An Arithmetic Inverse Result for Matrix Groups

Daniel Smertnig
(University of Ljubljana & IMFM)

based on joint work with **Antoni Puch** (U Warsaw)

arXiv:2410.03444

Warsaw Algebra Seminar,
November 27, 2025

UNIVERSITY OF LJUBLJANA
Faculty of Mathematics and Physics

(Fake) Motivation

(Fake) Motivation

Burnside problem (1902)

Is every finitely generated torsion group finite?

No! (Golod–Shafarevitch 1964)

Let K be a field.

Theorem (Burnside–Schur)

Every finitely generated torsion subgroup $G \leq \mathrm{GL}_d(K)$ is finite.

Also true for f.g. periodic subsemigroups of $K^{d\times d}$.

(Fake) Motivation

Theorem (Burnside–Schur)

Every finitely generated torsion subgroup $G \leq \mathrm{GL}_d(K)$ is finite.

Let $K = \overline{K}$, e.g. $K = \mathbb{C}$ or $K = \overline{\mathbb{Q}}$.

Let the spectrum $\sigma(G)$ be the set of all eigenvalues of all matrices in G.

- G torsion implies that $\sigma(G)$ consists of roots of unity, so $|\sigma(G)| < \infty$ (using f.g.).
- Converse? Suppose G is irreducible (no proper G-invariant subspace of K^d).
  Then there exists a K-basis $A_1, \ldots, A_{d^2} \in G$ of $K^{d\times d}$, and

  $$\varphi\colon K^{d\times d} \to K^{d^2}, \quad X \mapsto \big(\mathrm{Tr}(XA_1), \ldots, \mathrm{Tr}(XA_{d^2})\big)$$

  is a vector space isomorphism.

  Since $\varphi(G) \subseteq (\underbrace{\sigma(G) + \cdots + \sigma(G)}_{d \text{ times}})^{d^2}$, the group G is finite.

(Fake) Motivation

Proposition

Let $K = \overline{K}$ and $G \leq \mathrm{GL}_d(K)$ be finitely generated.

1. If G is irreducible, then $|\sigma(G)| < \infty \Leftrightarrow |G| < \infty$.
2. $|\sigma(G)| < \infty$ if and only if there exists $T \in \mathrm{GL}_d(K)$ such that there is a block-structure

$$TGT^{-1} = \begin{bmatrix} G_1 & * & \cdots & * \\ 0 & G_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & * \\ 0 & \cdots & 0 & G_r \end{bmatrix}$$

   with finite groups G_i. ("G is tame").

Weakening the restriction on $\sigma(G)$

Definition

Let $G \leq \mathrm{GL}_d(K)$. The spectrum $\sigma(G)$ is finitely generated (equivalently, satisfies the Pólya property) if there exists a finitely generated subgroup $\Gamma \leq \overline{K}^\times$ such that

$$\sigma(G) \subseteq \Gamma.$$

Lemma

If $K = \overline{K}$ and G is irreducible with f.g. spectrum, then there exists $M \geq 0$, f.g. $\Gamma \leq K^\times$ such that

$$G \subseteq (M \cdot \Gamma_0)^{d \times d} \quad \text{with} \quad \Gamma_0 \coloneqq \Gamma \cup \{0\}, \quad M \cdot \Gamma_0 = \underbrace{\Gamma_0 + \cdots + \Gamma_0}_{M \text{ times}}.$$

If $G \subseteq (M \cdot \Gamma_0)^{d \times d}$ (for some Γ, M), then G has the Bézivin property.

Examples

Bézivin groups ($G \subseteq (M \cdot \Gamma_0)^{d \times d}$):

- Finite groups.
- Finitely generated groups of monomial matrices.
- The Bézivin property is closed under conjugation (M, Γ may change).
- If G is Bézivin and $V \subseteq K^d$ is G-invariant, the induced $G|_V \leq \mathrm{GL}(V)$ and $\overline{G} \leq \mathrm{GL}(K^d/V)$ are Bézivin,

$$\begin{bmatrix} G_V & * \\ 0 & \overline{G} \end{bmatrix}.$$

- G is Bézivin if the representation $j\colon G \hookrightarrow \mathrm{GL}_d(K)$ is the epimorphic image of a monomial representation.

$$\begin{array}{ccc} & & \mathrm{GL}(V) \\ & \overset{\varphi}{\nearrow} & \downarrow \pi \\ G & \xrightarrow{\;j\;} & \mathrm{GL}_d(K) \end{array}$$

($\pi\colon V \twoheadrightarrow K^d$ such that $\pi(Av) = A\pi(v)$ for $A \in G, v \in V$)

Examples

Finitely generated spectrum:

- block-triangular groups with diagonal blocks from the previous list, e.g.,
- block-triangular groups with monomial diagonal blocks.
- closed under conjugation, epimorphic images.

