

A survey on power semigroups

Salvatore TRINGALI

School of Mathematical Sciences, Hebei Normal University

School of Mathematics, Sun Yat-sen University

Zhuhai, Guangdong Province, China · Dec 28, 2024



1. Generalities on semigroups, monoids, and groups
2. Power semigroups and the Tamura–Shafer problem
3. Power monoids and the Bienvenu–Geroldinger conjecture
4. Morphology of power semigroups, I
5. Morphology of power semigroups, II
6. References



What is a semigroup?

A **semigroup** (shortly, sgrp) is an ordered pair (S, \otimes) consisting of a (possibly empty) set S , called the **underlying set** of the sgrp, and an **associative (binary) operation** \otimes on S , meaning that \otimes is a function (shortly, fnc) $S \times S \rightarrow S$ s.t.⁽¹⁾

$$x \otimes (y \otimes z) = (x \otimes y) \otimes z, \quad \text{for all } x, y, z \in S. \quad (1)$$

Eq. (1) is referred to as the **associativity law** (for the operation \otimes) and allows for the *unambiguous* usage of “long expressions” of the form $x_1 \otimes \cdots \otimes x_n$, where n is a positive integer and (x_1, \dots, x_n) is an n -tuple of elements of S .

There are two standard notations commonly used for the operation of a sgrp (unless a different symbol is explicitly required):

- the **multiplicative notation**, where the sgrp operation is called **multiplication** and denoted by a centered dot \cdot (with or without subscripts or superscripts);
- the **additive notation**, where the sgrp operation is called **addition** and denoted by a plus sign $+$ (with or without subscripts or superscripts).

NOTE. Later on, we will typically identify a sgrp with its underlying set (especially if there is no serious risk of confusion), denote the sgrp operation multiplicatively, and write xy in place of $x \cdot y$.

⁽¹⁾Here as usual, we define $u \otimes v := \otimes(u, v)$ for every $u, v \in S$.

Examples and non-examples of semigroups

We denote by \mathbb{N}^+ the (set of) positive int[eger]s, by \mathbb{N} the non-negative ints, by \mathbb{Z} the ints, by \mathbb{Q} the rationals, by \mathbb{R} the reals, and by \mathbb{C} the complex numbers.

- (1) Let \otimes be the (binary) operation of **exponentiation** $(a, b) \mapsto a^b$ on \mathbb{N}^+ . The pair (\mathbb{N}^+, \otimes) is *not* a sgrp: \otimes is not associative, since $(2 \otimes 2) \otimes 3 = 2^6 \neq 2^8 = 2 \otimes (2 \otimes 3)$.
- (2) The set of *odd* ints does not form a sgrp under the (usual) operation of addition inherited from \mathbb{Z} : the sum of two odd ints is even.
- (3) For all $a, b \in \mathbb{N}$ s.t. $b^2 \equiv b \pmod{a}$, the set $\{ak + b : k \in \mathbb{N}\} \subseteq \mathbb{N}$ is a sgrp under the (usual) operation of multiplication inherited from \mathbb{N} .
- (4) Let $\mathbb{H} \in \{\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}$. For all $n \in \mathbb{N}^+$ and $a_1, \dots, a_n \in \mathbb{H}$, the set

$$\{a_1 x_1 + \dots + a_n x_n : x_1, \dots, x_n \in \mathbb{N}\} \subseteq \mathbb{H}$$

is a sgrp under the (usual) operation of addition inherited from \mathbb{H} .

- (5) Given $n \in \mathbb{N}^+$, the set of n -by- n singular matrices A with entries in a commutative ring R forms a sgrp under the (usual) operation of row-by-column multiplication. (We call the matrix A **singular** if its determinant is a zero divisor of R .)
- (6) The non-empty finite tuples with components in a set X form a sgrp, called the **free sgrp over X** and denoted by $\mathcal{F}^+(X)$, under the (binary) operation $*$ of **concatenation**:

$$(x_1, \dots, x_m) * (y_1, \dots, y_n) := (x_1, \dots, x_m, y_1, \dots, y_n),$$

for all $m, n \in \mathbb{N}^+$ and $x_1, \dots, x_m, y_1, \dots, y_n \in X$.



Monoids and groups

A sgrp (S, \otimes) is a **monoid** if there exists a (provably unique) element $e \in S$, called *the identity [element]* or **neutral element** (of the monoid itself), s.t.

$$x \otimes e = x = e \otimes x, \quad \text{for every } x \in S.$$

A **unit** (or **invertible element**) of a monoid $\mathbb{S} = (S, \otimes)$ with neutral element e is then an element $u \in S$ for which there is a (provably unique) element $v \in S$, accordingly called *the inverse* of u (wrt to \otimes), s.t.

$$u \otimes v = e = v \otimes u.$$

We denote the set of units of \mathbb{S} by \mathbb{S}^\times and call \mathbb{S} a **group** if $\mathbb{S}^\times = S$. Properties:

- The neutral element is a unit, and its inverse is itself.
- $u \in S$ is a unit iff the inverse of u is a unit.
- If $u, v \in \mathbb{S}^\times$, then $u \otimes v \in \mathbb{S}^\times$.

A couple of remarks about the notation:

- In a multiplicatively written monoid H , the neutral element is commonly denoted by 1_H (also without the subscript ' H ') and the inverse of a unit u is denoted by u^{-1} .
- In an additively written monoid K , the neutral element is commonly denoted by 0_K (also without the subscript ' K ') and the inverse of a unit u is denoted by $-u$.

Examples and non-examples of monoids

- (1) Endowed with the (usual) operation of multiplication inherited from \mathbb{Z} , the *even* ints form a sgrp but not a monoid: there is no even integer e s.t. $2e = 2$.
- (2) Example (5) on Slide 4 is a monoid iff R is a zero ring (i.e., R has one element), or $n = 1$ and R is a domain (i.e., R has no zero divisors apart from the zero element).
- (3) The elements of a *unital* ring R form a monoid under the operation of multiplication of the ring itself, accordingly called the **multiplicative monoid** of R .
- (4) Example (4) on Slide 4 is a monoid for any choice of \mathbb{H} , n , and a_1, \dots, a_n .
- (5) Every sgrp (S, \otimes) can be (canonically) made into a monoid as follows:
 - If the sgrp has already a neutral element, we have nothing to do.
 - Otherwise, we adjoin a *new* element e to S and extend \otimes to a (binary) operation on $S \cup \{e\}$ by taking $x \otimes e := x := e \otimes x$ for every $x \in S \cup \{e\}$.

