Word-Measure Twins and Pfaffian Moduli in Class-Two p-Groups

Luca Blanchi

June 2026

Abstract

For a finite group G and a word $w \in F_s$, let

$$\mu_{w,G}$$

denote the probability distribution of the word map

$$w_G : G^s \to G.$$

We construct large families of pairwise non-isomorphic finite p-groups with identical word-measure distributions for every word. More precisely, for every integer $d \geq 4$ and all sufficiently large odd primes p, there exist at least

$$c_d p^g, \qquad g = \frac{(d-1)(d-2)}{2},$$

pairwise non-isomorphic special p-groups of nilpotency class 2, exponent p, and order

$$p^{2d+3},$$

such that, after a fixed bijection of their underlying sets, every word has the same distribution on all groups in the family. Thus the complete collection of word-map distributions does not determine a finite group. The construction uses Pfaffian representations of a fixed smooth plane curve

$$C = F = 0 \subset \mathbb{P}^2_{\mathbb{F}_p}.$$

A linear Pfaffian representation of F is a skew-symmetric $2d \times 2d$ matrix $M(x_0, x_1, x_2)$ with linear entries and

$$\mathrm{Pf}(M) = F.$$

It defines an alternating tensor

$$\beta_M : \Lambda^2 \mathbb{F}_p^{2d} \to \mathbb{F}_p^3$$

and hence a special class-two exponent-p group G_M. The key compression theorem says that for groups of the form G_β, the distribution of every word is determined by

$$\dim V, \qquad \dim W, \qquad \lambda \mapsto \mathrm{rank}(\lambda \circ \beta).$$

For Pfaffian representations of the same smooth curve, this rank profile depends only on the curve:

$$\mathrm{rank}\, M(\lambda) = \begin{cases} 2d, & [\lambda] \notin C, \\ 2d-2, & [\lambda] \in C. \end{cases}$$

Thus all Pfaffian representations of C give word-measure twins. The groups are nevertheless non-isomorphic whenever the Pfaffian representations are inequivalent. Using decomposable Pfaffian representations associated with line bundles

$$L \in \mathrm{Pic}^{g-1}(C), \qquad h^0(C, L) = 0,$$

we obtain $\gg_d p^g$ pairwise non-isomorphic examples. We also record a stronger geometric refinement. Over an algebraically closed field, the scalar word-measure profile collapses a whole open subset of the moduli space

$$M_C(2, K_C),$$

of dimension (3g-3). Under the standard finite-field rationality hypothesis for this Pfaffian moduli open, the finite-field family can be enlarged to size $\gg_d p^{3g-3}$. The examples have the same hom-counts from every one-relator group, the same untwisted surface-group hom-counts, the same probabilistic identities, the same commutator-factorization profiles, and the same irreducible character-degree zeta function. They are separated by kernel tomography: Kernel-MVMT recovers the projectivized Pfaffian kernel bundle

$$\mathbb{P}\mathcal{K}_M = \{(x, [v]) \in C \times \mathbb{P}^{2d-1} : M(x)v = 0\},$$

which is invisible to ordinary word-map distributions.

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

Word maps are natural probes of finite groups. Given a word

$$w \in F_s,$$

every group G has a word map

$$w_G : G^s \to G.$$

For finite G, this yields a probability distribution

$$\mu_{w,G}(g) = \frac{|\{(g_1, \ldots, g_s) \in G^s : w(g_1, \ldots, g_s) = g\}|}{|G|^s}.$$

It is natural to ask how much of G is encoded by the collection

$$\mu_{w,G} : w \in F_s, \ s \geq 1.$$

For abelian groups this collection is strong enough to determine the group. More generally, word-map distributions encode substantial structural information. The present paper proves that, nevertheless, the complete collection of all word-map distributions does not determine a finite group.

We construct large families of pairwise non-isomorphic p-groups of nilpotency class 2, exponent p, and fixed order, such that every word has the same distribution on all groups in the family. The construction is geometric. Let

$$C = F = 0 \subset \mathbb{P}^2$$

be a smooth plane curve of degree d. A linear Pfaffian representation of C is a skew-symmetric $2d \times 2d$ matrix

$$M(x_0, x_1, x_2)$$

with linear entries and

$$\mathrm{Pf}(M) = F.$$

It defines an alternating tensor

$$\beta_M : \Lambda^2 V \to W, \qquad \dim V = 2d, \quad \dim W = 3,$$

and hence a class-two exponent-p group

$$G_M = V \oplus W.$$

All Pfaffian representations of the same smooth curve have the same scalar rank profile:

$$\lambda \longmapsto \operatorname{rank} M(\lambda).$$

The first main theorem proves that, for class-two exponent-p groups, this rank profile determines the distribution of every word. Thus Pfaffian representations of the same curve give word-measure twins. However, Pfaffian representations of a fixed curve are not unique. They are parametrized by vector bundles on C. In particular, line bundles

