AIMS Mathematics, 11(6): 15561–15580.
DOI: 10.3934/math.2026640
Received: 20 February 2026
Revised: 02 May 2026
Accepted: 14 May 2026
Published: 03 June 2026

https://www.aimspress.com/journal/Math

Research article

Commutator-constrained factorizations in class-two exponent-p-groups

Ghaliah Alhamzi[1], **Mdi Begum Jeelani**[1,*], **Wael Mahmoud Mohammad Salameh**[2] **and Prakash Jadhav**[3]

[1] Department of Mathematics and Statistics, College of Science, Imam Mohammad Ibn Saud Islamic University (IMSIU), Riyadh, Saudi Arabia

[2] Faculty of Information Technology, Abu Dhabi University, Abu Dhabi, United Arab Emirates

[3] Department of Mechanical Engineering, SRM University AP, Andhra Pradesh, India

* **Correspondence:** Email: mbshaikh@imamu.edu.sa.

Abstract: Groups of nilpotency class 2 and exponent p (with p odd) admit concrete coordinate models governed by alternating $\mathbb{F}_p$-bilinear commutator data, a viewpoint central in both the structure theory of p-groups and algorithmic approaches to isomorphism testing and related problems. Motivated by decomposition primitives in computational group theory and by rank-based filters used in modern isomorphism pipelines, we introduce the *commutator-constrained factorization problem*: given $g \in G$ and a target commutator value $h \in [G, G]$, count and construct pairs (x, y) with $xy = g$ and $[x, y] = h$. In an explicit bilinear-data input model, we show that the decision, counting, and search variants reduce to solvability of a single linear system $T_w(u) = h$ over $\mathbb{F}_p$, where T_w: $u \mapsto b(u, w)$ is the contraction map determined by the V-projection w of g. When solvable, the solution set $\mathcal{S}(g, h)$ is exhibited as an explicit torsor for $\ker(T_w)\times W$, yielding a closed counting formula and a certified witness construction by elementary linear algebra. We derive exact secondary laws: a complete description of the attainable commutator set $\mathcal{H}(g) = \mathrm{im}(T_w)$, an exact uniformity law over attainable values, and a factor-swap bijection relating $\mathcal{S}(g, h)$ to a shifted product constraint. Finally, we define rank-profile polynomials $P_G(t) = \sum_{w\in V} t^{\mathrm{rank}(T_w)}$, prove isomorphism invariance, and extract further invariants (radical size, extremal attainable-set size) directly from counting oracles. The odd-prime hypothesis is made explicit throughout: the centered coordinate law uses the scalar $1/2 \in \mathbb{F}_p$, whereas characteristic two requires a cocycle or quadratic-refinement formulation. We also record coordinate-invariance, conversion costs from power-commutator input, sparse implementation refinements, and limitations of the rank-profile invariant.

Keywords: computational group theory; nilpotent p-groups; class-two groups; Baer correspondence; commutator map; exact counting; linear algebra over finite fields; isomorphism invariants
Mathematics Subject Classification: 20D15, 20D45, 20F10, 68Q25

1. Introduction

Computational group theory develops algorithmic methods for finite groups represented by permutations, matrices, polycyclic data, or Cayley tables; standard references include [1, 2]. For finite p-groups, a large part of practical computation is driven by structural input that permits certified reductions to linear algebra, especially in low nilpotency class and bounded exponent settings [3–5]. This structural viewpoint has become increasingly important in the complexity-theoretic study of the group isomorphism problem: broad advances for many group orders [6] coexist with longstanding barrier cases. Among these barrier cases, Rosenbaum [7] broke the $n^{\log n}$ barrier for solvable-group isomorphism. Subsequently, Rosenbaum [8] gave improved generator-enumeration bounds for p-group isomorphism. More recently, Sun [9] obtained faster isomorphism algorithms specifically for p-groups of class two and exponent p. Related work in allied areas includes the study of Boas–Buck–Sheffer polynomials and quasi-monomiality by Wani and Nisar [10], and fractional calculus aspects of special polynomials by Khan and Wani [11]. Further contributions in allied directions include advances on q-Hermite–Appell polynomials by Zayed et al. [12], and degenerate bivariate Appell polynomials by Wani et al. [13].

A key reason for the prominence of this class is an explicit coordinatization in terms of alternating bilinear maps (often presented as alternating matrix spaces) that goes back to Baer and related work on central extensions [14, 15]. In modern algorithmic language, this correspondence links isomorphism testing for class-two exponent-p groups to isometry and pseudo-isometry problems for alternating matrix tuples [9, 16, 17], and it connects naturally to extension/cohomology strategies for group isomorphism [18]. Implementations and theory for specialized subclasses also emphasize bilinear-map structure, adjoint algebras, and tensor-product symmetries [19, 20]. Related algorithmic themes include efficient computations in nilpotent groups under compressed encodings [21] and equation-solving problems in nilpotent groups [22, 23]. The word factorization also appears in matrix-factorization approaches to network analysis, including constrained symmetric nonnegative matrix-factorization with deep autoencoders for community detection [24]; the present use is group-theoretic and concerns products inside a nilpotent group subject to a prescribed commutator constraint.

Remark 1.1. The contribution of the paper lies in isolating a small algebraic primitive whose output contains more than a solvability certificate. The bilinear commutator map is a standard object in the theory and algorithms of class-two exponent-p groups; here, it is used to derive, in one unified statement, the exact decision criterion, exact cardinality, full torsor parametrization, uniform distribution over attainable commutator values, and rank-profile data recoverable from counting access. These secondary laws are the main structural content of the formulation and make the primitive directly usable as a counting and sampling subroutine.

This paper isolates a concrete exact-counting primitive inside the class-two exponent-p regime that interacts cleanly with bilinear commutator structure. Given $g \in G$ and a desired commutator target $h \in [G, G]$, we study constrained factorizations $g = xy$ with $[x, y] = h$. The central observation is that, under bilinear-data coordinatization, the constraints collapse to a single linear equation over $\mathbb{F}_p$ involving a contraction map T_w derived from the V-projection of g. This yields closed formulas, explicit parametrizations of the full solution set, and certified constructions suitable for direct implementation.

Throughout, p denotes an odd prime and $\mathbb{F}_p$ denotes the field with p elements. We consider finite groups G satisfying:

- G is a p-group of nilpotency class 2;
- G has exponent p.

Let $W := [G, G]$ and let $V := G/[G, G]$. Lemma 2.1 gives $\mathbb{F}_p$-vector space structures on V and W. The commutator induces an alternating $\mathbb{F}_p$-bilinear map

$$b : V \times V \to W, \qquad b(\bar{x}, \bar{y}) = [x, y].$$

We adopt an explicit bilinear-data input model (Definition 2.4) that records structure constants for b relative to fixed bases, aligning with matrix-space viewpoints used in contemporary isomorphism algorithms [9, 16, 17] and with classical extension-theoretic perspectives [18, 25].

Remark 1.2. The fixed bases in this model are an input representation rather than an additional group-theoretic assumption. A change of ordered basis in V and W replaces the tensor of structure constants by the corresponding $\mathrm{GL}(V) \times \mathrm{GL}(W)$ transform, whereas statements involving $\mathrm{im}(T_w)$, $\ker(T_w)$, ranks, torsors, attainable sets, and the polynomial $P_G(t)$ remain intrinsic. Thus the coordinates serve the same role as matrices for a linear map: They enable computation, whereas the resulting assertions are basis independent.

