No. 2, 279–308.
- Sect. 4.2 in T., J. Algebra **602** (July 2022), 352–380.
- pp. 101–102 in Geroldinger & Khadam, Ark. Mat. **60** (2022), 67–106.
- Bienvenu & Geroldinger, Israel J. Math., to appear (arXiv:2205.00982).
- Example 4.5(3) and Remark 5.5 in Cossu & T., J. Algebra **630** (Sep 2023), 128–161.
- T. & Yan, three manuscripts (soon on arXiv).

PMs are also the subject of a CrowdMath project recently launched by F. Gotti:

`https://artofproblemsolving.com/polymath/mitprimes2023`

Most of these papers focus on the arithmetic of PMs (and related structures), and especially on questions concerning the possibility (or impossibility) of factoring a set into a (finite) product of *irreducibles*[(7)] (see also Slide 10).

(7) In a multiplicative monoid H, an element a is irreducible if a is a non-unit and $a \neq xy$ for all non-units $x, y \in H$ such that $HxH \neq HaH \neq HyH$.

Why caring?

1) PMs are a leading example in the ongoing development of a *unifying theory of factorization*, with monoids & irreducibles replaced by premons & irreds (...):

- T., J. Algebra **602** (July 2022), 352–380.
- Cossu & T., Israel J. Math., to appear (arXiv:2108.12379).
- Cossu & T., J. Algebra **630** (Sep 2023), 128–161.
- T., Math. Proc. Cambridge Philos. Soc., to appear (`arXiv:2209.05238`).
- [Preprints] Cossu & T. (`arXiv:2301.09961`), Casabella, García-Sánchez, & D'Anna (arXiv:2302.09647), and Ajran & F. Gotti (arXiv:2305.00413).

2) PMs are a natural algebraic framework for arithmetic combinatorics:

- **Sárközy's conjecture[(8)].** For all but finitely many primes p, the set $\mathcal{Q}_p \subseteq \mathbb{F}_p$ of quadratic residues mod p is an atom in the FPM of the additive group of $\mathbb{F}_p$.
- **Inverse Goldbach conjecture[(9)].** Every set of integers that differ from the set of (positive rational) primes by finitely many elements is an atom in the LPM of $(\mathbb{Z}, +)$.

3) The monoid of non-empty (2-sided) ideals of M is a submonoid of $\mathcal{P}(M)$.

4) PMs play a key role in the study of formal languages and automata[(10)].

[(8)] Conjecture 1.6 in A. Sárközy, Acta Arith. **155** (2012), No. 1, 41–51.
[(9)] See C. Elsholtz, Mathematika **48** (2001), Nos. 1–2, 151–158.
[(10)] See (the refs in) K. Auinger and B. Steinberg, Theoret. Comput. Sci. **341** (2005), 1–21.

A zoo of wild beasts

$\mathcal{P}(M)$, $\mathcal{P}_\times(M)$, and $\mathcal{P}_1(M)$ are rather complicated objects — their "finitary analogues" are much tamer, although $\mathcal{P}_{\rm fin}(M)$ can still be a real headache.

$$
\begin{tikzcd}
\{1_M\} \arrow[r, hook] \arrow[d, tail] & M^\times \arrow[r, hook] \arrow[d, tail] & M \arrow[d, tail] \\
\mathcal{P}_{\mathrm{fin},1}(M) \arrow[r, hook] \arrow[d, hook] & \mathcal{P}_{\mathrm{fin},\times}(M) \arrow[r, hook] \arrow[d, hook] & \mathcal{P}_{\mathrm{fin}}(M) \arrow[d, hook] \\
\mathcal{P}_1(M) \arrow[r, hook] & \mathcal{P}_\times(M) \arrow[r, hook] & \mathcal{P}(M)
\end{tikzcd}
$$

In the above diagram, a "hooked arrow" $P \hookrightarrow Q$ means the inclusion map from P to Q and a "tailed arrow" $P \rightarrowtail Q$ means the embedding $P \to Q\colon x \mapsto \{x\}$.

Fact 1. If M is cancellative, then $\mathcal{P}_{\rm fin}(M)$ is divisor-closed[11] in $\mathcal{P}(M)$.