Aside: Submultiplicative Spectrum

Definition

A semigroup $S \subseteq K^{d\times d}$ has submultiplicative spectrum if $\sigma(AB) \subseteq \sigma(A)\sigma(B)$ for A, $B \in S$ (Lambrou–Longstaff–Radjavi '92).

- A finitely generated S with submultiplicative spectrum has finitely generated spectrum.
- Submultiplicative spectrum is much more restrictive.

Theorem (Radjabalipour–Radjavi '99, Radjavi '00)

If $S \subseteq \mathbb{C}^{d\times d}$ is irreducible and has submultiplicative spectrum, then there is a finite nilpotent group $G \leq \mathrm{GL}_d(\mathbb{C})$ such that, up to conjugation,

$$\mathbb{C}S = \mathbb{C}G.$$

Kramar '04, '05, '06; Grunenfelder–Košir–Omladič–Radjavi '12

Problem and Main Result

The problem

Problem

(I) Which matrix groups are Bézivin?
($G \subseteq (M \cdot \Gamma_0)^{d \times d}$ with $M \geq 0$, $\Gamma \leq K^\times$ finitely generated)

(II) Which matrix groups have finitely generated spectrum?
($\sigma(G) \subseteq \Gamma$ with $\Gamma \leq \overline{K}^\times$ finitely generated)

Main Results

Reminder: G being Bézivin means $G \subseteq (M \cdot \Gamma_0^{d\times d})$.

Theorem (Puch-S. '24)

Let $K = \overline{K}$ and $G \leq \mathrm{GL}_d(K)$ finitely generated. The following are equivalent.

(a) G is Bézivin.

(b) $G \hookrightarrow \mathrm{GL}_d(K)$ is an epimorphic image of a monomial representation of G.

(c) G is virtually simultaneously diagonalizable.

Similar result with $\mathrm{char}\, K = 0$ characterizing linear groups (of diagonalizable matrices) with bounded generation (BG) by Corvaja–Demeio–Rapinchuk–Ren–Zannier '23.

G has the BG property if and only if $G = \langle A_1 \rangle \cdots \langle A_n \rangle$.

Main Results

Theorem (Puch-S. '24)

Let $K = \overline{K}$ and $G \leq \mathrm{GL}_d(K)$ finitely generated. The following are equivalent.

(a) $\sigma(G)$ is finitely generated (Pólya property).

(b) $G \hookrightarrow \mathrm{GL}_d(K)$ is the epimorphic image of a block-triangular representation with monomial diagonal blocks.

(c) G is virtually solvable.

- For irreducible G: G Bézivin $\Leftrightarrow \sigma(G)$ finitely generated.
- (a) $\Leftrightarrow$ (c) was observed before by Bernik '05 in characteristic 0.
- Tits' alternative: f.g. $G \leq \mathrm{GL}_d(K)$ is either virtually solvable or contains a non-cyclic free subgroup.

Main Results (More General)

Theorem (Puch-S. '24)

Let K be a field, and $S \subseteq \mathrm{GL}_d(K)$ a semigroup that is finitely generated or $\mathrm{char}\, K = 0$.

(I) The following are equivalent.
- (a) S is locally Bézivin and K is uniformly power-splitting for S.
- (b) $S \hookrightarrow \mathrm{GL}_d(K)$ is an epimorphic image of a monomial representation of S (over K).
- (c) $\langle S \rangle$ is virtually simultaneously diagonalizable (over K).

(II) The following are equivalent.
- (a) S has locally finitely generated spectrum and K is uniformly power-splitting for S.
- (b) $S \hookrightarrow \mathrm{GL}_d(K)$ is the epimorphic image of a block-triangular representation with monomial diagonal blocks (over K).

K is uniformly power-splitting for S if there exists $N \geq 1$ such that for all eigenvalues $\lambda \in \overline{K}$ of all $A \in S$, we have $\lambda^N \in K$.

On the Proof

Key Tool: Unit Equations

Let $\operatorname{char} K = 0$, and $\Gamma \le K^\times$ finitely generated.

Solve

$$a_1 X_1 + \cdots + a_n X_n = 0$$

in $\Gamma_0 = \Gamma \cup \{0\}$.

Theorem (Evertse '84, van der Poorten–Schlickewei '82, '91)

Unit equations have only finitely many non-degenerate solutions (as projective points).

- A solution $(x_1, \ldots, x_n)$ is non-degenerate if $\sum_{i \in I} a_i x_i \neq 0$ for all $\varnothing \neq I \subsetneq \{1, \ldots, n\}$.
- Each solution can be partitioned into non-degenerate solutions of subequations.
- Characteristic $p > 0$ is different: Derksen–Masser '12, Adamczewski–Bell '12.