Contributions. We introduce the commutator-constrained factorization problem and show that, in the bilinear-data model for class-two exponent-p groups, the decision, counting, and witness-construction tasks reduce to solvability of a single linear system $T_w(u) = h$ over $\mathbb{F}_p$, where T_w is the contraction map $u \mapsto b(u, w)$ determined by the V-projection w of the target product element g (Theorem 3.4). This reduction yields a closed exact counting formula and an explicit certified parametrization of the entire solution set as a torsor for $\ker(T_w) \times W$ (Theorem 3.9), making the computational core elementary linear algebra.

We then derive exact structural consequences for each fixed g: The attainable commutator set $\mathcal{H}(g)$ is exactly the image $\mathrm{im}(T_w)$, its size is $p^{\mathrm{rank}(T_w)}$, and the commutator distribution across all factorizations $xy = g$ is uniform on $\mathrm{im}(T_w)$ (Theorems 3.6 and 3.7). We also establish a factor-swap law that transports commutator-constrained factorizations of g to a shifted product constraint, with an explicit bijection (Theorem 3.11).

Finally, we define rank-profile polynomials

$$P_G(t) = \sum_{w \in V} t^{\mathrm{rank}(T_w)}$$

and prove that they are preserved under group isomorphism (Theorem 5.2); this yields a family of rank-distribution invariants directly aligned with bilinear-map isometry perspectives [9, 20]. We extract further invariant data from P_G, including the radical size and the extremal attainable-set size, and we provide certified complexity bounds for all required linear algebra in terms of $d = \dim V$ and $m = \dim W$ (Theorem 4.1).

Organization of the paper. Section 2 develops the bilinear-data model and the associated class-two exponent-p group law. Section 3 presents the commutator-constrained factorization problem, proves the linear reduction theorem, and derives attainable-set, uniformity, torsor, and swap laws. Section 4

records deterministic complexity bounds. Section 5 develops rank-profile invariants and oracle recovery. Section 6 gives a worked Heisenberg example and basic verification checks, and Section 7 outlines extensions motivated by current algorithmic and structural directions in the area.

2. Preliminaries

2.1. Vector space structure and bilinearity

Lemma 2.1. *Let G be a finite group of exponent p. Every abelian quotient of G is canonically an $\mathbb{F}_p$-vector space with addition induced by the group operation.*

Proof. Let A be an abelian quotient of G. Exponent p implies $a^p = e$ for all $a \in A$, hence A is an elementary abelian p-group. The map $\mathbb{F}_p \times A \to A$ given by $(k, a) \mapsto a^k$ defines scalar multiplication compatible with the abelian group law, and the axioms of an $\mathbb{F}_p$-vector space follow from the rules of exponents in an abelian group (see, e.g., [26, Ch. 2]). □

Lemma 2.2. *(Alternating bilinear commutator map) Let G have nilpotency class 2 and exponent p, and set $W = [G, G]$ and $V = G/W$. Define*

$$b : V \times V \to W, \qquad b(\bar{x}, \bar{y}) := [x, y].$$

Then b is well-defined, alternating, and $\mathbb{F}_p$-bilinear.

Proof. Well-definedness. Fix $\bar{x}, \bar{y} \in V$ and choose representatives $x, y \in G$. For any $w_1, w_2 \in W$, class 2 implies $W \subseteq Z(G)$, hence w_1, w_2 commute with all elements. Compute:

$$\begin{aligned}
[xw_1, yw_2] &= (xw_1)(yw_2)(xw_1)^{-1}(yw_2)^{-1} \\
&= xy\, w_1 w_2\, (w_1^{-1}x^{-1})(w_2^{-1}y^{-1}) \\
&= xy\, x^{-1}y^{-1} \\
&= [x, y].
\end{aligned}$$

Therefore, $b(\bar{x}, \bar{y})$ is independent of representatives.

Alternating property. For any $x \in G$,

$$[x, x] = xxx^{-1}x^{-1} = e,$$

hence $b(\bar{x}, \bar{x}) = 0$ in the $\mathbb{F}_p$-vector space W.

$\mathbb{F}_p$-bilinearity. Class 2 implies all commutators lie in $Z(G)$, and the standard identities

$$[x_1x_2, y] = [x_1, y]\,[x_2, y], \qquad [x, y_1y_2] = [x, y_1]\,[x, y_2]$$

hold exactly (see, e.g., [26, Ch. 5]). Passing to V yields additivity in each variable. Exponent p yields

$$\left[x^k, y\right] = [x, y]^k, \qquad \left[x, y^k\right] = [x, y]^k, \qquad (k \in \mathbb{F}_p),$$

matching $\mathbb{F}_p$-linearity under the vector space structure on W from (2.1). □

2.2. Bilinear-data coordinatization

Remark 2.3. Scope of the bilinear model and the odd-prime hypothesis: For a class-two exponent-p group with p odd, the passage from G to the pair (V, W, b) is the standard Baer/Lazard linearization in this range. Because $V = G/[G, G]$ and $W = [G, G]$ are elementary abelian, a choice of vector-space section s: $V \to G$ gives central coordinates, and the commutator is exactly the alternating bilinear map

$$b(u, v) = [s(u), s(v)].$$

After replacing the section by the centered one, the multiplication can be written in the form

$$(v, w)(v', w') = (v + v', w + w' + \tfrac{1}{2}b(v, v')),$$

which is the coordinate model used below. The scalar $1/2$ is therefore a structural convenience available in the odd characteristic. In characteristic two, the same commutator map is alternating with $b(v, v) = 0$, yet the centered multiplication above cannot be formed by dividing by 2. A characteristic-two version requires retaining a normalized 2-cocycle, and in exponent-4 variants one must also track a quadratic square map. The present paper works in the odd-prime regime where the commutator data alone determine the centered model and where the contraction equation $T_w(u) = h$ gives the stated exact formulas.

Equivalently, this bilinear-data model covers precisely the finite p-groups, for p odd, of nilpotency class at most 2 and exponent p: Such groups are classified, after choice of central coordinates, by their alternating commutator maps; see Jonah and Konvisser [14]. Thus Proposition 2.7 is used throughout as a coordinate realization of this full odd-prime class.

Definition 2.4. (Bilinear-data input model) Fix an odd prime p. A *bilinear-data instance* consists of:

- Integers $d, m \geq 0$;
- Vector spaces $V \cong \mathbb{F}_p^d$ and $W \cong \mathbb{F}_p^m$ with fixed ordered bases;
- An alternating bilinear map b: $V \times V \to W$ given by structure constants

$$b(e_i, e_j) = \sum_{k=1}^{m} c_{ij}^k f_k \quad (1 \leq i < j \leq d),$$

where (e_i) is the basis of V and (f_k) is the basis of W.

Remark 2.5. (Basis changes) Let $A \in \mathrm{GL}(V)$ and $C \in \mathrm{GL}(W)$ be changes of basis. The coordinate tensor b is replaced by $b'(u, v) = Cb(A^{-1}u, A^{-1}v)$. For $w' = Aw$, the corresponding contraction maps satisfy $T'_{w'} = C \circ T_w \circ A^{-1}$. Hence $\mathrm{rank}(T'_{w'}) = \mathrm{rank}(T_w)$ and $C(\mathrm{im}\, T_w) = \mathrm{im}\, T'_{w'}$. All formulas below are therefore intrinsic after translating coordinates by A and C.

