EVERY SEMIGROUP OF ORDER AT MOST FIVE IS GLOBALLY DETERMINED

KOREA SUPERINTELLIGENCE LABS

ABSTRACT. The *power semigroup* $\mathcal{P}(S)$ of a semigroup S is the set of nonempty subsets of S under $A \cdot B = \{ab : a \in A,\ b \in B\}$, and S is *globally determined* when $\mathcal{P}(S) \cong \mathcal{P}(T)$ forces $S \cong T$. Whether every finite semigroup is globally determined is a question of Schein and, independently, Tamura, recorded as Problem 5.1 of the recent edition of Lyapin's notebook of open problems; it is open, notwithstanding a 1987 announcement without proof that has propagated through the literature as a theorem. We settle the question for all semigroups of order at most five, with the second semigroup ranging over *all* finite semigroups: if $|S_1| \le 5$, S_2 is finite and $\mathcal{P}(S_1) \cong \mathcal{P}(S_2)$, then $|S_1| = |S_2|$ and $S_1 \cong S_2$. The second order is not assumed but forced, because $|\mathcal{P}(S)| = 2^{|S|} - 1$. The proof combines an isomorph-free enumeration of the 2 133 semigroups of order at most five with a single individualization–refinement invariant of a finite magma, proved to be an isomorphism invariant, and checked once per order to be injective on the power semigroups of the catalogue. The whole argument, including the finite searches, is machine-checked in Lean 4; separately, an independent implementation in C carries the census through order six.

1. INTRODUCTION

Let S be a semigroup. Its *power semigroup* $\mathcal{P}(S)$ is the set of nonempty subsets of S, made a semigroup by the setwise product

$$A \cdot B \;=\; \{ab \;:\; a \in A,\; b \in B\}.$$

The construction is faithful in one direction — isomorphic semigroups have isomorphic power semigroups — and the question is whether it is faithful in the other. Call S *globally determined* if $\mathcal{P}(S) \cong \mathcal{P}(T)$ implies $S \cong T$ for every semigroup T.

The question was raised by B. M. Schein at the 1966 ICM and, independently, by T. Tamura, who conjectured a positive answer. Mogiljanskaja [8] refuted it for the class of all semigroups; her counterexamples are infinite. For finite semigroups the question is recorded, in the current edition of Lyapin's notebook of unsolved problems in semigroup theory [1, §5], as

> **Problem 5.1.** (E. M. Mogiljanskaja) Does the isomorphism of power semigroups implies the isomorphism of the original semigroups in the class of finite semigroups?

It is open. This has to be said plainly, because the literature says otherwise in places. Gan and Zhao [3, p. 63] list "finite semigroups" among the classes known to be globally determined, citing Tamura's 1987 survey [13]; that survey states the result *without proof* and promises details that never appeared. Hamilton and Nordahl [4, p. 5] record the isomorphism problem for finite semigroups as open, and Liu and Tringali [14, §1] write that the question "remains open for *finite* semigroups (despite some authors having claimed otherwise)"; the same status statement appears in Tringali's survey [15, §1], and the documentary trail behind the 1987 announcement is assembled in [9].

A good deal is known for restricted classes. Groups, semilattices, completely 0-simple semigroups, rectangular groups, Clifford semigroups [3, Thm. 4.7], bands, normal orthogroups and cancellative commutative semigroups have all been shown globally determined — references for each are collected in the introductions of [2] and [14] — and, the strongest of these for present purposes, so has the whole class $\mathcal{CR}$ of completely regular semigroups [2]. Every finite union of groups is therefore already covered by published theorems. What is not covered is the non-regular remainder, and no result of the shape "every semigroup of order at most n is globally determined" appears to have been published for any n.

This paper supplies such a result for $n = 5$.

Theorem 1.1 (Theorem 3.4 below)**.** *Let S_1 be a semigroup with $|S_1| \leq 5$ and let S_2 be any finite semigroup. If $\mathcal{P}(S_1) \cong \mathcal{P}(S_2)$ then $|S_1| = |S_2|$ and $S_1 \cong S_2$.*

Only the first order is bounded. The second is forced rather than assumed, because $|\mathcal{P}(S)| = 2^{|S|}-1$ (Lemma 3.1) and $x \mapsto 2^x - 1$ is injective; so a semigroup of order at most 5 can have a power semigroup isomorphic only to the power semigroup of a semigroup of the same order.

