

Quadratic Presentational Complexity and Exact Observable Barriers for Class-Two p -Groups

Luca Blanchi

June 2026

Abstract

Let p be an odd prime and let $\mathcal{N}_{2,p}$ be the variety of finite groups of nilpotency class at most two and exponent p . We study coefficient-free word-equation observables on groups in $\mathcal{N}_{2,p}$, with particular attention to the number of variables required to distinguish nonisomorphic groups. The first result is a quadratic normal form theorem: every word in k variables, when evaluated in $\mathcal{N}_{2,p}$, is represented by a linear exponent-sum part in $\mathbb{F}_p^k$ and an alternating commutator part in $\Lambda^2 \mathbb{F}_p^k$. Thus every finite word-equation system is equivalent, in this variety, to a finite system of linear and alternating-quadratic equations. We formalize such systems as quadratic presentations and give an exact solution-counting formula for class-two exponent- p groups associated with alternating maps. For graphical p -groups arising from the Baer–Lovasz–Tutte construction, we show that quadratic presentational observables are exactly right homomorphism counts toward finite alternating-orthogonality targets. This gives a semantic core for such observables, a complexity dichotomy for fixed observables on input graphs, and a right-profile completeness theorem. Finally, using Wilson-type subgroup-profile families, we obtain an exact arity barrier: there are nonisomorphic groups $G, H \in \mathcal{N}_{2,p}$ whose least distinguishing coefficient-free observable arity is $\log_p |G| - 2$. Thus arity is an irreducible observational resource in this setting.

1 Introduction

Let (G) be a finite group. A finite system of word equations

$$w_1(x_1, \dots, x_k) = 1, \dots, w_m(x_1, \dots, x_k) = 1$$

defines a numerical invariant

$$G \longmapsto \#\{(g_1, \dots, g_k) \in G^k : w_i(g_1, \dots, g_k) = 1 \ \forall i\}.$$

Such invariants include commuting probabilities, higher commuting probabilities, homomorphism counts from finitely presented groups, and many centralizer-type statistics. They are among the most elementary ways to observe a finite group using only its multiplication. This paper studies such observables in the variety

$$\mathcal{N}_{2,p} = \{G : \text{class}(G) \leq 2, \ \exp(G) = p\},$$

where (p) is an odd prime. Groups in $\mathcal{N}_{2,p}$ are naturally represented by alternating bilinear maps. If

$$\beta : V \times V \rightarrow W$$

is alternating over $\mathbb{F}_p$, then

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

with multiplication

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

is a group of class at most 2 and exponent (p). Conversely, special groups in $\mathcal{N}_{2,p}$ arise in this way from their commutator maps. The basic observation is that word equations collapse in this variety. Every word in (k) variables has a unique normal form consisting of:

- a linear exponent-sum part in $\mathbb{F}_p^k$;
- an alternating quadratic commutator part in $\Lambda^2 \mathbb{F}_p^k$. Thus, from the perspective of $\mathcal{N}_{2,p}$, every word observable is a quadratic observable. We call the resulting theory quadratic presentational complexity. Its basic objects are quadratic presentations

$$(X, R, a, b), \quad a : R \rightarrow X, \quad b : R \rightarrow \Lambda^2 X.$$

The map (a) records the linear part of the relations, while (b) records the commutator part. The paper has two main parts. The first part develops the general quadratic formalism and proves an exact solution-counting formula. Given an alternating map

$$\beta : V \times V \rightarrow W,$$

the number of solutions of a quadratic presentation in G_β is a linear factor times the number of noncentral assignments whose quadratic obstruction lies in a specified linear image. The second part specializes to graphical (p)-groups. Given a graph Γ , the Baer–Lovasz–Tutte construction associates a class-two exponent-(p) group G_Γ . This construction is faithful to graph isomorphism: $G_\Gamma \cong G_{\Gamma'}$ if and only if $\Gamma \cong \Gamma'$. For these groups we prove a transfer theorem:

$$|\text{Sol } \mathcal{P}(G_\Gamma)| p^{\dim S \cdot |E(\Gamma)|} \text{hom}(\Gamma, \Omega(S, K)).$$

Here $\Omega(S, K)$ is a reflexive graph with vertex set (S), where

$$K \leq \Lambda^2 S$$

and

$$s \sim t \iff s \wedge t \in K.$$

Thus, on graphical groups, quadratic presentational observables are exactly right homomorphism counts toward alternating-orthogonality targets. This viewpoint gives:

- a canonical semantic normal form for quadratic observables on graphical groups;
- a complexity dichotomy for evaluating a fixed observable;
- a right-profile completeness theorem;

- and an exact arity lower bound using Wilson's examples. The final theorem says that there exist nonisomorphic groups in $\mathcal{N}_{2,p}$ that cannot be distinguished by any coefficient-free observable in fewer than

$$\log_p |G| - 2$$

variables. The bound is exact. This result shows that arity is a real observational resource. It is not enough to choose more equations or longer equations in too few variables.