Definition 2.6. (Radical and image of an alternating map) Given b: $V \times V \to W$ as alternating bilinear, define

$$\mathrm{rad}(b) := \{v \in V : \ b(v, u) = 0 \text{ for all } u \in V\}, \qquad \mathrm{im}(b) := \mathrm{span}\{b(u, v) : u, v \in V\} \subseteq W.$$

Proposition 2.7. *(Group law from bilinear-data, with explicit commutator structure) Let* (V, W, b) *be a bilinear-data instance with* p *odd. Define a binary operation on* $V \times W$ *by*

$$(v, w) \cdot (v', w') := \big(v + v',\ w + w' + \tfrac{1}{2}\, b(v, v')\big), \tag{2.1}$$

where $1/2 \in \mathbb{F}_p$ *is the inverse of* 2*. Then* $G := (V \times W, \cdot)$ *is a group of nilpotency class* 2 *and exponent* p*. Moreover:*

(1) The inverse is $(v, w)^{-1} = (-v, -w)$*.*
(2) The commutator satisfies

$$[(v, w), (v', w')] = (0,\ b(v, v')). \tag{2.2}$$

(3) The derived subgroup is $[G, G] = \{0\} \times \mathrm{im}(b)$*.*
(4) The center is $Z(G) = \mathrm{rad}(b) \times W$*.*

Proof. Associativity. Let $(v, w), (v', w'), (v'', w'') \in V \times W$. Compute using (2.1):

$$\begin{aligned}
\big((v, w) \cdot (v', w')\big) \cdot (v'', w'') &= \big(v + v',\ w + w' + \tfrac{1}{2} b(v, v')\big) \cdot (v'', w'') \\
&= \Big(v + v' + v'',\ w + w' + w'' + \tfrac{1}{2} b(v, v') + \tfrac{1}{2} b(v + v', v'')\Big) \\
&= \Big(v + v' + v'',\ w + w' + w'' + \tfrac{1}{2} b(v, v') + \tfrac{1}{2} b(v, v'') + \tfrac{1}{2} b(v', v'')\Big),
\end{aligned}$$

where the final step uses bilinearity of b. Similarly,

$$\begin{aligned}
(v, w) \cdot \big((v', w') \cdot (v'', w'')\big) &= (v, w) \cdot \big(v' + v'',\ w' + w'' + \tfrac{1}{2} b(v', v'')\big) \\
&= \Big(v + v' + v'',\ w + w' + w'' + \tfrac{1}{2} b(v', v'') + \tfrac{1}{2} b(v, v' + v'')\Big) \\
&= \Big(v + v' + v'',\ w + w' + w'' + \tfrac{1}{2} b(v', v'') + \tfrac{1}{2} b(v, v') + \tfrac{1}{2} b(v, v'')\Big),
\end{aligned}$$

which matches the previous expression. Hence, $\cdot$ is associative.

Identity. Let $e := (0, 0)$. Then,

$$(v, w) \cdot e = (v + 0,\ w + 0 + \tfrac{1}{2} b(v, 0)) = (v, w), \qquad e \cdot (v, w) = (0 + v,\ 0 + w + \tfrac{1}{2} b(0, v)) = (v, w),$$

as $b(v, 0) = b(0, v) = 0$ by bilinearity.

Inverse. Let $(v, w)^{-1} := (-v, -w)$. Then,

$$(v, w) \cdot (-v, -w) = (0,\ 0 + \tfrac{1}{2} b(v, -v)) = (0,\ -\tfrac{1}{2} b(v, v)) = (0, 0),$$

as alternation gives $b(v, v) = 0$. A symmetric computation yields $(-v, -w) \cdot (v, w) = (0, 0)$.

Exponent p*.* For $k \in \{1, \ldots, p\}$, prove by induction that

$$(v, w)^k = (kv, kw),$$

where (kv, kw) denotes scalar multiplication in the $\mathbb{F}_p$-vector spaces. The case $k = 1$ holds. Assume $(v, w)^k = (kv, kw)$. Then,

$$(v, w)^{k+1} = (v, w)^k \cdot (v, w) = (kv, kw) \cdot (v, w) = \big((k + 1)v, (k + 1)w + \tfrac{1}{2} b(kv, v)\big).$$

Bilinearity gives $b(kv, v) = k\, b(v, v) = 0$ since $b(v, v) = 0$. Hence,

$$(v, w)^{k+1} = ((k + 1)v, (k + 1)w).$$

For $k = p$, scalar multiplication by p is zero in $\mathbb{F}_p$, hence, $(v, w)^p = (0, 0)$.

Commutator formula. Let $x = (v, w)$ and $y = (v', w')$. Using the inverse formula and associativity,

$$[x, y] = xyx^{-1}y^{-1} = (v, w) \cdot (v', w') \cdot (-v, -w) \cdot (-v', -w').$$

First,

$$(v, w) \cdot (v', w') = \big(v + v',\ w + w' + \tfrac{1}{2}b(v, v')\big).$$

Multiply by $(-v, -w)$:

$$\begin{aligned}
\big(v + v',\ w + w' + \tfrac{1}{2}b(v, v')\big) \cdot (-v, -w) &= \Big(v',\ w' + \tfrac{1}{2}b(v, v') + \tfrac{1}{2}b(v + v', -v)\Big) \\
&= \Big(v',\ w' + \tfrac{1}{2}b(v, v') - \tfrac{1}{2}b(v + v', v)\Big) \\
&= \Big(v',\ w' + \tfrac{1}{2}b(v, v') - \tfrac{1}{2}b(v, v) - \tfrac{1}{2}b(v', v)\Big) \\
&= \Big(v',\ w' + \tfrac{1}{2}b(v, v') + \tfrac{1}{2}b(v, v')\Big) \\
&= (v',\ w' + b(v, v')),
\end{aligned}$$

using $b(v, v) = 0$ and alternation $b(v', v) = -b(v, v')$. Finally, multiply by $(-v', -w')$:

$$(v',\ w' + b(v, v')) \cdot (-v', -w') = \big(0,\ b(v, v') + \tfrac{1}{2}b(v', -v')\big) = (0, b(v, v')),$$

as $b(v', v') = 0$. This proves (2.2).

Derived subgroup and center. Equation (2.2) yields that every commutator lies in $\{0\} \times \mathrm{im}(b)$, and every element $(0, z)$ with $z \in \mathrm{im}(b)$ arises as a commutator $(0, b(u, v)) = [(u, 0), (v, 0)]$. Hence, $[G, G] = \{0\} \times \mathrm{im}(b)$.

For the center, $(v, w) \in Z(G)$ holds exactly when $[(v, w), (u, a)] = e$ for all $(u, a) \in G$. Using (2.2), this condition is

$$(0, b(v, u)) = (0, 0) \quad \text{for all } u \in V,$$

equivalent to $v \in \mathrm{rad}(b)$. The w-coordinate is arbitrary because W is central under (2.1). Hence, $Z(G) = \mathrm{rad}(b) \times W$. □

Remark 2.8. (What changes in characteristic two) The formula (2.1) uses $1/2$ and is tied to odd characteristic. For $p = 2$, a central extension of V by W is described by a cocycle $f\colon V \times V \to W$ with commutator $b(u, v) = f(u, v) - f(v, u)$, where subtraction equals addition in characteristic two. The product constraint then contains the cocycle term $f(u, w - u)$ rather than $1/2b(u, w - u)$, and the square map may contribute extra data in exponent-4 settings. Thus, an analogous problem can be formulated, but the clean contraction-only reduction of Theorem 3.4 belongs to the odd-prime centered model.

3. Main results

This section formulates commutator-constrained factorization and develops the linear-algebraic reduction, followed by exact attainable-set and uniformity laws, an explicit torsor parametrization of all solutions, and a factor-swap bijection.

Definition 3.1. (Commutator-constrained factorization) Given a group G of class 2 and exponent p, an element $g \in G$, and an element $h \in [G, G]$, determine the set

$$\mathcal{S}(g, h) := \{(x, y) \in G^2 : \ xy = g, \ [x, y] = h\}.$$

The associated tasks are: decide emptiness of $\mathcal{S}(g, h)$, compute $|\mathcal{S}(g, h)|$ when $\mathcal{S}(g, h)$ is nonempty, and construct a witness pair (x, y) when $\mathcal{S}(g, h)$ is nonempty.

