KTREND JOURNALS
International Journal of Mathematics and Statistics

DOI: 10.5281/zenodo.20506460 **Volume:** 1 **Issue:** 1 **ISSN:** Pending

Homomorphism Counting, Fuzzy Group Actions and Conjugacy-Based Cryptography in Finite Algebraic Structures

Michael Nsikan John

Department of Mathematics, Edo State University, Iyamho, Nigeria

Corresponding Author: john.michael@edouniversity.edu.ng

Abstract

The interaction between finite algebraic structures and cryptographic systems motivates the search for unified frameworks that can connect homomorphism enumeration, quotient constructions, fuzzy algebraic actions, and conjugacy-class methods. In this paper, a structural framework is developed for finite groups acting on near-rings and for homomorphic images that induce modular B-algebras. The paper is motivated by previous works of the author on B-algebras generated by modulo integer groups, conjugacy-class key agreement, fuzzy group actions on near-rings, and homomorphism enumeration from the quaternion group. We define homomorphic complexity indices, fuzzy stabilizer indices, conjugacy complexity indices, and induced modular B-algebra invariants. Several results are proved: kernels of homomorphisms act trivially under induced actions; cyclic homomorphic images give canonical B-algebras; fuzzy stabilizers are subgroups; orbit-stabilizer relations persist in the fuzzy-invariant setting; and conjugacy-based key agreement can be interpreted through commuting subgroups and algebraic invariants. Examples involving cyclic groups, the quaternion group, dihedral groups, and nilpotent groups illustrate the theory. The framework gives a mathematical basis for combining quotient-based algebra, fuzzy symmetry, and conjugacy structures in the analysis of algebraic cryptographic protocols.

Keywords: finite groups; homomorphism counting; B-algebras; near-rings; fuzzy group actions; conjugacy classes; quaternion groups; algebraic cryptography.

1 Introduction

Finite algebraic structures occur naturally in many areas of mathematics and theoretical computer science. Groups, rings, near-rings, semigroups and their homomorphisms provide tools for

studying symmetry, quotient formation, representation, and computation. In cryptography, these structures are especially important because computational difficulty may be obtained from algebraic problems such as the discrete logarithm problem, conjugacy search problem, word problem, decomposition problem, and homomorphism-related reconstruction problems.

The present paper develops a unified framework joining four algebraic directions. The first direction is homomorphism counting in finite groups. Counting homomorphisms from a group into another algebraic object often reveals information about quotient groups, kernels, subgroup lattices and automorphism groups. In particular, the quaternion group Q_8 provides a useful test case because it is non-abelian but has a simple central quotient.

The second direction is the construction of B-algebras from modulo integer groups. If A is an abelian group written additively, then the operation $x * y = x - y$ gives a natural B-algebra structure. When $A \cong \mathbb{Z}_n$, this becomes a modular B-algebra. Thus cyclic homomorphic images of finite groups naturally produce B-algebras.

The third direction is fuzzy group action on near-rings. Fuzzy sets allow degrees of membership rather than binary membership, and group actions on fuzzy subsets lead to stabilizer and orbit structures that refine classical group action theory. Such stabilizers measure symmetries preserving a membership function.

The fourth direction is conjugacy-based cryptography. In a non-abelian group G, the conjugacy class

$$\mathrm{Cl}_G(g) = \{xgx^{-1} : x \in G\}$$

may be used to define protocols whose security is related to the difficulty of recovering a conjugating element. Such ideas motivate key agreement protocols based on finitely generated groups and non-commutative algebraic structures.

This paper is motivated especially by four previous works of the author: *On Finding B-Algebras Generated by Modulo Integer Groups* $\mathbb{Z}_n$ [1]; *Key Agreement Protocol Using Conjugacy Classes of Finitely Generated Groups* [2]; *Fuzzy Group Action on an R-Subgroup in a Near-Ring* [3]; and *On Finding the Number of Homomorphisms from* Q_8 [4]. Additional related works by the author and collaborators on nilpotent groups, lattice-based cryptography, conjugacy classes and algebraic cryptography also motivate the present approach [5, 6, 7, 8].