A Special Case of Our Theorem

Proposition (Special Case)

Let $K = \overline{K}$, $\operatorname{char} K = 0$, and $G \leq \mathrm{GL}_d(K)$ Bézivin, say,

$$G \subseteq (M \cdot \Gamma_0)^{d \times d}.$$

Assume there exists $A = \operatorname{diag}(\lambda_1, \ldots, \lambda_d) \in G$ **with** $(\lambda_i/\lambda_j)^n \neq 1$ **for all** $i \neq j$, $n \neq 0$**.**
Then every $B = (b_{ij}) \in G$ is monomial.

$$(B^k)_{i_0 i_k} = \sum_{1 \leq i_1, \ldots, i_{k-1} \leq d} \underbrace{b_{i_0 i_1} b_{i_1 i_2} \cdots b_{i_{k-1} i_k}}_{=: \beta(\mathbf{i}) \text{ with } \mathbf{i} = (i_0, i_1, \ldots, i_k)} = \sum_{1 \leq i_1, \ldots, i_{k-1} \leq d} \beta(\mathbf{i}).$$

Key Claim: For all $k \geq 0$: $\left| \{ \mathbf{i} : \beta(\mathbf{i}) \neq 0 \} \right| \leq M$.

$$(BA^{n_1} BA^{n_2} \cdots BA^{n_{k-1}} B)_{i_0 i_k} = \sum_{1 \leq i_1, \ldots, i_{k-1} \leq d} \beta(\mathbf{i}) \lambda_{i_1}^{n_1} \ldots \lambda_{i_{k-1}}^{n_{k-1}} \qquad \text{where} \qquad n_i \in \mathbb{Z}.$$

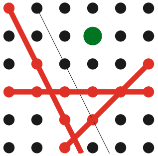
By the Bézivin property,

$$(BA^{n_1}BA^{n_2}\cdots A^{n_{k-1}}B)_{i_0 i_k} = \sum_{1\le i_1,\dots,i_{k-1}\le d} \beta(\mathbf{i})\lambda_{i_1}^{n_1}\cdots\lambda_{i_{k-1}}^{n_{k-1}} = \gamma_1(\mathbf{n}) + \cdots + \gamma_M(\mathbf{n}).$$

with $\gamma_i(\mathbf{n}) \in \Gamma_0$. **Unit equation!** Consider partitions into subequations:

1) Bad partitions: two terms $\mathbf{i} \neq \mathbf{j}$ on LHS in same non-degenerate subequation.
This is rare:

$$\varphi_{\mathbf{i},\mathbf{j}}\colon (\mathbb{Z}^{k-1}, +) \mapsto (\Gamma, \cdot), \quad \mathbf{n} \mapsto \left(\frac{\lambda_{i_1}}{\lambda_{j_1}}\right)^{n_1} \cdots \left(\frac{\lambda_{i_{k-1}}}{\lambda_{j_{k-1}}}\right)^{n_{k-1}}$$



has $\operatorname{rank} \operatorname{im} \varphi_{\mathbf{i},\mathbf{j}} \ge 1$, so $\operatorname{rank} \ker(\varphi_{\mathbf{i},\mathbf{j}}) \le k-2$.

Only possible for $\mathbf{n}$ in finitely many cosets (by unit equations).

2) Look at one $\mathbf{n}$ with a good partition:

- either $\mathbf{i}$ isolated (then $\beta(\mathbf{i}) = 0$), or
- $\mathbf{i}$ uses up at least one $\gamma_j(\mathbf{n})$ from RHS, so at most M nonzero $\beta(\mathbf{i})$.

We proved the **Key Claim:** For all $k \ge 0$: $|\{\mathbf{i} : \beta(\mathbf{i}) \neq 0\}| \le M$.

(We have: $\beta(\mathbf{i}) = b_{i_0 i_1} b_{i_1 b_2} \cdots b_{i_{k-1} i_k}$ with $B = (b_{ij})$ invertible.)

Know the **Key Claim:** For all $k \geq 0$: $|\{\mathbf{i} : \beta(\mathbf{i}) \neq 0\}| \leq M$.

Show: B is monomial.

Observe:

1. Each $\mathbf{i} = (i_0, \ldots, i_k)$ with $\beta(\mathbf{i}) \neq 0$ extends to some $\mathbf{i}' = (i_0, \ldots, i_k, i_{k+1})$ with $\beta(\mathbf{i}') \neq 0$. (Since row i_k of B is nonzero.)
2. For large enough k, these extension are unique. (By the claim!).
3. For each $1 \leq j \leq d$ and $k \geq 0$, there exist $\mathbf{i} = (i_0, \ldots, i_k)$ with $\beta(\mathbf{i}) \neq 0$ and $i_k = j$. (Since column j of B^k is nonzero)

So: for each i there exists exactly one j with $b_{ij} \neq 0$, i.e., B is monomial!