3.1. Contraction maps

The commutator constraint is encoded linearly by fixing the second argument of b and viewing $u \mapsto b(u, w)$ as a linear map.

Definition 3.2. (Contraction maps) Fix (V, W, b) and define, for each $w \in V$, the $\mathbb{F}_p$-linear map

$$T_w : V \to W, \qquad T_w(u) := b(u, w).$$

The next lemma records basic identities that will enter every subsequent counting and structure statement.

Lemma 3.3. *(Basic identities for T_w) For all $w \in V$:*

(1) $\mathrm{im}(T_w) \subseteq \mathrm{im}(b)$.
(2) $\mathrm{rank}(T_w) + \dim \ker(T_w) = \dim V$.
(3) $w \in \mathrm{rad}(b)$ *holds exactly when* $T_w = 0$.

Proof. Fix $w \in V$.

Proof of (1). By definition,

$$\mathrm{im}(T_w) = \{T_w(u) : u \in V\} = \{b(u, w) : u \in V\}.$$

Every value $b(u, w)$ belongs to the $\mathbb{F}_p$-span of all commutator values $\{b(u', v') : u', v' \in V\}$, which is precisely $\mathrm{im}(b)$ by (2.6). Hence, each element of $\mathrm{im}(T_w)$ lies in $\mathrm{im}(b)$, giving $\mathrm{im}(T_w) \subseteq \mathrm{im}(b)$.

Proof of (2). The map T_w: $V \to W$ is $\mathbb{F}_p$-linear, so the standard rank-nullity theorem for finite-dimensional vector spaces applies:

$$\dim V = \dim \ker(T_w) + \dim \mathrm{im}(T_w).$$

By definition, $\mathrm{rank}(T_w) := \dim \mathrm{im}(T_w)$, hence,

$$\mathrm{rank}(T_w) + \dim \ker(T_w) = \dim V.$$

Proof of (3). By (2.6), the condition $w \in \mathrm{rad}(b)$ means

$$b(w,u) = 0 \quad \text{for all } u \in V.$$

Because b is alternating, $b(w,u) = -b(u,w)$ for all u, hence, the above condition is equivalent to

$$b(u,w) = 0 \quad \text{for all } u \in V.$$

The last display is exactly the statement that $T_w(u) = 0$ for all $u \in V$, which is equivalent to $T_w = 0$ as a linear map. Conversely, if $T_w = 0$, then $b(u,w) = 0$ for all u, hence also $b(w,u) = 0$ for all u by alternation, giving $w \in \mathrm{rad}(b)$. □

3.2. Decision, counting, and construction

We now show that all three tasks in (3.1) reduce to a single linear equation over $\mathbb{F}_p$ and admit closed forms when solvable.

Theorem 3.4. *(Linear reduction and closed counting formula) Let p be an odd prime, and let $G = (V \times W, \cdot)$ be the group from* (2.7)*. Fix $g = (w,c) \in V \times W$ and $h \in W$. Then:*

(1) $\mathcal{S}(g,h)$ is nonempty exactly when the linear equation

$$T_w(u) = h \tag{3.1}$$

admits a solution $u \in V$.

(2) If $\mathcal{S}(g,h)$ is nonempty, then

$$|\mathcal{S}(g,h)| = p^{\dim W}\, p^{\dim \ker(T_w)}. \tag{3.2}$$

(3) A witness pair can be constructed as follows: choose any $u \in V$ solving (3.1)*, set $v := w - u$, choose any $a \in W$, set $b' := c - a - 1/2h$, and output $x := (u,a)$ and $y := (v,b')$.*

Proof. Write $x = (u,a)$ and $y = (v,b')$ with $u, v \in V$ and $a, b' \in W$.

Step 1: Expand the constraints. By the group law (2.1),

$$xy = (u,a) \cdot (v,b') = \big(u + v,\ a + b' + \tfrac{1}{2}b(u,v)\big). \tag{3.3}$$

By the commutator formula (2.2),

$$[x,y] = (0, b(u,v)). \tag{3.4}$$

Thus $xy = g = (w,c)$ and $[x,y] = h$ are equivalent to the system

$$u + v = w, \tag{3.5}$$

$$b(u,v) = h, \tag{3.6}$$

$$a + b' + \tfrac{1}{2}\, b(u,v) = c. \tag{3.7}$$

Step 2: Reduce to a single linear equation in V. From (3.5), $v = w - u$. Substitute into (3.6):

$$b(u, w-u) = h.$$

Bi-linearity gives

$$b(u, w-u) = b(u, w) - b(u, u).$$

Alternation yields $b(u, u) = 0$, hence,

$$b(u, w) = h,$$

which is precisely $T_w(u) = h$.

Therefore, solvability of the original system is equivalent to solvability of (3.1), proving (1).

Step 3: Count solutions when solvable. Assume (3.1) has a solution u_0. The full solution set in V is the affine coset

$$u_0 + \ker(T_w),$$

so the number of admissible u equals $|\ker(T_w)| = p^{\dim \ker(T_w)}$. For each such u, the value $v = w - u$ is determined. Equation (3.7) becomes, using (3.6),

$$a + b' + \tfrac{1}{2}h = c,$$

hence,

$$b' = c - a - \tfrac{1}{2}h.$$

Each choice of $a \in W$ yields exactly one $b' \in W$, so the number of admissible (a, b') equals $|W| = p^{\dim W}$. Multiplying the independent counts yields (3.2), proving (2).

Step 4: Construct a witness. The explicit construction in (3) satisfies $u + v = w$ and $b(u, v) = b(u, w - u) = b(u, w) = h$, and it enforces $a + b' + 1/2h = c$ by direct substitution. □

3.3. Attainable commutators and uniformity laws

The next results describe exactly which commutator values can occur in factorizations $xy = g$ and show that, among attainable values, the distribution is uniform.

Definition 3.5. (Attainable commutator set for a fixed g) Fix $g \in G$. Define

$$\mathcal{H}(g) := \{h \in W : \mathcal{S}(g, h) \text{ is nonempty}\}.$$

Theorem 3.6. *(Attainable set and its cardinality) Let $g = (w, c) \in G$. Then,*

$$\mathcal{H}(g) = \operatorname{im}(T_w) \subseteq W, \qquad |\mathcal{H}(g)| = p^{\operatorname{rank}(T_w)}.$$

Proof. By Theorem 3.4(1), $\mathcal{S}(g, h)$ is nonempty exactly when the linear equation $T_w(u) = h$ is solvable. This holds exactly when $h \in \operatorname{im}(T_w)$. Hence, $\mathcal{H}(g) = \operatorname{im}(T_w)$.

Because $T_w \colon V \to W$ is $\mathbb{F}_p$-linear, $\operatorname{im}(T_w)$ is an $\mathbb{F}_p$-subspace of W of dimension $\operatorname{rank}(T_w)$, hence, its cardinality equals $p^{\operatorname{rank}(T_w)}$. □

Theorem 3.7. *(Exact uniformity across attainable commutators) Fix $g = (w, c) \in G$. For each $h \in W$,*

$$|\mathcal{S}(g, h)| = \begin{cases} p^{\dim W}\, p^{\dim \ker(T_w)}, & h \in \operatorname{im}(T_w), \\ 0, & h \notin \operatorname{im}(T_w). \end{cases}$$

Equivalently, the commutator values across all factor pairs (x, y) with $xy = g$ form a uniform distribution over the attainable set $\operatorname{im}(T_w)$.