Fact 2. If M is Dedekind-finite, then (i) $\mathcal{P}_\times(M)$ is divisor-closed in $\mathcal{P}(M)$, and so is $\mathcal{P}_{\mathrm{fin},\times}(M)$ in $\mathcal{P}_{\rm fin}(M)$; (ii) $\mathcal{P}_{\mathrm{fin},1}(M)$ and $\mathcal{P}_{\mathrm{fin},\times}(M)$ have *essentially* the same factorizations into irreducibles, and so also do $\mathcal{P}_1(M)$ and $\mathcal{P}_\times(M)$.

[11] A submonoid K of a monoid H is divisor-closed if "$x \in H$ and $y \in K \cap HxH$" $\Rightarrow x \in K$.

Going nuts with a hard nut

The facts mentioned on the previous slide suggest that, at least for a *cancellative* (and hence Dedekind-finite) M, there is much about $\mathcal{P}(M)$ and other PMs that we can understand from the study of $\mathcal{P}_{\mathrm{fin},1}(M)$. In addition:

Proposition 3.2(iii) in [Antoniou & T., 2019]

$\mathcal{P}_{\mathrm{fin},1}(N)$ is divisor-closed in $\mathcal{P}_{\mathrm{fin},1}(M)$ for *every* submonoid N of M.

So, we can understand many properties of PMs by looking at corresponding properties of $\mathcal{P}_{\mathrm{fin},1}(M)$ when M is monogenic (i.e., generated by one element).

It is thus natural[12] to focus on the reduced FPMs of $(\mathbb{N}, +)$ and $(\mathbb{Z}/n\mathbb{Z}, +)$, herein denoted by $\mathcal{P}_{\mathrm{fin},0}(\mathbb{N})$ and $\mathcal{P}_{\mathrm{fin},0}(\mathbb{Z}/n\mathbb{Z})$, resp., and written additively:

- The arithmetic of $\mathcal{P}_{\mathrm{fin},0}(\mathbb{N})$ is the object of Sect. 4 in [Fan & T., 2018].
- The arithmetic of $\mathcal{P}_{\mathrm{fin},0}(\mathbb{Z}/n\mathbb{Z})$ for an *odd* modulus n is the object of Sect. 5 in [Antoniou & T., 2019] (see also Sect. 4.2 in [T., 2022]).
- Bienvenu & Geroldinger have addressed algebraic and (sort of) analytic properties of $\mathcal{P}_{\mathrm{fin},0}(\mathbb{N})$ and closely related structures (see Slide 11).

[12] When M is cancellative, there are no other monogenic submonoids (up to iso).

Outline

Factorizations and length sets

To sum up, recent work on PMs has brought new life to the subject, a major problem being the following conjecture:

Sect. 5 of [Fan & T., 2018]

If M is linearly orderable[a], then every non-empty *finite* subset L of $\mathbb{N}_{\geq 2}$ is the length set (LS) of a set $X \in \mathcal{P}_{\mathrm{fin},1}(M)$, i.e., L is the set of all and only the integers $k \geq 0$ such that X is a product of k atoms[b] of $\mathcal{P}_{\mathrm{fin},1}(M)$.

[a] Namely, there is a total order $\preceq$ on M s.t. if $x \prec y$ then $uxv \prec uyv$ for all $u, v \in H$.
[b] Here, an atom is a non-unit that does not factor as a product of two non-units.

As noted in [Fan & T., 2018], the conjecture boils down to the case $M = (\mathbb{N}, +)$, and what is known to date amounts to the following:

Propositions 4.8–4.10 in [Fan & T., 2018]

For every integer $n \geq 2$, each of the sets $\{n\}$, $\{2, n\}$, and $[\![2, n]\!]$ can be realized as the length set of a set in the reduced FPM of $(\mathbb{N}, +)$.

Problem 1: L is a length set of $\mathcal{P}_{\mathrm{fin},0}(\mathbb{N})$ iff so is $L + k$ for all $k \in \mathbb{N}$. (Easy in the FPM of $(\mathbb{N}, +)$, see Theorem 1.2.3 in [Bienvenu & Geroldinger, 202?].)

The Bienvenu–Geroldinger conjecture

True or not, the conjecture has motivated new questions.

