

Pfaffian Degree as Observable Complexity in Class-Two p -Groups

Luca Blanchi

June 2026

Abstract

We prove exact observable-depth theorems for regular alternating pencils and the associated class-two exponent- p groups. The results identify Pfaffian degree as the intrinsic obstruction to bounded-arity local observation. Let p be odd. A regular affine alternating pencil is modeled by a finite $\mathbb{F}_p[t]$ -module

$$R_F = \mathbb{F}_p[t]/(F)$$

and the symplectic block

$$V_F = R_F^2.$$

For a direct sum of spectral blocks

$$\mathcal{F} = (F_1, \dots, F_s),$$

we obtain an alternating pencil

$$\beta_{\mathcal{F}} : \Lambda^2 V_{\mathcal{F}} \rightarrow \mathbb{F}_p^2.$$

Define the spectral divisor function

$$D_{\mathcal{F}}(h) = \sum_{\nu} \deg \gcd(h, F_{\nu}).$$

The first main theorem is an exact support-image tomography theorem. For every structured CSI observable of arity (r) , the rank transform is governed by Smith normal form:

$$\rho_r^{\beta_{\mathcal{F}}}(U) = 2 \sum_{\nu, i} (M_{\nu} - \deg \gcd(s_i, F_{\nu})),$$

where $M_{\nu} = \deg F_{\nu}$ and s_i are the nonzero Smith factors of the linear polynomial matrix attached to (U) . Consequently,

$$\text{CSI}_{\leq r}(\beta_{\mathcal{F}})$$

determines, and is determined by, the truncated spectral divisor function

$$D_{\mathcal{F}, \leq r} : h \mapsto \sum_{\nu} \deg \gcd(h, F_{\nu}), \quad \deg h \leq r.$$

Thus support-image observables of arity (r) see exactly the elementary-divisor data testable by polynomials of degree at most (r) , and nothing more. The second main theorem extends the spectral barrier to arbitrary coefficient-free systems of word equations in the variety of class-two exponent- p groups. After class-two normal form, every word system reduces to a finite system of quadratic commutator equations. A Fourier expansion and the skew-Smith normal form of

linear alternating polynomial matrices show that every word observable in (k) variables factors through

$$D_{\mathcal{F}, \leq \lfloor k/2 \rfloor}.$$

This yields an exact factor-of-two law. For irreducible spectral blocks of degree (m) ,

$$\text{depth}_{\text{CSI}} = m,$$

whereas

$$\text{depth}_{\text{word}} = 2m.$$

Equivalently, if $f, h \in \mathbb{F}_p[t]$ are irreducible of degree (m) and are not projectively equivalent, then all coefficient-free word observables in fewer than $(2m)$ variables have identical counts on the associated groups G_f, G_h , while two explicit word equations in $(2m)$ variables distinguish them. Moreover, no single word equation can distinguish such G_f, G_h , regardless of the number of variables. The associated Baer groups G_f are directly indecomposable special class-two exponent- p groups of order

$$p^{2m+2}.$$

Thus

$$\text{depth}_{\text{word}}(G_f, G_h) = 2m = \log_p |G_f| - 2.$$

A single indistinguishability fibre below the threshold contains

$$p^{m-o(m)} = |G_f|^{1/2-o(1)}$$

pairwise nonisomorphic directly indecomposable special groups. We also derive consequences for Hom profiles, bounded-generator subgroup occurrence profiles, quantifier-free counting word logic, and classical character/conjugacy data. The results give a precise spectral explanation for the failure of bounded local observables on genus-two p -groups: global pencil algorithms can recover the spectrum efficiently, but support-image and word-count observables cannot see an irreducible Pfaffian factor before its degree, and word observables pay an exact factor of two because their polynomial matrices are alternating.

Declaration of generative AI and AI-assisted technologies in the writing process

This article belongs to the Presentation theory section. Generative AI, including ChatGPT by OpenAI, was used to assist with mathematical drafting, formalization, review, and editing. The note may be preliminary, may have been only partially reviewed, and in some cases may be only AI-reviewed.

1 Introduction

Groups of nilpotency class two and exponent p are controlled by alternating maps

$$\beta : \Lambda^2 V \rightarrow W$$

over $\mathbb{F}_p$. If p is odd, such a map defines a group

$$G_\beta = V \oplus W$$

with multiplication

$$(v, z)(u, w) = \left(v + u, z + w + \frac{1}{2}\beta(v, u) \right).$$

Then

$$[(v, z), (u, w)] = (0, \beta(v, u)).$$

Thus pseudo-isometry of alternating maps is the linear-algebraic core of isomorphism for special class-two exponent- p groups. This paper studies the power and limits of bounded-arity observables on such groups. There are two observable hierarchies. The first is the structured support-image hierarchy, or CSI. For

$$\mathbf{x} = (x_1, \dots, x_r) \in V^r,$$

one forms the contraction map

$$A_{\mathbf{x}} : V \rightarrow W^r, \quad z \mapsto (\beta(x_1, z), \dots, \beta(x_r, z)).$$

The level-(r) support-image profile records the image subspaces

$$\text{im } A_{\mathbf{x}} \leq W^r$$

as $\mathbf{x}$ varies. The second is the hierarchy of coefficient-free word observables. Given a system of word equations

$$w_1 = 1, \dots, w_s = 1$$

in (k) variables, one records the number of (k) -tuples in G_β satisfying the system. These observables include Hom-counts from finitely generated class-two exponent- p groups. The main discovery of this paper is that, for regular alternating pencils, both hierarchies are governed by a single spectral divisor function. Let

$$R_F = \mathbb{F}_p[t]/(F)$$

and consider the regular symplectic block

$$V_F = R_F^2.$$

For a direct sum of such blocks

$$\mathcal{F} = (F_1, \dots, F_s),$$

define

$$D_{\mathcal{F}}(h) = \sum_{\nu} \deg \gcd(h, F_{\nu}).$$

This function measures how a test polynomial (h) intersects the spectral elementary divisors of the pencil. The first main theorem states:

$$\boxed{\text{CSI}_{\leq r} \iff D_{\mathcal{F}}(h) \text{ for all } \deg h \leq r.}$$