The main contribution of this paper is not to claim that a single invariant fully determines security. Rather, it develops a mathematically consistent way to place homomorphism enumeration, induced B-algebras, fuzzy stabilizers, and conjugacy classes within one algebraic language. The main results may be summarized as follows:

(i) kernels of homomorphisms are contained in stabilizers of induced actions;

(ii) cyclic homomorphic images canonically determine modular B-algebras;

(iii) fuzzy stabilizers are subgroups and admit orbit-stabilizer decompositions;

(iv) conjugacy-class key agreement can be formulated using commuting subgroups;

(v) combined invariants give a structured way to compare algebraic complexity.

2 Preliminaries

Throughout this paper, all groups are finite unless explicitly stated otherwise. The identity element of a group G is denoted by e_G or simply e.

Definition 2.1. *Let G and H be groups. A map $\phi : G \to H$ is a group homomorphism if*

$$\phi(xy) = \phi(x)\phi(y)$$

for all $x, y \in G$. The set of all homomorphisms from G to H is denoted by $\mathrm{Hom}(G, H)$.

Definition 2.2. *For finite groups G and H, define the homomorphism counting function by*

$$h(G, H) = |\operatorname{Hom}(G, H)|.$$

If $\mathcal{C}$ is a class of finite groups, define the restricted homomorphic complexity of G relative to $\mathcal{C}$ by

$$\Omega_{\mathcal{C}}(G) = \sum_{H \in \mathcal{C}} |\operatorname{Hom}(G, H)|\,|H|.$$

When $\mathcal{C}$ is fixed, we write $\Omega(G)$.

Definition 2.3. *The quaternion group Q_8 is*

$$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\},$$

where

$$i^2 = j^2 = k^2 = ijk = -1.$$

Its center is $Z(Q_8) = \{\pm 1\}$ and $Q_8/Z(Q_8) \cong C_2 \times C_2$.

Definition 2.4. *A B-algebra is an algebraic system $(X, *, 0)$ satisfying*

$$x * x = 0,$$
$$x * 0 = x,$$
$$(x * y) * z = (x * z) * y$$

for all $x, y, z \in X$.

Proposition 2.5. *Let $(A, +, 0)$ be an abelian group. Define $x * y = x - y$. Then $(A, *, 0)$ is a B-algebra.*

Proof. For $x \in A$, $x * x = x - x = 0$ and $x * 0 = x - 0 = x$. Also

$$(x * y) * z = (x - y) - z = x - y - z$$

and

$$(x * z) * y = (x - z) - y = x - z - y.$$

Since A is abelian, $x - y - z = x - z - y$. Hence $(x * y) * z = (x * z) * y$. □

Definition 2.6. *A right near-ring $(N, +, \cdot)$ consists of a group $(N, +)$, a semigroup $(N, \cdot)$, and the right distributive law*

$$(a + b)c = ac + bc$$

for all $a, b, c \in N$.

Definition 2.7. *A fuzzy subset of a set X is a map $\mu : X \to [0, 1]$. If a group G acts on X, the stabilizer of μ is*

$$\mathrm{Stab}_G(\mu) = \{g \in G : \mu(gx) = \mu(x) \text{ for all } x \in X\}.$$

For a fixed $x \in X$, the pointwise fuzzy stabilizer is

$$\mathrm{Stab}_G(\mu, x) = \{g \in G : \mu(gx) = \mu(x)\}.$$

Definition 2.8. *For $g \in G$, the conjugacy class and centralizer of g are respectively*

$$\mathrm{Cl}_G(g) = \{xgx^{-1} : x \in G\}, \qquad C_G(g) = \{x \in G : xg = gx\}.$$

The conjugacy complexity of g is $\kappa(g) = |\,\mathrm{Cl}_G(g)|$.

By the orbit-stabilizer theorem,

$$|\,\mathrm{Cl}_G(g)| = [G : C_G(g)].$$

3 Homomorphic Actions and Quotient Structures

Let $\phi : G \to H$ be a homomorphism and suppose H acts on a set X. Then G acts on X by

$$g \cdot x = \phi(g)x.$$

This is called the action induced by ϕ.

