From Polynomial Rings to Approximation Spaces via Conjugacy Relation

Tabarak Wissam Sahb and Nisreen Najm Alokbi
Department of Mathematics, College of Education for Pure Sciences, Wasit University, 52001 Al-Kut, Iraq
std.2024205.t.sahb@uowasit.edu.iq, nisreen@uowasit.edu.iq

Keywords: Irreducible Polynomials Rings, Approximation Spaces, Conjugacy Relation, Equivalence Relation, Externally Definable Sets, Galois Field $GF(2^n)$, Internally Definable Sets, Rough Sets, Rough Membership Function, Topological Basis.

Abstract: This paper examines the reduction of polynomials over Galois Fields (GFs) to determine whether their coefficients truly belong to the field, based on irreducibility into non-trivial polynomials. The field GF(2^n) is constructed as a quotient ring formed from a primitive irreducible polynomial of degree n over the binary polynomial ring, providing an ideal algebraic environment for studying finite field structures. The study links this algebraic construction to the theory of Approximation Spaces, where a binary relation generated through the algebraic conjugacy relation is proven to be an equivalence relation, and is used to derive the two approximation limits (lower and upper) of subsets within the field. Through these relations, the polynomials are partitioned into equivalence classes, which in turn serve as the basis for a topological space, allowing the study of proximity and connectivity among field elements. This approach enables a classification of subsets into exact and rough sets, offering a deeper understanding of the structure of GFs and their irreducible polynomials from both an algebraic and topological perspective. For precise partitioning and classification of field elements, an accuracy (rough membership) measure is introduced, quantifying the degree of belonging of elements to a subset and distinguishing exact sets from rough ones. This combined algebraic-topological-rough set framework offers a systematic approach to analyzing polynomial characteristics within approximation spaces and is shown to have promising applications in cryptographic frameworks, where precise.

1 INTRODUCTION

Pawlak's theory of rough sets has garnered significant interest from researchers, due to its widespread use and numerous applications across various fields [1], [2].

This research presents a study and construction of an approximation space derived from GFs and their properties, in addition to irreducible polys. To build the space, we start from the poly ring $\mathbb{Z}_2[u]$, characterized by its coefficients lying in the set $\{0,1\}$ and operations within it being according to modulo 2. This ring provides an ideal algebraic environment for analyzing and studying robust top space.

This study extends to link with the theory of finite fields represented by the GF, which constitutes an important cornerstone in modern mathematics and numerous applications, including coding theory and the field of cryptography [3]. In 1830, the foundation of the theory of fields with finite elements, was laid by the famous scientist Évariste Galois, usually denoted as $GF(2^n)$, through his research into finding solutions for algebraic equations by radicals. Galois's work provided a shift in algebra by linking the irreducibility of polys with the construction of field extensions. To generate a field, Galois proved that a poly $p(u)$ that is irreducible within $GF(2)$ and possesses a degree n over the field GF serves as an algebraic tool used to generate the extension field $GF(2^n)$.

The field of integrating algebraic structures with rough set theory has seen remarkable development in recent times. Among the most notable contributions in this regard is the study by Abd-Ellatif and Ramadan in 2025 [4], which addressed the conjugacy relation as an equivalence tool for defining rough subgroups, introducing the concept of "internal edges" to bridge the structural gaps between subgroups and their lower approximations. However, this study appears to be limited in scope, as it is confined to the internal characterization of groups in a general manner. Unlike previous studies that were limited to addressing rough subgroups in a general algebraic setting, this study presents a specialized framework targeting $GF(2^n)$, by employing the conjugacy relation to construct a topological base suitable for cryptographic applications.

Our research, on the other hand, distinguishes itself by dedicating this algebraic-topological framework specifically to GFs $GF(2^n)$, employing the conjugacy relation to partition the field elements and construct a robust topological base derived from irreducible polys, thereby providing a suitable framework for cryptographic applications.

For instance, to construct the field $GF(2^3)$ which contains 8 elements, we need an irreducible poly of degree three over the ring $\mathbb{Z}_2$. The connection between the poly ring $\mathbb{Z}_2[u]$ and GFs $GF(2^n)$ is established through the quotient ring of the form $\mathbb{Z}_2[u]/\langle p(u)\rangle$, where $p(u)$ is chosen as an irreducible poly of degree n (such as $u^3 + u + 1$) to construct $GF(2^n)$.

In this context, the scientist laid a proof for the existence of a finite field of order p^n, where $p = 2$ is a prime number, nnn is a positive integer, and the corresponding multiplicative group forms a cyclic group of order $p^n - 1$ [5].