2 The variety N2p

Let (p) be an odd prime. Let $\mathcal{N}_{2,p}$ denote the variety of groups of nilpotency class at most 2 and exponent (p) . For $G \in \mathcal{N}_{2,p}$,

$$[x, y] \in Z(G),$$

$$[x^a, y^b] = [x, y]^{ab},$$

and every element has order dividing (p) . Let F_k be the free group on generators

$$x_1, \dots, x_k.$$

Let

$$F_{k,2,p}$$

be the free object in $\mathcal{N}_{2,p}$ on (k) generators. Equivalently,

$$F_{k,2,p} F_k / \langle F_k^{(3)}, x^p \ (x \in F_k) \rangle,$$

where $F_k^{(3)}$ is the third term of the lower central series. Every element of $F_{k,2,p}$ has a unique normal form

$$x_1^{a_1} \cdots x_k^{a_k} \prod_{1 \leq i < j \leq k} [x_i, x_j]^{B_{ij}},$$

where

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

Thus, as a set and as an $\mathbb{F}_p$ -vector space,

$$F_{k,2,p} \cong \mathbb{F}_p^k \oplus \Lambda^2 \mathbb{F}_p^k.$$

The first summand records the image in the abelianization. The second records the commutator coordinates.

3 Quadratic normal forms for words

Let $w \in F_k$. Its image in $F_{k,2,p}$ has a unique coordinate pair

$$(a(w), B(w)) \in \mathbb{F}_p^k \oplus \Lambda^2 \mathbb{F}_p^k.$$

This pair is the quadratic normal form of (w) in $\mathcal{N}_{2,p}$. Now let

$$\beta : V \times V \rightarrow W$$

be alternating bilinear over $\mathbb{F}_p$, and define

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

with multiplication

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

Then

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

Theorem 3.1 (Quadratic normal form). *For every word $w \in F_k$, there are unique*

$$a(w) \in \mathbb{F}_p^k, \quad B(w) \in \Lambda^2 \mathbb{F}_p^k$$

such that, for every alternating map $\beta : V \times V \rightarrow W$ and every

$$g_i = (v_i, z_i) \in G_\beta,$$

one has

$$w(g_1, \dots, g_k) \left(\sum_i a_i(w)v_i, \sum_i a_i(w)z_i + \sum_{i < j} B_{ij}(w)\beta(v_i, v_j) \right).$$

Moreover, $(a(w))$ and $(B(w))$ are computable in time linear in the length of (w) .

Proof. The word (w) maps to a unique element of the free class-two exponent- (p) group $F_{k,2,p}$, and therefore has a unique normal form

$$(a(w), B(w)).$$

Evaluation in G_β is the unique homomorphism from $F_{k,2,p}$ sending x_i to g_i . The image of the abelian component gives the term

$$\sum_i a_i(w)v_i$$

in (V) , and

$$\sum_i a_i(w)z_i$$

in (W) . The commutator component contributes

$$\sum_{i < j} B_{ij}(w) \beta(v_i, v_j).$$

The computational statement follows by scanning the word and updating the pair $((a, B))$. $\square$
Thus every word equation in $\mathcal{N}_{2,p}$ is linear-quadratic. $\square$

4 Quadratic presentations

A quadratic presentation over $\mathbb{F}_p$ is a quadruple

$$\mathcal{P} = (X, R, a, b),$$

where (X) and (R) are finite-dimensional $\mathbb{F}_p$ -vector spaces and

$$a : R \rightarrow X, \quad b : R \rightarrow \Lambda^2 X$$

are linear maps. The space (X) is the variable space. The space (R) is the relation space. The map (a) records the linear exponent-sum part of the relations, while (b) records the alternating commutator part. Let

$$\beta : V \times V \rightarrow W$$

be alternating. An assignment of the variables of $\mathcal{P}$ in G_β consists of two linear maps

$$f : X \rightarrow V, \quad g : R \rightarrow W.$$

The assignment satisfies $\mathcal{P}$ if

$$f \circ a = 0$$

and

$$g \circ a + \beta \circ \Lambda^2 f \circ b = 0.$$

Let

$$\text{Sol}_{\mathcal{P}}(\beta)$$

be the set of satisfying assignments.

Proposition 4.1 (Equivalence with word systems). *Every finite system of word equations in $\mathcal{N}_{2,p}$ defines a quadratic presentation. Conversely, every quadratic presentation is realized by a finite system of word equations in $\mathcal{N}_{2,p}$.*

Proof. Given a word equation $w = 1$, Theorem 3.1 gives a pair

$$(a(w), B(w)).$$

A finite system of equations gives a finite list of such pairs, hence a relation space (R) together with maps

$$a : R \rightarrow X, \quad b : R \rightarrow \Lambda^2 X.$$

Conversely, if $a \in X$ and $B \in \Lambda^2 X$, then, after choosing a basis of (X) , the word

$$x_1^{a_1} \cdots x_k^{a_k} \prod_{i < j} [x_i, x_j]^{B_{ij}}$$

has normal form $((a, B))$. Applying this to a basis of (R) realizes the presentation. $\square$