$$L \in \mathrm{Pic}^{g-1}(C), \qquad h^0(C, L) = 0,$$

give determinantal representations, hence decomposable Pfaffian representations. This produces $\gg p^g$ non-isomorphic groups with identical word distributions. The theorem has several consequences. First, hom-counts from all one-relator groups do not determine a finite group. Indeed,

$$|\operatorname{Hom}(\langle x_1, \ldots, x_s \mid w = 1\rangle, G)|$$

is exactly the identity fibre of w_G. Second, all surface-group hom-counts agree in our examples, since orientable surface groups have one-relator presentations. Third, no isomorphism procedure using only a word-map distribution oracle can distinguish the constructed groups. Fourth, the examples have the same character-degree distribution and the same character-degree zeta function. Finally, the examples show a strict hierarchy. Ordinary word maps see only the Pfaffian curve. Kernel tomography sees the kernel bundle over the curve, which is the missing moduli datum.

2 Alternating tensors and class-two exponent-p groups

Let $k = \mathbb{F}_p$, where $p \neq 2$. Let

$$\beta : \Lambda_k^2 V \to W$$

be an alternating tensor. Define

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

with multiplication

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

Then G_β has nilpotency class at most 2 and exponent p. Its commutator is

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

The center is

$$Z(G_\beta) = \mathrm{rad}(\beta) \oplus W,$$

where

$$\mathrm{rad}(\beta) = \{v \in V : \beta(v, V) = 0\}.$$

The derived subgroup is

$$G'_\beta = \mathrm{im}\,\beta \subseteq W.$$

Thus G_β is special precisely when

$$\mathrm{rad}(\beta) = 0, \qquad \mathrm{im}\,\beta = W.$$

If G_β and $G_{\beta'}$ are special, then

$$G_\beta \cong G_{\beta'}$$

if and only if the tensors are pseudo-isometric: there exist

$$S \in GL(V), \qquad T \in GL(W)$$

such that

$$T\beta(u, v) = \beta'(Su, Sv)$$

for all $u, v \in V$.

3 Strong word-measure twins

Let G, H be finite groups. We call G and H strong word-measure twins if there exists a bijection

$$\Phi : G \to H$$

such that, for every word $w \in F_s$, for every $s \geq 1$,

$$\Phi_* \mu_{w,G} = \mu_{w,H}.$$

Equivalently, for every word w and every $h \in H$,

$$\mu_{w,H}(h) = \mu_{w,G}(\Phi^{-1}(h)).$$

This is stronger than saying that the word-map fibre-size multisets agree. The equality is word-by-word under one fixed bijection of underlying sets.

4 Word measures in class two and exponent p

Let

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

Let

$$w \in F_s$$

be a word. In the relatively free group of nilpotency class 2 and exponent p, every word has a unique normal form

$$w = x_1^{a_1} \cdots x_s^{a_s} \prod_{1 \leq i < j \leq s} [x_i, x_j]^{b_{ij}},$$

where

$$a_i, b_{ij} \in \mathbb{F}_p.$$

Let

$$a = (a_1, \ldots, a_s).$$

Let $B = (B_{ij})$ be the alternating $s \times s$ matrix with

$$B_{ij} = b_{ij} \quad (i < j), \qquad B_{ji} = -b_{ij}, \qquad B_{ii} = 0.$$

We separate two cases.

Lemma 4.1 (Noncentral words are uniformly distributed)**.** *If*

$$a \neq 0,$$

then the word map

$$w : G_\beta^s \to G_\beta$$

has the uniform distribution on G_β.

Proof. Write

$$g_i = (v_i, z_i) \in V \oplus W.$$

The V-coordinate of $w(g_1, \dots, g_s)$ is

$$\sum_{i=1}^{s} a_i v_i.$$

Since some $a_i \neq 0$, this is uniformly distributed on V. The W-coordinate has the form

$$\sum_{i=1}^{s} a_i z_i + Q(v_1, \dots, v_s),$$

where Q is a fixed W-valued expression depending on β and w. Condition on all v_i's and on all z_j's except one z_i with $a_i \neq 0$. Then the term

$$a_i z_i$$

makes the W-coordinate uniform on W. Since the V-coordinate depends only on the v_i's, the total output is uniform on

$$V \oplus W.$$

□

Lemma 4.2 (Central word distributions are determined by scalar ranks)**.** *Assume*

$$a = 0.$$

Then the word is central and

$$w(g_1, \dots, g_s) = \sum_{i<j} b_{ij} \beta(v_i, v_j) \in W.$$

Let

$$2t = \operatorname{rank} B.$$

For every $\lambda \in W^*$, the Fourier coefficient of the word distribution at λ is

$$\widehat{\mu}_{w,\beta}(\lambda) = p^{-t \operatorname{rank}(\lambda \circ \beta)}.$$