The methodology followed in this research paper is based on a pivotal tool represented by the conjugacy relation in order to partition the algebraic elements in Galois field into equivalence classes, and we introduce a top space through this binary relation such that this space helps to understand and comprehend more deeply the topological properties within finite systems, and also we introduce an approximation space that achieves an effective connection representing the transition from algebraic properties to rough set theory. Through this, the upper and lower approximations of the subsets within the field can be derived.

The research adds an accuracy measure for the elements of sets using the membership accuracy measure and that is through analyzing them numerically, and its purpose is to classify the subsets and distinguish the exact and rough ones among them, and this is what gives us a deeper view of the structure of finite fields and their irreducible polys from the topological perspective and strengthens their analysis, whereby this approach opens horizons for linking algebra with topology and analytical structures.

2 PRELIMINARIES AND MATHEMATICAL BACKGROUND

This section reviews the fundamental concepts and pivotal results related to GFs and rough set theory, using the symbol (X, R) to represent the approximation space, where X denotes a finite set of elements of $GF(2^n)$ constructed from the irreducible poly ring, while R represents a binary relation defined on X.

Definition 2.1 [6]: A field is defined as a commutative ring F where $1 \neq 0$, and for every element $a \neq 0$ in F there exists a multiplicative inverse a^{-1}, satisfying the condition a $\cdot\, a^{-1} = a^{-1} \cdot a = 1$.

Definition 2.2 [7]: The poly ring $R[u]$ over R consists of all polys in u with coefficients in R, and is given in the following form:

$$f(u) = a_0 + a_1 u + a_2 u^2 + \cdots + a_{\,n} u^n,$$

where $a_i \in R, \forall i \geq 0$, and all but finitely many coefficients aia_iai are zero. The addition and multiplication operations are defined according to the rules of the ring R.

Example 2.1: For $R = Z_2$, the poly ring is:

$$Z_2[u] = \{a_0 + a_1 u + a_2 u^2 + \cdots + a_n u^n | a_i \in \{0,1\}.$$

Definition 2.3 [6]: A single-variable poly $p(u) \in F[u]$ is called irreducible over F if $deg(p(u) \geq 1$ and it cannot be factored into of two polys $g(u), h(u) \in F[u]$, each having degree smaller than $deg(p(u)$.

Example 2.2: When examining the poly $f(u) = u^4 + u^3 + u^2 + u + 1$ in $\mathbb{Z}_2[u]$, it becomes clear through algebraic analysis that it is irreducible over $\mathbb{Z}_2$, as there exist no two non-trivial polys in $\mathbb{Z}_2[u]$ whose product equals $f(u)$.

Definition 2.4 [8]: The field F is termed a finite field if it contains a finite number of elements.

Definition 2.5 [9]: A Galois field, denoted by $GF(p^n)$, is a finite field of order p^n, where p is a prime characteristic and $n \in \mathbb{Z}^+$. In the special case $p = 2$, the field is written as $GF(2^n)$. Moreover, a poly is called monic when its leading coefficient is equal to 1, and the term containing the highest power of u, namely u^n, is referred to as the leading term.

Remark 2.1: A polynomial is monic if its leading coefficient is 1.

Theorem 2.1 [10]: Let p be a prime number, and $p(u)$ be a monic and irreducible poly ring of degree n. As a result, from the field of order p^n the quotient ring Z is formed.

The reader may refer to [7] for further details regarding the proof.

Theorem 2.2 [11]: An equivalence relation produces a unique partition of the elements for that set.

Definition 2.6 [11]: A pair (X, τ) is said to be a top space if $\tau \subseteq P(X)$ and the following axioms hold: $X, \emptyset \in \tau$; the union of any collection of members of τ belongs to τ; and the intersection of any finite number of members of τ also belongs to τ.

Definition 2.7 [1], [12]: The pair (X, R) is known an approximation space (approx. space) if $X \neq \emptyset$ is a finite set and R is a binary relation on X, that is, $R \subseteq X \times X$.

Definition 2.8 [1]: Let (X, R) be an approx. space with X as a non-empty universe and R as an equivalence relation on X. For each subset $A \subseteq X$, the rough set associated with A relative to R is characterized by two approximations, namely the lower approximation and the upper approximation.