$\square$

5 The counting formula

Let

$$\mathcal{P} = (X, R, a, b)$$

be a quadratic presentation and let

$$\beta : V \times V \rightarrow W$$

be alternating. For

$$f : X \rightarrow V,$$

define the quadratic obstruction

$$Q_f = \beta \circ \Lambda^2 f \circ b \in \text{Hom}(R, W).$$

Let

$$a^* : \text{Hom}(X, W) \rightarrow \text{Hom}(R, W)$$

be the map

$$g \mapsto g \circ a.$$

Theorem 5.1 (Counting formula). *Let*

$$d = \dim W.$$

Then

$$|\text{Sol}_{\mathcal{P}}(\beta)| p^{d(\dim X - \text{rank } a)} |\{f : X \rightarrow V : f \circ a = 0, Q_f \in \text{im } a^*\}|.$$

Proof. Fix $f : X \rightarrow V$. The noncentral equation is

$$f \circ a = 0.$$

Assume this holds. The central assignments $g : X \rightarrow W$ must satisfy

$$g \circ a = -Q_f.$$

This linear equation is solvable if and only if

$$Q_f \in \text{im } a^*.$$

When it is solvable, its solution set is a coset of

$$\ker a^*.$$

Since

$$\dim \ker a^* d(\dim X - \text{rank } a),$$

the number of possible (g) is

$$p^{d(\dim X - \text{rank } a)}.$$

Summing over all admissible (f) proves the formula. $\square$ Thus every solution count is a linear factor multiplied by the number of assignments for which a quadratic obstruction vanishes in a quotient.

$\square$

6 Graphical (p)-groups

Let

$$\Gamma = (U, E)$$

be a finite simple graph. Fix an arbitrary orientation of (E). Define

$$V_\Gamma = \mathbb{F}_p^U, \quad W_\Gamma = \mathbb{F}_p^E.$$

For $x, y \in V_\Gamma$, define

$$\beta_\Gamma(x, y)_e x_u y_v - x_v y_u$$

if the oriented edge (e) is $u \rightarrow v$. Let

$$G_\Gamma = G_{\beta_\Gamma}.$$

Changing the orientation of an edge changes the sign of the corresponding basis vector of W_Γ , so the isomorphism type of G_Γ does not depend on the orientation. This is the standard graphical class-two exponent-(p) construction, equivalent to the Baer–Lovasz–Tutte graph-to-group construction. We use the following known fact.

Theorem 6.1 (Faithfulness of the graphical construction). *For finite simple graphs Γ, Γ' ,*

$$\Gamma \cong \Gamma' \iff G_\Gamma \cong G_{\Gamma'}.$$

This is a theorem of He and Qiao for the Baer–Lovasz–Tutte construction.

7 From quadratic presentations to alternating targets

Let

$$\mathcal{P} = (X, R, a, b)$$

be a quadratic presentation. An assignment of the noncentral parts of the variables in G_Γ is a linear map

$$f : X \rightarrow V_\Gamma.$$

For each vertex $u \in U$, define

$$s_u = \text{ev}_u \circ f \in X^*.$$

The equation

$$f \circ a = 0$$

is equivalent to

$$s_u \circ a = 0$$

for every (u) . Therefore the allowed spins lie in

$$S_{\mathcal{P}} = \ker(a : X \rightarrow R^*).$$

The commutator part defines an alternating map

$$\tilde{q}_{\mathcal{P}} : \Lambda^2 S_{\mathcal{P}} \rightarrow R^*$$

by

$$\tilde{q}_{\mathcal{P}}(s, t)(r)(s \wedge t)(b(r)).$$

Let

$$q_{\mathcal{P}} : \Lambda^2 S_{\mathcal{P}} \rightarrow Y_{\mathcal{P}}$$

be the map induced by $\tilde{q}_{\mathcal{P}}$. Define

$$K_{\mathcal{P}} = \ker q_{\mathcal{P}} \leq \Lambda^2 S_{\mathcal{P}}.$$

Now define a reflexive graph

$$\Omega(S_{\mathcal{P}}, K_{\mathcal{P}})$$

with vertex set $S_{\mathcal{P}}$ and adjacency

$$s \sim t \iff s \wedge t \in K_{\mathcal{P}}.$$

Since $s \wedge s = 0$, every vertex has a loop.

8 Protocol-to-target transfer

Theorem 8.1 (Transfer theorem). *For every finite graph Γ ,*

$$|\text{Sol } \mathcal{P}(G\Gamma)| p^{\dim S_{\mathcal{P}} \cdot |E(\Gamma)|} \text{hom}(\Gamma, \Omega(S_{\mathcal{P}}, K_{\mathcal{P}})).$$