Proof. The stated piecewise formula is Theorem 3.4(2) combined with Theorem 3.4(1). Uniformity follows because the value $p^{\dim W} p^{\dim \ker(T_w)}$ is constant for all h in $\mathrm{im}(T_w)$. □

Corollary 3.8. *(Partition identity) Fix $g = (w, c) \in G$. Then,*

$$\sum_{h \in W} |\mathcal{S}(g, h)| = |G| = p^{\dim V + \dim W}.$$

Proof. By (3.7), the sum over $h \in W$ reduces to the sum over $h \in \mathrm{im}(T_w)$, giving

$$\sum_{h \in W} |\mathcal{S}(g, h)| = |\mathrm{im}(T_w)| \cdot p^{\dim W}\, p^{\dim \ker(T_w)} = p^{\mathrm{rank}(T_w)} \cdot p^{\dim W}\, p^{\dim \ker(T_w)}.$$

Rank-nullity (Lemma 3.3(2)) gives $\mathrm{rank}(T_w) + \dim \ker(T_w) = \dim V$, hence, the product equals $p^{\dim V + \dim W} = |G|$. □

3.4. Torsor parametrization of the full solution set

Beyond cardinalities, one can parametrize *all* solutions explicitly, which is useful for a certified generation of witnesses and for deterministic enumeration strategies.

Theorem 3.9. *(Explicit torsor structure) Let $g = (w, c) \in G$ and $h \in W$. If $\mathcal{S}(g, h)$ is nonempty, fix one solution $u_0 \in V$ to $T_w(u) = h$. Define a map*

$$\Phi : \ \ker(T_w) \times W \ \longrightarrow \ \mathcal{S}(g, h)$$

by, for $(k, a) \in \ker(T_w) \times W$,

$$\Phi(k, a) := (x_{k,a}, y_{k,a}), \quad \textit{where} \quad x_{k,a} := (u_0 + k,\ a), \qquad y_{k,a} := (w - u_0 - k,\ c - a - \tfrac{1}{2}h).$$

Then, Φ is a bijection. In particular, $\mathcal{S}(g, h)$ is a torsor for $\ker(T_w) \times W$.

Proof. Assume $\mathcal{S}(g, h)$ is nonempty and fix u_0 with $T_w(u_0) = h$.

Step 1: $\Phi(k, a) \in \mathcal{S}(g, h)$ for all (k, a). Let $k \in \ker(T_w)$ and $a \in W$. Set $u := u_0 + k$ and $v := w - u_0 - k$, so that $u + v = w$ in V. Compute the commutator using (2.7):

$$[x_{k,a}, y_{k,a}] = (0, b(u, v)).$$

Because $v = w - u$, bilinearity and alternation give

$$b(u, v) = b(u, w - u) = b(u, w) - b(u, u) = b(u, w).$$

Next,

$$b(u, w) = b(u_0 + k, w) = b(u_0, w) + b(k, w) = T_w(u_0) + T_w(k).$$

Here, $T_w(u_0) = h$ by choice, and $T_w(k) = 0$ because $k \in \ker(T_w)$. Hence, $b(u, v) = h$, so $[x_{k,a}, y_{k,a}] = h$.

For the product, use (2.1):

$$x_{k,a}\, y_{k,a} = (u, a) \cdot (v, c - a - \tfrac{1}{2}h) = \left(u + v,\ a + c - a - \tfrac{1}{2}h + \tfrac{1}{2}b(u, v)\right) = (w, c),$$

since $b(u, v) = h$. Therefore, $\Phi(k, a) \in \mathcal{S}(g, h)$.

Step 2: Φ is injective. Suppose $\Phi(k, a) = \Phi(k', a')$. Then the first factors coincide:

$$(u_0 + k, a) = (u_0 + k', a').$$

Equality in $V \times W$ yields $u_0 + k = u_0 + k'$ and $a = a'$, hence $k = k'$.

Step 3: Φ is surjective. Let $(x, y) \in \mathcal{S}(g, h)$ with $x = (u, a)$. By Theorem 3.4(1), $T_w(u) = h$. Because also $T_w(u_0) = h$, subtraction yields

$$T_w(u - u_0) = T_w(u) - T_w(u_0) = h - h = 0,$$

so $k := u - u_0 \in \ker(T_w)$. With this k and the given a, the definition of Φ produces

$$x_{k,a} = (u_0 + k, a) = (u, a) = x.$$

The equations $xy = g$ and the explicit form in Theorem 3.4(3) forces

$$y = (w - u,\ c - a - \tfrac{1}{2}h) = y_{k,a}.$$

Thus, $(x, y) = \Phi(k, a)$, proving surjectivity. □

3.5. Refined counting with additional constraints

The next theorem fixes the V-coordinate of the first factor and isolates the remaining degrees of freedom, which is useful in constrained sampling and in deterministic witness generation.

Theorem 3.10. *(Fixed first factor in V-coordinates) Fix $g = (w, c) \in G$ and $h \in W$. Fix also $u \in V$. Define*

$$\mathcal{S}_u(g, h) := \{(x, y) \in \mathcal{S}(g, h) :\ x = (u, a) \text{ for some } a \in W\}.$$

Then:

(1) $\mathcal{S}_u(g, h)$ is nonempty exactly when $T_w(u) = h$.
(2) If $\mathcal{S}_u(g, h)$ is nonempty, then $|\mathcal{S}_u(g, h)| = p^{\dim W}$.
(3) In the nonempty case, every $a \in W$ yields a unique pair in $\mathcal{S}_u(g, h)$ via

$$x = (u, a), \qquad y = (w - u,\ c - a - \tfrac{1}{2}h).$$

Proof. Fix $u \in V$ and set $v := w - u$. For any $a \in W$ and any $b' \in W$, the conditions $xy = g$ and $[x, y] = h$ are equivalent to (3.5)–(3.7) from the proof of (3.4). With $v = w - u$ fixed, the commutator constraint becomes $b(u, v) = h$. Using $v = w - u$,

$$b(u, v) = b(u, w - u) = b(u, w) - b(u, u) = b(u, w) = T_w(u),$$

since $b(u, u) = 0$. This proves (1).

Assume $T_w(u) = h$. Then Eq (3.7) becomes $a + b' + 1/2h = c$, hence $b' = c - a - 1/2h$, giving existence and uniqueness of b' for each $a \in W$. Therefore $|\mathcal{S}_u(g, h)| = |W| = p^{\dim W}$, proving (2) and (3). □

3.6. Factor-swap law

Swapping factors converts the product constraint by a central commutator shift; the next theorem records the precise bijection.

Theorem 3.11. *(Swap bijection with shifted product constraint) Let $g \in G$ and let $h \in W = [G, G]$. Define $g_h := g \cdot (0, -h) \in G$. Then, the swap map σ: $G^2 \to G^2$, $\sigma(x, y) = (y, x)$ restricts to a bijection*

$$\sigma : \mathcal{S}(g, h) \longrightarrow \mathcal{S}(g_h, -h).$$

In $V \times W$ coordinates, if $g = (w, c)$ then $g_h = (w, c - h)$.

Proof. Fix $(x, y) \in \mathcal{S}(g, h)$. Then $xy = g$ and $[x, y] = h$. In a class-two group, commutators lie in the center, and the standard identity

$$yx = xy \cdot [x, y]^{-1}$$

holds exactly. Using $[x, y] = h$, this yields

$$yx = g \cdot h^{-1}.$$

In the additive W-coordinate used throughout, h^{-1} corresponds to $-h$, hence, $g \cdot h^{-1} = g \cdot (0, -h) = g_h$. Also,

$$[y, x] = [x, y]^{-1}$$

holds in any group, hence, $[y, x] = -h$ in W-coordinates. Therefore $(y, x) \in \mathcal{S}(g_h, -h)$.