The proof is a Smith-normal-form computation. Every level-(r) CSI test produces a matrix ($C(t)$) with linear entries. Its Smith factors $s_i(t)$ have degree at most (r), and the rank of the test on the block R_F is governed by

$$\deg \gcd(s_i, F).$$

The second main theorem extends this to all coefficient-free systems of word equations. After reduction to pure commutator equations and Fourier expansion, each frequency produces a linear alternating polynomial matrix. Since skew-Smith factors occur in pairs, a word observable in (k) variables can only test polynomials of degree at most

$$\left\lfloor \frac{k}{2} \right\rfloor.$$

Therefore

$$\boxed{\text{word observables in } k \text{ variables} \iff D_{\mathcal{F}}(h) \text{ for } \deg h \leq \lfloor k/2 \rfloor.}$$

This gives an exact factor-of-two law. For an irreducible factor (f) of degree (m),

CSI

detects (f) exactly at arity (m), whereas word observables require ($2m$) variables. This is optimal. A companion linearization

$$L_f(t) = tI_m - C_f$$

gives a CSI witness at arity (m). Its skew-symmetrization

$$K_f(t) = \begin{pmatrix} 0 & L_f(t) \\ -L_f(t)^T & 0 \end{pmatrix}$$

gives two explicit word equations in ($2m$) variables distinguishing the associated groups. No single word equation ever distinguishes irreducible blocks of the same degree. The conclusion is that Pfaffian degree is observable complexity.

$$\boxed{\text{Pfaffian degree} = \text{CSI arity.}}$$

$$\boxed{2 \cdot \text{Pfaffian degree} = \text{word-observable arity.}}$$

The final consequences are group-theoretic. For every (m), there are

$$p^{m-o(m)}$$

pairwise nonisomorphic directly indecomposable special groups of order

$$p^{2m+2}$$

which no word observable in fewer than ($2m$) variables can distinguish. Since

$$2m = \log_p |G| - 2,$$

this is a logarithmic arity lower bound with a matching upper bound inside the word-observable hierarchy. The result should be read as a local-observable lower bound, not as a time lower bound for group isomorphism. Genus-two groups are globally tractable through their pencil structure. Our theorem shows that, even in this globally tractable setting, bounded local invariants cannot see the irreducible Pfaffian factor before its exact degree.

2 Related work and positioning

Class-two exponent- p groups are a central bottleneck in finite group isomorphism. Their isomorphism problem is governed by pseudo-isometry of alternating bilinear maps, or equivalently by isometry of alternating matrix spaces. Several global algorithms and reductions exploit this linear-algebraic structure. Alternating matrix space isometry has been studied as a linear-algebraic analogue of graph isomorphism, and genus-two groups admit efficient isomorphism algorithms using the structure of pencils and their adjoint algebras. More recently, faster algorithms for class-two exponent- p groups and reductions between tensor, group, and polynomial isomorphism problems have clarified the central role of these groups. This paper does not improve those global algorithms. Instead, it gives a sharp lower bound for local observable hierarchies inside a globally tractable family. The closest group-theoretic comparison is Wilson’s construction of genus-two p -groups with identical proper subgroup and quotient profiles, character tables, and power maps. Our groups belong to the same genus-two universe. The contribution here is different: we give an exact spectral formula for all CSI and coefficient-free word-count observables, prove optimal arity thresholds, produce explicit optimal witnesses, and explain the obstruction through Smith normal form and Pfaffian degree. We also separate our results from Weisfeiler–Leman and full counting-logic lower bounds. We prove indistinguishability for quantifier-free coefficient-free word-counting observables and for Hom profiles from bounded-generator sources. We do not claim a lower bound for full bounded-variable counting logic with quantifier alternation, nor for all WL variants on groups.

3 Regular affine alternating pencils

Throughout, p is an odd prime. Let

$$F(t) \in \mathbb{F}_p[t]$$

be monic of degree

$$M.$$

Put

$$R_F = \mathbb{F}_p[t]/(F).$$

Let

$$\lambda_F : R_F \rightarrow \mathbb{F}_p$$

be the linear functional extracting the coefficient of t^{M-1} from the representative of degree $< M$.

Lemma 3.1 (Frobenius pairing). *The pairing*

$$R_F \times R_F \rightarrow \mathbb{F}_p, \quad (u, v) \mapsto \lambda_F(uv)$$

is nondegenerate.

Proof. Let $0 \neq u \in R_F$, represented by a polynomial of degree $a < M$ with leading coefficient $c \neq 0$. Take

$$v = t^{M-1-a}.$$

Then

$$\lambda_F(uv) = c \neq 0.$$

□

Set

$$V_F = R_F^2.$$

For

$$x = (x_1, x_2), \quad y = (y_1, y_2)$$

define

$$\delta_F(x, y) = x_1 y_2 - x_2 y_1 \in R_F.$$

Define the alternating pencil

$$\beta_F : V_F \times V_F \rightarrow \mathbb{F}_p^2$$

by

$$\beta_F(x, y) (\lambda_F(\delta_F(x, y)), \lambda_F(t\delta_F(x, y))). \quad (3.1)$$

Let B_0, B_1 be the two scalar coordinate forms. For a finite list

$$\mathcal{F} = (F_1, \dots, F_s)$$

of monic polynomials, define

$$V_{\mathcal{F}} = \bigoplus_{\nu=1}^s V_{F_{\nu}},$$

and

$$\beta_{\mathcal{F}} = \bigoplus_{\nu=1}^s \beta_{F_{\nu}}.$$

Let

$$M_{\nu} = \deg F_{\nu}, \quad M = \sum_{\nu=1}^s M_{\nu}.$$

Then

$$\dim_{\mathbb{F}_p} V_{\mathcal{F}} = 2M.$$

This model captures the affine regular part of an alternating pencil with a chosen nondegenerate scalar member. The homogeneous treatment, including spectral factors at infinity, should be obtained by the corresponding binary-form version; we do not need it here.

4 Structured CSI and its rank transform

Let

$$\beta : \Lambda^2 V \rightarrow W$$

be an alternating map. For

$$\mathbf{x} = (x_1, \dots, x_r) \in V^r$$

define

$$A_{\mathbf{x}} : V \rightarrow W^r, \quad z \mapsto (\beta(x_1, z), \dots, \beta(x_r, z)).$$

The level-(r) structured support-image profile is the function

$$E_r^\beta(T) \# \{\mathbf{x} \in V^r : \text{im } A_{\mathbf{x}} = T\}, \quad T \leq W^r.$$

It is often easier to use the rank transform. Let

$$U \leq (W^r)^*.$$

Choose a basis $u_1, \dots, u_a$ of (U) , and define

$$\Psi_U^\beta : V^r \rightarrow (V^*)^a$$

by

$$\Psi_U^\beta(\mathbf{x})(u_1 \circ A_{\mathbf{x}}, \dots, u_a \circ A_{\mathbf{x}}).$$

Let

$$\rho_r^\beta(U) = \text{rank } \Psi_U^\beta.$$

Proposition 4.1 (CSI/rank-transform equivalence). *For fixed (r), the functions*

$$T \mapsto E_r^\beta(T)$$

and

$$U \mapsto \rho_r^\beta(U)$$

determine one another.