- The lower approximation: $\underline{R}(A) = \{u \in X \mid [u]_R \subseteq A\}$, meaning the elements whose equivalence class belongs entirely to A.
- The upper approximation: $\overline{R}(A) = \{u \in X \mid [u]R \cap A \neq \emptyset\}$, meaning the elements whose equivalence class shares at least one element with A.

Definition 2.9 [2]: Let (X, R) be approx. space. If $A \subseteq X$, and the sets can be characterized as follows:

- A is exact set if $\underline{R}A = A = \overline{R}A$.
- A is an internally R-definable set if $A = \underline{R}A$.
- A is an externally R-definable set if $A = \overline{R}A$.
- A is rough set if $A \neq \underline{R}A$ and $A \neq \overline{R}A$.

Proposition 2.1 [13]: Let $X \neq \emptyset$, and R be a binary relation on X. For a subset $A \subseteq X$, Then:

- $\underline{R}A \subseteq A \subseteq \overline{R}A$.
- $\underline{R}(\emptyset) = \overline{R}(\emptyset) = \emptyset$ (or $\underline{R}X = \overline{R}X = X$).
- $\underline{R}A = \overline{R}A = A$ (This holds if and only if A is an exact set).

3 APPROXIMATION SPACE STRUCTURES DERIVED BY CONJUGACY CLASSES ON $GF(2^3)$

Based on the concepts of polys and GFs, this study emerges from the quotient ring $\mathbb{Z}_2[u]/(u^m + u + 1) \cong GF(2^n)$, where m represents the degree of the irreducible poly while $n \in \{2, 3\}$ represents the degree of field extension. This research focuses on the transition from the algebraic relation to the approx. space through the conjugacy relation, and proving that an equivalence relation that generates classes which partition the field into an organized space, according to the following conjugacy relation:

$$(a^{-1} + b) = (a + b^{-1}). \quad (1)$$

By using the equivalence classes resulting from the conjugacy relation as a fundamental basis for constructing a topology, we transition from algebraic operations to an integrated topological framework. The top space allows the study of proximity and connectivity in the field $GF(2^n)$.

In rough set theory, the approx. space (X, R) is induced by the algebraic partition of the universe, and the two limit approximations are used to characterize each subset of the Galois field. A subset is called exact whenever the two approximations are identical, while it is classified as a rough set when they are not equal, indicating the presence of uncertainty in the algebraic structure [1].

For a quantitative description of this uncertainty, the membership function is employed to measure the precision of subset elements and their corresponding degrees of membership, thereby contributing to narrowing the gap between algebraic elements and continuous approximation measures. The space is divided according to set A into four types reflecting its internal and external structure [2].

Theorem 3.1: The conjugacy relation defined by $(q^{-1} + b) = (q + b^{-1})$ yields an equivalence relation on the set $GF(2^n)\backslash\{0\}$.

Proof: To prove that every conjugacy relation yields an equivalence relation, the following three conditions must be satisfied:

- Reflexivity. By leveraging the commutative property of addition in $GF(2^n)$, we deduce that $(q^{-1} + q) = (q + q^{-1})$. Thereby satisfying the definition of the relation R, and thus proving that $(q, q) \in R$.
- Symmetry. Assume $(q, b) \in R$, we have $(q^{-1} + b) = (q + b^{-1})$. By swapping the position of the terms and applying the symmetric property of equality, it becomes evident that $(b^{-1} + q) = (b + q^{-1})$, thus proving that $(b, q) \in R$.
- Transitivity. Assume $(q, b) \in R$ and $(b, c) \in R$. Then We begin by isolating the terms associated with each element individually. Through $(q, b) \in R$ and $(b, c) \in R$, we are able to classify the terms of a, b, and c

separately, in order to eliminate the common element b:

$$(q^{-1}+b)=(q+b^{-1}),$$
$$(q^{-1}+(-q))=(b^{-1}+(-b)),$$
$$(b^{-1}+c)=(b+c^{-1}),$$
$$(b^{-1}+(-b))=(c^{-1}+(-c)).$$

Where (q^{-1}) is the additive inverse of (q). By substituting the middle term, we get($q^{-1}+(-q))=(c^{-1}+(-c))$. Rearranging this result gives $(q^{-1}+c)=(c^{-1}+a)$, which means $(q,c)\in R$. Since all three properties are satisfied, R yields an equivalence relation ■.

Corollary 3.1: The conjugacy relation on the GFs $GF(2^n)$ yields an equivalence relation.

Proof: Since the three conditions of an equivalence relation are satisfied, for the conjugacy relation defined on the finite field $GF(2^n)$, it follows that the relation is an equivalence relation ■.