The monoid obtained in this way is called a (**conditional**) **unitization** of (S, \otimes) .

- (6) The unitization of the free sgrp $\mathcal{F}^+(X)$ over a set X (Example (6) on Slide 4) is named the **free monoid over X** and denoted by $\mathfrak{F}(X)$. The elements of $\mathcal{F}(X)$ are referred to as X -words, and the neutral element as the **empty X -word**. If the set X is clear from the context, we just say “word” instead of “ X -word”.
- (7) A **group** is, by def., a monoid in which every element is a unit. It follows from the basic properties of units on Slide 5 that, under the operation inherited from H , the units of a monoid H form a group, accordingly called the **group of units** of H .

Homomorphisms

A **sgrp homomorphism** (shortly, hom) is a triple $(\mathbb{S}, \mathbb{T}, \phi)$, where $\mathbb{S} = (S, \otimes)$ and $\mathbb{T} = (T, \odot)$ are sgrps (called the **domain** and the **codomain** of the hom, resp.), and ϕ is the graph of a fnc from S to T s.t.

$$\phi(x \otimes y) = \phi(x) \odot \phi(y), \quad \text{for all } x, y \in S. \quad (2)$$

We will typically denote a sgrp hom $(\mathbb{S}, \mathbb{T}, \phi)$ by the **arrow notation** $\phi: \mathbb{S} \rightarrow \mathbb{T}$ and say that ϕ is a *sgrp hom from \mathbb{S} to \mathbb{T}* . Accordingly, we refer to ϕ as

- a **monomorphism** (or a **monic** or **injective** hom) if ϕ is an injective fnc;
- an **epimorphism** (or an **epic** or **surjective** hom) if ϕ is a surjective fnc;
- an **isomorphism** if ϕ is both injective and surjective (i.e., a bijection);
- an **endomorphism** (of \mathbb{S}) if domain and codomain coincide (i.e., $\mathbb{S} = \mathbb{T}$);
- an **automorphism** (of \mathbb{S}) if ϕ is both an isomorphism and an endomorphism;
- a **monoid hom** if \mathbb{S} and \mathbb{T} are both monoids, and ϕ maps the neutral/identity element of \mathbb{S} to the neutral/identity element of \mathbb{T} .

In particular, we say that \mathbb{S} is (**sgrp-**)**isomorphic** to \mathbb{T} , written $\mathbb{S} \simeq \mathbb{T}$, if there is an isomorphism from \mathbb{S} to \mathbb{T} .

NOTE. A sgrp hom from a monoid to a monoid need not be a monoid hom (e.g., consider the integers under multiplication and the fnc $\mathbb{Z} \rightarrow \mathbb{Z}: x \mapsto 0$).

A **subsemigroup** (shortly, **subsgpr**) of a **sgrpr** $\mathbb{S} = (S, \otimes)$ is a set $T \subseteq S$ that is **closed** (and hence becomes itself a **sgrpr**) under the operation inherited from \mathbb{S} :

$$x \otimes y \in T, \quad \text{for all } x, y \in T. \quad (3)$$

It is easily checked that the following hold for a **sgrpr** hom $f: \mathbb{H} \rightarrow \mathbb{K}$:

- If T is a **subsgpr** of \mathbb{S} , then $f[T] := \{f(x) : x \in T\}$ is a **subsgpr** of \mathbb{K} .
- If T is a **subsgpr** of \mathbb{K} , then $f^{-1}[T] := \{x \in H : f(x) \in T\}$ is a **subsgpr** of \mathbb{H} .

In a similar vein, a **submonoid** (resp., a **subgroup**) of \mathbb{S} is a (necessarily non-empty) **subsgpr** T of \mathbb{S} s.t. the pair (T, \otimes_T) is a **monoid** (resp., a **group**) in its own right, where \otimes_T is the binary operation $(x, y) \mapsto x \otimes y$ on T (which is a well-defined fnc $T \times T \rightarrow T$ as we are supposing that Eq. (3) holds).

In general, a **submonoid/subgroup** K of a **monoid** \mathbb{H} need *not* contain the neutral element e of \mathbb{H} (e.g., the singleton $\{0\} \subseteq \mathbb{Z}$ is a **subgroup** of the multiplicative **monoid** of the ring of integers, and the neutral element of the latter is the integer 1). If, on the other hand, K contains e , then e is a fortiori the neutral element of K , and we call K a **unital** **submonoid/subgroup** of \mathbb{H} .

Most notably, the set of units, \mathbb{H}^\times , of a **monoid** \mathbb{H} is a **unital subgroup** of \mathbb{H} , accordingly called the **group of units** of \mathbb{H} .



Composing homomorphisms

The **composition** of a sgrp hom $f: \mathbb{H} \rightarrow \mathbb{K}$ with a sgrp hom $\mathbb{K} \rightarrow \mathbb{L}$ is the triple $(\mathbb{H}, \mathbb{L}, g \circ f)$, where $g \circ f$ is the composite fnc “ g after f ”, i.e., the fnc

$$H \rightarrow L: x \mapsto g(f(x)),$$

where H and L are the underlying sets of \mathbb{H} and \mathbb{L} , resp.

Assuming for ease of notation that \mathbb{H} , \mathbb{K} , and \mathbb{L} are all written multiplicatively, and considering that both f and g satisfy Eq. (2), we find that, for all $x, y \in H$,

$$g \circ f(xy) = g(f(xy)) = g(f(x)f(y)) = g(f(x))g(f(y)) = (g \circ f(x))(g \circ f(y)).$$

That is, $g \circ f$ is a sgrp hom from \mathbb{H} to \mathbb{L} .

It follows that, under the operation of composition, the endomorphisms of a sgrp $\mathbb{S} = (S, \otimes)$ form a *monoid*, herein denoted by $\text{End}(\mathbb{S})$, whose neutral element is the **identity fnc** id_S on the set S (i.e., the fnc $S \rightarrow S: x \mapsto x$).

The units of $\text{End}(\mathbb{S})$ are then the endomorphisms ϕ of \mathbb{S} s.t. $\phi \circ \phi' = \phi' \circ \phi = \text{id}_S$ for some $\phi' \in \text{End}(\mathbb{S})$, namely, the automorphisms of \mathbb{S} .