Proof. For

$$S \leq W^r,$$

define

$$F_r^\beta(S) \# \{\mathbf{x} : \text{im } A_{\mathbf{x}} \leq S\}.$$

The condition

$$\text{im } A_{\mathbf{x}} \leq S$$

is equivalent to

$$u \circ A_{\mathbf{x}} = 0 \quad \text{for all } u \in S^\perp.$$

Therefore

$$F_r^\beta(S) = |\ker \Psi_{S^\perp}^\beta| = p^{r \dim V - \rho_r^\beta(S^\perp)}. \quad (4.1)$$

Also,

$$F_r^\beta(S) = \sum_{T \leq S} E_r^\beta(T). \quad (4.2)$$

Möbius inversion on the subspace lattice gives

$$E_r^\beta(T) = \sum_{S \leq T} \mu(S, T) F_r^\beta(S).$$

Thus ρ_r^β determines E_r^β , and conversely E_r^β determines F_r^β and hence ρ_r^β . □

5 Spectral divisor functions

For a list

$$\mathcal{F} = (F_1, \dots, F_s)$$

define the spectral divisor function

$$D_{\mathcal{F}} : \mathbb{F}_p[t] \rightarrow \mathbb{Z}_{\geq 0}$$

by

$$D_{\mathcal{F}}(h) = \sum_{\nu=1}^s \deg \gcd(h, F_\nu). \quad (5.1)$$

For $r \geq 0$, write

$$D_{\mathcal{F}, \leq r}$$

for the restriction of $D_{\mathcal{F}}$ to polynomials of degree at most (r) . The theorem below says that $D_{\mathcal{F}, \leq r}$ is exactly the spectral content of CSI through level (r) .

6 Exact CSI spectral tomography

Let

$$W = \mathbb{F}_p^2.$$

Identify

$$W^*$$

with the two-dimensional space of linear polynomials

$$\mathcal{L} = a + bt : a, b \in \mathbb{F}_p.$$

Let

$$U \leq (W^*)^r.$$

After choosing a basis of (U) , represent (U) by an $a \times r$ matrix

$$C_U(t)$$

whose entries are linear polynomials. Let

$$s_1(t), \dots, s_k(t)$$

be the nonzero Smith factors of $C_U(t)$ over $\mathbb{F}_p[t]$.

Theorem 6.1 (CSI Smith formula). *For the regular affine pencil $\beta_{\mathcal{F}}$,*

$$\rho_r^{\beta_{\mathcal{F}}}(U) = 2 \sum_{\nu=1}^s \sum_{i=1}^k (M_{\nu} - \deg \gcd(s_i, F_{\nu})). \quad (6.1)$$

Equivalently,

$$\rho_r^{\beta_{\mathcal{F}}}(U) = 2 \sum_{i=1}^k (M - D_{\mathcal{F}}(s_i)). \quad (6.2)$$

Proof. First consider one block (F) . The form

$$B_0(x, y) = \lambda_F(\delta_F(x, y))$$

is nondegenerate, by Lemma 3.1. Using B_0 to identify $V_F \cong V_F^*$, the map $\Psi_U^{\beta_F}$ is represented by

$$C_U(t) : R_F^{2r} \rightarrow R_F^{2a}.$$

Because $V_F = R_F^2$, this is two copies of the map

$$C_U(t) : R_F^r \rightarrow R_F^a.$$

Thus

$$\rho_r^{\beta_F}(U) = 2 \operatorname{rank}_{\mathbb{F}_p}(C_U(t) : R_F^r \rightarrow R_F^a). \quad (6.3)$$

Take Smith normal form

$$P(t)C_U(t)Q(t) = \operatorname{diag}(s_1, \dots, s_k, 0, \dots, 0),$$

with P, Q unimodular over $\mathbb{F}_p[t]$. These matrices induce invertible maps over R_F , so the rank is the sum of the ranks of multiplication by s_i on R_F . Multiplication by s_i on

$$R_F = \mathbb{F}_p[t]/(F)$$

has kernel dimension

$$\deg \gcd(s_i, F).$$

Indeed, if

$$g = \gcd(s_i, F), \quad F = gF',$$

then $s_i x \equiv 0 \pmod{F}$ iff $F' \mid x$, and the subspace of classes divisible by (F') has dimension $\deg g$. Thus the rank of multiplication by s_i is

$$M - \deg \gcd(s_i, F).$$

Doubling gives the single-block formula. The direct-sum formula follows by additivity of rank over the blocks F_ν . □

Theorem 6.2 (Exact CSI tomography). *For regular affine pencils,*

$$\boxed{\operatorname{CSI}_{\leq r}(\beta_{\mathcal{F}}) \iff D_{\mathcal{F}, \leq r}.$$

More explicitly, for two lists $\mathcal{F}, \mathcal{G}$ of the same total degree (M),

$$\operatorname{CSI}_{\leq r}(\beta_{\mathcal{F}}) = \operatorname{CSI}_{\leq r}(\beta_{\mathcal{G}})$$

in fixed pencil coordinates if and only if

$$D_{\mathcal{F}}(h) = D_{\mathcal{G}}(h)$$

for every polynomial h with

$$\deg h \leq r.$$

Proof. By Proposition 4.1, CSI through level (r) is equivalent to all rank functions

$$\rho_d^\beta \quad (d \leq r).$$

By Theorem 6.1, these rank values depend on $\mathcal{F}$ only through

$$D_{\mathcal{F}}(s_i)$$

for Smith factors s_i of matrices with linear entries and width $d \leq r$. Such Smith factors have degree at most $d \leq r$. Therefore $D_{\mathcal{F}, \leq r}$ determines $\text{CSI}_{\leq r}$. Conversely, let $h(t)$ be monic of degree

$$d \leq r.$$

Let

$$L_h(t) = tI_d - C_h$$

be a companion linearization of h . Its Smith normal form is

$$\text{diag}(1, \dots, 1, h).$$

Let

$$U_h \leq (W^*)^d$$

be the row space of $L_h(t)$. Theorem 6.1 gives

$$\rho_d^{\beta_{\mathcal{F}}}(U_h) = 2(dM - D_{\mathcal{F}}(h)).$$

Thus

$$\boxed{D_{\mathcal{F}}(h) = dM - \frac{1}{2}\rho_d^{\beta_{\mathcal{F}}}(U_h).} \tag{6.4}$$

Hence $\text{CSI}_{\leq r}$ recovers $D_{\mathcal{F}}(h)$ for every $\deg h \leq r$.