Most notably, let S be a numerical monoid, i.e., a submonoid of $(\mathbb{N}, +)$ s.t. $\mathbb{N} \setminus S$ is finite. Bienvenu & Geroldinger have

- obtained quantitative results on the "density" of the atoms of the reduced FPM of S, herein denoted by $\mathcal{P}_{\mathrm{fin},0}(S)$ and written additively;
- started a foray into the ideal theory of $\mathcal{P}_{\mathrm{fin},0}(S)$, with emphasis on prime ideals.

Moreover, they have formulated (and proved special cases of) the following:

Bienvenu–Geroldinger conjecture

The reduced FPM of a numerical monoid S_1 is isomorphic (shortly, $\simeq$) to the reduced FPM of a numerical monoid S_2 iff $S_1 = S_2$.

It is worth noting that:

i) The Bienvenu–Geroldinger conjecture is ultimately asking to show that, in a certain class of multiplicative monoids, $\mathcal{P}_{\mathrm{fin},1}(H) \simeq \mathcal{P}_{\mathrm{fin},1}(K)$ iff $H \simeq K$, as it is folklore that two numerical monoids are isomorphic iff they are equal[13].

ii) The unrestricted conjecture is false — if H is an idempotent (multiplicative) monoid with two elements, then $H \simeq \mathcal{P}_{\mathrm{fin},1}(H) \simeq \mathcal{P}_{\mathrm{fin},0}(\mathbb{Z}/2\mathbb{Z}) \not\simeq (\mathbb{Z}/2\mathbb{Z}, +)$.

[13] See, e.g., Theorem 3 in J. C. Higgins, Bull. Austral. Math. Soc. **1** (1969), 115–125.

Sketch of proof

The Bienvenu–Geroldinger conjecture was recently settled by Weihao Yan and myself in a 4-page note. *In hindsight*, the proof is rather simple — the most "advanced technology" we use is a classic[14]:

Nathanson's Thm (or Fundamental Thm of Additive Combinatorics)

Given $A \in \mathcal{P}_{\mathrm{fin},0}(\mathbb{N})$ with $\gcd A = 1$, there exist $b, c \in \mathbb{N}$, $B \subseteq [\![0, b-2]\!]$, and $C \subseteq [\![0, c-2]\!]$ s.t. $kA = B \cup [\![b, ka-c]\!] \cup (ka - C)$ for all large $k \in \mathbb{N}$, where $a := \max A$ and $kA := A + \cdots + A$ (k times).

The proof breaks down to the following steps:

1) Show by Nathanson's theorem that, given $A \in \mathcal{P}_{\mathrm{fin},0}(\mathbb{N})$, we have $(k+1)A = kA + B$ for all large $k \in \mathbb{N}$ and every $B \subseteq A$ with $\{0, \max A\} \subseteq B$.
2) Use 1) to prove that, if S_1 and S_2 are numerical monoids and $\phi\colon \mathcal{P}_{\mathrm{fin},0}(S_1) \to \mathcal{P}_{\mathrm{fin},0}(S_2)$ is an iso, then ϕ sends 2-element sets to 2-element sets.
3) Use 2) to show that, if $\phi(\{0, a_1\}) = \{0, b_1\}$ and $\phi(\{0, a_2\}) = \{0, b_2\}$ for some $a_1, a_2 \in S_1$, then $\phi(\{0, a_1 + a_2\}) = \{0, b_1 + b_2\}$.
4) Use 3) to conclude that, if S_1 and S_2 are numerical monoids and ϕ is an iso $\mathcal{P}_{\mathrm{fin},0}(S_1) \to \mathcal{P}_{\mathrm{fin},0}(S_2)$, then the fnc $\Phi\colon S_1 \to S_2 : a \mapsto \max \phi(\{0, a\})$ is also an iso.

Problem 2. Generalize the result to a larger class of monoids.

[14] See M. B. Nathanson, Amer. Math. Monthly **79** (1972), No. 9, 1010–1012.

Looking for extensions

Let a Puiseux monoid H be a submonoid of $(\mathbb{R}_{\geq 0}, +)$. We denote the reduced FPM of H by $\mathcal{P}_{\mathrm{fin},0}(H)$, write it additively, and say that H is a rational Puiseux monoid if H is made of (non-negative) rational numbers[15].

Nathanson's theorem has a natural extension to (non-empty, finite) sets of rationals, so the proof outlined on the previous slide can be adapted to show:

Theorem 1.

$\mathcal{P}_{\mathrm{fin},0}(H) \simeq \mathcal{P}_{\mathrm{fin},0}(K)$, *for* rational *Puiseux monoids* H *and* K, *iff* $H \simeq K$.