So, under the operation of composition, the automorphisms of \mathbb{S} form a group, called the **automorphism group** (or **autogroup**) of \mathbb{S} and denoted by $\text{Aut}(\mathbb{S})$.

Congruences and quotients

A (**sgrp**) **congruence** on a sgrp $\mathbb{S} = (S, \otimes)$ is an equivalence relation \sim on the set S with the additional property that

$$\text{if } u \sim v \text{ and } x \sim y, \text{ then } u \otimes x \sim v \otimes y.$$

An equivalence class in the quotient (set) of S by \sim is then referred to as a **congruence class modulo** \sim . In particular, we write $[x]_{\sim}$ for the congruence class modulo \sim represented by an element $x \in S$, that is, we set

$$[x]_{\sim} := \{y \in S : x \sim y\}.$$

The quotient of S by \sim is in fact a sgrp under the binary operation that maps a pair $(\mathfrak{u}, \mathfrak{v})$ of equivalence classes in the quotient to the equivalence class of the element $u \otimes v$, where $u \in \mathfrak{u}$ and $v \in \mathfrak{v}$ (it is routine to check that this definition does not depend on the choice of the representatives u and v).

The sgrp obtained in this way is the **quotient** (or **factor**) **sgrp** of \mathbb{S} by \sim , and it is denoted by \mathbb{S}/\sim . Accordingly, (the graph of) the fnc

$$\pi: S \rightarrow \mathbb{S}/\sim: x \mapsto [x]_{\sim}$$

is a sgrp hom $\mathbb{S} \rightarrow \mathbb{S}/\sim$, named the **canonical projection** of \mathbb{S} onto \mathbb{S}/\sim .



1. Generalities on semigroups, monoids, and groups
- 2. Power semigroups and the Tamura–Shafer problem**
3. Power monoids and the Bienvenu–Geroldinger conjecture
4. Morphology of power semigroups, I
5. Morphology of power semigroups, II
6. References

Power semigroups

From now on, all sgrps are written multiplicatively unless stated otherwise

The **large power sgrp** of a sgrp S is the sgrp $\mathcal{P}(S)$ obtained by endowing the *non-empty* subsets of S with the (provably associative) operation

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

Loosely speaking, a **power sgrp** is any of a variety of sgrps that sit between a sgrp and its large power sgrp (no precise definition). For instance:

- (1) The non-empty *finite* subsets of S form a subsgrp of $\mathcal{P}(S)$, herein denoted by $\mathcal{P}_{\text{fin}}(S)$ and called the **finitary power sgrp** of S .
- (2) If κ is an idempotent cardinal number (i.e., $\kappa = 0$, $\kappa = 1$, or κ is infinite), then the family of all non-empty sets $X \subseteq S$ such that $|X| < \kappa$ (resp., $|X| \leq \kappa$) is a subsgrp of $\mathcal{P}(S)$, hereafter denoted by $\mathcal{P}_{<\kappa}(S)$ (resp., by $\mathcal{P}_{\leq\kappa}(S)$). In particular, $\mathcal{P}_{\text{fin}}(S) = \mathcal{P}_{<|\mathbb{N}|}(S)$.

A couple of remarks:

- $\mathcal{P}_{\leq 1}(S)$ is sgrp-isomorphic to S via the fnc $S \rightarrow \mathcal{P}(S): x \mapsto \{x\}$ (corestricted to its image), i.e., $\mathcal{P}(S)$ contains an isomorphic copy of S .
- If S is a monoid with neutral element 1_S , then $\mathcal{P}(S)$ is a monoid with neutral element $\{1_S\}$ and $\mathcal{P}_{\text{fin}}(S)$ is a unital submonoid of $\mathcal{P}(S)$. Accordingly, we call $\mathcal{P}(S)$ and $\mathcal{P}_{\text{fin}}(S)$ the **large power monoid** and the **finitary power monoid** of S , resp.



Older literature and origins

To my knowledge, power sgrps made their first *explicit* appearance in a 1953 paper by Dubreil and later on in Lyapin's influential book on sgrp theory⁽²⁾. They were studied quite intensively in the 1980s and 1990s⁽³⁾.

In fact, $\mathcal{P}(S)$ was first *systematically* tackled by Tamura & Shafer⁽⁴⁾ in 1967, while being a special case of the general notion of power algebra⁽⁵⁾.

Tamura & Shafer were especially interested in the following problem:

Problem 1.

Given a class \mathcal{O} of sgrps, prove/disprove that $\mathcal{P}(H) \simeq \mathcal{P}(K)$, for some $H, K \in \mathcal{O}$, iff $H \simeq K$. (Here and later, \simeq means “is sgrp-isomorphic to”).

The heart of the problem lies in the “only if” direction, for every (sgrp) isomorphism $f: H \rightarrow K$ lifts to a **global isomorphism** $H \rightarrow K$ (i.e., to an isomorphism $\mathcal{P}(H) \rightarrow \mathcal{P}(K)$) via the mapping $X \mapsto f[X] := \{f(x) : x \in X\}$.

⁽²⁾Their definition is however *implicit* to the early work on additive combinatorics, including Cauchy's 1813 paper containing the first-known proof of the Cauchy-Davenport inequality.

⁽³⁾Almeida, Semigroup Forum **64** (2002), 159–179.

⁽⁴⁾Tamura & Shafer, Math. Japon. **12** (1967), 25–32.

⁽⁵⁾Sect. 2 in Brink, Algebra Universalis **30** (1993), 177–216.

Partial history of a problem

The Tamura–Shafer problem was quickly answered in the negative for *arbitrary* sgrps⁽⁶⁾, but has a positive answer in many cases (the list is *not* complete):

- *finite* groups and *finite* chains, see Theorems 5.8 and 5.9 in [Tamura & Shafer, Math. Japon. **12** (1967), 25–32].
- groups [Shafer, Math. Japon. **12** (1967), 32].
- *unital* semilattices, chains, and lattices, see Theorems 1.3, 1.4, and 2.2 in [Gould, Iskra, & Tsinakis, Algebra Univ. **19** (1984), 137–141].
- *finite* simple sgrps and *finite* semilattices of torsion groups, see Theorems 3.3 and 2.2 in [Gould & Iskra, Semigroup Forum **28** (1984), 1–11].
- semilattices, see p. 218 in [Kobayashi, Semigroup Forum **29** (1984), 217–222].
- completely 0-simple sgrps and completely simple sgrps, see Theorems 5.9 and 6.8 in [Tamura, J. Algebra **98** (1986), 319–361].
- Clifford sgrps, see Theorem 4.7 in [Gan & Zhao, J. Aust. Math. Soc. **97** (2014), 63–77].