□

7 Recovery of elementary divisors

Suppose the spectral list is written in primary form

$$\mathcal{F} = p_{\alpha}(t)^{e_{\alpha,j}}_{\alpha,j},$$

where the p_{α} are distinct monic irreducibles. For $a \geq 1$,

$$D_{\mathcal{F}}(p_{\alpha}^a) \deg p_{\alpha} \sum_j \min(a, e_{\alpha,j}). \tag{7.1}$$

Define

$$N_{\alpha}(a) = \frac{D_{\mathcal{F}}(p_{\alpha}^a) - D_{\mathcal{F}}(p_{\alpha}^{a-1})}{\deg p_{\alpha}}.$$

Then

$$N_{\alpha}(a) = \#\{j : e_{\alpha,j} \geq a\}.$$

Therefore

$$\#\{j : e_{\alpha,j} = a\} = N_{\alpha}(a) - N_{\alpha}(a+1). \tag{7.2}$$

Corollary 7.1 (Complete regular spectral recovery). *Let*

$$\tau(\mathcal{F}) \max_{\alpha,j} e_{\alpha,j} \deg p_\alpha.$$

Then

$$\text{CSI}_{\leq \tau(\mathcal{F})}$$

recovers the complete primary spectral multiset $\mathcal{F}$. Moreover, the pairwise CSI separation depth in fixed pencil coordinates is

$$\boxed{\delta_{\text{CSI}}(\mathcal{F}, \mathcal{G}) \min \deg h : D_{\mathcal{F}}(h) \neq D_{\mathcal{G}}(h)}. \quad (7.3)$$

That is,

$$\text{CSI}_{\leq r}(\beta_{\mathcal{F}}) = \text{CSI}_{\leq r}(\beta_{\mathcal{G}})$$

if and only if

$$r < \delta_{\text{CSI}}(\mathcal{F}, \mathcal{G}).$$

8 Irreducible spectral blocks and CSI threshold

Let

$$f, h \in \mathbb{F}_p[t]$$

be monic irreducible polynomials of degree $m \geq 3$. If

$$\deg h_0 < m,$$

then

$$\gcd(h_0, f) = 1$$

for every nonzero h_0 . Hence

$$D_{f, \leq m-1}$$

is independent of (f) . At level (m) , taking

$$h_0 = f$$

gives

$$D_f(f) = m,$$

whereas

$$D_h(f) = 0$$

if $h \neq f$. Thus:

Theorem 8.1 (Exact CSI threshold for irreducible blocks). *For irreducible degree-(m) blocks,*

$$\text{depth}_{\text{CSI}} = m.$$

In fixed pencil coordinates,

$$\text{CSI}_{\leq m-1}(\beta_f) \text{CSI}_{\leq m-1}(\beta_h)$$

for all irreducible f, h of degree (m), while

$$\text{CSI}_{\leq m}$$

distinguishes (f) from (h) unless ($f=h$). Projectively, equality at level (m) holds precisely when (f) and (h) are in the same $\text{PGL}_2(p)$ -orbit.

9 Word observables and QCO

We now pass from CSI to word equations. Let

$$\Sigma = w_1 = 1, \dots, w_s = 1$$

be a coefficient-free system of words in (k) variables in the variety

$$\mathcal{N}_{2,p}$$

of class-two exponent- p groups. Every word has a normal form

$$w_j \longleftrightarrow (\alpha_j, D_j),$$

where

$$\alpha_j \in \mathbb{F}_p^k$$

is its linear exponent vector and

$$D_j \in \text{Alt}_k(\mathbb{F}_p)$$

is its commutator matrix. Let

$$A : \mathbb{F}_p^k \rightarrow \mathbb{F}_p^s$$

be the matrix with rows α_j . Put

$$n = \dim \ker A, \quad t = \dim \text{coker } A.$$

After choosing a basis of $\ker A$ and projecting central equations to $\text{coker } A$, the system becomes (t) pure commutator equations in (n) variables:

$$Q_\ell(\mathbf{x}) = \sum_{a < b} (D'_\ell)_{ab} \beta(x_a, x_b) = 0, \quad 1 \leq \ell \leq t, \quad (9.1)$$

where

$$D'_\ell \in \text{Alt}_n(\mathbb{F}_p).$$

The central coordinates lift with multiplicity

$$p^{2n}.$$

Proposition 9.1 (QCO reduction). *For every alternating map $\beta : \Lambda^2 V \rightarrow W$ with $\dim W = 2$,*

$$|\text{Sol}_\Sigma(G_\beta)| = p^{2n} N_{\mathbf{D}'}(\beta), \quad (9.2)$$

where $N_{\mathbf{D}'}(\beta)$ is the number of solutions of the pure commutator system (9.1) in V^n .

Proof. The linear parts of the words impose the linear equations

$$A(v_1, \dots, v_k) = 0$$

in (V), leaving $n = \dim \ker A$ free (V)-variables. The central coordinates $z_i \in W$ appear linearly through the same matrix (A). For each choice of the (V)-variables satisfying the projected commutator equations in $\text{coker } A$, the central coordinates form an affine space of dimension $(2n)$. Hence there are p^{2n} central lifts. □

A finite Boolean combination of word equations and disequations is a finite integer linear combination of counts of systems of equations, by inclusion–exclusion. Thus the same analysis applies to quantifier-free Boolean word observables.

10 Fourier–Smith formula for word counts

Fix a nontrivial additive character

$$\psi : \mathbb{F}_p \rightarrow \mathbb{C}^\times.$$

Let

$$\lambda = (\lambda_1, \dots, \lambda_t) \in (W^*)^t.$$

Write

$$\lambda_\ell = a_\ell + b_\ell t.$$

Define the linear alternating polynomial matrix

$$C_\lambda(t) = \sum_{\ell=1}^t (a_\ell + b_\ell t) D'_\ell \in \text{Alt}_n(\mathbb{F}_p[t]). \quad (10.1)$$

Because $C_\lambda(t)$ is alternating over the PID $\mathbb{F}_p[t]$, its nonzero Smith factors occur in pairs. We write the skew-Smith factors as

$$s_{\lambda,1}, \dots, s_{\lambda,u(\lambda)},$$

meaning that the ordinary Smith form contains

$$s_{\lambda,1}, s_{\lambda,1}, \dots, s_{\lambda,u}, s_{\lambda,u}$$

as its nonzero factors.