However, no analogue of Nathanson's theorem is available for (finite) sets of real numbers, and the question arises whether rationality is really necessary.

Definition 2.

The monoid M is positively orderable if there is a total order $\preceq$ on M such that (i) $1_M \preceq x$ for each $x \in M$ and (ii) $x \prec y$ implies $uxv \prec uyv$ for all $u, v \in M$.

Puiseux monoids are positively orderable, and so is every submonoid of the non-negative cone of a totally orderable group.

[15] Rational Puiseux monoids have been intensively studied by F. Gotti since 2018. They are indeed much older, but Felix' work has brought many new ideas to the topic.

A generalization

Proposition 1.

The monoid M is torsion-free iff so is its reduced power monoid.

Proof.

Assume M is torsion-free, let X be a set in $\mathcal{P}_{\mathrm{fin},1}(M)$ with $X \neq \{1_H\}$, and suppose for a contradiction that $X^m = X^n$ for some $m, n \in \mathbb{N}$, $m < n$. Then (by induction) $X^m = X^{nk-m(k-1)} \supseteq X^k$ for each $k \in \mathbb{N}^+$. So, considering that $|X| \geq 2$ and picking $x \in X \setminus \{1_M\}$, we find $|X^m| \geq |X^k| \geq |\{1_M, x\}^k| = k+1$ for all $k \in \mathbb{N}^+$ (absurd).

If, on the other hand, there are $x \in M \setminus \{1_M\}$ and $m, n \in \mathbb{N}^+$ with $m < n$ s.t. $x^m = x^n$, then $\{1_M, x\}^n = \{1_M, \ldots, x^n\} = \{1_M, \ldots, x^{n-1}\} = \{1_M, x\}^{n-1}$. ∎

Proposition 2.

Let H and K be (multiplicative) monoids with H torsion-free, and ϕ be an iso $\mathcal{P}_{\mathrm{fin},1}(H) \to \mathcal{P}_{\mathrm{fin},1}(K)$. Then $|\phi(X)| = |X|$ for all $X \in \mathcal{P}_{\mathrm{fin},1}(H)$ s.t. $|X| \leq 3$.

Theorem 3.

Let H and K be commutative monoids and assume K is positively orderable. Then $\mathcal{P}_{\mathrm{fin},1}(H) \simeq \mathcal{P}_{\mathrm{fin},1}(K)$ iff $H \simeq K$.

Outline

1. Power monoids

2. A new wave of questions

3. References

Bibliography

- A. A. Antoniou & S. Tringali, *On the Arithmetic of Power Monoids and Sumsets in Cyclic Groups*, Pacific J. Math. **312** (2021), No. 2, 279–308 (`arXiv:1804.10913`).
- P.-Y. Bienvenu and A. Geroldinger, *On algebraic properties of power monoids of numerical monoids*, Israel J. Math., to appear (`https://arxiv.org/abs/2205.00982`).
- L. Cossu & S. Tringali, *Abstract Factorization Theorems with Applications to Idempotent Factorizations*, to appear in Israel J. Math. (`arXiv:2108.12379`).
- L. Cossu & S. Tringali, *Factorization under local finiteness conditions*, J. Algebra **630** (Sep 2023), 128–161 (`arXiv:2208.05869`).
- L. Cossu & S. Tringali, *On the finiteness of certain factorization invariants*, preprint (under review, `arXiv:2301.09961`).
- Y. Fan & S. Tringali, *Power monoids: A bridge between Factorization Theory and Arithmetic Combinatorics*, J. Algebra **512** (2018), 252–294.
- S. Tringali, *An abstract factorization theorem and some applications*, J. Algebra **602** (July 2022), 352–380 (`arXiv:2102.01598`).
- S. Tringali, *A characterization of atomicity*, to appear in Math. Proc. Cambridge Philos. Soc. (`arXiv:2209.05238`).
- S. Tringali and W. Yan, *A conjecture by Bienvenu and Geroldinger on power monoids*, manuscript (available upon request)
- S. Tringali and W. Yan, *PMs and their automorphisms*, manuscript (available upon request).
- S. Tringali and W. Yan, *A conjecture by Bienvenu and Geroldinger on power monoids, II*, manuscript (available upon request).