The problem is open, e.g., for *finite* sgrps and *cancellative*⁽⁷⁾ sgrps, but was solved in the cancellative *commutative* setting, both in its original form and in the variant for *finitary* power sgrps [T., 2024]. The latter result has been further generalized to the cancellative *duo* setting [Li & T., work in progress].

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

⁽⁷⁾A sgrp S is **cancellative** if $x \mapsto ax$ and $x \mapsto xa$ are injective fncs on S for every $a \in S$.



Categories go on stage

The Tamura–Shafer problem and its variants are in fact a special instance of a much more general problem, whose formulation is categorial in nature⁽⁸⁾:

Functorial isomorphism problem

Given a functor $F: \mathcal{C} \rightarrow \mathcal{D}$ and a class $\mathcal{O} \subseteq \text{Ob}(\mathcal{C})$ that is closed under isos, prove/disprove that $F(A) \simeq_{\mathcal{D}} F(B)$, for some $A, B \in \mathcal{O}$, iff $A \simeq_{\mathcal{C}} B$.

Of course, the answer is generally in the negative, and the only interesting part of the problem lies in the “only if” clause.

The Tamura–Shafer problem is in particular the special case where F is the endofunctor of the (usual) category Sgrp of sgrps and sgrp homs, hereinafter referred to as the **large power functor** of Sgrp , that maps

- a sgrp S to its large power semigroup $\mathcal{P}(S)$, and
- a sgrp hom $f: S \rightarrow T$ to its **augmentation** $f^*: \mathcal{P}(S) \rightarrow \mathcal{P}(T): X \mapsto f[X]$.

Reframing the problem in the language of categories won't make it easier, but provides a uniform approach to the formulation of many analogous problems.

⁽⁸⁾We write $\text{Ob}(\mathcal{Q})$ for the object class of a category \mathcal{Q} , and we write $X \simeq_{\mathcal{Q}} Y$ to mean that X and Y are isomorphic objects in \mathcal{Q} .



Recent literature and popularization

Power sgrps went dormant for about 20 years, until Yushuang Fan and I (unaware of any previous literature!) rediscovered them in 2018:

- Fan & T., J. Algebra **512** (2018), 252–294.

The paper brought new life to the topic and has been followed by a few more:

- 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. (2024). DOI: 10.1007/s11856-024-2683-0
- Example 4.5(3) and Remark 5.5 in Cossu & T., J. Algebra **630** (2023), 128–161.
- T. & Yan, Proc. Amer. Math. Soc., to appear (arXiv:2310.17713).
- Gonzalez et al., Intl. J. Algebra Comput. (2024). DOI: 10.1142/S0218196724500565
- T. & Yan, J. Comb. Theory Ser. A **209** (2025), #105961, 16 pp.
- [Preprints] Cossu & T., under review (soon on arXiv), Aggarwal et al. (arXiv:2412.05857)

In 2023, power sgrps were the subject of a CrowdMath project led by F. Gotti:

<https://artofproblemsolving.com/polymath/mitprimes2023>



Why caring?

1) A leading example in the development of a *unifying theory of factorization*:

- T., J. Algebra **602** (July 2022), 352–380.
- Cossu & T., Israel J. Math. **263** (2024), 349–395.
- Cossu & T., J. Algebra **630** (2023), 128–161.
- T., Math. Proc. Cambridge Philos. Soc. **175** (2023), 459–465.
- Cossu & T., Ark. Mat. **62** (2024), No. 1, 21–38.
- Casabella, García-Sánchez, & D’Anna, Mediterr. J. Math. **21** (2024), #7, 28 pp.
- García-Sánchez, Semigroup Forum **108** (2024), 365–376.
- [Preprints] Ajran & Gotti (arXiv:2305.00413) and Cossu & T. (soon on arXiv).

2) A natural algebraic framework for arithmetic combinatorics:

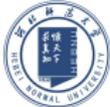
- **Sárközy’s conjecture**⁽⁹⁾. For all but finitely many primes p , the set of [non-zero] quadratic residues mod p is an atom in the finitary power sgrp of $(\mathbb{Z}/p\mathbb{Z}, +)$.
- **Ostmann’s conjecture**⁽¹⁰⁾. Every set of integers that differ from the set of primes by finitely many elements is an atom in the large power sgrp of $(\mathbb{Z}, +)$.

3) A key role in the study of formal languages and automata⁽¹¹⁾.

⁽⁹⁾Conjecture 1.6 in Sárközy, Acta Arith. **155** (2012), No. 1, 41–51.

⁽¹⁰⁾Elsholtz, Mathematika **48** (2001), Nos. 1–2, 151–158.

⁽¹¹⁾See (the refs in) Auinger & Steinberg, Theoret. Comput. Sci. **341** (2005), 1–21.



Age of Ultron

In the 1980s and early 1990s, semigroup theorists, computer scientists, and model theorists worked on the “**block groups = power groups**” conjecture.

A **pseudovariety** (of semigroups) is a class of *finite* semigroups that is closed under taking homomorphic images, subsemigroups, and finite (direct) products.

Denote by \mathcal{BG} the pseudovariety generated by the *finite monoids* all of whose *regular*⁽¹²⁾ one-sided principal ideals⁽¹³⁾ are Brandt⁽¹⁴⁾, and by \mathcal{PG} the pseudovariety generated by the power monoids of the *finite groups*.

In 1984, S. W. Margolis and J.-E. Pin proved that $\mathcal{PG} \subseteq \mathcal{BG}$, but whether the opposite inclusion is true remained open for many years.

Settled (in the positive) by K. Henckell and J. Rhodes in [“The theorem of Knast, the $PG = BG$ and Type II Conjectures”, pp. in 453–463 in J. Rhodes (ed.), *Monoids and Semigroups with Applications*, Word Scientific, 1991].

⁽¹²⁾The one-sided ideals of M are subsemigroups of M , and a semigroup S is **regular** if, for each $a \in S$, there exists $x \in S$, called a (von Neumann) inverse of a , such that $a = axa$.