Proof. Let

$$A_\lambda = \lambda \circ \beta.$$

The Fourier coefficient is

$$\widehat{\mu}_{w,\beta}(\lambda) = \mathbb{E}_{v_1,\dots,v_s \in V} \psi \left(\sum_{i<j} b_{ij} A_\lambda(v_i, v_j) \right).$$

Since B is alternating of rank (2t), there is a linear change of variables in $\mathbb{F}_p^s$ putting B into the standard form

$$H(1)^{\oplus t} \oplus 0.$$

This induces a measure-preserving linear bijection of V^s. Therefore the exponent becomes

$$\sum_{\ell=1}^{t} A_\lambda(u_\ell, v_\ell).$$

The expectation factors:

$$\widehat{\mu}_{w,\beta}(\lambda) = \prod_{\ell=1}^{t} \mathbb{E}_{u_\ell, v_\ell \in V} \psi(A_\lambda(u_\ell, v_\ell)).$$

For any bilinear form A,

$$\mathbb{E}_{u,v\in V} \psi(A(u,v)) = p^{-\operatorname{rank} A}.$$

Thus

$$\widehat{\mu}_{w,\beta}(\lambda) = p^{-t \operatorname{rank} A_\lambda}.$$

□

Theorem 4.3 (Word-measure compression theorem)**.** *Let*

$$\beta : \Lambda^2 V \to W, \qquad \beta' : \Lambda^2 V' \to W'$$

be alternating tensors over $\mathbb{F}_p$, with

$$\dim V = \dim V', \qquad \dim W = \dim W'.$$

Suppose there exists an isomorphism

$$T : W \to W'$$

such that

$$\operatorname{rank}(\lambda \circ \beta) = \operatorname{rank}((\lambda \circ T^{-1}) \circ \beta')$$

for every

$$\lambda \in W^*.$$

Then, for any linear isomorphism

$$S : V \to V',$$

the bijection

$$\Phi : G_\beta \to G_{\beta'}, \qquad \Phi(v, z) = (Sv, Tz),$$

satisfies

$$\Phi_* \mu_{w, G_\beta} = \mu_{w, G_{\beta'}}$$

for every word w. In particular, G_β and $G_{\beta'}$ are strong word-measure twins.

Proof. Let $w \in F_s$. Write its class-two exponent-p normal form as above. If $a \neq 0$, Lemma 4.1 shows that both word distributions are uniform. The bijection Φ sends the uniform distribution on G_β to the uniform distribution on $G_{\beta'}$. If $a = 0$, the distribution is supported on W. By Lemma 4.2, its Fourier coefficient at $\lambda \in W^*$ is

$$p^{-t\,\mathrm{rank}(\lambda\circ\beta)}.$$

For $G_{\beta'}$, the Fourier coefficient at

$$\lambda \circ T^{-1} \in (W')^*$$

is

$$p^{-t\,\mathrm{rank}((\lambda\circ T^{-1})\circ\beta')}.$$

These are equal by hypothesis. Fourier inversion on the finite abelian group W gives equality of the central distributions after identifying W and W' by T. Therefore every word distribution is preserved by Φ.

□

5 Pfaffian nets

Let

$$V = k^{2d}, \qquad W = k^3.$$

A tensor

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

is a net of alternating forms. Choose coordinates

$$x_0, x_1, x_2$$

on W^*. The tensor gives a skew-symmetric matrix

$$M_\beta(x_0, x_1, x_2) = x_0 A_0 + x_1 A_1 + x_2 A_2.$$

Its Pfaffian

$$F_\beta = \mathrm{Pf}(M_\beta)$$

is a homogeneous polynomial of degree d. It defines a plane curve

$$C_\beta = \{F_\beta = 0\} \subseteq \mathbb{P}^2.$$

If C_β is smooth, then

$$\mathrm{rank}\, M_\beta(\lambda) = \begin{cases} 2d, & [\lambda] \notin C_\beta, \\ 2d-2, & [\lambda] \in C_\beta. \end{cases}$$

Indeed, away from C_β, the Pfaffian is nonzero, so the matrix is invertible. On C_β, smoothness excludes corank at least 4, since the singular locus of the Pfaffian hypersurface is exactly the corank-≥ 4 locus.

Theorem 5.1 (Same Pfaffian curve gives word-measure twins)**.** *Let*

$$M,\ M'$$

be two linear Pfaffian representations of the same smooth plane curve

$$C = F = 0 \subset \mathbb{P}^2_k$$

of degree d. Let

$$\beta_M, \beta_{M'} : \Lambda^2 k^{2d} \to k^3$$

be the associated tensors. Then

$$G_{\beta_M}$$

and

$$G_{\beta_{M'}}$$

are strong word-measure twins.