Proof. A noncentral assignment

$$f : X \rightarrow V_{\Gamma}$$

is the same as a spin assignment

$$u \mapsto s_u \in X^*$$

for every vertex $u \in U$. The linear relations are equivalent to

$$s_u \in S_{\mathcal{P}}$$

for all (u). Now fix an oriented edge

$$e = u \rightarrow v.$$

The central components of the variables along (e) form an element

$$z_e \in X^*.$$

The central relations along (e) have the form

$$a^*(z_e) + \tilde{q}_{\mathcal{P}}(s_u, s_v) = 0.$$

This equation is solvable precisely when

$$\tilde{q}_{\mathcal{P}}(s_u, s_v) \in \text{im } a^*,$$

equivalently when

$$q_{\mathcal{P}}(s_u, s_v) = 0,$$

equivalently when

$$s_u \wedge s_v \in K_{\mathcal{P}}.$$

Thus the spin assignment is valid exactly when it is a graph homomorphism

$$\Gamma \rightarrow \Omega(S_{\mathcal{P}}, K_{\mathcal{P}}).$$

If the edge equation is solvable, the number of possible z_e is

$$|\ker a^*| = p^{\dim S_{\mathcal{P}}}.$$

The choices for different edges are independent. Hence every graph homomorphism contributes

$$p^{\dim S_{\mathcal{P}} \cdot |E(\Gamma)|}$$

central lifts. This proves the formula. $\square$ Thus, on graphical (p)-groups, every quadratic observable is a right homomorphism count toward a finite alternating-orthogonality target. $\square$

9 Realization of all alternating-orthogonality targets

Let (S) be a finite-dimensional $\mathbb{F}_p$ -vector space and let

$$K \leq \Lambda^2 S.$$

Define

$$\Omega(S, K)$$

as before:

$$V(\Omega(S, K)) = S,$$

$$s \sim t \iff s \wedge t \in K.$$

Proposition 9.1 (Realization). *For every pair $((S, K))$, there exists a quadratic presentation $\mathcal{P}$ such that*

$$(S_{\mathcal{P}}, K_{\mathcal{P}}) \cong (S, K).$$

Proof. Take

$$X = S^*.$$

Then

$$X^* \cong S.$$

Take no linear relations, so $a = 0$ and

$$S_{\mathcal{P}} = X^* \cong S.$$

Let

$$Y = \Lambda^2 S / K$$

and let

$$q : \Lambda^2 S \rightarrow Y$$

be the quotient map. Choose a basis of (Y) , and represent the coordinate functionals of (q) as elements of

$$(\Lambda^2 S)^* \cong \Lambda^2 X.$$

These elements define the commutator part (b). Then the induced kernel is exactly (K) . $\square$ Therefore the graphical semantics of QPC is precisely the family

$$\mathcal{O}_p \Omega(S, K) : S \text{ finite-dimensional over } \mathbb{F}_p, K \leq \Lambda^2 S.$$

$\square$

10 The contraction-kernel core

The target $\Omega(S, K)$ may contain many twin vertices. Its semantic content as a graph homomorphism target is captured by a weighted twin-free core. For $s \in S$, define

$$K_s = t \in S : s \wedge t \in K.$$

This is precisely the neighborhood of (s) in $\Omega(S, K)$. Define an equivalence relation on (S) by

$$s \equiv_K s' \iff K_s = K_{s'}.$$

Let

$$\mathcal{K}(S, K) = \{K_s : s \in S\}.$$

For $L \in \mathcal{K}(S, K)$, define its multiplicity

$$\mu(L) = |s \in S : K_s = L|.$$

We define a weighted reflexive graph

$$\text{Core}(S, K)$$

as follows:

- the vertex set is $\mathcal{K}(S, K)$;
- the vertex weight of L is $\mu(L)$;
- vertices (L) and (M) are adjacent if, for some equivalently every $s, t \in S$ with $K_s = L$ and $K_t = M$, one has

$$s \wedge t \in K.$$

Lemma 10.1 (Well-defined adjacency). *The adjacency relation on $\text{Core}(S, K)$ is well-defined.*

Proof. Suppose

$$K_s = K_{s'}$$

and

$$K_t = K_{t'}.$$

Then

$$s \wedge t \in K \iff t \in K_s \iff t \in K_{s'} \iff s' \wedge t \in K.$$

Similarly,

$$s' \wedge t \in K \iff s' \in K_t \iff s' \in K_{t'} \iff s' \wedge t' \in K.$$

Thus adjacency depends only on the two kernel classes. $\square$

$\square$

Proposition 10.2 (Weighted-core identity). *For every finite graph Γ ,*

$$\text{hom}(\Gamma, \Omega(S, K)) = \sum_{\phi: \Gamma \rightarrow \text{Core}(S, K)} \prod_{u \in V(\Gamma)} \mu(\phi(u)).$$

Proof. Every homomorphism

$$\psi : \Gamma \rightarrow \Omega(S, K)$$

induces a homomorphism

$$\phi : \Gamma \rightarrow \text{Core}(S, K)$$

by sending

$$u \mapsto K_{\psi(u)}.$$

Conversely, if

$$\phi : \Gamma \rightarrow \text{Core}(S, K)$$

is a homomorphism, then it lifts to $\Omega(S, K)$ by choosing, independently for each vertex (u), one of the

$$\mu(\phi(u))$$

spins in the corresponding kernel class. Multiplying over all vertices and summing over ϕ gives the formula. $\square$

$\square$

11 Semantic equivalence of quadratic presentations

Two quadratic presentations may have different variable and relation spaces but produce identical observables on all graphical groups. The weighted core gives the exact criterion.