⁽¹³⁾The one-sided principal ideals of a semigroup S are the sets of the form $\{a\} \cup aS$ or $\{a\} \cup Sa$ with $a \in S$. They are also known in semigroup theory as **\mathcal{D} -classes**.

⁽¹⁴⁾A sgrp S is Brandt if it is an **inverse sgrp** (i.e., a regular sgrp where each element has a *unique* inverse) without *non-trivial* (2-sided) ideals, the trivial ideals being S and \emptyset .



1. Generalities on semigroups, monoids, and groups
2. Power semigroups and the Tamura–Shafer problem
- 3. Power monoids and the Bienvenu–Geroldinger conjecture**
4. Morphology of power semigroups, I
5. Morphology of power semigroups, II
6. References



Focus on power monoids

A closer look at the refs on the previous slides will reveal that most of the *recent* work on power sgrps has in fact focused on **power monoids** (PMs), where the “ground sgrp” has a neutral element (i.e., is a monoid).

One reason is that PMs are usually much tamer than arbitrary power sgrps, which is partly reflected in the richness of the lattice of their subgrps.

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.)

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

- $\mathcal{P}_\times(M) := \{X \in \mathcal{P}(M) : X \cap M^\times \neq \emptyset\}$, the **restricted large PM** of M .
- $\mathcal{P}_1(M) := \{X \in \mathcal{P}(M) : 1_M \in X\}$, the **reduced large PM** of M .
- $\mathcal{P}_{\text{fin}}(M) = \{X \in \mathcal{P}(M) : |X| < \infty\}$, the **finitary PM** of M (already on Slide 12).
- $\mathcal{P}_{\text{fin},\times}(M) := \mathcal{P}_{\text{fin}}(M) \cap \mathcal{P}_\times(M)$, the **restricted finitary PM** of M .
- $\mathcal{P}_{\text{fin},1}(M) := \mathcal{P}_{\text{fin}}(M) \cap \mathcal{P}_1(M)$, the **reduced finitary PM** of M .

Follow the arrows

In the diagram below, a “hooked arrow” $P \hookrightarrow Q$ means the inclusion map from P to Q and a “tailed arrow” $P \rightsquigarrow Q$ means the embedding $P \rightarrow Q: x \mapsto \{x\}$:

$$\begin{array}{ccccc}
 \{1_M\} & \hookrightarrow & M^\times & \hookrightarrow & M \\
 \downarrow & & \downarrow & & \downarrow \\
 \mathcal{P}_{\text{fin},1}(M) & \hookrightarrow & \mathcal{P}_{\text{fin},\times}(M) & \hookrightarrow & \mathcal{P}_{\text{fin}}(M) \\
 \downarrow & & \downarrow & & \downarrow \\
 \mathcal{P}_1(M) & \hookrightarrow & \mathcal{P}_\times(M) & \hookrightarrow & \mathcal{P}(M)
 \end{array}$$

There are many objective reasons why PMs are “smoother” than power sgrps:

- If M is cancellative, then $\mathcal{P}_{\text{fin}}(M)$ is **divisor-closed**⁽¹⁵⁾ in $\mathcal{P}(M)$.
- If M is **Dedekind-finite** (that is, $xy = 1_M$ iff $yx = 1_M$), then (i) $\mathcal{P}_\times(M)$ is divisor-closed in $\mathcal{P}(M)$, and so is $\mathcal{P}_{\text{fin},\times}(M)$ in $\mathcal{P}_{\text{fin}}(M)$; (ii) $\mathcal{P}_{\text{fin},1}(M)$ and $\mathcal{P}_{\text{fin},\times}(M)$ have, in a way, the same arithmetic⁽¹⁶⁾, and so do $\mathcal{P}_1(M)$ and $\mathcal{P}_\times(M)$.
- $\mathcal{P}_{\text{fin},1}(N)$ is divisor-closed in $\mathcal{P}_{\text{fin},1}(M)$ for every submonoid N of M ⁽¹⁷⁾.

⁽¹⁵⁾A submonoid K of a monoid H is **divisor-closed** if “ $x \in H$ and $y \in K \cap HxH$ ” $\Rightarrow x \in K$.

⁽¹⁶⁾Propositions 3.5 and 4.10 in [Antoniou & T., 2021].

⁽¹⁷⁾Proposition 3.2(iii) in [Antoniou & T., 2021].

From Slide 21, there is much we can learn about power sgrps from restricting our attention on the reduced finitary PMs of $(\mathbb{N}, +)$ and $(\mathbb{Z}/n\mathbb{Z}, +)$ ⁽¹⁸⁾, herein denoted by $\mathcal{P}_{\text{fin},0}(\mathbb{N})$ and $\mathcal{P}_{\text{fin},0}(\mathbb{Z}/n\mathbb{Z})$, resp., and written additively:

- The arithmetic of $\mathcal{P}_{\text{fin},0}(\mathbb{N})$ is the object of Sect. 4 in [Fan & T., 2018].
- The arithmetic of $\mathcal{P}_{\text{fin},0}(\mathbb{Z}/n\mathbb{Z})$ for an *odd* modulus n is the object of Sect. 5 in [Antoniou & T., 2021] (see also Sect. 4.2 in [T., 2022]).
- Bienvenu & Geroldinger have addressed ideal-theoretic and (sort of) analytic properties of $\mathcal{P}_{\text{fin},0}(\mathbb{N})$ and closely related structures (more on that on the next slide).

In this regard, a major open problem is the following **conjecture**:

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

Every non-empty *finite* $L \subseteq \mathbb{N}_{\geq 2}$ is the **length set** of a set $X \in \mathcal{P}_{\text{fin},0}(\mathbb{N})$, i.e., L is the set of all $k \in \mathbb{N}$ s.t. X is a sum of k atoms^a of $\mathcal{P}_{\text{fin},0}(\mathbb{N})$.

^aIn a monoid, an **atom** is a non-unit that does not factor as a product of two non-units.

Propositions 4.8–4.10 in [Fan & T., 2018] show that, for all $n \geq 2$, each of $\{n\}$, $\{2, n\}$, and $\llbracket 2, n \rrbracket$ can be realized as the length set of a set in $\mathcal{P}_{\text{fin},0}(\mathbb{N})$.

⁽¹⁸⁾Or more generally on the PMs of monogenic (i.e., one-generated) monoids.



The Bienvenu–Geroldinger conjecture

True or not, Fan & T.'s conjecture has spurred a new wave of questions.