Proof. For every nonzero

$$\lambda \in (k^3)^*,$$

we have

$$\operatorname{rank} M(\lambda) = \begin{cases} 2d, & [\lambda] \notin C, \\ 2d-2, & [\lambda] \in C. \end{cases}$$

The same formula holds for M'. For $\lambda = 0$, both ranks are 0. Thus the scalar rank profiles coincide. Theorem 4.3 gives strong word-measure equivalence.

□

Corollary 5.2 (Geometric word-measure twins over all finite extensions)**.** *Suppose $k = \mathbb{F}_p$, and M, M' are Pfaffian representations over k of the same smooth plane curve C/k. Then for every finite extension*

$$K/k,$$

the groups

$$G_{\beta_M}(K) \quad \textit{and} \quad G_{\beta_{M'}}(K)$$

are strong word-measure twins.

Proof. After base change to K, the two representations still have the same smooth Pfaffian curve C_K. Hence their scalar rank profiles over K coincide. Theorem 4.3 applies over K.

□

6 Non-isomorphism

Two Pfaffian representations

$$M, M'$$

of a plane curve are equivalent if there exist

$$P \in GL_{2d}(k), \qquad T \in GL_3(k), \qquad c \in k^\times,$$

such that

$$M'(x) = c\, P^\mathsf{T} M(Tx) P.$$

If

$$G_{\beta_M} \cong G_{\beta_{M'}}$$

and both groups are special, then

$$\beta_M$$

and

$$\beta_{M'}$$

are pseudo-isometric. This is exactly equivalence of the corresponding Pfaffian representations, allowing the target change T. If M and M' represent the same fixed curve C, then any such target change T must preserve C. Therefore, if C has trivial projective automorphism group, pseudo-isometry forces equivalence with fixed projective coordinates.

7 Pfaffian representations from line bundles

Let

$$C \subset \mathbb{P}^2_k$$

be a smooth plane curve of degree d. Its genus is

$$g = \frac{(d-1)(d-2)}{2}.$$

A theorem of Beauville identifies linear determinantal representations of C with line bundles

$$L \in \operatorname{Pic}^{g-1}(C)$$

satisfying

$$h^0(C, L) = 0.$$

For such L, there is a $d \times d$ matrix of linear forms

$$D_L(x_0, x_1, x_2)$$

such that

$$\det D_L = F.$$

From D_L, define the skew-symmetric $2d \times 2d$ matrix

$$P_L = \begin{pmatrix} 0 & D_L \\ -D_L^{\intercal} & 0 \end{pmatrix}.$$

Then

$$\mathrm{Pf}(P_L) = \pm F.$$

After changing sign if necessary, P_L is a Pfaffian representation of C. The associated rank-2 bundle is

$$E_L = L \oplus (K_C \otimes L^{-1}).$$

The involution

$$L \longmapsto K_C \otimes L^{-1}$$

interchanges the two summands. Apart from this involution, the decomposable Pfaffian representations are distinct. Indeed, if

$$L \oplus (K_C \otimes L^{-1}) \cong L' \oplus (K_C \otimes L'^{-1}),$$

then by Krull–Schmidt for vector bundles on curves,

$$L' = L \quad \text{or} \quad L' = K_C \otimes L^{-1},$$

except at the fixed points of the involution.

8 Counting finite-field examples

Fix

$$d \geq 4.$$

Let

$$\mathcal{P}_d$$

be the projective space of homogeneous ternary forms of degree d. The locus parameterizing smooth plane curves with trivial projective automorphism group contains a nonempty open subset. For all sufficiently large primes p, this open subset has $\mathbb{F}_p$-points. Choose

$$C/\mathbb{F}_p$$

in this open subset. For $p \gg_d 1$, the Hasse–Weil bound gives

$$C(\mathbb{F}_p) \neq \varnothing.$$

Hence

$$\mathrm{Pic}^{g-1}(C)(\mathbb{F}_p)$$

has a rational point and is a torsor under

$$J_C(\mathbb{F}_p),$$

where J_C is the Jacobian. Therefore

$$|\,\mathrm{Pic}^{g-1}(C)(\mathbb{F}_p)| = |J_C(\mathbb{F}_p)|.$$

The Weil bounds for J_C give

$$|J_C(\mathbb{F}_p)| = p^g + O_d(p^{g-\frac{1}{2}}).$$

Let

$$\Theta = \{L \in \mathrm{Pic}^{g-1}(C) : h^0(C, L) > 0\}$$

be the theta divisor. Since Θ is a divisor of bounded degree depending only on d,

$$|\Theta(\mathbb{F}_p)| = O_d(p^{g-1}).$$

Thus

$$U_C(\mathbb{F}_p) = \{L \in \mathrm{Pic}^{g-1}(C)(\mathbb{F}_p) : h^0(C, L) = 0\}$$

satisfies

$$|U_C(\mathbb{F}_p)| = p^g + O_d(p^{g-\frac{1}{2}}).$$

The involution

$$L \mapsto K_C \otimes L^{-1}$$

has fibres of size at most 2. Its fixed points are contained in

$$\mathrm{Pic}(C)[2],$$

which has cardinality at most

$$2^{2g}.$$

Therefore, for $p \gg_d 1$, the quotient contains at least

$$c_d p^g$$

classes, for some constant

$$c_d > 0.$$

For every such class choose L, build P_L, and let

$$\beta_L : \Lambda^2 \mathbb{F}_p^{2d} \to \mathbb{F}_p^3$$

be the associated tensor.