Conversely, applying the same computation to a pair in $\mathcal{S}(g_h, -h)$ shows that swapping returns a pair in $\mathcal{S}(g, h)$. Hence, σ is a bijection between the two sets. □

Remark 3.12. (Meaning and use of the shifted element g_h) The element $g_h = g \cdot (0, -h)$ is obtained from g by multiplying by the inverse of the prescribed central commutator. In coordinates, this leaves the abelianized component $w \in V$ fixed and shifts only the central coordinate from c to $c - h$. The swap law is therefore a controlled central translation: The factor order is reversed, the commutator target changes from h to $-h$, and the product is adjusted by the central commutator forced by the original pair. Algorithmically, this gives an immediate reuse principle. Any solver, enumerator, or sampler for $\mathcal{S}(g, h)$ can be transported to one for $\mathcal{S}(g_h, -h)$ without resolving a fresh linear system, since T_w and its row-reduced data are unchanged.

4. Algorithmic complexity

The next theorem records certified complexity bounds for the linear algebra underpinning decision, counting, and witness construction.

Theorem 4.1. *(Deterministic polynomial-time algorithm) Fix a prime p and a bilinear-data instance (V, W, b) with $\dim V = d$ and $\dim W = m$. Given $g = (w, c) \in V \times W$ and $h \in W$, one can decide whether $\mathcal{S}(g, h)$ is empty, and when $\mathcal{S}(g, h)$ is nonempty, compute $|\mathcal{S}(g, h)|$ and construct a witness pair, using:*

- *$O(d^2 m)$ arithmetic operations in $\mathbb{F}_p$ to assemble a matrix representing T_w.*

- $O(\min\{d,m\}^2 \max\{d,m\})$ *arithmetic operations in* $\mathbb{F}_p$ *to solve* $T_w(u) = h$ *and compute* $\dim\ker(T_w)$ *via Gaussian elimination.*

Proof. Let $(e_1, \ldots, e_d)$ be the fixed basis of V and write $w = \sum_{j=1}^{d} \omega_j e_j$. For each i,

$$T_w(e_i) = b(e_i, w) = \sum_{j=1}^{d} \omega_j\, b(e_i, e_j).$$

The structure constants $b(e_i, e_j)$ for $i < j$ determine the full set of $b(e_i, e_j)$ using alternation:

$$b(e_j, e_i) = -b(e_i, e_j), \qquad b(e_i, e_i) = 0.$$

Computing each $T_w(e_i) \in W \cong \mathbb{F}_p^m$ requires $O(dm)$ field operations, repeating for $i = 1, \ldots, d$ gives $O(d^2 m)$ operations to assemble the $m \times d$ matrix of T_w.

Gaussian elimination over $\mathbb{F}_p$ solves $T_w(u) = h$ and yields $\dim\ker(T_w)$ with the stated arithmetic complexity. If the system is solvable, Theorem 3.4(3) provides a witness by evaluating vector additions in V and W and multiplying by $1/2 \in \mathbb{F}_p$. □

Remark 4.2. (Sparse and structured implementation) The dense assembly bound $O(d^2 m)$ is a worst-case arithmetic bound for explicit structure constants. If the alternating tensor is stored sparsely, let $\nu(b)$ be the number of nonzero triples (i, j, k) with $i < j$ and $c_{ij}^k \neq 0$. For a fixed vector $w = \sum_j \omega_j e_j$, assembling T_w only requires triples incident to indices j with $\omega_j \neq 0$. Hence the assembly cost is $O(\nu_w)$, where

$$\nu_w := \#\{(i, j, k) : c_{ij}^k \neq 0,\ \omega_i \neq 0 \text{ or } \omega_j \neq 0\} \leq \nu(b),$$

plus vector additions in W. For many queries, one may precompute and cache the matrices corresponding to the contractions against basis vectors, then form T_w as a linear combination and reuse row-echelon forms for repeated w or for vectors lying in the same symmetry orbit of the tensor. Over $\mathbb{F}_p$ the arithmetic is exact, so implementation issues are modular reduction, memory locality, sparse storage, and bit complexity for large p, rather than floating-point stability.

Remark 4.3. (Conversion from power-commutator or polycyclic input) Suppose the input is a consistent power-commutator presentation adapted to a class-two exponent-p group, with noncentral generators $x_1, \ldots, x_d$ projecting to a basis of V and central generators $z_1, \ldots, z_m$ giving a basis of $W = [G, G]$. Relations of the form

$$[x_i, x_j] = z_1^{c_{ij}^1} \cdots z_m^{c_{ij}^m}, \qquad (1 \leq i < j \leq d)$$

are exactly the structure constants of b. Reading all such relations costs $O(d^2 m)$ field operations in dense form, or $O(\nu(b))$ if the relators are sparse. If the supplied polycyclic sequence is not already split into quotient and derived generators, one first computes the elementary abelian quotients $G/[G, G]$ and $[G, G]$ by linear algebra over $\mathbb{F}_p$ and then expresses the pairwise commutators in the chosen central basis. With n total generators and collection cost C_{col} per commutator, this preprocessing is bounded by $O(n^2 C_{\mathrm{col}})$ group-collection operations plus polynomial-time row reduction over $\mathbb{F}_p$. Once the bilinear tensor has been extracted, all results of the paper apply unchanged.

5. Rank-profile invariants and recovery from counting

This section formalizes rank-distribution invariants arising from the family of contraction maps and shows how counting access recovers these invariants.

Definition 5.1. (Rank-profile polynomial) Let $G = (V \times W, \cdot)$ arise from (V, W, b). Define the polynomial

$$P_G(t) := \sum_{w \in V} t^{\mathrm{rank}(T_w)} \in \mathbb{Z}[t],$$

where $T_w(u) = b(u, w)$.

Theorem 5.2. *(Isomorphism invariance of the rank-profile polynomial) If G_1 and G_2 arise from bilinear-data instances (V_1, W_1, b_1) and (V_2, W_2, b_2) via (2.7), and if $G_1 \cong G_2$ as groups, then*

$$P_{G_1}(t) = P_{G_2}(t).$$

Proof. Let φ: $G_1 \to G_2$ be a group isomorphism. Since φ preserves commutators, it induces $\mathbb{F}_p$-linear isomorphisms

$$\bar{\varphi} : V_1 = G_1/[G_1, G_1] \to V_2 = G_2/[G_2, G_2], \qquad \varphi_W : [G_1, G_1] \to [G_2, G_2].$$

For $\bar{x}, \bar{y} \in V_1$,

$$\varphi_W(b_1(\bar{x}, \bar{y})) = b_2(\bar{\varphi}(\bar{x}), \bar{\varphi}(\bar{y})),$$

because both sides equal the image of $[x, y]$ under φ.

Fix $w \in V_1$ and define $w' := \bar{\varphi}(w) \in V_2$. For any $u \in V_1$,

$$\varphi_W(T_w^{(1)}(u)) = \varphi_W(b_1(u, w)) = b_2(\bar{\varphi}(u), w') = T_{w'}^{(2)}(\bar{\varphi}(u))$$

commutes and the vertical maps are isomorphisms. Therefore, $\mathrm{rank}(T_w^{(1)}) = \mathrm{rank}(T_{w'}^{(2)})$. As w ranges over V_1, $w' = \bar{\varphi}(w)$ ranges over all of V_2, hence, the multiset of ranks is preserved, implying $P_{G_1}(t) = P_{G_2}(t)$. □

Remark 5.3. (Distinguishing power and limitations) The polynomial $P_G(t)$ is an isomorphism invariant, and it records the rank distribution of all one-argument contractions of the commutator tensor. Its information content is deliberately coarse: It records how large the attainable sets can be and how frequently each contraction rank occurs, while it discards the relative positions of the subspaces $\mathrm{im}(T_w) \subseteq W$, the incidence geometry among kernels, and the full orbit data of the alternating tensor under $\mathrm{GL}(V) \times \mathrm{GL}(W)$. Thus $P_G(t)$ is best used as a fast filter or certificate of distinction when the polynomials differ.