The proof is a census, and its two components are standard technique. One is an isomorph-free enumeration of the multiplication tables of order n, cell by cell, pruned by partial associativity and by a partial-canonicity test in the style of orderly generation (Read; Faradžev; McKay). The other is a single isomorphism invariant Φ of a finite magma, built by individualization and refinement — the standard graph-isomorphism toolkit [7] — and proved invariant under relabelling. What makes the combination cheap is a change of quantifier: instead of certifying, for each colliding pair of power semigroups, that the two are *not* isomorphic, one shows that a single invariant takes pairwise distinct values on the whole catalogue of power semigroups, which is one injectivity check per order.

Nothing here settles Problem 5.1, and nothing here suggests that it is easy. The census is exhausted at order six (Remark 6.2), and a counterexample, if there is one, is larger than anything a census of this kind will reach.

2. Notation and preliminaries

Fix $n \geq 1$ and write $[n] = \{0, 1, \ldots, n-1\}$. A *table* of order n is a map $m\colon [n] \times [n] \to [n]$, written $m(x, y)$ or xy; it is *associative* when $m(m(x, y), z) = m(x, m(y, z))$ for all x, y, z, and a semigroup of order n is exactly an associative table of order n. Every finite semigroup is isomorphic to one, so nothing is lost by working with tables throughout.

The symmetric group $\mathfrak{S}_n$ acts on tables of order n by relabelling,

$$(\sigma \cdot m)(x, y) \;=\; \sigma\big(m(\sigma^{-1}x,\ \sigma^{-1}y)\big), \tag{1}$$

and two tables m, m' of the same order are *isomorphic*, $m \cong m'$, when $\sigma \cdot m = m'$ for some $\sigma \in \mathfrak{S}_n$. This is the same relation as the existence of a bijection e with $e(m(x, y)) = m'(e(x), e(y))$.

For a table m of order n let $\mathcal{P}(m)$ denote the set of nonempty subsets of $[n]$ under $A \cdot B = \{m(a, b) : a \in A,\ b \in B\}$. If m is associative so is $\mathcal{P}(m)$. For tables m_1, m_2 of orders n_1, n_2 — possibly different — we write $\mathcal{P}(m_1) \cong \mathcal{P}(m_2)$ for the existence of a bijection $e\colon \mathcal{P}(m_1) \to \mathcal{P}(m_2)$ with $e(A \cdot B) = e(A) \cdot e(B)$. Allowing the two orders to differ is what lets the main theorem quantify S_2 over all finite semigroups while bounding only $|S_1|$.

Two constructions used repeatedly. First, *multiset hashing*: a finite list ℓ of naturals is summarized by

$$h(\ell) \;=\; \prod_{v \in \ell} g(v) \bmod p, \qquad p = 2^{31} - 1,$$

for a fixed injectivity-agnostic mixing map g. Since the value is a product, h depends only on the multiset of entries; that is the only property of h used anywhere, and it is the reason no theory of sorting is needed. Hash collisions can merge two distinct multisets, which weakens any invariant built from h; they can never make it fail to be an invariant.

Second, the *index bridge*. The invariant of §4 runs on a table, so $\mathcal{P}(m)$ is transported to a table on $[2^n - 1]$ by numbering a nonempty subset $A \subseteq [n]$ by its bit mask less one, $\varepsilon(A) = \sum_{i \in A} 2^i - 1$, with inverse δ reading the bits of $e + 1$. Write $\mathcal{P}^\flat(m)$ for the resulting table of order $2^n - 1$. The two round-trip identities

$$\delta(e) \neq \emptyset \quad \text{and} \quad \varepsilon(\delta(e)) = e \qquad (e \in [2^n - 1]) \tag{2}$$

are a finite check at each fixed n, and by a counting argument they already give $\delta(\varepsilon(A)) = A$ for every nonempty A; so no bit arithmetic enters any proof.