9 Speciality of the associated groups

We verify that the groups obtained from the tensors β_L are special.

Lemma 9.1 (Surjectivity)**.** *The image of*

$$\beta_L : \Lambda^2 \mathbb{F}_p^{2d} \to \mathbb{F}_p^3$$

is all of

$$\mathbb{F}_p^3.$$

Proof. If the image were a proper subspace, then the coefficient matrices of

$$P_L(x_0, x_1, x_2)$$

would span a subspace of dimension at most 2. After a linear change of coordinates, P_L would depend on at most two variables. Then

$$\mathrm{Pf}(P_L) = F$$

would depend on at most two variables. A homogeneous plane curve defined by a binary form of degree at least 2 is singular: over an algebraic closure, the binary form is a product of linear forms, and all corresponding lines pass through a common point. This contradicts smoothness of C.

□

Lemma 9.2 (Radical-freeness)**.** *The radical of*

$$\beta_L$$

is zero.

Proof. If

$$0 \neq v \in \mathrm{rad}(\beta_L),$$

then

$$P_L(x)v = 0$$

for every

$$x = (x_0, x_1, x_2).$$

Thus every matrix $P_L(x)$ is singular. Therefore

$$\mathrm{Pf}(P_L)$$

is identically zero. But

$$\mathrm{Pf}(P_L) = \pm F$$

and

$$F \neq 0.$$

Contradiction.

□

Corollary 9.3. *The group*

$$G_L = G_{\beta_L}$$

is special, of nilpotency class 2*, exponent* p*, and order*

$$p^{2d+3}.$$

10 Main finite-field theorem

Theorem 10.1 (Large families of word-measure twins)**.** *For every integer*

$$d \geq 4,$$

there exist constants

$$p_0(d), \quad c_d > 0$$

such that, for every odd prime

$$p \geq p_0(d),$$

there exist at least

$$c_d p^g, \qquad g = \frac{(d-1)(d-2)}{2},$$

pairwise non-isomorphic special p*-groups*

$$G_1, \dots, G_N$$

of nilpotency class 2*, exponent* p*, and order*

$$p^{2d+3},$$

such that

$$G_i$$

and

$$G_j$$

are strong word-measure twins for all i, j*.*

Proof. Choose a smooth plane curve

$$C/\mathbb{F}_p$$

of degree d with trivial projective automorphism group, as in Section 8. From the set

$$U_C(\mathbb{F}_p)$$

of line bundles $L \in \mathrm{Pic}^{g-1}(C)(\mathbb{F}_p)$ with $h^0(L) = 0$, quotient by the involution

$$L \sim K_C \otimes L^{-1}.$$

For $p \gg_d 1$, this gives at least

$$c_d p^g$$

inequivalent decomposable Pfaffian representations

$$P_L$$

of the same curve C. Each P_L gives a special group

$$G_L$$

of order

$$p^{2d+3}.$$

Since all P_L have the same Pfaffian curve C, Theorem 5.1 implies that all G_L are strong word-measure twins. It remains to prove pairwise non-isomorphism. If

$$G_L \cong G_{L'},$$

then, since the groups are special, their commutator tensors are pseudo-isometric. Hence the Pfaffian representations

$$P_L, \quad P_{L'}$$

are equivalent up to a projective automorphism of C. But C has trivial projective automorphism group. Therefore the Pfaffian representations are equivalent with fixed projective coordinates. By the decomposable classification,

$$L' = L \quad \text{or} \quad L' = K_C \otimes L^{-1}.$$

These have already been identified in the quotient. Thus the selected groups are pairwise non-isomorphic. □

11 Entropy of the word-measure fibre

Let

$$N_G = \log_p |G|.$$

For the groups above,

$$N_G = 2d + 3.$$

The fibre of the complete word-measure profile contains at least

$$c_d p^g$$

groups, where

$$g = \frac{(d-1)(d-2)}{2} = \frac{(N_G - 5)(N_G - 7)}{8}.$$

Therefore

$$\log_p |\operatorname{Fib}_{\mathrm{word}}(G)| \geq \frac{(N_G - 5)(N_G - 7)}{8} + O_d(1).$$