Theorem 10.1 (Fourier–Smith word-count formula). *For the regular affine pencil $\beta_{\mathcal{F}}$,*

$$|\mathrm{Sol}_{\Sigma}(G_{\mathcal{F}})| = p^{2n-2t} \sum_{\lambda \in (W^*)^t} p^{2nM-2 \sum_{i=1}^{u(\lambda)} (M - D_{\mathcal{F}}(s_{\lambda,i}))}. \quad (10.2)$$

Proof. The indicator of the equations

$$Q_{\ell}(\mathbf{x}) = 0 \quad (1 \leq \ell \leq t)$$

is

$$p^{-2t} \sum_{\lambda \in (W^*)^t} \psi \left(\sum_{\ell=1}^t \lambda_{\ell}(Q_{\ell}(\mathbf{x})) \right).$$

On a single block R_F^2 , write each variable as

$$x_i = (u_i, v_i) \in R_F^2.$$

Then the phase for a fixed λ becomes

$$\psi \left(\lambda_F(u^T C_{\lambda}(t)v) \right).$$

Since

$$(u, v) \mapsto \lambda_F(uv)$$

is nondegenerate, summing first over (v) gives zero unless

$$C_{\lambda}(t)^T u = 0$$

in R_F^n . Hence the character sum over R_F^{2n} equals

$$p^{nM} \cdot |\ker C_{\lambda}(t)^T| = p^{2nM - \mathrm{rank}_{\mathbb{F}_p} C_{\lambda}(A_F)}.$$

By skew-Smith normal form, the rank of C_{λ} on the direct sum of spectral blocks is

$$2 \sum_i (M - D_{\mathcal{F}}(s_{\lambda,i})).$$

Multiplying by the Fourier factor p^{-2t} and the central-lift factor p^{2n} from Proposition 9.1 gives (10.2). □

11 The degree budget for alternating matrices

Let $C(t) \in \mathrm{Alt}_n(\mathbb{F}_p[t])$ have entries of degree at most (1) . Suppose its rational rank is $(2u)$. Let its skew-Smith factors be

$$s_1, \dots, s_u.$$

Then

$$\sum_{i=1}^u \deg s_i \leq u \leq \left\lfloor \frac{n}{2} \right\rfloor. \quad (11.1)$$

Indeed, the determinantal divisor of order $(2u)$ is

$$(s_1 \cdots s_u)^2.$$

It divides every nonzero $2u \times 2u$ minor. Such a minor has degree at most $(2u)$, because every entry is linear. Hence

$$2 \sum_i \deg s_i \leq 2u.$$

In particular, every individual skew-Smith factor satisfies

$$\deg s_i \leq \left\lfloor \frac{n}{2} \right\rfloor. \quad (11.2)$$

12 Word-spectrum factorization

Theorem 12.1 (Word observables factor through truncated spectral data). *Let $\beta_{\mathcal{F}}$ and $\beta_{\mathcal{G}}$ be regular affine pencils with the same total spectral degree (M) . Suppose*

$$D_{\mathcal{F}}(h) = D_{\mathcal{G}}(h)$$

for every polynomial h with

$$\deg h \leq \left\lfloor \frac{k}{2} \right\rfloor.$$

Then every coefficient-free word observable in at most (k) variables has the same count on

$$G_{\mathcal{F}} \quad \text{and} \quad G_{\mathcal{G}}.$$

The same holds for quantifier-free Boolean combinations of word equations and disequations in at most (k) variables.

Proof. A word system in (k) variables reduces, by Proposition 9.1, to a pure commutator system in

$$n \leq k$$

variables. For each Fourier frequency λ , the associated alternating polynomial matrix has size (n) and linear entries. By the degree budget (11.2), all skew-Smith factors appearing in (10.2) have degree at most

$$\left\lfloor \frac{n}{2} \right\rfloor \leq \left\lfloor \frac{k}{2} \right\rfloor.$$

Therefore every term in the Fourier–Smith formula depends only on

$$D_{\mathcal{F}, \leq \lfloor k/2 \rfloor}.$$

If this truncated spectral data agrees for $\mathcal{F}$ and $\mathcal{G}$, then all word-system counts agree. Boolean combinations follow from inclusion–exclusion. $\square$

Corollary 12.2 (Quantifier-free counting word logic). *Let f, h be irreducible of degree (m) . If $(k < 2m)$, then every coefficient-free quantifier-free formula in the group language with at most (k) free variables has the same number of satisfying assignments in G_f and G_h .*

13 Hom profiles and subgroup occurrence profiles

Let $H \in \mathcal{N}_{2,p}$ be generated by at most (k) elements. A presentation of (H) in the variety $\mathcal{N}_{2,p}$ uses (k) generators and some system of word equations. Therefore Theorem 12.1 immediately gives:

Corollary 13.1 (Hom-profile lower bound). *Under the hypotheses of Theorem 12.1,*

$$|\text{Hom}(H, G_{\mathcal{F}})| = |\text{Hom}(H, G_{\mathcal{G}})|$$

for every $H \in \mathcal{N}_{2,p}$ generated by at most (k) elements. Now fix $K \in \mathcal{N}_{2,p}$. Every homomorphism

$$K \rightarrow G$$

has kernel $N \trianglelefteq K$ and induces an injection

$$K/N \hookrightarrow G.$$

Thus

$$|\text{Hom}(K, G)| \geq \sum_{N \trianglelefteq K} |\text{Inj}(K/N, G)|. \quad (13.1)$$

This triangular relation over the normal-subgroup lattice recovers injection counts from Hom counts of quotients.