3. The main theorem

Lemma 3.1. *$|\mathcal{P}(m)| = 2^n - 1$ for every table m of order n.*

Proof. The nonempty subsets of $[n]$ are the subsets other than $\emptyset$. $\square$

Lemma 3.2. *If $\mathcal{P}(m_1) \cong \mathcal{P}(m_2)$ for tables of orders n_1, n_2, then $n_1 = n_2$.*

Proof. By Lemma 3.1 the bijection gives $2^{n_1} - 1 = 2^{n_2} - 1$, and $x \mapsto 2^x$ is injective on $\mathbb{N}$. $\square$

Let R_n denote the catalogue of §5: an explicit list of associative tables of order n meeting every isomorphism class exactly once. The engine of the proof is the following reduction, which converts the theorem for one order into one injectivity statement about one invariant.

Proposition 3.3. *Let Φ be the invariant of §4 and let $n \geq 1$. Suppose the round-trips* (2) *hold at n and that*

$$c \longmapsto \Phi\big(\mathcal{P}^\flat(c)\big), \qquad c \in R_n,$$

is injective. Then any two semigroups m_1, m_2 of order n with $\mathcal{P}(m_1) \cong \mathcal{P}(m_2)$ are isomorphic.

Proof. Choose $c_i \in R_n$ with $m_i \cong c_i$. Isomorphic tables have isomorphic power semigroups, so $\mathcal{P}(c_1) \cong \mathcal{P}(c_2)$; by (2) the index bridge turns this into an isomorphism of the tables $\mathcal{P}^\flat(c_1) \cong \mathcal{P}^\flat(c_2)$; by Theorem 4.1 the two have the same invariant; by hypothesis $c_1 = c_2$; and therefore $m_1 \cong c_1 = c_2 \cong m_2$. $\square$

Theorem 3.4. *Let m_1 be an associative table of order $n_1 \leq 5$ and m_2 an associative table of any order n_2. If $\mathcal{P}(m_1) \cong \mathcal{P}(m_2)$ then $n_1 = n_2$ and $m_1 \cong m_2$. Equivalently: every semigroup of order at most five is globally determined within the class of finite semigroups.*

Proof. Lemma 3.2 gives $n_1 = n_2$, so both tables have the same order $n \leq 5$; the case $n = 0$ is vacuous. For each $n \in \{1, 2, 3, 4, 5\}$ apply Proposition 3.3, whose two hypotheses at that n are Theorem 4.2 (injectivity of Φ on the catalogue) and the round-trip check (2). Both are finite computations, listed in §7. $\square$

Remark 3.5. The restriction of S_2 to finite semigroups in Theorem 3.4 is not a real restriction: if S_2 were infinite then $\mathcal{P}(S_2)$ would be infinite while $\mathcal{P}(S_1)$ has $2^{n_1} - 1 \leq 31$ elements. This one-line argument is outside the formal development, which is stated for carriers $[n]$ throughout.

Remark 3.6. The conclusion is isomorphism, not equality of tables, and it cannot be strengthened: Proposition 6.1 (v) exhibits two distinct tables of order three with isomorphic power semigroups.

4. The invariant

Let M be a table of order N (in the application $N = 2^n - 1$ and $M = \mathcal{P}^\flat(c)$). A *colouring* is a map $c\colon [N] \to \mathbb{N}$. One round of refinement replaces c by the rank function of a signature. The signature of x combines $c(x)$ with two multiset hashes:

$$\operatorname{row}(x) = h\Big(\big\langle\, (c(a),\, c(xa),\, c(ax)) \;:\; a \in [N] \,\big\rangle\Big), \qquad \operatorname{pre}(x) = h\Big(\big\langle\, (c(a), c(b)) \;:\; ab = x \,\big\rangle\Big),$$

the second taken over all ordered pairs (a, b) with $ab = x$. Write $\operatorname{sig}(x)$ for the packed combination of $c(x)$, $\operatorname{row}(x)$ and, when the preimage term is switched on, $\operatorname{pre}(x)$; the new colour of x is $\#\{y : \operatorname{sig}(y) < \operatorname{sig}(x)\}$, a rank, hence canonical. Each round also emits the multiset $h(\langle \operatorname{sig}(x) \rangle_x)$ into a running transcript.

The preimage term is what makes refinement start at all. From the constant colouring, row is constant on any magma — every row and column of the table is a full list of elements' colours, all equal — so plain colour refinement never separates anything on the first round. With the preimage term as a seed it does.