Lemma 3.1. *Let $\phi : G \to H$ be a homomorphism and let G act on X through ϕ. Then every element of $\ker \phi$ acts trivially on X.*

Proof. If $k \in \ker \phi$, then $\phi(k) = e_H$. Hence, for every $x \in X$,

$$k \cdot x = \phi(k)x = e_H x = x.$$

Thus k fixes every point of X. □

Theorem 3.2. *Let $\phi : G \to H$ be a homomorphism, and let G act on a set X through ϕ. If $\mu : X \to [0, 1]$ is any fuzzy subset, then*

$$\ker \phi \subseteq \mathrm{Stab}_G(\mu).$$

Proof. Let $k \in \ker \phi$. By Lemma 3.1, $kx = x$ for all $x \in X$. Therefore $\mu(kx) = \mu(x)$ for all $x \in X$, and so $k \in \mathrm{Stab}_G(\mu)$. □

Corollary 3.3. *If G acts faithfully through ϕ, then $\ker \phi = \{e\}$. If the action is not faithful, the kernel gives a non-trivial fuzzy stabilizing subgroup for every fuzzy subset μ.*

4 B-Algebras Induced by Homomorphic Images

The earlier construction of B-algebras generated by modulo integer groups may be extended through homomorphic images. The key point is that the B-algebra operation $x * y = x - y$ is naturally defined on abelian groups. Therefore cyclic images produce canonical B-algebras.

Definition 4.1. *Let $\phi : G \to A$ be a homomorphism from a group G to an abelian group A. The induced B-algebra of ϕ is*

$$B_\phi = (\mathrm{Im}\, \phi, *, 0), \qquad u * v = u - v.$$

Theorem 4.2. *Let $\phi : G \to A$ be a homomorphism into an abelian group. Then $B_\phi = (\mathrm{Im}\, \phi, *, 0)$ is a B-algebra.*

Proof. Since A is abelian and $\mathrm{Im}\, \phi$ is a subgroup of A, $\mathrm{Im}\, \phi$ is an abelian group. The result follows immediately from Proposition 2.5. □

Corollary 4.3. *If $\mathrm{Im}\, \phi \cong \mathbb{Z}_n$, then ϕ induces the modular B-algebra*

$$B_n = (\mathbb{Z}_n, *, 0), \qquad x * y = x - y \pmod{n}.$$

Proof. Since every cyclic group of order n is isomorphic to $\mathbb{Z}_n$, Theorem 4.2 gives the stated B-algebra up to isomorphism. □

Definition 4.4. *Let G be a finite group. Define*

$$\mathcal{B}(G) = \{[B_n] : \textit{there exists an epimorphism } G \to \mathbb{Z}_n\},$$

where $[B_n]$ denotes the isomorphism class of the modular B-algebra of order n.

Proposition 4.5. *The number of modular B-algebras induced by cyclic quotients of G is equal to the number of positive integers n for which G has a normal subgroup N such that $G/N \cong \mathbb{Z}_n$.*

Proof. If $G/N \cong \mathbb{Z}_n$, the quotient map induces B_n. Conversely, if B_n is induced by an epimorphism $\phi : G \to \mathbb{Z}_n$, then $G/\ker \phi \cong \mathbb{Z}_n$ by the First Isomorphism Theorem. The two constructions are inverse at the level of quotient orders. □

5 Homomorphism Enumeration from Q_8

This section connects the present framework with the author's earlier work on counting homomorphisms from Q_8.

Lemma 5.1. *Let A be an abelian group. Every homomorphism $\phi : Q_8 \to A$ factors through $Q_8/Z(Q_8)$.*

Proof. For any homomorphism $\phi : Q_8 \to A$, since A is abelian, all commutators are mapped to the identity. Hence $Q_8' \leq \ker \phi$. Since $Q_8' = Z(Q_8) = \{\pm 1\}$, the universal property of quotient groups gives a homomorphism $\overline{\phi} : Q_8/Z(Q_8) \to A$ satisfying $\phi = \overline{\phi} \circ \pi$, where $\pi : Q_8 \to Q_8/Z(Q_8)$ is the quotient map. □

Theorem 5.2. *For every finite abelian group A,*

$$|\operatorname{Hom}(Q_8, A)| = |A[2]|^2,$$

where

$$A[2] = \{a \in A : 2a = 0\}$$

is the subgroup of elements of order dividing 2.