Most notably, let S be a **numerical monoid**, i.e., a submonoid of $(\mathbb{N}, +)$ with finite complement in \mathbb{N} . Bienvenu & Geroldinger have

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

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

The Bienvenu–Geroldinger conjecture

The reduced finitary PM of a numerical monoid S_1 is isomorphic to the reduced finitary PM of a numerical monoid S_2 iff $S_1 = S_2$.

A couple of remarks:

- The Bienvenu–Geroldinger conjecture is ultimately asking to show that, in a certain class of multiplicative monoids, $\mathcal{P}_{\text{fin},1}(H) \simeq \mathcal{P}_{\text{fin},1}(K)$ iff $H \simeq K$, as it is folklore that two numerical monoids are isomorphic iff they are equal⁽¹⁹⁾.
- The equivalence i) is false for arbitrary monoids — if H is an idempotent (multiplicative) monoid with two elements, then $H \simeq \mathcal{P}_{\text{fin},1}(H) \simeq \mathcal{P}_{\text{fin},0}(\mathbb{Z}/2\mathbb{Z}) \not\cong (\mathbb{Z}/2\mathbb{Z}, +)$.

⁽¹⁹⁾See, e.g., Theorem 3 in 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 7-page note (to appear in Proc. AMS). *In hindsight*, the proof is rather simple — the most advanced technology we use is a classic⁽²⁰⁾:

Nathanson's Theorem (or Fundamental Theorem of Additive NT)

Given $A \in \mathcal{P}_{\text{fin},0}(\mathbb{N})$ with $\gcd A = 1$, there exist $b, c \in \mathbb{N}$, $B \subseteq \llbracket 0, b-2 \rrbracket$, and $C \subseteq \llbracket 0, c-2 \rrbracket$ s.t., for all large $k \in \mathbb{N}$,

$$kA = B \cup \llbracket b, ka - c \rrbracket \cup (ka - C),$$

where $a := \max A$ and $kA := A + \dots + A$ (k times).

The proof breaks down to the following steps:

- 1) Show by Nathanson's theorem that, given $A \in \mathcal{P}_{\text{fin},0}(\mathbb{N})$, 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 $\phi: \mathcal{P}_{\text{fin},0}(S_1) \rightarrow \mathcal{P}_{\text{fin},0}(S_2)$ 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 $\phi(\{0, a_1 + a_2\}) = \{0, b_1 + b_2\}$.

⁽²⁰⁾See Nathanson, Amer. Math. Monthly **79** (1972), No. 9, 1010–1012.



A good question fights back

Let a **Puiseux monoid** H be a submonoid of $(\mathbb{R}_{\geq 0}, +)$. We denote the reduced finitary PM of H by $\mathcal{P}_{\text{fin},0}(H)$, write it additively, and say that H is a **rational Puiseux monoid**⁽²¹⁾ if $H \subseteq \mathbb{Q}_{\geq 0}$.

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 (T. & Yan · PAMS, 202*)

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

No analogue of Nathanson's theorem is available for (finite) subsets of \mathbb{R} , and the question arises whether rationality is really necessary. More generally, the following is another instance of the Functorial Isomorphism Problem (Slide 15).

Problem 2.

Given a class \mathcal{O} of monoids, prove/disprove that $\mathcal{P}_{\text{fin},1}(H) \simeq \mathcal{P}_{\text{fin},1}(K)$, for some $H, K \in \mathcal{O}$, iff $H \simeq K$.

I conjecture a “Yes!” for cancellative monoids (cf. the remarks on Slide 23).

⁽²¹⁾Rational Puiseux monoids have been intensively studied by F. Gotti since 2018. They are indeed much older, but Gotti's work has bolstered a revival of the topic.



1. Generalities on semigroups, monoids, and groups
2. Power semigroups and the Tamura–Shafer problem
3. Power monoids and the Bienvenu–Geroldinger conjecture
- 4. Morphology of power semigroups, I**
5. Morphology of power semigroups, II
6. References



Be transformed!

The previous problems motivate the study of morphisms between power sgrps. In particular, Weihao Yan and I have posed the following:

Problem 3.

Given a monoid M , “determine” the (sgrp) automorphisms of $\mathcal{P}_{\text{fin},1}(M)$.

In the notation of Slide 9, it is readily seen that, for each $f \in \text{Aut}(M)$, the fnc

$$\mathcal{P}_{\text{fin},1}(M) \rightarrow \mathcal{P}_{\text{fin},1}(M): X \mapsto f[X]$$

is an automorphism of $\mathcal{P}_{\text{fin},1}(M)$, called the (**reduced finitary**) **augmentation** of f . An automorphism of $\mathcal{P}_{\text{fin},1}(M)$ is **inner** if it is the (reduced finitary) augmentation of an automorphism of M . So, we have a well-defined map

$$\Phi: \text{Aut}(M) \rightarrow \text{Aut}(\mathcal{P}_{\text{fin},1}(M))$$

sending an automorphism of M to its (reduced finitary) augmentation. In fact, Φ is an *injective (group) homomorphism* from $\text{Aut}(M)$ to $\text{Aut}(\mathcal{P}_{\text{fin},1}(M))$.

The question becomes whether Φ is also *surjective* and hence an isomorphism.



Place your bets, ladies and gents

Unsurprisingly, the answer is that, in general, Φ (as defined on Slide 34) is not surjective. This is already so in the fundamental case of $\mathcal{P}_{\text{fin},0}(\mathbb{N})$:

The only automorphism of a numerical monoid is the identity. Yet, the autogroup of $\mathcal{P}_{\text{fin},0}(\mathbb{N})$ is non-trivial, because it contains the **reversion map** $\text{rev}: \mathcal{P}_{\text{fin},0}(\mathbb{N}) \rightarrow \mathcal{P}_{\text{fin},0}(\mathbb{N}): X \mapsto \max X - X$.

What may be, however, surprising is that $\text{Aut}(\mathcal{P}_{\text{fin},0}(\mathbb{N}))$ is... small:

Theorem (T. & Yan · JCTA, 2025)

The only non-trivial automorphism of $\mathcal{P}_{\text{fin},0}(\mathbb{N})$ is the reversion map.

Somehow, this hints that homomorphisms are not the “right morphisms” when it comes, say, to additive problems in the integers⁽²²⁾. Moreover:

Conjecture

If H is a numerical monoid $\neq \mathbb{N}$, then $\text{Aut}(\mathcal{P}_{\text{fin},0}(H))$ is trivial.