Corollary 13.2 (Bounded-generator subgroup profiles). *Let f, h be irreducible of degree (m) . If $K \in \mathcal{N}_{2,p}$ is generated by fewer than $(2m)$ elements, then*

$$|\text{Inj}(K, G_f)| = |\text{Inj}(K, G_h)|.$$

Consequently,

$$\#\{L \leq G_f : L \cong K\} = \#\{L \leq G_h : L \cong K\}.$$

Proof. Every quotient of (K) is also generated by fewer than $(2m)$ elements. Hence all Hom counts from all quotients of (K) agree on G_f and G_h . By the triangular relation (13.1), the injection counts agree. Dividing by $|\text{Aut } K|$ gives equality of subgroup occurrence counts. $\square$

14 Irreducible blocks and the factor-of-two law

Let $f, h \in \mathbb{F}_p[t]$ be monic irreducibles of degree (m) . If

$$\deg a < m,$$

then

$$\gcd(a, f) = \gcd(a, h) = 1$$

for every nonzero (a) . Therefore

$$D_{f, \leq m-1} = D_{h, \leq m-1}.$$

Theorem 14.1 (Complete word-observable blindness below $(2m)$). *If*

$$k < 2m,$$

then every coefficient-free word observable in (k) variables has the same count on

$$G_f \quad \text{and} \quad G_h.$$

Equivalently,

$$G_f \equiv_{2m-1}^{\text{word}} G_h.$$

In particular,

$$|\text{Hom}(H, G_f)| = |\text{Hom}(H, G_h)|$$

for every $H \in \mathcal{N}_{2,p}$ generated by fewer than $(2m)$ elements.

Proof. If $(k < 2m)$, then

$$\left\lfloor \frac{k}{2} \right\rfloor < m.$$

Thus the truncated spectral divisor functions agree through degree $\lfloor k/2 \rfloor$. Apply Theorem 12.1. $\square$

15 An optimal two-equation word witness

We now construct a distinguishing word observable in exactly $(2m)$ variables. Let

$$L_f(t) = tI_m - C_f$$

be the companion linearization of (f) . Define the skew-linearization

$$K_f(t) = \begin{pmatrix} 0 & L_f(t) \\ -L_f(t)^T & 0 \end{pmatrix}. \tag{15.1}$$

Write

$$K_f(t) = K_{f,0} + tK_{f,1},$$

with

$$K_{f,0}, K_{f,1} \in \text{Alt}_{2m}(\mathbb{F}_p).$$

Introduce variables

$$x_1, \dots, x_{2m}.$$

Define two pure commutator words

$$w_{f,j}(\mathbf{x}) \prod_{a < b} [x_a, x_b]^{(K_{f,j})_{ab}}, \quad j = 0, 1. \quad (15.2)$$

Let

$$Z_f(G) = \#\{\mathbf{x} \in G^{2m} : w_{f,0}(\mathbf{x}) = 1, w_{f,1}(\mathbf{x}) = 1\}.$$

Theorem 15.1 (Optimal word witness). *If (h) is not $PGL_2(p)$ -equivalent to (f), then*

$$Z_f(G_f) > Z_f(G_h).$$

More precisely,

$$Z_f(G_f) - Z_f(G_h) = p^{4m-4}(p-1)|\text{Stab}_{PGL_2(p)}(f)| \left(p^{2m^2+2m} - p^{2m^2} \right). \quad (15.3)$$

Proof. For the two equations, Fourier frequencies are pairs

$$(\lambda_0, \lambda_1) \in (W^*)^2.$$

Write

$$\lambda_i = a_i + b_i t.$$

The associated alternating polynomial matrix is

$$C_\lambda(t)(a_0 + b_0 t)K_{f,0} + (a_1 + b_1 t)K_{f,1}. \quad (15.4)$$

The pair (λ_0, λ_1) may have rank (0,1,) or (2) as a pair of linear forms in W^* . If the rank is (0), the contribution is the same for every target group. If the rank is (1), then

$$C_\lambda(t) = \ell(t)D$$

where $\ell(t)$ is linear and (D) is a constant alternating matrix congruent to a nonzero specialization of $K_f(t)$. Since (f) is irreducible of degree $m \geq 2$, no linear ℓ shares a factor with (f) or (h). Thus the rank contribution is the same for G_f and G_h . If the rank is (2), then (λ_0, λ_1) is a basis of W^* . The matrix $C_\lambda(t)$ is obtained from $K_f(t)$ by a projective change of pencil coordinates and multiplication by a nonzero scalar. Its skew-Smith factors are

$$1, \dots, 1, g \cdot f$$

for the corresponding element

$$g \in PGL_2(p).$$

On the target G_h , a rank defect occurs exactly when

$$h = g \cdot f.$$

By assumption, this never happens for (h). On the target G_f , it happens precisely for those (g) in

$$\text{Stab}_{PGL_2(p)}(f).$$

Each projective element has $(p-1)$ representatives in $GL_2(p)$, so the number of rank-two frequencies producing the defect on G_f is

$$(p-1)|\text{Stab}_{PGL_2(p)}(f)|.$$

For all other frequencies, the contributions agree. For a full-rank frequency without defect, the rank of the polynomial matrix on the irreducible degree-(m) block is

$$2m^2.$$

With the defect, it drops by

$$2m.$$

Since there are $(2m)$ variables, the character sum exponent is

$$2(2m)m - 2m^2 = 2m^2$$

without defect, and

$$2m^2 + 2m$$

with defect. Finally, the two equations contribute the Fourier normalizing factor p^{-4} , and the central variables contribute p^{4m} . Therefore each defective frequency contributes the excess

$$p^{4m-4} \left(p^{2m^2+2m} - p^{2m^2} \right).$$

Multiplying by the number of defective frequencies gives (15.3).

□

16 One equation never distinguishes

Theorem 16.1 (Two equations are necessary). *Let $f, h \in \mathbb{F}_p[t]$ be monic irreducibles of the same degree $m \geq 2$. No single coefficient-free word equation distinguishes*

$$G_f \quad \text{from} \quad G_h,$$

regardless of the number of variables.

Proof. Consider one word equation. If its linear part is nonzero, then the matrix (A) of linear parts has rank (1), and hence

$$\text{coker } A = 0.$$

After solving the linear equation, there is no residual commutator equation. The count is independent of β . If its linear part is zero, then after reduction there is one pure commutator equation with some constant alternating matrix

$$D \in \text{Alt}_n(\mathbb{F}_p).$$

A Fourier frequency is a single covector

$$\ell(t) = a + bt \in W^*.$$

The associated alternating polynomial matrix is

$$C_\ell(t) = \ell(t)D.$$

Its nonzero skew-Smith factors are linear multiples of $\ell(t)$. Since (f) and (h) are irreducible of degree $m \geq 2$, $\ell(t)$ is coprime to both. Therefore every Fourier term is independent of (f) and (h). Thus the count of any single word equation is the same on G_f and G_h . □

17 The factor-of-two law

Define

$$\text{depth}_{\text{CSI}}(f, h)$$

to be the least (r) such that $\text{CSI}_{\leq r}$ distinguishes β_f from β_h , up to projective pencil equivalence. Define

$$\text{depth}_{\text{word}}(G_f, G_h)$$

to be the least (k) such that a coefficient-free word system in (k) variables has different solution count on G_f and G_h .