Proof. By Lemma 5.1,

$$\operatorname{Hom}(Q_8, A) \cong \operatorname{Hom}(Q_8/Z(Q_8), A).$$

Since $Q_8/Z(Q_8) \cong C_2 \times C_2$, a homomorphism from $C_2 \times C_2$ to A is determined independently by the images of the two standard generators. Each image must be an element of $A[2]$. Therefore the number of choices is $|A[2]|^2$. □

Example 5.3. *If $A = \mathbb{Z}_n$, then*

$$|A[2]| = \gcd(n, 2).$$

Thus

$$|\operatorname{Hom}(Q_8, \mathbb{Z}_n)| = \gcd(n, 2)^2.$$

In particular, if n is odd, there is only the trivial homomorphism, while if n is even, there are four homomorphisms.

Corollary 5.4. *The only non-trivial modular B-algebra induced by an epimorphic abelian image of Q_8 is B_2.*

Proof. The abelianization of Q_8 is $C_2 \times C_2$. Its cyclic quotients have order 1 or 2. Therefore the only non-trivial cyclic quotient is C_2, which induces B_2. □

6 Fuzzy Group Actions and Stabilizer Decomposition

Let G act on a near-ring N by near-ring automorphisms. That is, for each $g \in G$, the map $x \mapsto gx$ preserves the near-ring operations.

Proposition 6.1. *For every fuzzy subset $\mu : N \to [0,1]$, $\mathrm{Stab}_G(\mu)$ is a subgroup of G.*

Proof. The identity satisfies $\mu(ex) = \mu(x)$, so $e \in \mathrm{Stab}_G(\mu)$. If $g, h \in \mathrm{Stab}_G(\mu)$, then

$$\mu((gh)x) = \mu(g(hx)) = \mu(hx) = \mu(x),$$

so $gh \in \mathrm{Stab}_G(\mu)$. If $g \in \mathrm{Stab}_G(\mu)$, then for every $x \in N$, put $y = g^{-1}x$. Since $x = gy$,

$$\mu(x) = \mu(gy) = \mu(y) = \mu(g^{-1}x).$$

Hence $g^{-1} \in \mathrm{Stab}_G(\mu)$. □

Definition 6.2. *For $x \in N$, the fuzzy-invariant orbit of x is*

$$\mathcal{O}_\mu(x) = \{gx : g \in G,\ \mu(gx) = \mu(x)\}.$$

Theorem 6.3 (Fuzzy Orbit-Stabilizer Relation)**.** *Let G act on N and let $\mu : N \to [0,1]$. For each $x \in N$, if $\mathrm{Stab}_G(\mu, x) = \{g \in G : \mu(gx) = \mu(x)\}$, then*

$$|\mathcal{O}_\mu(x)| \leq [G : G_x],$$

where $G_x = \{g \in G : gx = x\}$ is the ordinary stabilizer of x. If the equality condition $\mu(gx) = \mu(x)$ holds for every $g \in G$, then

$$|Gx| = [G : G_x].$$

Proof. By definition $\mathcal{O}_\mu(x) \subseteq Gx$, the ordinary orbit of x. Hence $|\mathcal{O}_\mu(x)| \leq |Gx|$. The ordinary orbit-stabilizer theorem gives $|Gx| = [G : G_x]$. If $\mu(gx) = \mu(x)$ for all $g \in G$, then $\mathcal{O}_\mu(x) = Gx$, and equality follows. □

Definition 6.4. *The fuzzy symmetry index of the action is*

$$\Sigma_\mu(G, N) = |\,\mathrm{Stab}_G(\mu)|.$$

When G and N are understood, we write Σ_μ.

Theorem 6.5. *If the action of G on N is induced by a homomorphism $\phi : G \to H$, then*

$$|\ker \phi| \leq \Sigma_\mu \leq |G|.$$

Proof. By Theorem 3.2, $\ker \phi \subseteq \mathrm{Stab}_G(\mu)$. Therefore $|\ker \phi| \leq \Sigma_\mu$. Since $\mathrm{Stab}_G(\mu)$ is a subgroup of G by Proposition 6.1, $\Sigma_\mu \leq |G|$. □

7 Conjugacy Classes and Key Agreement

Conjugacy classes are basic non-commutative invariants. They also provide one route to algebraic cryptographic protocols.