A counting argument also shows that completeness cannot hold uniformly. For fixed (d, m), the number of possible rank-profile polynomials is at most $(p^d + 1)^{\min\{d,m\}+1}$, since the coefficients are non-negative integers summing to p^d. Meanwhile, the vector space of alternating maps $\bigwedge^2 V \to W$ has size $p^{m\binom{d}{2}}$, and the group $\mathrm{GL}(V) \times \mathrm{GL}(W)$ has size at most $p^{d^2+m^2}$. Hence, the number of isomorphism classes of such tensors is at least

$$p^{m\binom{d}{2} - d^2 - m^2}.$$

For large enough d and m, this lower bound exceeds the number of possible rank-profile polynomials, so distinct isomorphism classes must share the same $P_G(t)$.

The next theorem extracts additional invariant information directly from the rank-profile distribution.

Theorem 5.4. *(Radical size and extremal attainable-set size) Let G arise from (V, W, b), and let $r_{\max} := \max_{w\in V} \operatorname{rank}(T_w)$. Then:*

(1) The constant term of $P_G(t)$ equals $|\operatorname{rad}(b)|$, hence, $\dim \operatorname{rad}(b)$ is determined by P_G.
(2) The maximum attainable commutator-set size over all $g \in G$ equals $p^{r_{\max}}$.

Proof. (1). The constant term of $P_G(t)$ counts those $w \in V$ with $\operatorname{rank}(T_w) = 0$. A linear map has rank 0 exactly when it is the zero map, so $\operatorname{rank}(T_w) = 0$ holds exactly when $T_w = 0$. By Lemma 3.3(3), this holds exactly when $w \in \operatorname{rad}(b)$. Therefore, the constant term equals $|\operatorname{rad}(b)|$. Since $\operatorname{rad}(b)$ is an $\mathbb{F}_p$-subspace, $|\operatorname{rad}(b)| = p^{\dim \operatorname{rad}(b)}$, so $\dim \operatorname{rad}(b)$ is determined by the constant term.

(2). For $g = (w, c)$, Eq (3.6) gives $|\mathcal{H}(g)| = p^{\operatorname{rank}(T_w)}$. Maximizing over g is equivalent to maximizing over $w \in V$, so the maximum equals $p^{r_{\max}}$. □

Theorem 5.5. *(Recovery of rank data from attainable-set counting) Fix $g = (w, c) \in G$ and define*

$$N(g) := |\mathcal{H}(g)| = |\{h \in W : \mathcal{S}(g, h) \text{ is nonempty}\}|.$$

Then

$$N(g) = p^{\operatorname{rank}(T_w)}.$$

Consequently, the polynomial $P_G(t)$ is determined by the multiset $\{N(g) : g \in G\}$.

Proof. The equality $N(g) = p^{\operatorname{rank}(T_w)}$ is (3.6). For recovery, the V-projection $\pi : V\times W \to V$ is surjective and each $w \in V$ occurs as $\pi(g)$ for exactly $|W|$ choices of g. Hence the multiset $\{N(g) : g \in G\}$ contains each value $p^{\operatorname{rank}(T_w)}$ with multiplicity $|W|$, and therefore determines the multiset $\{\operatorname{rank}(T_w) : w \in V\}$, hence, $P_G(t)$. □

6. Worked examples and verification checks

6.1. Heisenberg group

Let H_p be the order-p^3 Heisenberg group, realized with

$$V = \mathbb{F}_p^2, \quad W = \mathbb{F}_p, \quad b((a, b), (a', b')) := ab' - a'b.$$

For $w = (\alpha, \beta) \in V$, $T_w(u) = \det(u, w)$ is an $\mathbb{F}_p$-linear functional. When $w \neq 0$, T_w has rank 1 and kernel dimension 1. When $w = 0$, $T_w = 0$ has rank 0 and kernel dimension 2. Hence,

$$P_{H_p}(t) = t^0 + (p^2 - 1)t^1.$$

For $g = (w, c)$ and $h \in W$, Theorem 3.7 yields:

$$|\mathcal{S}(g, h)| = \begin{cases} p^1 p^2 = p^3, & w = 0,\ h = 0, \\ 0, & w = 0,\ h \neq 0, \\ p^1 p^1 = p^2, & w \neq 0,\ h \in \mathbb{F}_p. \end{cases}$$

The partition identity Corollary 3.8 gives:

$$\sum_{h\in\mathbb{F}_p} |\mathcal{S}(g,h)| = \begin{cases} p^3, & w = 0, \\ p \cdot p^2 = p^3, & w \neq 0, \end{cases}$$

matching $\left|H_p\right| = p^3$.

6.2. Explicit torsor in the Heisenberg case

The torsor parametrization can be written completely. Let $g = ((\alpha,\beta),c)$ and let $h \in \mathbb{F}_p$. The contraction equation is

$$T_w(a,b) = a\beta - \alpha b = h.$$

If $(\alpha,\beta) \neq (0,0)$, this affine line has p solutions. For example, if $\alpha \neq 0$, choose a free parameter $r \in \mathbb{F}_p$ and write

$$u_r = \left(r, \frac{r\beta - h}{\alpha}\right).$$

For each $A \in \mathbb{F}_p$, the corresponding factor pair is

$$x_{r,A} = (u_r, A), \qquad y_{r,A} = \left((\alpha,\beta) - u_r,\ c - A - \tfrac{1}{2}h\right).$$

Thus, the p^2 solutions form a torsor for $\ker(T_w) \times \mathbb{F}_p$. If $w = (0,0)$, the attainable set is $\{0\}$; for $h = 0$, every $u \in \mathbb{F}_p^2$ and every $A \in \mathbb{F}_p$ give

$$x = (u, A), \qquad y = (-u, c - A),$$

which gives p^3 solutions.

6.3. A two-channel class-two example

Consider

$$V = \mathbb{F}_p^4 = U_1 \oplus U_2, \qquad W = \mathbb{F}_p^2,$$

where U_1 and U_2 have coordinates (a_1, b_1) and (a_2, b_2), respectively. Define

$$b((a_1,b_1,a_2,b_2),(a_1',b_1',a_2',b_2')) = (a_1b_1' - a_1'b_1,\ a_2b_2' - a_2'b_2).$$

Write $w = (w_1, w_2)$ with $w_i \in U_i$. The map T_w has rank equal to the number of nonzero components among w_1, w_2. Therefore,

$$P_G(t) = (1 + (p^2-1)t)^2 = 1 + 2(p^2-1)t + (p^2-1)^2t^2.$$

The attainable set for $g = (w, c)$ has size

$$|\mathcal{H}(g)| = \begin{cases} 1, & w_1 = 0,\ w_2 = 0, \\ p, & \text{exactly one of } w_1, w_2 \text{ is nonzero}, \\ p^2, & w_1 \neq 0,\ w_2 \neq 0. \end{cases}$$

For every attainable $h \in \mathcal{H}(g)$, the number of constrained factorizations is

$$|\mathcal{S}(g,h)| = p^{\dim W} p^{\dim \ker(T_w)} = p^2 p^{4-\mathrm{rank}(T_w)}.$$

This example illustrates how the rank-profile polynomial records a nontrivial distribution of attainable-set sizes beyond the single-channel Heisenberg group.