Thus the complete collection of all single-word distributions may leave an ambiguity whose logarithmic size is quadratic in

$$\log_p |G|.$$

12 Full-moduli geometric refinement

The previous construction used only the decomposable Pfaffian representations

$$E_L = L \oplus (K_C \otimes L^{-1}).$$

There is a larger geometric family. Let k be algebraically closed. Buckley–Košir identify equivalence classes of linear Pfaffian representations of a smooth plane curve C with an open subset

$$\mathcal{U}_C \subset M_C(2, K_C),$$

where $M_C(2, K_C)$ is the moduli space of semistable rank-2 vector bundles with determinant K_C, and the open condition is

$$h^0(C, E) = 0.$$

The dimension is

$$\dim M_C(2, K_C) = 3g - 3.$$

All Pfaffian representations in $\mathcal{U}_C$ have the same Pfaffian curve C, and therefore the same word-measure profile. Thus, over an algebraically closed field, the word-measure fibre contains an open subset of dimension

$$3g - 3.$$

Over finite fields, the same reasoning gives the following refinement under an explicit rationality hypothesis.

Remark 12.1 (Hypothesis FM)**.** *For a smooth plane curve $C/\mathbb{F}_p$, assume: the Pfaffian moduli open*

$$\mathcal{U}_C \subset M_C(2, K_C)$$

is geometrically irreducible and nonempty over $\mathbb{F}_p$; every rational point of $\mathcal{U}_C(\mathbb{F}_p)$ corresponds to a Pfaffian representation defined over $\mathbb{F}_p$; the quotient by projective equivalence has fibres of size bounded by a constant depending only on d.

Theorem 12.2 (Full-moduli finite-field refinement)**.** *Assume Hypothesis FM for a smooth plane curve*

$$C/\mathbb{F}_p$$

of degree d with trivial projective automorphism group. Then, for $p \gg_d 1$, there are at least

$$c'_d p^{3g-3}$$

pairwise non-isomorphic special class-two exponent-p groups of order

$$p^{2d+3}$$

with identical word-map distributions for every word.

Proof. By Lang–Weil,

$$|\mathcal{U}_C(\mathbb{F}_p)| = p^{3g-3} + O_d(p^{3g-\frac{7}{2}}).$$

By Hypothesis FM, these rational points give Pfaffian representations over $\mathbb{F}_p$, and equivalence classes have bounded fibres. All representations have the same Pfaffian curve C, hence give strong word-measure twins by Theorem 5.1. The same speciality and non-isomorphism arguments from Sections 9 and 10 apply.

□

13 Local scalar collapse

The previous results concern ordinary word maps over finite groups. We now record a stronger local scalar statement. Let R be a finite local principal ring with residue field of odd characteristic. Let

$$H(a) = \begin{pmatrix} 0 & a \\ -a & 0 \end{pmatrix}.$$

Lemma 13.1 (Local alternating normal form)**.** *Let*

$$M \in M_{2d}(R)$$

be skew-symmetric. If the reduction of M modulo the maximal ideal has rank at least

$$2d - 2,$$

then M is congruent over R to

$$H(1)^{\oplus(d-1)} \oplus H(a)$$

for some

$$a \in R.$$

Moreover,

$$\mathrm{Pf}(M) = ua$$

for some unit

$$u \in R^{\times}.$$

Proof. Since the reduction has rank at least (2d-2), there is a skew-symmetric minor of size (2d-2) whose Pfaffian is a unit. Thus one has a free direct summand on which the alternating form is unimodular. Symplectic Gram–Schmidt over the local ring splits off

$$d - 1$$

unit hyperbolic planes

$$H(1).$$

The orthogonal complement has rank 2, and every alternating form on a free rank-2 module has the form

$$H(a).$$

The Pfaffian is multiplicative under orthogonal direct sums, and each $H(1)$ contributes a unit. Hence

$$\mathrm{Pf}(M) = ua.$$

□

Theorem 13.2 (Universal scalar local collapse)**.** *Let*

$$M, \ M'$$

be two Pfaffian representations of the same smooth plane curve

$$C = F = 0.$$

Let

$$R$$

be a finite local principal ring of odd residue characteristic, and let

$$\lambda \in \mathbb{P}^2(R).$$

Then

$$M(\lambda)$$

and

$$M'(\lambda)$$

are congruent over R.