Definition 7.1. *Define the global conjugacy index of G by*

$$\Gamma(G) = \sum_{g \in G} |\operatorname{Cl}_G(g)|.$$

Proposition 7.2. *For every finite group G,*

$$|G| \leq \Gamma(G) \leq |G|^2.$$

Moreover, $\Gamma(G) = |G|$ if and only if G is abelian.

Proof. Every conjugacy class has size at least 1, so $\Gamma(G) \geq |G|$. Also $|\operatorname{Cl}_G(g)| \leq |G|$ for every g, so $\Gamma(G) \leq |G|^2$. If G is abelian, every conjugacy class has size 1, hence $\Gamma(G) = |G|$. Conversely, if $\Gamma(G) = |G|$, then every conjugacy class has size 1, so every element commutes with every other element; hence G is abelian. □

7.1 A Conjugacy-Based Key Agreement Scheme

Let G be a non-abelian group. Let A and B be subgroups of G such that every element of A commutes with every element of B. Publicly choose $g \in G$. Alice chooses $a \in A$ and publishes

$$X = a^{-1}ga.$$

Bob chooses $b \in B$ and publishes

$$Y = b^{-1}gb.$$

Alice computes

$$K_A = a^{-1}Ya = a^{-1}b^{-1}gba.$$

Bob computes

$$K_B = b^{-1}Xb = b^{-1}a^{-1}gab.$$

Theorem 7.3. *If $ab = ba$, then $K_A = K_B$.*

Proof. Since $ab = ba$, we also have $a^{-1}b^{-1} = b^{-1}a^{-1}$ and $ba = ab$. Therefore

$$K_A = a^{-1}b^{-1}gba = b^{-1}a^{-1}gab = K_B.$$

Thus Alice and Bob obtain the same group element as their shared key. □

Remark 7.4. *The theorem proves correctness of the protocol. A security proof would require specifying the platform group, representation, key distribution, adversarial model, and reductions to an accepted hard problem. The invariants developed in this paper should therefore be understood as algebraic complexity indicators, not as complete security guarantees.*

8 Combined Algebraic Complexity Invariants

We now combine homomorphic, fuzzy and conjugacy structures.

Definition 8.1. *Let G act on a near-ring N and let $\mu : N \to [0,1]$. Define*

$$\Lambda_{\mathcal{C}}(G) = \Omega_{\mathcal{C}}(G)\Gamma(G)$$

and

$$\Theta(G,\mu) = \Sigma_{\mu}\Gamma(G).$$

The first is the homomorphic-conjugacy index, and the second is the fuzzy-conjugacy index.

Theorem 8.2. *For every finite group action,*

$$\Theta(G,\mu) \leq |G|\Gamma(G).$$

Proof. Since $\Sigma_{\mu} = |\operatorname{Stab}_G(\mu)| \leq |G|$, multiplying by $\Gamma(G)$ gives the result. □

Definition 8.3. *For a fixed class $\mathcal{C}$ of target groups, define the unified algebraic invariant*

$$\mathcal{U}_{\mathcal{C}}(G,N,\mu) = \big(\Omega_{\mathcal{C}}(G), \Sigma_{\mu}, \Gamma(G), \mathcal{B}(G)\big).$$

Theorem 8.4 (Unified Structural Theorem)**.** *Let G be a finite group acting on a near-ring N, and let $\mu : N \to [0,1]$ be a fuzzy subset. Let $\mathcal{C}$ be a class of finite target groups closed under isomorphism. Then $\mathcal{U}_{\mathcal{C}}(G,N,\mu)$ is invariant under simultaneous isomorphism of the group, the near-ring action, and the fuzzy membership function.*

Proof. Let $\alpha : G \to G'$ be a group isomorphism and let $\beta : N \to N'$ be a near-ring isomorphism satisfying

$$\beta(gx) = \alpha(g)\beta(x)$$

for all $g \in G$ and $x \in N$. Let $\mu' : N' \to [0,1]$ be defined by $\mu'(y) = \mu(\beta^{-1}(y))$.