7. Conclusions and directions

Commutator-constrained factorizations admit a complete exact solution in class-two exponent-p groups under bilinear-data encoding. Decision, counting, and witness construction reduce to solving a single contraction equation $T_w(u) = b(u, w) = h$ over $\mathbb{F}_p$, and the full solution set is an explicit torsor for $\ker(T_w) \times W$, yielding closed formulas and certified procedures. The attainable commutator set $\mathcal{H}(g) = \mathrm{im}(T_w)$ and the uniformity law across attainable values supply refined structural information for each fixed product constraint $xy = g$. The swap law further relates constrained factorizations across centrally shifted product constraints, enabling controlled transformations and reuse of computed contraction data. Rank-profile polynomials and their derived invariants provide isomorphism-invariant rank distributions aligned with modern reductions of class-two exponent-p isomorphism to alternating matrix tuple isometries [9, 16, 20]. The polynomial $P_G(t)$ is a useful fast invariant, with explicit radical and extremal-attainability information, and its rank-only nature makes it a filter rather than a complete classification invariant.

Several extensions motivate further study. Input models beyond explicit bilinear structure constants, such as power-commutator and polycyclic presentations, motivate certified conversions to bilinear-data, connecting to practical group libraries and p-group generation methods [3, 5]. Rank-profile invariants suggest integration as a filtering stage inside isomorphism pipelines developed for the barrier case (see [6, 8, 9]). Enriched constraints involving additional algebraic predicates beyond a single commutator target link naturally to equation-solving problems in nilpotent groups [22, 23] and to extension/cohomology-based isomorphism strategies [18].

Author contributions

Ghaliah Alhamzi: conceptualization, methodology, writing – original draft, formal analysis; Mdi Begum Jeelani: supervision, project administration, writing – review and editing, funding acquisition; Wael Mahmoud Mohammad Salameh: validation, formal analysis, writing – review and editing; Prakash Jadhav: software, visualization, writing – review and editing. All authors have read and agreed to the published version of the manuscript.

Use of Generative-AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

Acknowledgments

This work was supported and funded by the deanship of scientific research at Imam Mohammad Ibn Saud Islamic University (IMSIU) (grant number IMSIU-DDRSP2602).

Conflict of interest

The authors declare no conflicts of interest.

References

1. D. F. Holt, B. Eick, E. A. O'Brien, *Handbook of computational group theory*, Chapman and Hall/CRC, 2005. https://doi.org/10.1201/9781420035216
2. Á. Seress, *Permutation group algorithms*, Cambridge University Press, 2003. https://doi.org/10.1017/CBO9780511546549
3. E. A. O'Brien, The p-group generation algorithm, *J. Symb. Comput.*, **9** (1990), 677–698. https://doi.org/10.1016/S0747-7171(08)80082-X
4. M. F. Newman, Determination of groups of prime-power order, In: R. A. Bryce, J. Cossey, M. F. Newman, *Group theory*, Springer, 1977, 73–84. https://doi.org/10.1007/BFb0087814
5. H. U. Besche, B. Eick, E. A. O'Brien, *The smallgroups library*, A refereed GAP package, 2005. Avaible from: `https://www.math.rwth-aachen.de/~GAP/WWW2/Packages/sgl.html`.
6. H. Dietrich J. B. Wilson, Group isomorphism is nearly-linear time for most orders, *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)*, 2021, 457–467. https://doi.org/10.1109/FOCS52979.2021.00053
7. D. J. Rosenbaum, Breaking the $n^{\log n}$ barrier for solvable-group isomorphism, *Proceedings of the Twenty-Fourth Annual ACM-SIAM Symposium on Discrete Algorithms*, 2013. https://doi.org/10.5555/2627817.2627893
8. D. J. Rosenbaum, Beating the generator-enumeration bound for p-group isomorphism, *Theor. Comput. Sci.*, **593** (2015), 16–25. https://doi.org/10.1016/j.tcs.2015.05.036
9. X. Sun, Faster isomorphism for p-groups of class 2 and exponent p, *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, 2023. https://doi.org/10.1145/3564246.3585250
10. S. A. Wani, K. S. Nisar, Quasi-monomiality and convergence theorem for the Boas-Buck-Sheffer polynomials, *AIMS Math.*, **5** (2020), 4432–4443. https://doi.org/10.3934/math.2020283
11. S. Khan, S. A. Wani, Fractional calculus and generalized forms of special polynomials associated with Appell sequences, *Georgian Math. J.*, **28** (2021), 261–270. https://doi.org/10.1515/gmj-2019-2028
12. M. Zayed, S. A. Wani, W. Ramírez, C. Cesarano, Advancements in q-Hermite-Appell polynomials: a three-dimensional exploration, *AIMS Math.*, **9** (2024), 26799–26824. https://doi.org/10.3934/math.20241303
13. S. A. Wani, A. Warke, J. G. Dar, Degenerate 2D bivariate Appell polynomials: properties and applications, *Appl. Math. Sci. Eng.*, **31** (2023), 2194645. https://doi.org/10.1080/27690911.2023.2194645
14. M. Konvisser, D. Jonah, Counting abelian subgroups of p-groups: a projective approach, *J. Algebra*, **34** (1975), 309–330. https://doi.org/10.1016/0021-8693(75)90186-6
15. G. Karpilovsky, *The Schur multiplier*, Oxford University Press, Inc., 1987. https://doi.org/10.5555/27673
16. G. Ivanyos, Y. Qiao, Algorithms based on $*$-algebras, and their applications to tuples of (skew-)symmetric matrices, *SIAM J. Comput.*, **48** (2019), 926–963.

17. Y. Li, Y. Qiao, Linear algebraic analogues of the graph isomorphism problem and the Erdős–Rényi model, *2017 IEEE 58th Annual Symposium on Foundations of Computer Science (FOCS)*, 2017. https://doi.org/10.1109/FOCS.2017.49

18. J. A. Grochow, Y. Qiao, Algorithms for group isomorphism via group extensions and cohomology, *SIAM J. Comput.*, **46** (2017), 115–171. https://doi.org/10.1137/15M1009767

19. P. A. Brooksbank, J. B. Wilson, Groups acting on tensor products, *J. Pure Appl. Algebra*, **218** (2014), 405–416. https://doi.org/10.1016/j.jpaa.2013.06.011

20. P. A. Brooksbank, J. Maglione, J. B. Wilson, A fast isomorphism test for groups whose Lie algebra has genus 2, *J. Algebra*, **473** (2017), 545–590. https://doi.org/10.1016/j.jalgebra.2016.12.007

21. J. Macdonald, A. Myasnikov, A. Nikolaev, S. Vassileva, Logspace and compressed-word computations in nilpotent groups, *Trans. Amer. Math. Soc.*, **375** (2022), 5425–5459. https://doi.org/10.1090/tran/8623

22. M. Duchin, H. Liang, M. Shapiro, Equations in nilpotent groups, *ArXiv*, 2014. https://doi.org/10.48550/arXiv.1401.2471

23. A. Levine, Equations in virtually class 2 nilpotent groups, *Groups Complexity Cryptology*, **14** (2022), 9776. https://doi.org/10.46298/jgcc.2022.14.1.9776

24. W. Zhang, S. Yu, L. Wang, W. Guo, M. F. Leung, Constrained symmetric non-negative matrix factorization with deep autoencoders for community detection, *Mathematics*, **12** (2024), 1554. https://doi.org/10.3390/math12101554

25. R. Baer, Groups with preassigned central and central quotient group, *Trans. Amer. Math. Soc.*, **44** (1938), 387–412. https://doi.org/10.1090/S0002-9947-1938-1501973-3

26. J. J. Rotman, *An introduction to the theory of groups*, 4 Eds., Springer, 1995. https://doi.org/10.1007/978-1-4612-4176-8

AIMS Press