Theorem 11.1 (Semantic equivalence theorem). *Let $\mathcal{P}$ and $\mathcal{P}'$ be quadratic presentations with associated pairs*

$$(S, K), \quad (S', K').$$

The following are equivalent:

- for every finite graph Γ ,

$$|\text{Sol } \mathcal{P}(G_\Gamma)| = |\text{Sol } \mathcal{P}'(G_\Gamma)|;$$

-

$$\dim S = \dim S'$$

and the weighted reflexive graphs

$$\text{Core}(S, K) \quad \text{and} \quad \text{Core}(S', K')$$

are isomorphic.

Proof. By Theorem 8.1 and Proposition 10.2,

$$|\text{Sol } \mathcal{P}(G\Gamma)| p^{\dim S \cdot |E(\Gamma)|} \text{hom}_\mu(\Gamma, \text{Core}(S, K)),$$

where

$$\text{hom}_\mu(\Gamma, \text{Core}(S, K)) = \sum_{\phi: \Gamma \rightarrow \text{Core}(S, K)} \prod_{u \in V(\Gamma)} \mu(\phi(u)).$$

Evaluating on edgeless graphs forces

$$|S| = |S'|,$$

hence

$$\dim S = \dim S'.$$

After this, the edge factor

$$p^{\dim S \cdot |E(\Gamma)|}$$

is the same for both presentations. Thus equality of solution counts for all Γ is equivalent to equality of all weighted homomorphism functions of the two weighted cores. The cores are twin-free by construction. By the weighted form of Lovasz's theorem for graph homomorphism functions, twin-free finite weighted graphs with the same homomorphism function from all finite graphs are isomorphic as weighted graphs. The converse follows immediately from the same formula. $\square$ This gives a canonical semantic representation of a quadratic observable on graphical (p)-groups. $\square$

12 Quadratic right-profile completeness

Let

$$\mathcal{O}_p = \Omega(S, K) : S \text{ finite-dimensional over } \mathbb{F}_p, \ K \leq \Lambda^2 S.$$

For a graph Γ , define its quadratic right profile by

$$\text{QRProf}_p(\Gamma) (\text{hom}(\Gamma, \Omega))_{\Omega \in \mathcal{O}_p}.$$

Theorem 12.1 (Quadratic right-profile completeness). *For finite graphs Γ, Γ' , the following are equivalent:*

- $\Gamma \cong \Gamma'$;
- $G_\Gamma \cong G_{\Gamma'}$;
- all coefficient-free quadratic presentation counts agree on G_Γ and $G_{\Gamma'}$;
- Γ and Γ' have the same number of edges and

$$\text{QRProf}_p(\Gamma) = \text{QRProf}_p(\Gamma').$$

Proof. The equivalence of 1 and 2 is Theorem 6.1. The implication $2 \Rightarrow 3$ is immediate because solution counts of coefficient-free systems are group isomorphism invariants. The implication $3 \Rightarrow 4$ follows from Theorem 8.1 and Proposition 9.1. The implication $4 \Rightarrow 3$ also follows from Theorem 8.1: every quadratic presentation has an associated target $\Omega(S, K)$, and the only additional factor is

$$p^{\dim S \cdot |E(\Gamma)|},$$

which agrees because the two graphs have the same number of edges. It remains to show that 3 implies 2. Let $L \in \mathcal{N}_{2,p}$ be finite. Choose a finite presentation of (L) inside the variety $\mathcal{N}_{2,p}$. By the quadratic normal form theorem, this is a quadratic presentation $\mathcal{P}_L$. For every $X \in \mathcal{N}_{2,p}$,

$$|\text{Sol}_{\mathcal{P}_L}(X)| |\text{Hom}(L, X)|.$$

Thus 3 implies

$$|\text{Hom}(L, G_\Gamma)| |\text{Hom}(L, G_{\Gamma'})|$$

for every finite $L \in \mathcal{N}_{2,p}$. We now use Hom/Inj inversion inside the finite class $\mathcal{N}_{2,p}$. If G_Γ and $G_{\Gamma'}$ have different orders, then they are already distinguished by homomorphism counts from elementary abelian groups. Thus assume they have the same order. Taking (L) to range over all quotients of G_Γ , we have

$$|\text{Hom}(G_\Gamma/N, G_\Gamma)| |\text{Hom}(G_\Gamma/N, G_{\Gamma'})|$$

for every normal subgroup $N \trianglelefteq G_\Gamma$. For $X \in \mathcal{N}_{2,p}$,

$$|\text{Hom}(G_\Gamma/N, X)| = \sum_{\substack{M \trianglelefteq G_\Gamma \\ N \leq M}} |\text{Inj}(G_\Gamma/M, X)|.$$