Theorem 17.1 (Exact factor-of-two law). *If f, h are irreducible of degree (m) and are not $\text{PGL}_2(p)$ -equivalent, then*

$$\boxed{\text{depth}_{\text{CSI}}(f, h) = m,}$$

and

$$\boxed{\text{depth}_{\text{word}}(G_f, G_h) = 2m.}$$

Moreover, $(2m)$ variables suffice with two equations, and one equation never suffices.

Proof. The CSI statement is Theorem 8.1. The lower bound for word observables is Theorem 14.1. The upper bound is Theorem 15.1. The one-equation statement is Theorem 16.1. □

Since

$$|G_f| = p^{2m+2},$$

we obtain

$$\boxed{\text{depth}_{\text{word}}(G_f, G_h) = \log_p |G_f| - 2.} \tag{17.1}$$

18 Direct indecomposability and large fibres

For irreducible (f), the associated group G_f is special and directly indecomposable.

Proposition 18.1. *The group G_f is a directly indecomposable special class-two exponent- p group of order*

$$p^{2m+2}.$$

Proof. The group is special because the pencil is radical-free and surjective. The order is

$$|G_f| = |V_f||W| = p^{2m}p^2 = p^{2m+2}.$$

It remains to prove direct indecomposability. Suppose

$$V_f = V_1 \perp V_2$$

were a nontrivial orthogonal decomposition for both scalar forms B_0, B_1 . Since B_0 is nondegenerate, each V_i is B_0 -nondegenerate. Let (A) be multiplication by a root θ of (f) on

$$V_f = \mathbb{F}_{p^m}^2.$$

Since

$$B_1(x, y) = B_0(Ax, y),$$

orthogonality for B_1 implies that each V_i is (A)-invariant. Because (f) is irreducible, (A)-invariant $\mathbb{F}_p$ -subspaces of $\mathbb{F}_{p^m}^2$ are exactly $\mathbb{F}_{p^m}$ -subspaces. Every proper nonzero $\mathbb{F}_{p^m}$ -subspace of $\mathbb{F}_{p^m}^2$ is an $\mathbb{F}_{p^m}$ -line. Such a line is totally isotropic for the determinant form

$$\delta(x, y) = x_1y_2 - x_2y_1,$$

and hence for B_0 . This contradicts nondegeneracy of V_i . Therefore G_f is directly indecomposable. □

The number of monic irreducible polynomials of degree (m) is

$$I_p(m) \frac{p^m}{m} + O_p(p^{m/2}).$$

Every $PGL_2(p)$ -orbit has size at most

$$|PGL_2(p)| = p(p^2 - 1).$$

Thus there are at least

$$\frac{I_p(m)}{|PGL_2(p)|} p^{m-o(m)}$$

pairwise nonisomorphic groups G_f of order p^{2m+2} in the same $\text{CSI}_{\leq m-1}$ -fibre and in the same word-observable fibre below $(2m)$ variables. In terms of

$$N = |G_f|,$$

this fibre has size

$$N^{1/2-o(1)}.$$

19 Classical character and conjugacy data

The irreducible blocks also collapse many classical invariants.

Proposition 19.1. *Let (f) be irreducible of degree (m) . For every nonzero $v \in V_f$, the map*

$$u \mapsto \beta_f(v, u)$$

is surjective onto $W = \mathbb{F}_p^2$.

Proof. Over $E = \mathbb{F}_{p^m}$, for nonzero $v \in E^2$, the map

$$u \mapsto \delta(v, u)$$

is surjective onto (E) . The map

$$E \rightarrow \mathbb{F}_p^2, \quad z \mapsto (\lambda_F(z), \lambda_F(\theta z))$$

has rank (2) for $m \geq 2$. Hence the composite is surjective. $\square$

Corollary 19.2 (Classical invariants). *For irreducible f, h of the same degree (m) , the groups G_f, G_h have: the same conjugacy class size distribution; the same irreducible character degrees; the same character table form, up to relabelling of the center and its dual; the same power maps.*

Proof. By Proposition 19.1, every noncentral conjugacy class is a coset of the center (W) , and hence has size

$$|W| = p^2.$$

Central classes have size (1) . For every nontrivial central character $\lambda \in W^*$, the scalar form $\lambda \circ \beta_f$ is nondegenerate. The corresponding irreducible representation has degree p^m , and the nonlinear characters vanish off the center. There is one nonlinear irreducible character for each nontrivial central character. The remaining irreducible characters are the linear characters of G_f/W . This description depends only on (m) and (W) , not on (f) , up to relabelling of (W) and W^* . Finally, all groups have exponent p , so their power maps agree. $\square$

20 Hom-profile hierarchy

Let

$$G \equiv_k^{\text{Hom}} H$$

mean that

$$|\text{Hom}(K, G)| = |\text{Hom}(K, H)|$$

for every $K \in \mathcal{N}_{2,p}$ generated by at most (k) elements.

Corollary 20.1. *If f, h are irreducible of degree (m) , then*

$$G_f \equiv_{2m-1}^{\text{Hom}} G_h.$$

If f, h are not projectively equivalent, then

$$G_f \not\equiv_{2m}^{\text{Hom}} G_h.$$

Proof. The equivalence below $(2m)$ follows from Corollary 13.1. The separation at $(2m)$ follows from the two-equation witness, which defines a finitely generated source group K_f with $(2m)$ generators and relators corresponding to $w_{f,0}, w_{f,1}$. □

21 Local observable lower bounds

The preceding results may be summarized as a lower bound for local invariant-refinement procedures. Consider any invariant procedure whose decisions factor through any finite combination of: CSI, rank-support, flag, or star data of arity $< m$; coefficient-free word-system counts in $< 2m$ variables; Hom counts from $< 2m$ -generated sources; quantifier-free coefficient-free counting word formulas in $< 2m$ variables; subgroup occurrence counts for $< 2m$ -generated subgroups. Then the procedure is constant on a fibre of size

$$|G|^{1/2-o(1)}$$

inside the directly indecomposable special groups of order (G) . This is not a lower bound for all algorithms. It is an observable-complexity lower bound for a broad class of local and counting invariants.