⁽²²⁾A better alternative is offered by Freiman homomorphisms (see, e.g., Sects. 2.8, 3.1, and 4.5 and Chap. 20 in D. Gryniewicz, *Structural Additive Theory*, Springer, 2013).

A characterization

In fact, things are even more surprising if we consider the next:

Theorem (T. & Yan · JCTA, 2025)

The following are equivalent for an endomorphism f of $\mathcal{P}_{\text{fin},0}(\mathbb{N})$:

- (a) f is injective and $f(\{0, 1\}) = \{0, 1\}$.
- (b) f is surjective.
- (c) f is an automorphism.

One consequence of the previous result is the following corollary, which is crucial to the proof of the (main) theorem stated on Slide 28:

Corollary (T. & Yan · JCTA, 2025)

If f is an automorphism of $\mathcal{P}_{\text{fin},0}(\mathbb{N})$, then the following hold:

- (i) $\max X = \max f(X)$ for every $X \in \mathcal{P}_{\text{fin},0}(\mathbb{N})$.
- (ii) $\{0, k\}$ and $\llbracket 0, k \rrbracket$ are fixed points of f for all $k \in \mathbb{N}$.
- (iii) Either $f(\{0, 2, 3\}) = \{0, 1, 3\}$ or $f(\{0, 2, 3\}) = \{0, 2, 3\}$.



Hidden symmetries

In turn, one “strategically important” consequence of the corollary on Slide 29 is that each $f \in \text{Aut}(\mathcal{P}_{\text{fin},0}(\mathbb{N}))$ gives rise to a well-defined function

$$f^* : \mathcal{P}_{\text{fin},0}(\mathbb{N}) \rightarrow \mathcal{P}_{\text{fin},0}(\mathbb{N}) : \max X - f(X),$$

henceforth referred to as the **reversal** of f .

Interestingly enough, f^* is something more than just a function (which reveals the existence of a “hidden symmetry” in the problem):

Lemma

The reversal of an automorphism of $\mathcal{P}_{\text{fin},0}(\mathbb{N})$ is itself an automorphism.

In particular, the reversion map (Slide 28) is the reversal of the identity.

It follows that the automorphism group of $\mathcal{P}_{\text{fin},0}(\mathbb{N})$ is determined by those automorphisms that fix the set $\{0, 2, 3\}$.

Thus, we are *naturally* led to consider the behavior of the automorphisms of $\mathcal{P}_{\text{fin},0}(\mathbb{N})$ w.r.t. the sets of the form $\{0, a, a + 1\}$ with $a \in \mathbb{N}$.



A bridging lemma

We have already mentioned (Slide 29) that every automorphism f of $\mathcal{P}_{\text{fin},0}(\mathbb{N})$ does belong to one of two classes, as we have that

$$\text{either } f(\{0, 2, 3\}) = \{0, 2, 3\} \text{ or } f(\{0, 2, 3\}) = \{0, 1, 3\}.$$

The goal is now to show that an automorphism in the first class must also fix *certain* sets of the form $\{0\} \cup \llbracket b, c \rrbracket$ with $b, c \in \mathbb{N}$.

Lemma 1.

Assume $\{0, 2, 3\}$ is a fixed point of an automorphism f of $\mathcal{P}_{\text{fin},0}(\mathbb{N})$.

- (i) The set $\{0, a, a + 1\}$ is a fixed point of f for every $a \in \mathbb{N}$.*
- (ii) The set $\{0\} \cup \llbracket a, na + \frac{1}{2}n(n + 1) \rrbracket$ is a fixed point of f for all $a, n \in \mathbb{N}$ with $n \geq a + 1$.*

Key to the proof is the observation that, for all $a, n \in \mathbb{N}$ with $n \geq a + 1$,

$$\sum_{i=0}^{n-1} \{0, a + i, a + i + 1\} = \{0\} \cup \llbracket a, na + \frac{1}{2}n(n + 1) \rrbracket.$$



A non-standard induction

Based on the previous slides, proving that the only non-trivial automorphism of $\mathcal{P}_{\text{fin},0}(\mathbb{N})$ is the reversion map (Slide 28) is tantamount to showing that, if $\{0, 2, 3\}$ is fixed by an automorphism f of $\mathcal{P}_{\text{fin},0}(\mathbb{N})$, then f is the identity.

The proof is essentially a (sophisticated) induction on the boxing dimension of X , where we let the **boxing dimension** $\text{b.dim}(S)$ of a set $S \subseteq \mathbb{Z}$ be the smallest integer $k \geq 0$ for which there exist k (discrete) intervals whose union is S , with the understanding that if no such k exists then $\text{b.dim}(S) := \infty$.

It is fairly obvious that, for all $X, Y \subseteq \mathbb{Z}$,

$$\text{b.dim}(X \cup Y) \leq \text{b.dim}(X) + \text{b.dim}(Y), \quad (4)$$

a property we refer to as *subadditivity*.

The induction basis comes down to the observation that the boxing dimension of a set $X \in \mathcal{P}_{\text{fin},0}(\mathbb{N})$ is 1 iff X is an interval (and we already know from item (ii) of the corollary on Slide 29 that intervals are fixed by *any* automorphism).

We then prove certain identities on sumsets which, when combined with Eq. (4), make it possible to perform the inductive step and complete the proof.



1. Generalities on semigroups, monoids, and groups
2. Power semigroups and the Tamura–Shafer problem
3. Power monoids and the Bienvenu–Geroldinger conjecture
4. Morphology of power semigroups, I
- 5. Morphology of power semigroups, II**
6. References

Don't stop the music now

Of course, what we did with the autogroup of reduced finitary PMs in the previous section can also be done with the autogroup of other power sgrps.

Most notably, Kerou Wen and I have recently considered the following:

Problem 4.

Given a sgrp S , “determine” the autogroup of $\mathcal{P}_{\text{fin}}(S)$.