Individualization is the map $\mathrm{ind}(c,v)(x) = 2c(x) + [x = v]$, giving v a colour of its own. The invariant is then

$$\Phi(M) \;=\; \Big(\tau_{r_b,s}(M)\ ,\ h\big(\langle\, \tau_{r_i}\big(M, \mathrm{ind}(c_{r_b}, v)\big)\ :\ v \in [N]\,\rangle\big)\Big), \tag{3}$$

where $\tau_{r_b,s}(M)$ is the transcript of r_b refinement rounds from the constant colouring with the preimage term used in the first s of them, c_{r_b} is the colouring they produce, and τ_{r_i} is the transcript of r_i further rounds after individualizing v. The settings used throughout are

$$r_b = 3, \qquad s = 1, \qquad r_i = 2.$$

Theorem 4.1. $\Phi(\sigma \cdot M) = \Phi(M)$ *for every table* M *of order* N *and every* $\sigma \in \mathfrak{S}_N$*. Consequently isomorphic tables have equal invariants, and distinct invariants certify non-isomorphism.*

Proof sketch. Every constituent of (3) is either a multiset hash or a rank. Relabelling permutes the list $[N]$ and, in the preimage term, permutes the list of ordered pairs while commuting with the filter $ab = x$; so each hashed list is carried to a permutation of itself and h is unchanged. Ranks are counts over the same multiset of signatures, hence unchanged as well. Formally one shows $\mathrm{sig}_{\sigma\cdot M,\, c\circ\sigma^{-1}}(\sigma x) = \mathrm{sig}_{M,c}(x)$, then that a round transforms as $\mathrm{step}(\sigma \cdot M, c\circ\sigma^{-1}) = \mathrm{step}(M, c)\circ\sigma^{-1}$, and induction along the rounds does the rest; individualization commutes with relabelling in the same way, and the outer hash over v absorbs the permutation of $[N]$. No computation enters this proof. ☐

Theorem 4.2. *For each* $n \in \{1, 2, 3, 4, 5\}$ *the map* $c \mapsto \Phi(\mathcal{P}^\flat(c))$ *is injective on the catalogue* R_n*.*

Proof: exhaustive computation. For each n the list R_n of $|R_n| \in \{1, 5, 24, 188, 1915\}$ tables is enumerated, each representative's power table $\mathcal{P}^\flat(c)$ of order $2^n - 1 \in \{1, 3, 7, 15, 31\}$ is materialized, Φ is evaluated on it at the settings $(r_b, s, r_i) = (3, 1, 2)$, and the resulting list of values is tested for duplicates. The largest instance is $n = 5$: 1 915 power tables of order 31, about 1.8×10^6 table cells in all. No collisions occur at any of the five orders. This check, together with the round-trip check (2), is the whole computational content of Theorem 3.4. ☐

Remark 4.3. The two ingredients of Φ are both load-bearing, and this is checked rather than argued: Proposition 6.1 (ii) records that refinement without individualization fails to separate R_n already at $n = 3$, and continues to fail at $n = 4$ and $n = 5$. What the checked control asserts is only that a collision occurs; counting the collisions is a measurement, made with the C implementation of Remark 6.2. With the individualization half of (3) dropped, the base transcript $\tau_{3,1}$ takes 1 778 distinct values on the 1 915 order-five power semigroups, leaving 273 of them in 136 colliding buckets. Proposition 6.1 (iii) records that Φ is not injective on tables in general, as an invariant must not be.

5. The catalogue

Order the n^2 cells of a table row-major and read the resulting string of base-n digits as an integer $\kappa(m)$; call m *canonical* when $\kappa(m) \le \kappa(\sigma \cdot m)$ for all $\sigma \in \mathfrak{S}_n$. Each isomorphism class contains exactly one canonical table, so the canonical associative tables form a transversal.

They are found by a cell-by-cell search. A partial assignment of the first k cells is kept when (a) every associativity instance all four of whose cells are already filled holds, and (b) no relabelling σ makes the image's digit string strictly smaller on the filled prefix. Test (b) is the partial-canonicity prune: since cells are filled in order of decreasing significance for κ, a beaten prefix has no canonical completion. The prune must stop at the first position whose *source* cell under σ is unfilled; unfilled cells read as 0, and because σ acts on values as well as on cells, 0 bounds the image entry neither above nor below, so comparing there would be unsound in both directions.