The homomorphism sets $\operatorname{Hom}(G,H)$ and $\operatorname{Hom}(G',H')$ correspond under isomorphism whenever $H \cong H'$; since $\mathcal{C}$ is closed under isomorphism, $\Omega_{\mathcal{C}}(G) = \Omega_{\mathcal{C}}(G')$. Conjugacy classes are preserved by group isomorphisms, so $\Gamma(G) = \Gamma(G')$. Also,

$$g \in \operatorname{Stab}_G(\mu)$$

if and only if

$$\mu(gx) = \mu(x) \quad \text{for all } x \in N,$$

which is equivalent, after applying β, to

$$\mu'(\alpha(g)y) = \mu'(y) \quad \text{for all } y \in N'.$$

Thus α maps $\operatorname{Stab}_G(\mu)$ bijectively onto $\operatorname{Stab}_{G'}(\mu')$, so $\Sigma_{\mu} = \Sigma_{\mu'}$. Finally, cyclic quotients and their induced modular B-algebras are preserved under isomorphism. Hence all four components of $\mathcal{U}_{\mathcal{C}}$ are invariant. □

9 Applications and Examples

9.1 Cyclic Groups

Let $G = C_m$. Since C_m is abelian, $\Gamma(C_m) = m$. For every divisor n of m, there is an epimorphism $C_m \to C_n \cong \mathbb{Z}_n$, hence $B_n \in \mathcal{B}(C_m)$. Therefore the induced B-algebras are exactly those of orders dividing m.

9.2 Quaternion Group

For Q_8, the conjugacy classes are

$$\{1\}, \quad \{-1\}, \quad \{i, -i\}, \quad \{j, -j\}, \quad \{k, -k\}.$$

Hence

$$\Gamma(Q_8) = 1 + 1 + 2 + 2 + 2 + 2 + 2 + 2 = 14,$$

where the sum is taken over elements, equivalently each element contributes the size of its class. More explicitly, two central elements contribute 1 each and six non-central elements contribute 2 each.

The abelianization of Q_8 is $C_2 \times C_2$. Thus the only non-trivial cyclic quotient of Q_8 is C_2, and the only non-trivial modular B-algebra induced by cyclic quotients is B_2.

9.3 Dihedral Groups

Let

$$D_{2n} = \langle r, s : r^n = s^2 = 1,\ srs = r^{-1} \rangle.$$

The quotient $D_{2n}/\langle r \rangle \cong C_2$ always gives an induced B_2. If n has non-trivial divisors, rotation quotients may produce additional cyclic images. The conjugacy class structure is richer than that of cyclic groups, so dihedral groups provide natural examples where $\Gamma(G)$ detects non-commutative complexity.

9.4 Nilpotent Groups

If G is finite nilpotent, then

$$G = P_1 \times P_2 \times \cdots \times P_r,$$

where P_i are Sylow subgroups. Homomorphisms from G are determined by compatible homomorphisms from the P_i, especially when the target decomposes into primary components. This makes nilpotent groups attractive in algebraic cryptography because their subgroup and quotient structures are rich but still decomposable.

Proposition 9.1. *If $G = P_1 \times \cdots \times P_r$ and A is abelian, then*

$$\mathrm{Hom}(G, A) \cong \prod_{i=1}^{r} \mathrm{Hom}(P_i, A).$$

Proof. A homomorphism $\phi : G \to A$ restricts to homomorphisms $\phi_i : P_i \to A$. Conversely, given homomorphisms $\phi_i : P_i \to A$, define

$$\phi(x_1, \ldots, x_r) = \phi_1(x_1) + \cdots + \phi_r(x_r).$$

Since A is abelian, this is a homomorphism. The two constructions are inverse. □

10 Conclusion

This paper developed a unified framework connecting homomorphism counting, B-algebras induced by modulo integer groups, fuzzy group actions on near-rings, and conjugacy-class cryptographic structures. The framework was motivated by previous works on B-algebras generated by $\mathbb{Z}_n$, conjugacy-class key agreement, fuzzy group actions, and homomorphism enumeration from Q_8.