It is straightforward to show (cf. Slide 34) that, for each $f \in \text{Aut}(S)$, the fnc

$$\mathcal{P}_{\text{fin}}(S) \rightarrow \mathcal{P}_{\text{fin}}(S): X \mapsto f[X]$$

is an automorphism of $\mathcal{P}_{\text{fin}}(S)$, herein called the **(finitary) augmentation** of f . An automorphism of $\mathcal{P}_{\text{fin}}(S)$ is **inner** if it is the (finitary) augmentation of an automorphism of S . So, we have a well-defined map

$$\Phi: \text{Aut}(S) \rightarrow \text{Aut}(\mathcal{P}_{\text{fin}}(S))$$

sending an automorphism of S to its (finitary) augmentation. In fact, Φ is an *injective (group) homomorphism* from $\text{Aut}(S)$ to $\text{Aut}(\mathcal{P}_{\text{fin}}(S))$.

It is natural to ask whether Φ is also *surjective* and hence an isomorphism.



Not quite a déjà vu

In general, the answer is that Φ (as defined on Slide 34) is not surjective. Indeed, the main theorem of the previous section (Slide 28) implies that $\mathcal{P}_{\text{fin}}(\mathbb{N})$ has (exactly) one non-trivial automorphism, i.e., the fnc

$$\mathcal{P}_{\text{fin}}(\mathbb{N}) \rightarrow \mathcal{P}_{\text{fin}}(\mathbb{N}): X \mapsto \min X + \max X - X,$$

which is not particularly surprising in light of the results on $\text{Aut}(\mathcal{P}_{\text{fin},0}(\mathbb{N}))$.

However, let $\mathcal{P}_{\text{fin}}(\mathbb{Z})$ be the finitary PM (written additively) of $(\mathbb{Z}, +)$, the additive group of integers. The only non-trivial automorphism of $(\mathbb{Z}, +)$ is the fnc $\mathbb{Z} \rightarrow \mathbb{Z}: x \mapsto -x$. On the other hand, the autogroup of $\mathcal{P}_{\text{fin}}(\mathbb{Z})$ is infinite:

Theorem (T. & Wen)

The autogroup of $\mathcal{P}_{\text{fin}}(\mathbb{Z})$ is isomorphic to $\mathbb{Z}_2 \times \text{Dih}_\infty$, where \mathbb{Z}_2 is the (canonical realization of a) cyclic group of order 2 and

$$\text{Dih}_\infty := \text{Grp}\langle a, b \mid a = a^{-1}, aba = b^{-1} \rangle$$

is the infinite dihedral group on two generators a and b .

The result was a big surprise to me: I had “conjectured” $\text{Aut}(\mathcal{P}_{\text{fin}}(\mathbb{Z})) \simeq \mathbb{Z}_2$.



Sketch of proof

STEP 1: For every $\phi \in \text{Aut}(\mathcal{P}_{\text{fin}}(\mathbb{Z}))$, there exist an automorphism f of $\mathcal{P}_{\text{fin},0}(\mathbb{N})$ and a homomorphism $\alpha: \mathcal{P}_{\text{fin}}(\mathbb{Z}) \rightarrow (\mathbb{Z}, +)$ s.t.

$$\phi(X) = f(X - \min X) + \alpha(X), \quad \text{for all } X \in \mathcal{P}_{\text{fin}}(\mathbb{Z}).$$

STEP 2: If α is a homomorphism $\mathcal{P}_{\text{fin}}(\mathbb{Z}) \rightarrow (\mathbb{Z}, +)$, there exist $a, b \in \mathbb{Z}$ s.t.

$$\alpha(X) = a \min X + b \max X,$$

STEP 3: If f is an automorphism of $\mathcal{P}_{\text{fin}}(\mathbb{Z})$, then so is the fnc

$$-f: \mathcal{P}_{\text{fin}}(\mathbb{Z}) \rightarrow \mathcal{P}_{\text{fin}}(\mathbb{Z}): X \mapsto -X := \{-x: x \in X\}.$$

STEP 4: Up to a sign, the automorphisms of $\mathcal{P}_{\text{fin}}(\mathbb{Z})$ are precisely the fncs

$$\mathcal{P}_{\text{fin}}(\mathbb{Z}) \rightarrow \mathcal{P}_{\text{fin}}(\mathbb{Z}): X \mapsto X + a \min X - a \max X \quad (a \in \mathbb{Z})$$

or

$$\mathcal{P}_{\text{fin}}(\mathbb{Z}) \rightarrow \mathcal{P}_{\text{fin}}(\mathbb{Z}): X \mapsto X + (a - 1) \min X - (a + 1) \max X \quad (a \in \mathbb{Z}).$$

STEP 4: Use a characterization of Dih_{∞} from Robinson's book on groups.



1. Generalities on semigroups, monoids, and groups
2. Power semigroups and the Tamura–Shafer problem
3. Power monoids and the Bienvenu–Geroldinger conjecture
4. Morphology of power semigroups, I
5. Morphology of power semigroups, II
- 6. References**



References

- 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 & A. Geroldinger, *On algebraic properties of power monoids of numerical monoids*, Israel J. Math. (2025). DOI: 10.1007/s11856-024-2683-0 (arXiv:2205.00982).
- L. Cossu & S. Tringali, *Abstract Factorization Theorems with Applications to Idempotent Factorizations*, Israel J. Math **263** (2024), 349–395 (arXiv:2108.12379).
- L. Cossu & S. Tringali, *Factorization under local finiteness conditions*, J. Algebra **630** (Sep 2023), 128–161 (arXiv:2208.05869).
- Y. Fan & S. Tringali, *Power monoids: A bridge between Factorization Theory and Arithmetic Combinatorics*, J. Algebra **512** (2018), 252–294 (arXiv:1701.09152).
- P. A. García-Sánchez & S. Tringali, *Semigroups of ideals and isomorphism problems*, Proc. Amer. Math. Soc., to appear (arXiv: 2410.15622).
- S. Tringali, *An abstract factorization theorem and some applications*, J. Algebra **602** (July 2022), 352–380 (arXiv:2102.01598).
- S. Tringali, “On the isomorphism problem for power semigroups”, to appear in M. Brešar, A. Geroldinger, B. Olberding, and D. Smertnig (eds.), *Recent Progress in Ring and Factorization Theory*, Springer Proc. Math. Stat. **477**, Springer, 2025 (arXiv: 2402.11475).
- S. Tringali & W. Yan, *A conjecture by Bienvenu and Geroldinger on power monoids*, Proc. Amer. Math. Soc., to appear (arXiv:2310.17713).
- S. Tringali & W. Yan, *On power monoids and their automorphisms*, J. Comb. Theory Ser. A **209** (2025), #105961, 16 pp. (arXiv:2312.04439).