Theorem 5.1. *For* $n \in \{1, 2, 3, 4, 5\}$ *the list* R_n *produced by this search is a catalogue of the semigroups of order* n*: every member is associative, every associative table of order* n *is isomorphic to a member, no two members are isomorphic, and*

$$|R_1|, \ldots, |R_5| \;=\; 1,\ 5,\ 24,\ 188,\ 1915.$$

Proof sketch. Membership implies associativity because the last level of the search tests every associativity instance. Completeness — every canonical associative table survives to every level — follows from the soundness of the prune: a `true` verdict at level k exhibits a relabelling with strictly smaller key, which a canonical table does not admit. Pairwise non-isomorphism is *not* taken from the canonical form: it is read off Theorem 4.2, since two isomorphic members would have equal invariants. This is deliberate — it means the search needs no completeness property of its list of candidate relabellings, and a missing relabelling could only weaken the prune and leave more tables in R_n, never fewer. The five lengths are exhaustive computations: the order-five search visits 119 100 nodes and returns exactly 1 915 tables, against 125 624 130 nodes for the same cell-by-cell search with the canonicity prune switched off. □

The lengths reproduce the known counts of semigroups of order n up to isomorphism, A027851 [10]; they are quoted here as a check on the enumeration, not as a new determination.

6. Controls

A census can be satisfied by a misplaced quantifier while every proof in it still succeeds. The following are refutations rather than arguments, each a finite check.

Proposition 6.1. (i) *The catalogue counts are neither the counts up to isomorphism* and *anti-isomorphism (A001423:* 18*,* 126*,* 1160 *at orders* $3, 4, 5$ [11]*) nor the counts of associative operations on labelled points (A023814:* 113*,* 3492*,* $183\,732$ [12]*):* $|R_3| \neq 18, 113$*;* $|R_4| \neq 126, 3492$*;* $|R_5| \neq 1160, 183732$.

(ii) *Colour refinement without individualization does not separate* R_n *for* $n = 3, 4, 5$.

(iii) Φ *is not injective on tables: there are distinct tables* $T \neq U$ *of order three with* $\Phi(\mathcal{P}^\flat(T)) = \Phi(\mathcal{P}^\flat(U))$ *— they are isomorphic, exactly as Theorem 4.1 demands.*

(iv) $\mathcal{P}^\flat(c)$ *is associative for every* $c \in R_4$ *and every* $c \in R_5$*, checked on the table the invariant actually runs on and independently of the abstract proof that* $\mathcal{P}(S)$ *is a semigroup.*

(v) *The conclusion of Theorem 3.4 cannot be strengthened to equality: there are associative tables* $T \neq U$ *of order three with* $\mathcal{P}(T) \cong \mathcal{P}(U)$*. The same witness shows the hypotheses of Theorem 3.4 are not vacuous.*

Proof sketch. (i) is arithmetic on Theorem 5.1. (ii) is the exhaustive evaluation of the refinement-only invariant on R_3, R_4, R_5 followed by a duplicate test, which reports a duplicate in each case. (iii) and (v) use the two null semigroups on [3] with zero 0 and zero 1: they are distinct tables, isomorphic by the transposition (0 1), so Theorem 4.1 gives (iii) and the forward direction of the power construction gives (v). (iv) is an exhaustive associativity test on the 188 power tables of order 15 and the 1 915 of order 31. □

The two-sided form of (i) matters: the count could be wrong by quotienting too much or too little, and A027851 sits between A001423 and A023814. Quotienting by anti-isomorphism as well would be unsound here without a further argument, since $\mathcal{P}(S^{\mathrm{op}}) = \mathcal{P}(S)^{\mathrm{op}}$ and an anti-isomorphism class does not by itself carry an isomorphism question.

Remark 6.2. Outside the formal development, the census has been carried one order further, to order six, by an independent implementation in C that shares no code with the verified one and makes its own choice of round counts. It enumerates the 28 634 semigroups of order six and evaluates the invariant on their power semigroups of order 63; all but one pair of representatives separate. That pair is settled negatively twice over — by a stronger invariant obtained by running the preimage term in every refinement round, and by an exact backtracking isomorphism search that terminates in 11 nodes — so, since distinct invariant values certify non-isomorphism and different pairs may legitimately use different invariants, every semigroup of order six is globally determined within the class of finite semigroups as well. This is reported as a computation, not as a theorem of this paper: it is not machine-checked, and it is not carried by the uniform invariant that the theorems above use.