The main mathematical results show that kernels of homomorphisms act trivially under induced actions and are contained in fuzzy stabilizers; cyclic homomorphic images generate modular B-algebras; fuzzy stabilizers are subgroups; conjugacy complexity is measured by conjugacy class sizes; and commuting subgroups give a correct conjugacy-based key agreement construction. The unified invariant

$$\mathcal{U}_{\mathcal{C}}(G, N, \mu) = \big(\Omega_{\mathcal{C}}(G), \Sigma_{\mu}, \Gamma(G), \mathcal{B}(G)\big)$$

collects the principal algebraic data of the framework.

The examples of cyclic groups, Q_8, dihedral groups and nilpotent groups demonstrate how the invariant captures quotient complexity, fuzzy symmetry and conjugacy structure. Future work may extend the theory to profinite groups, transformation semigroups, hyperstructures, non-commutative multirings with involution, and lattice-based cryptographic platforms.

Acknowledgements

The author acknowledges the Department of Mathematics, Edo State University, Iyamho, Nigeria, for academic support.

Conflict of Interest

The author declares no conflict of interest.

Funding Statement

This research received no external funding.

References

[1] M. N. John, E. Edet, and O. G. Udoaka, "On Finding B-Algebras Generated by Modulo Integer Groups $\mathbb{Z}_n$," *International Journal of Mathematics and Statistics Invention*, vol. 11, no. 6, pp. 1–4, 2023.

[2] M. N. John, O. G. Udoaka, and A. Musa, "Key Agreement Protocol Using Conjugacy Classes of Finitely Generated Groups," *International Journal of Scientific Research in Science and Technology*, vol. 10, no. 6, pp. 52–56, 2023. doi:10.32628/IJSRST2310645.

[3] M. N. John and I. U. Udoakpan, "Fuzzy Group Action on an R-Subgroup in a Near-Ring," *International Journal of Mathematics and Statistics Studies*, vol. 11, no. 4, pp. 27–31, 2023. doi:10.37745/ijmss.13/vol11n42731.

[4] M. N. John, E. E. Bassey, O. G. Udoaka, O. J. Tom, and O. U. Promise, "On Finding the Number of Homomorphisms from Q_8," *International Journal of Mathematics and Statistics Studies*, vol. 11, no. 4, pp. 20–26, 2023. doi:10.37745/ijmss.13/vol11n42026.

[5] M. N. John, O. G. Udoaka, and A. Musa, "Nilpotent Groups in Cryptographic Key Exchange Protocol for $N \geq 1$," *Journal of Mathematical Problems, Equations and Statistics*, vol. 4, no. 2, pp. 32–34, 2023. doi:10.22271/math.2023.v4.i2a.103.

[6] M. N. John, O. G. Udoaka, and I. U. Udoakpan, "Group Theory in Lattice-Based Cryptography," *International Journal of Mathematics and Its Applications*, vol. 11, no. 4, pp. 111–125, 2023.

[7] M. N. John and O. G. Udoaka, "Computational Group Theory and Quantum-Era Cryptography," *International Journal of Scientific Research in Science, Engineering and Technology*, vol. 10, no. 6, pp. 1–10, 2023. doi:10.32628/IJSRSET2310556.

[8] M. N. John, A. Musa, and O. G. Udoaka, "Conjugacy Classes in Finitely Generated Groups with Small Cancellation Properties," *European Journal of Statistics and Probability*, vol. 12, no. 1, pp. 1–9. doi:10.37745/ejsp.2013/vol12n119.

[9] J. J. Rotman, *An Introduction to the Theory of Groups*, 4th ed., Springer, 1995.

[10] D. J. S. Robinson, *A Course in the Theory of Groups*, 2nd ed., Springer, 1996.

[11] D. S. Dummit and R. M. Foote, *Abstract Algebra*, 3rd ed., Wiley, 2004.

[12] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications*, Cambridge University Press, 1994.

[13] L. A. Zadeh, “Fuzzy Sets,” *Information and Control*, vol. 8, no. 3, pp. 338–353, 1965.

[14] G. Pilz, *Near-Rings: The Theory and Its Applications*, 2nd ed., North-Holland, 1983.

[15] V. Shpilrain and A. Ushakov, “The Conjugacy Search Problem in Public Key Cryptography: Unnecessary and Insufficient,” *Applicable Algebra in Engineering, Communication and Computing*, vol. 17, pp. 285–289, 2006.

[16] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.