Beyond the Special Case

If such a nice A (all eigenvalues essentially distinct) does not exist:

- Decompose K^d into eigenspaces of any A^n, n sufficiently large.
- For every B, there exists suitable m such that B^m leaves the eigenspaces of A invariant (using a block variant of the key claim).
- Taking $D = \langle A^{n(A)} : A \in G \rangle$, the quotient G/D is torsion and linear.
- G/D is finite by Burnside–Schur.
- D is simultaneously diagonalizable by construction.

So G is virtually simultaneously diagonalizable.

More Generality

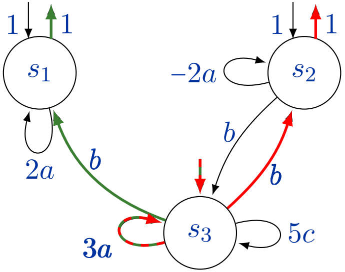
If K is not algebraically closed: descent from $\overline{K}$ (using uniform power-splitting).

If $\operatorname{char} K = p > 0$: the key claim still holds! By Derksen–Masser '12 unit equations have *few* solutions. The bad points are in a sufficiently sparse set of cosets of smaller rank.

The Actual Motivation/Application: Weighted Automata

Weighted Finite Automata

Let X be an alphabet, K a field.



$$f(a^2b) = 3 \cdot 3 \cdot 1 + 3 \cdot 3 \cdot 1 = 18,$$

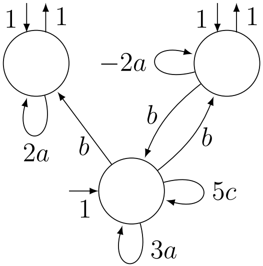
$$\sum_{w \in X^*} f(w)w = 2 + 2b + 8a^2 + 6ab + 2b^2 + \cdots$$
$$+ 10cb + 18a^2b + \cdots - 60b^3ababcb + \cdots$$
$$\in \mathbb{Q}\langle\langle a, b, c\rangle\rangle$$

Computational model

WFA computes a rational $f \colon X^* \to K$:

- Given $w \in X^*$, find all successful runs for w.
- On each run, take the product of all the weights, then sum over all runs.

Weighted Finite Automata



$$u = \begin{pmatrix} 1,1,1 \end{pmatrix}$$

$$\mu(a) = \begin{pmatrix} 2 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & 3 \end{pmatrix}$$

$$\mu(b) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

$$\mu(c) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 5 \end{pmatrix}$$

$$v = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$$

Using matrices:

- two vectors $u \in K^{1\times d}$, $v \in K^{d\times 1}$,
- for each letter x a transition matrix $\mu(x) \in K^{d\times d}$
- $f(x_{i_1} \cdots x_{i_l}) = u\mu(x_{i_1}) \cdots \mu(x_{i_l})v$.

- $|X| = 1$ are precisely linear recurrence sequences (LRS) ($f(n) = uA^n v$).

Ambiguity

WFA can be

$\{$deterministic$\} \subsetneq \{$unambiguous$\} \subsetneq \{$finitely ambiguous$\} \subsetneq \{$polynomially ambiguous$\}$

or exponentially ambiguous.

Problem

Given a WFA $\mathcal{A}$ recognizing f, is there WFA of certain lower ambiguity class recognizing the same f?

E.g. is $\mathcal{A}$ determinizable?

Reutenauer's Conjecture

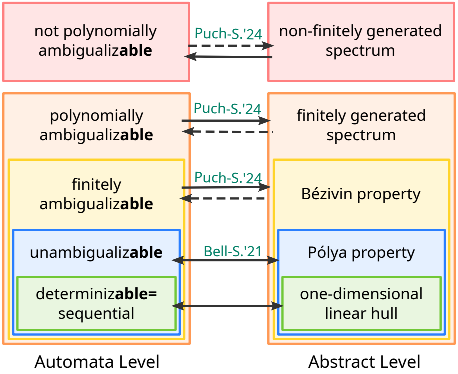
Reutenauer conjectured (1979): $\mathcal{A}$ unambigualizable $\Leftrightarrow$ $f(X^*)$ is Pólya ($\subseteq \Gamma_0$).

- Reutenauer proved it for $f(X^*)$ finite.
- For $|X| = 1$, i.e., LRS, known by Pólya 1920, Benzaghou 1970, Bézivin 1986.

Theorem (Bell-S. '21)

A WFA over a field is unambigualizable if and only if it its output is Pólya.

Ambiguity Hierarchy of Weighted Automata



Theorem

For WFA over (computable) fields,

1. (Bell-S. '21, '23) Determinizability and unambigualizability are decidable.
2. (Puch-S. '24) If the transition matrices are invertible, the full ambiguity hierarchy is decidable.