7. Verification

All statements above except the remarks explicitly marked as lying outside the formal development are machine-checked in Lean 4 [5] against Mathlib [6]. The structural mathematics — the enumeration's soundness and completeness, the soundness of the partial-canonicity prune, Theorem 4.1, Lemmas 3.1 and 3.2, the index bridge and Proposition 3.3 — is proved in the kernel with no evaluation of any kind, depending only on the axioms `propext`, `Classical.choice` and `Quot.sound`. The finite searches are discharged by compiled evaluation, and the trusted computational surface of Theorem 3.4 is exactly ten of them: for each $n \in \{1, \ldots, 5\}$, the separation check of Theorem 4.2 and the round-trip check (2). Theorem 5.1 adds the five catalogue lengths, and Proposition 6.1 the three refinement-only and the two power-associativity evaluations, each of which is the sole computational dependency of the statement using it; the witness for part (v) needs no evaluation at all. Because the evaluated definitions must be compilable into a shared library, they live in a module importing nothing, and a separate layer of transcription lemmas — itself free of evaluation — proves that this mirror computes exactly the objects the theorems are about. On a single machine the orders 1–4 checks take about 2 seconds and the order-five check about 80 seconds. The catalogue lengths and every separation check were independently reproduced by the C implementation mentioned in Remark 6.2. Repository reference to be added at submission.

References

[1] S. Bershadsky, S. Kublanovsky, G. Mashevitzky (eds.), *The Lyapin's notebook: a collection of unsolved problems in Semigroup Theory*, arXiv:2604.04763v1, 2026. (Problems are numbered by section; the quotation is from v1.)

[2] B. Yu, X. Zhao, *Global determinism of completely regular semigroups*, Comm. Algebra, published online 8 May 2026, doi:10.1080/00927872.2026.2659846; arXiv:2502.05746.

[3] A. Gan, X. Zhao, *Global determinism of Clifford semigroups*, J. Aust. Math. Soc. **97** (2014), no. 1, 63–77.

[4] H. B. Hamilton, T. E. Nordahl, *Tribute for Takayuki Tamura on his 90th birthday*, Semigroup Forum **79** (2009), 2–14.

[5] L. de Moura, S. Ullrich, *The Lean 4 theorem prover and programming language*, in: Automated Deduction — CADE-28, Lecture Notes in Comput. Sci. 12699, Springer, 2021, 625–635.

[6] The mathlib Community, *The Lean mathematical library*, in: Certified Programs and Proofs (CPP 2020), ACM, 2020, 367–381; arXiv:1910.09336.

[7] B. D. McKay, A. Piperno, *Practical graph isomorphism, II*, J. Symbolic Comput. **60** (2014), 94–112; arXiv:1301.1493.

[8] E. M. Mogiljanskaja, *Non-isomorphic semigroups with isomorphic semigroups of subsets*, Semigroup Forum **6** (1973), 330–333. (The construction is dated 1972 in [1, §5]; the paper appeared in 1973.)

[9] S. Tringali, *What is the status of the isomorphism problem for finite power semigroups?*, MathOverflow question 508548, 26 February 2026, `https://mathoverflow.net/q/508548`.

[10] OEIS Foundation Inc., *Sequence A027851: number of nonisomorphic semigroups of order n*, The On-Line Encyclopedia of Integer Sequences.

[11] OEIS Foundation Inc., *Sequence A001423: number of semigroups of order n, considered to be equivalent when they are isomorphic or anti-isomorphic (by reversal of the operator)*, The On-Line Encyclopedia of Integer Sequences.

[12] OEIS Foundation Inc., *Sequence A023814: number of associative binary operations on an n-set; number of labeled semigroups*, The On-Line Encyclopedia of Integer Sequences.

[13] T. Tamura, *On the recent results in the study of power semigroups*, in: S. M. Goberstein, P. M. Higgins (eds.), Semigroups and their Applications, Reidel, 1987, 191–200.

[14] S. Liu, S. Tringali, *Power semigroups and two rigidity theorems for groups*, arXiv:2606.01917, 2026.

[15] S. Tringali, *Power monoids and their arithmetic: a survey*, Amer. Math. Monthly, to appear; arXiv:2602.15754.