Mobius inversion on the finite lattice of normal subgroups of G_Γ gives

$$|\text{Inj}(G_\Gamma, G_\Gamma)| |\text{Inj}(G_\Gamma, G_{\Gamma'})|.$$

The left side is

$$|\text{Aut}(G_\Gamma)| > 0.$$

The right side is zero unless

$$G_\Gamma \cong G_{\Gamma'},$$

because the groups have the same order. Therefore

$$G_\Gamma \cong G_{\Gamma'}.$$

This proves 2, and hence all conditions are equivalent. $\square$

$\square$

13 Complexity dichotomy

For a fixed graph (H) , the problem

$$\Gamma \mapsto \text{hom}(\Gamma, H)$$

is the $\#H$ -Coloring problem. Dyer and Greenhill proved a dichotomy for this problem. In the case where H is connected and reflexive, the problem is polynomial-time computable precisely when H is a complete reflexive graph; otherwise it is $\#P$ -complete. Every target

$$\Omega(S, K)$$

is reflexive. It is also connected, because $0 \in S$ is adjacent to every vertex.

Theorem 13.1 (QPC dichotomy on graphical groups). *Let $\mathcal{P}$ be a fixed quadratic presentation with associated pair*

$$(S, K).$$

The problem

$$\Gamma \mapsto |\text{Sol}_{\mathcal{P}}(G_{\Gamma})|$$

is polynomial-time computable if

$$K = \Lambda^2 S,$$

and is $(\#P)$ -complete otherwise.

Proof. By Theorem 8.1,

$$|\text{Sol } \mathcal{P}(G_{\Gamma})| p^{\dim S \cdot |E(\Gamma)|} \text{hom}(\Gamma, \Omega(S, K)).$$

The prefactor is computable in polynomial time. The target $\Omega(S, K)$ is complete reflexive if and only if

$$s \wedge t \in K \quad \forall s, t \in S,$$

which is equivalent to

$$K = \Lambda^2 S.$$

If $K = \Lambda^2 S$, every map

$$V(\Gamma) \rightarrow S$$

is a homomorphism, so the count is

$$p^{\dim S \cdot |E(\Gamma)|} |S|^{|V(\Gamma)|},$$

which is polynomial-time computable. If $K \neq \Lambda^2 S$, then $\Omega(S, K)$ is connected, reflexive, and not complete. By the Dyer–Greenhill dichotomy, computing

$$\text{hom}(\Gamma, \Omega(S, K))$$

is $(\#P)$ -complete. Hence the QPC count is $(\#P)$ -complete as well. $\square$

$\square$

Example 13.2 (Commuting pairs). *The observable*

$$[x_1, x_2] = 1$$

has

$$S = \mathbb{F}_p^2$$

and

$$K = 0 \leq \Lambda^2 S.$$

Thus

$$s \sim t \iff s \wedge t = 0,$$

i.e. (s, t) are linearly dependent. The target is not complete. Therefore exact counting of commuting pairs in G_Γ , with Γ as input, is $(\#P)$ -complete.

14 Relation to left and right homomorphism profiles

The theory above is a right-profile theory. Lovasz’s classical theorem says that the full left profile

$$F \mapsto \text{hom}(F, \Gamma)$$

determines Γ . Restrictions of left profiles, for example to bounded-treewidth sources, are closely related to Weisfeiler–Leman equivalence and counting logics. By contrast, QPC on graphical groups produces restricted right profiles:

$$\Omega \mapsto \text{hom}(\Gamma, \Omega), \quad \Omega \in \mathcal{O}_p.$$

The expressive behavior of restricted right profiles is different from that of restricted left profiles. In particular, known results of Atserias–Kolaitis–Wu show that several equivalences captured by restrictions of left profiles, including fixed-variable counting logic equivalence, cannot in general be captured by restricting the right profile to a fixed class of targets. Accordingly, we do not interpret QPC as another form of Weisfeiler–Leman refinement. It is a different observational hierarchy, based on finite alternating-orthogonality targets.

15 Coefficient-free observables and arity

We now turn from graphical groups to arbitrary finite groups in $\mathcal{N}_{2,p}$. A coefficient-free observable in (k) variables is a Boolean combination of word equations and disequations in variables

$$x_1, \dots, x_k$$

with no named constants from the ambient group. For such an observable Φ , write

$$Z_\Phi(G)$$

for the number of satisfying (k) -tuples in (G) . For finite groups (G, H) , define

$$\text{qvar}(G, H)$$

to be the least (k) such that there exists a coefficient-free observable Φ in (k) variables with

$$Z_\Phi(G) \neq Z_\Phi(H).$$

If no such (k) exists, set

$$\text{qvar}(G, H) = \infty.$$

For finite groups, $\text{qvar}(G, H)$ is finite whenever $G \not\cong H$.

16 Locality through generated subgroups

Lemma 16.1 (Generated-subgroup decomposition). *Let Φ be a coefficient-free observable in (k) variables. For every finite group (G) ,*

$$Z_\Phi(G) = \sum_{L \leq G} \tau_\Phi(L),$$

where

$$\tau_\Phi(L) = \# \{ (l_1, \dots, l_k) \in L^k : \langle l_1, \dots, l_k \rangle = L, L \models \Phi(l_1, \dots, l_k) \}.$$

Moreover, $\tau_\Phi(L)$ depends only on the isomorphism type of (L) .