22 Relation to Wilson's genus-two groups

The groups G_f lie in the genus-two family of groups associated with quotients of the Heisenberg group over $\mathbb{F}_{p^m}$. Wilson showed that this family contains many directly and centrally indecomposable groups of order p^{2m+2} with identical proper subgroup and quotient profiles, character tables, and power maps. The present results are complementary. Wilson's theorem gives a strong subgroup/quotient-profile obstruction. Here we give a spectral explanation of bounded-arity word and support-image invisibility: Every CSI level (r) sees exactly spectral divisor data of degree $\leq r$. Every word observable in (k) variables sees exactly spectral divisor data of degree $\leq \lfloor k/2 \rfloor$. The irreducible Pfaffian degree (m) is invisible below CSI arity (m) and word arity $(2m)$. A concrete two-equation witness at $(2m)$ variables distinguishes the groups optimally. One equation never distinguishes. Thus the contribution is not merely another family of hard examples; it is an exact spectral formula explaining the observable barrier.

23 Algorithmic interpretation

The results are not time lower bounds for group isomorphism. In fact, genus-two p -groups admit efficient algorithms using global pencil structure. The theorem instead separates global isomorphism methods from bounded-local-observable methods. For regular pencils, a minimal CSI certificate of nonisomorphism between $\mathcal{F}$ and $\mathcal{G}$ is obtained by finding a polynomial (h) of least degree such that

$$D_{\mathcal{F}}(h) \neq D_{\mathcal{G}}(h).$$

The companion linearization $L_h(t)$ is then an optimal CSI witness. For irreducible (f), the skew-linearization $K_f(t)$ gives an optimal word-count witness with two equations in $(2m)$ variables. Thus the theory gives explicit, checkable nonisomorphism certificates whose arity is provably minimal inside the corresponding observable hierarchy.

24 Main theorem package

We collect the main statements.

Theorem 24.1 (Pfaffian degree as observable complexity). *Let p be odd. Let*

$$\mathcal{F} = (F_1, \dots, F_s)$$

be a regular affine spectral pencil and define

$$D_{\mathcal{F}}(h) = \sum_{\nu} \deg \gcd(h, F_{\nu}).$$

Then: $\text{CSI}_{\leq r}(\beta_{\mathcal{F}})$ determines and is determined by $D_{\mathcal{F}, \leq r}$. Every coefficient-free word observable in (k) variables factors through $D_{\mathcal{F}, \leq \lfloor k/2 \rfloor}$. If f, h are irreducible of degree (m) , then all CSI observables below arity (m) and all word observables below $(2m)$ variables are blind to the difference between G_f and G_h . If f, h are not projectively equivalent, then CSI at arity (m) and two explicit word equations in $(2m)$ variables distinguish them. One word equation never distinguishes irreducible degree- (m) blocks. The associated directly indecomposable special groups have order p^{2m+2} , so the exact word-observable threshold is

$$2m = \log_p |G_f| - 2.$$

A single lower-level observable fibre contains

$$|G_f|^{1/2-o(1)}$$

nonisomorphic directly indecomposable special groups. Hom profiles from $< 2m$ -generated sources, quantifier-free word-counting profiles in $< 2m$ variables, and subgroup occurrence profiles for $< 2m$ -generated subgroups are all blind on this fibre.

25 Further directions

25.1 Beyond affine regular pencils

The affine regular model assumes a chosen nondegenerate scalar member. A homogeneous treatment should include spectral factors at infinity. The same Smith/gcd mechanism should extend after replacing (t) by homogeneous binary forms.

25.2 Higher derived rank

For $\dim W > 2$, the corresponding spectral data are no longer elementary divisors of a pencil but Pfaffian systems. A higher-dimensional analogue would likely involve determinantal ideals and multivariate Smith-like invariants.

25.3 Logical observables

The present paper proves lower bounds for coefficient-free quantifier-free word-count observables. Extending the factorization theorem to bounded-variable counting logic fragments with quantifier alternation would require a separate translation from formulas to spectral divisor data.

25.4 Zeta functions and subgroup growth

Pfaffian geometry appears in local zeta functions of class-two groups. It would be interesting to determine whether truncations of the spectral divisor function $D_{\mathcal{F}}$ control corresponding truncations of subgroup or normal zeta functions.

References

- [1] V. A. Bovdi, T. G. Gerasimova, M. A. Salim, and V. V. Sergeichuk. Reduction of a pair of skew-symmetric matrices to its canonical form under congruence. *Linear Algebra and its Applications* 498 (2016), 403–433.
- [2] Peter A. Brooksbank, Yinan Li, Youming Qiao, and James B. Wilson. Improved algorithms for alternating matrix space isometry: From theory to practice. *ESA* 2020.
- [3] Peter A. Brooksbank, Joshua Maglione, and James B. Wilson. A fast isomorphism test for groups whose Lie algebra has genus 2. *Journal of Algebra* 473 (2017), 545–590.
- [4] Joshua A. Grochow and Youming Qiao. On p -Group Isomorphism: Search-to-Decision, Counting-to-Decision, and Nilpotency Class Reductions via Tensors. *CCC 2021*; Journal version, *ACM Transactions on Computation Theory*.
- [5] R. Gow and G. McGuire. Invariant rational functions, linear fractional transformations and irreducible polynomials over finite fields. *Finite Fields and Their Applications* 78 (2022), 101977.
- [6] I. M. Isaacs. *Finite Group Theory*. American Mathematical Society, 2008.
- [7] R. Lidl and H. Niederreiter. *Finite Fields*. Cambridge University Press, 1997.
- [8] V. Mehrmann, D. S. Mackey, N. Mackey, and H. Xu. Vector spaces of linearizations for matrix polynomials. *SIAM Journal on Matrix Analysis and Applications* 28 (2006), 971–1004.
- [9] L. Reis. Invariant theory of a special group action on irreducible polynomials over finite fields. *Designs, Codes and Cryptography* 87 (2019), 1095–1117.
- [10] V. V. Sergeichuk. Canonical matrices of forms and pairs of forms over finite and p -adic fields. *Linear Algebra and its Applications* 438 (2013), 2322–2339.
- [11] X. Sun. Faster Isomorphism for p -Groups of Class 2 and Exponent p . *STOC* 2023.
- [12] J. B. Wilson. Decomposing p -groups via Jordan algebras. *Journal of Algebra* 322 (2009), 2642–2679.
- [13] J. B. Wilson. The threshold for subgroup profiles to agree is $\Omega(\log n)$. *arXiv:1612.01444*.
- [14] J. Brachter and P. Schweitzer. On the Weisfeiler–Leman Dimension of Finite Groups. *LICS* 2020.

- [15] J. Brachter, P. Schweitzer, and related authors. A systematic study of isomorphism invariants of finite groups. ESA 2022.