Proof. Let

$$\bar{\lambda}$$

be the reduction of λ. If

$$\bar{\lambda} \notin C,$$

then

$$F(\lambda) \in R^{\times}.$$

Thus both

$$M(\lambda)$$

and

$$M'(\lambda)$$

are unimodular alternating forms. Every unimodular alternating form over a local ring with 2 invertible is congruent to

$$H(1)^{\oplus d}.$$

Hence they are congruent. Now suppose

$$\bar{\lambda} \in C.$$

Since C is smooth, the reduction of either matrix has corank exactly 2. Lemma 13.1 gives

$$M(\lambda) \sim H(1)^{\oplus(d-1)} \oplus H(a),$$

with

$$F(\lambda) = \mathrm{Pf}(M(\lambda)) = ua$$

for a unit u. Multiplying a by a unit does not change the congruence class of $H(a)$, so

$$M(\lambda) \sim H(1)^{\oplus(d-1)} \oplus H(F(\lambda)).$$

The same argument gives

$$M'(\lambda) \sim H(1)^{\oplus(d-1)} \oplus H(F(\lambda)).$$

Therefore

$$M(\lambda) \sim M'(\lambda).$$

$\square$

Corollary 13.3. *Every pointwise scalar observable invariant under congruence gives identical output on two Pfaffian representations of the same smooth curve. This includes: scalar rank profiles; scalar Smith profiles over finite principal local rings; scalar Fourier coefficients; scalar Artin moments; central single-output scalar commutator-word distributions.*

14 Kernel tomography separates the twins

The word-measure results show that ordinary word maps cannot distinguish the groups G_L. Kernel tomography can see the missing geometry. Let M be a Pfaffian representation of a smooth plane curve C. On C, the matrix $M(x)$ has corank 2. Therefore

$$\mathcal{K}_M = \ker(M|_C)$$

is a rank-2 vector bundle on C. Define the projectivized kernel incidence

$$\mathbb{P}\mathcal{K}_M = \{(x, [v]) \in C \times \mathbb{P}^{2d-1} : M(x)v = 0\}.$$

Kernel-MVMT recovers this incidence. Indeed, for a line

$$L \subset V$$

and a scalar tag

$$\lambda \in W^*,$$

consider the source-restricted commutator distribution

$$(u, v) \in L \times V \longmapsto \beta(u, v).$$

Its Fourier coefficient at λ is

$$\mathbb{E}_{u \in L,\ v \in V} \psi((\lambda \circ \beta)(u, v)) = p^{-\operatorname{rank}((\lambda\circ\beta)^\sharp|_L)}.$$

Since L is one-dimensional,

$$\operatorname{rank}((\lambda \circ \beta)^\sharp|_L) = 0$$

if and only if

$$L \subseteq \ker(\lambda \circ \beta).$$

Thus Kernel-MVMT detects the incidence

$$L \subseteq \ker M(\lambda).$$

As λ ranges over C, it recovers

$$\mathbb{P}\mathcal{K}_M.$$

The projectivization of a rank-2 bundle determines the bundle up to tensoring by a line bundle:

$$\mathbb{P}(E) \cong \mathbb{P}(E') \quad \Rightarrow \quad E' \cong E \otimes N.$$

If

$$\det E \cong \det E' \cong K_C,$$

then

$$N^{\otimes 2} \cong \mathcal{O}_C.$$

Hence projective kernel data reduces the word-measure fibre to at most a finite

$$\operatorname{Pic}(C)[2]$$

ambiguity. Over an algebraic closure,

$$|\operatorname{Pic}(C)[2]| = 2^{2g}.$$

Thus, even after quotienting by this finite ambiguity, the decomposable family still contains

$$\gg_d p^g$$

classes visible to Kernel-MVMT but invisible to all ordinary word maps. Under Hypothesis FM, the same conclusion holds with

$$\gg_d p^{3g-3}$$

in place of

$$\gg_d p^g.$$

15 Applications

15.1 Word maps do not classify finite groups

Theorem 10.1 proves that the complete collection of word-map probability distributions

$$\mu_{w,G} : w \in F_s, \ s \geq 1$$

does not determine a finite group up to isomorphism. The examples are special p-groups of class 2 and exponent p, and the word-measure fibre has size at least

$$c_d p^g.$$

15.2 One-relator hom-counts do not classify finite groups

Let

$$\Gamma_w = \langle x_1, \ldots, x_s \mid w = 1 \rangle$$

be a one-relator group. Then

$$|\operatorname{Hom}(\Gamma_w, G)| = |\{(g_1, \ldots, g_s) \in G^s : w(g_1, \ldots, g_s) = 1\}|.$$

Therefore, if G_i, G_j are groups from Theorem 10.1,

$$|\operatorname{Hom}(\Gamma_w, G_i)| = |\operatorname{Hom}(\Gamma_w, G_j)|$$

for every one-relator group Γ_w. Thus hom-counts from all one-relator groups do not determine a finite group.

15.3 Surface-group counts

The fundamental group of a closed orientable surface of genus h has presentation

$$\pi_1(\Sigma_h) = \left\langle a_1, b_1, \ldots, a_h, b_h \;\middle|\; \prod_{i=1}^{h} [a_i, b_i] = 1 \right\rangle.$$

Hence the groups in Theorem 10.1 have the same hom-counts from every closed orientable surface group:

$$|\operatorname{Hom}(\pi_1(\Sigma_h), G_i)| = |\operatorname{Hom}(\pi_1(\Sigma_h), G_j)|.$$

Equivalently, they have the same untwisted finite-gauge surface partition functions. We do not claim equality of twisted Dijkgraaf–Witten theories.