Proof. Every tuple

$$\mathbf{g} = (g_1, \dots, g_k) \in G^k$$

generates a unique subgroup

$$L = \langle g_1, \dots, g_k \rangle.$$

Since Φ has no coefficients from (G) , whether $\mathbf{g}$ satisfies Φ depends only on the marked subgroup generated by the tuple. Partitioning tuples according to their generated subgroup gives the formula.

□

□

Corollary 16.2. *Suppose (G) and (H) have the same multiset of isomorphism types of proper subgroups, counted with multiplicity. If*

$$k < \min d(G), d(H),$$

then every coefficient-free observable in (k) variables has the same number of solutions in (G) and (H) .

Proof. If

$$k < d(G),$$

then no (k) -tuple generates (G) . Hence every (k) -tuple generates a proper subgroup. The same holds for (H) . The result follows from Lemma 16.1 and the equality of proper subgroup profiles. □

□

17 A general arity upper bound

We now prove a complementary upper bound using Hom/Inj inversion.

Lemma 17.1 (Hom-count separation by a quotient). *Let (G, H) be finite groups of the same order with*

$$G \not\cong H.$$

Then there exists a normal subgroup

$$N \trianglelefteq G$$

such that

$$|\operatorname{Hom}(G/N, G)| \neq |\operatorname{Hom}(G/N, H)|.$$

Proof. Assume the contrary. For $N \trianglelefteq G$, put

$$h_N(X) = |\operatorname{Hom}(G/N, X)|$$

and

$$i_N(X) = |\operatorname{Inj}(G/N, X)|.$$

Every homomorphism

$$G/N \rightarrow X$$

has kernel

$$M/N$$

for some normal subgroup $M \trianglelefteq G$ with $N \leq M$. Hence

$$h_N(X) = \sum_{\substack{M \trianglelefteq G \\ N \leq M}} i_M(X).$$

If

$$h_N(G) = h_N(H)$$

for every (N) , then Mobius inversion on the lattice of normal subgroups of (G) gives

$$i_N(G) = i_N(H)$$

for every (N) . In particular,

$$|\operatorname{Inj}(G, G)| |\operatorname{Inj}(G, H)|.$$

The left side is

$$|\operatorname{Aut}(G)| > 0.$$

The right side is zero, since an injection $G \hookrightarrow H$ between groups of the same order would be an isomorphism. This contradicts $G \not\cong H$. $\square$

$\square$

Corollary 17.2 (General arity upper bound). *If $G, H \in \mathcal{N}_{2,p}$ are finite, nonisomorphic, and have the same order, then*

$$\text{qvar}(G, H) \leq \min d(G), d(H).$$

Proof. By Lemma 17.1, some quotient (G/N) has different homomorphism counts into (G) and (H) . The group (G/N) can be presented using at most $(d(G))$ generators. The number of homomorphisms from (G/N) into an ambient group (X) is the number of solutions in (X) of the relators of such a presentation. Since $G/N \in \mathcal{N}_{2,p}$, these relators are equivalent to a quadratic presentation. Thus (G) and (H) are distinguished by a coefficient-free observable in at most $(d(G))$ variables. Applying the same argument with (H) gives the stated bound. $\square$

$\square$

18 Wilson groups and the exact arity barrier

We use the following theorem of Wilson.

Theorem 18.1 (Wilson's subgroup-profile examples). *For primes*

$$p > 2$$

and integers

$$e > 3,$$

there exists a family $\mathcal{W}_{p,e}$ of at least

$$\frac{p^{e-3}}{e}$$

pairwise nonisomorphic (p) -groups such that every $G \in \mathcal{W}_{p,e}$ satisfies:

- $|G| = p^{2e+2}$;
- $(d(G)=2e)$;
- all groups in $\mathcal{W}_{p,e}$ have the same multiset of isomorphism types of proper subgroups;
- all groups in $\mathcal{W}_{p,e}$ have the same multiset of isomorphism types of proper quotients. These groups lie in the class of (p) -groups considered by Wilson's logarithmic subgroup-profile construction. We now obtain the exact arity barrier.

Theorem 18.2 (Exact observable arity barrier). *Let (G, H) be two nonisomorphic groups in $\mathcal{W}_{p,e}$. Then*

$$\text{qvar}(G, H) = 2e.$$

Equivalently,

$$\text{qvar}(G, H) = \log_p |G| - 2.$$

Moreover, for every

$$k < 2e,$$

all groups in $\mathcal{W}_{p,e}$ have identical values for every coefficient-free observable in (k) variables.