15.4 Word-map oracle lower bound

Suppose an isomorphism procedure is given oracle access to

$$w \longmapsto \mu_{w,G}$$

for every word w. On the families constructed in Theorem 10.1, this oracle is identical for all groups in the family. Therefore no procedure using only this oracle can decide isomorphism on these inputs. This is an information-theoretic obstruction: the invariant is not merely hard to compute; it is insufficient.

15.5 Character-degree zeta functions

For special class-two exponent-p groups, irreducible character degrees are controlled by the ranks of the scalar forms

$$\lambda \circ \beta.$$

Indeed, for a functional

$$\lambda \in W^*,$$

the corresponding coadjoint orbits have size

$$p^{\operatorname{rank}(\lambda\circ\beta)},$$

and the associated irreducible characters have degree

$$p^{\frac{1}{2}\operatorname{rank}(\lambda\circ\beta)}.$$

Thus the character-degree multiset and the character-degree zeta function are determined by the scalar rank profile. The groups in Theorem 10.1 therefore have the same character-degree zeta function. We do not claim that their full character tables coincide.

15.6 Commutator-factorization profiles

For every

$$t \geq 1$$

consider the word

$$c_t = [x_1, y_1] \cdots [x_t, y_t].$$

The groups in Theorem 10.1 have identical distributions of c_t. Therefore, for every corresponding central element z,

$$\#\{(x_i, y_i) : [x_1, y_1] \cdots [x_t, y_t] = z\}$$

is the same in all groups in the family. Thus all commutator-factorization statistics coincide, even though the groups are non-isomorphic.

15.7 Benchmark families for p-group isomorphism

The examples have: the same order; the same exponent; the same nilpotency class; the same derived subgroup dimension; the same Pfaffian curve; the same word-map distributions for every word; the same character-degree zeta function. They are nevertheless non-isomorphic. Thus they are natural benchmark families for invariants and algorithms for class-two exponent-p group isomorphism and for alternating matrix space isometry.

16 Limitations

This paper proves failure of all ordinary single-word distributions. It does not claim that all multi-output word systems fail. In fact, Kernel-MVMT is designed precisely to distinguish the examples by recovering kernel incidence data. The paper also does not claim equality of full character tables, nor equality of twisted Dijkgraaf–Witten theories. The unconditional finite-field construction gives

$$\gg_d p^g$$

examples. The larger

$$\gg_d p^{3g-3}$$

family is stated under Hypothesis FM, which isolates the finite-field rationality and descent issues for the full Pfaffian moduli open.

References

[1] A. Beauville, Determinantal hypersurfaces, Michigan Math. J. 48 (2000), 39–64.

[2] A. Buckley and T. Košir, Plane curves as Pfaffians, Ann. Sc. Norm. Super. Pisa Cl. Sci. 10 (2011), 363–388.

[3] W. Cocke and M.-C. Ho, The probability distribution of word maps on finite groups, arXiv:1807.07111.

[4] M. Levy, Enumerating fibres of commutator words over p-groups, arXiv:1602.04093.

[5] D. A. Buchsbaum and D. Eisenbud, Algebra structures for finite free resolutions, and some structure theorems for ideals of codimension 3, American Journal of Mathematics 99 (1977), 447–485.

[6] T. Harui, Automorphism groups of smooth plane curves, Kodai Mathematical Journal 42 (2019), 308–331.

[7] A. Weil, Numbers of solutions of equations in finite fields, Bulletin of the American Mathematical Society 55 (1949), 497–508.

[8] S. R. Ghorpade and G. Lachaud, Étale cohomology, Lefschetz theorems and number of points of singular varieties over finite fields, Moscow Mathematical Journal 2 (2002), 589–631.

[9] J. B. Wilson, Decomposing p-groups via Jordan algebras, Journal of Algebra 322 (2009), 2642–2679.

[10] P. A. Brooksbank and J. B. Wilson, Computing isometry groups of Hermitian maps, Transactions of the American Mathematical Society 364 (2012), 1975–1996.

[11] C. Qiao, J. B. Wilson, and J. A. Grochow, Polynomial-time isomorphism test of groups that are tame extensions, SIAM J. Comput. 51 (2022), 1217–1257.

[12] X. Sun, Faster Isomorphism for p-Groups of Class 2 and Exponent p, arXiv:2303.15412.

[13] M. Larsen and A. Lubotzky, Representation growth of linear groups, J. Eur. Math. Soc. 10 (2008), 351–390.

[14] M. J. Collins, Representations and Characters of Finite Groups, Cambridge University Press, 1990.