Proof. First, let $k < 2e$. Since

$$d(G) = 2e$$

for every $G \in \mathcal{W}_{p,e}$, no (k) -tuple generates (G) . Hence every (k) -tuple generates a proper subgroup. All groups in $\mathcal{W}_{p,e}$ have the same multiset of isomorphism types of proper subgroups. By Corollary 16.2, every coefficient-free observable in (k) variables has the same number of solutions in all groups in the family. Thus

$$\text{qvar}(G, H) \geq 2e.$$

For the upper bound, Corollary 17.2 gives

$$\text{qvar}(G, H) \leq \min d(G), d(H)2e.$$

Therefore

$$\text{qvar}(G, H) = 2e.$$

Since

$$|G| = p^{2e+2},$$

we have

$$2e = \log_p |G| - 2.$$

The final statement follows from the same lower-bound argument. $\square$ This proves that the logarithmic arity bound is both necessary and sufficient in the worst case.

$\square$

19 Interpretation of the arity barrier

Theorem 18.2 shows that arity is a genuine resource for coefficient-free observables. It is not enough to use:

- more relators;
- longer relators;
- more complicated Boolean combinations; if the number of variables is below the generator rank. For the Wilson families, every such observable is trapped inside proper subgroups, and the proper subgroup profiles are identical. Thus the subgroup-profile obstruction is not merely an obstruction to a particular algorithm or heuristic. It obstructs the entire coefficient-free observable hierarchy below the generator rank.

20 Main conclusions

The paper establishes the following principles.

20.1 Quadratic collapse

In $\mathcal{N}_{2,p}$, every word observable is quadratic.

20.2 Right-profile semantics

On graphical (p)-groups, every quadratic observable is exactly a right homomorphism count toward an alternating-orthogonality target.

20.3 Canonical semantic core

Every such target has a weighted twin-free core determined by the contraction kernels

$$K_s = t : s \wedge t \in K.$$

Two observables have the same values on all graphical groups if and only if their weighted cores agree.

20.4 Complexity dichotomy

Every fixed nondegenerate observable gives a $(\#P)$ -complete counting problem on input graphs.

20.5 Exact arity barrier

There exist nonisomorphic groups in $\mathcal{N}_{2,p}$ requiring exactly

$$\log_p |G| - 2$$

variables to distinguish by any coefficient-free observable.

21 Further directions

21.1 Budget beyond arity

Theorem 18.2 measures variables. It does not measure:

- number of relators;
- sparsity;
- circuit size;
- observable width. A refined theory should study trade-offs between these resources.

21.2 Restricted target families

The full family

$$\mathcal{O}_p$$

is complete for graphical groups. It remains to understand which subfamilies retain significant distinguishing power. Natural candidates include:

- symplectic targets;
- low-codimension kernels (K);
- targets of bounded contraction-kernel diversity;
- targets arising from small-rank commutator systems.

21.3 Canonization

This paper studies counting observables, not canonical forms. A natural next goal is to turn right-profile or quadratic-presentational data into canonical decompositions for alternating maps

$$\beta : V \times V \rightarrow W.$$

21.4 Relation to proof complexity

Reducing QPC counts modulo (p) gives polynomial functions in the structure constants of the alternating map. This suggests a connection with low-degree invariant theory and proof complexity for tensor isomorphism.

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

During the preparation of this work, ChatGPT, by OpenAI, was used to assist with mathematical drafting, formalization, review, and editing. This work is shared as a preliminary AI-assisted mathematical note. The mathematical content may have been only partially reviewed and may contain errors; it should not be treated as peer-reviewed or as a fully verified manuscript.

References

- [1] Albert Atserias, Phokion G. Kolaitis, and Wei-Lin Wu. On the Expressive Power of Homomorphism Counts. LICS 2021; arXiv:2101.12733.
- [2] Jin-Yi Cai and Artem Govorov. On a Theorem of Lovasz that $\text{hom}(\cdot, H)$ Determines the Isomorphism Type of (H). ITCS 2020; arXiv:1909.03693.
- [3] M. Dyer and C. Greenhill. The complexity of counting graph homomorphisms. Random Structures & Algorithms 17 2000, 260–289. See also the corrigendum in Random Structures & Algorithms 25 2004, 346–352.

- [4] Xiaoyu He and Youming Qiao. On the Baer–Lovasz–Tutte construction of groups from graphs: isomorphism types and homomorphism notions. arXiv:2003.07200.
- [5] László Lovasz. Operations with structures. *Acta Mathematica Academiae Scientiarum Hungaricae* 18 1967, 321–328.
- [6] László Lovasz. The rank of connection matrices and the dimension of graph algebras. *European Journal of Combinatorics* 27 2006, 962–970.
- [7] James B. Wilson. The Threshold for Subgroup Profiles to Agree is Logarithmic. *Theory of Computing* 15 2019, Article 19, 1–25.
- [8] Harald Dell, Martin Grohe, and Gaurav Rattan. Lovasz Meets Weisfeiler and Leman. *ICALP* 2018; arXiv:1802.08876.
- [9] James A. Grochow and Youming Qiao. On the complexity of isomorphism problems for tensors, groups, and polynomials. *SIAM Journal on Computing* 52 2023, 568–617.
- [10] Xiaorui Sun. Faster Isomorphism for (p) -Groups of Class 2 and Exponent (p) . arXiv:2303.15412.