Theorem 3.2: Let $X=GF(2^n)\backslash\{0\}$ be a finite field generated by an irreducible poly ring, and R is a binary relation on X, then R represents a basis for a top space.

Proof: Let X be a GF, and the conjugacy relation R is an equivalence relation by Theorem 3.1, and every equivalence relation on X induces a unique partition into disjoint equivalence classes $[u]_R$ by Theorem 2.2.

Since X is a union of all its conjugacy classes, the relation$\bigcup▒[u_i\ ]_R=X$, holds, which satisfies the first axiom of the topological basis, requiring that every element of the space belongs to at least one basis element, The intersection of any two classes $[u]\_R\cap[u]\_y=\emptyset$ (if they are distinct) or equal to the class itself in the case of their identity, which means the second axiom of the topological basis is satisfied (the intersection of any two basis elements represents a union of elements from it). Consequently, the collection $\beta=\{[u_i]_R : u_i\in X\}$ produces a topology on X ■.

Theorem 3.3: Let $X=GF(2^n)\backslash\{0\}$ be a finite field induced by the irreducible poly ring and $R=\{(q,b)$ in $X\times X$ if $(q^{-1}+b)=(q+b^{-1})\}$ is a binary relation, then every $A\subseteq X$ is either a rough or exact set in the approx. space (X,R).

Proof: The equivalence relation R produces an equivalence class:

$$[1],[u_1],[u_2],\dots,[u_k].$$

Where $k=2^{n-1}-1$, and each class contains only two elements.

For every subset $A\subseteq X$, we have two cases:

- If:

$$A=\bigcup_{i\in I}[u_i],\forall u_i\in A,$$
$$\underline{R}(A)=\{u\in X:[u]\subseteq A\}=A,$$
$$\overline{R}(A)=\{u\in X:[u]\cap A\neq\phi\}=A.$$

Since $\underline{R}(A)=A=\overline{R}(A)$, then A is an exact set.

- If:

$$A\subseteq\bigcup_{i\in I}[u_i],\forall u_i\in A,$$

$$\underline{R}(A)=\{u\in X:[u]\subseteq A\}\subseteq A,$$
$$\overline{R}(A)=\{u\in X:[u]\cap A\neq\phi\}\supseteq A.$$

Since $\underline{R}(A)\neq A$ and $\overline{R}(A)\neq A$, then A is a rough set.

- Such that the space set are classified into four cases. By Definition 2.9 since A is exact or rough set. Then $ID(X)$ and $ED(X)$ are empty set ■.

Corollary 3.3: For any $A\subseteq X$ in the approx. space (X,R), the internally and externally R −definable sets are equal to the empty set.

Remark 3.1: In the next section, we will denote the set of internally R-definable set by ID(X), and the externally R-definable sets by $ED(X)$.

Remark 3.2: To facilitate calculations and impart greater methodological clarity to computational operations, we will express the elements of Galois Field $GF(2^n)$ in numerical form rather than employing poly notation, while fully preserving the algebraic properties of the field structure.

4 NUMERICAL EXAMPLE IN $GF(2^n)$

In this section, we apply the aforementioned theorems and results to two specific finite fields.

4.1 Construction and Classification in $GF(2^2)$

In order to construct $GF(2^2)$, we utilize the irreducible poly $f(u)=u^2+u+1$ over $\mathbb{Z}_2$, whose elements are the remainders of division by $f(u)$, resulting in $2^2=4$ distinct elements:

$$\{0,1,u,u+1\}.$$

This structure forms the finite field $GF(2^2)$, where addition in this field is defined by the usual poly addition modulo 2 and multiplication are performed modulo $f(u)$.

Where it is applied the conjugacy relation R while excluding the zero element to ensure a valid equivalence relation on X and forming the equivalence classes that serve as the topological basis for the space (X, R). To distinguish between the four types of sets in the approx. space over $GF(2^2)$, we examine the power set $P(A)$, the power set contains $2^3 = 8$ subsets, and demonstrating that subsets are either exact or rough, while verifying that internally and externally definable sets are empty.

Example 4.1: Let $X = \{0,1,2,3\}$ be a finite field, R is an equivalence relation:

$$R = \{(1,1), (2,2), (2,3), (3,2), (3,3)\},$$

The equivalence classes derived from this relation are $[u] = \{\{1\}, \{2,3\}\}$ and the B is a base of τ, $B = \{\{1\}, \{2,3\}\}$, $\tau = \{\varphi, X, \{1\}, \{2,3\}, \{1,2,3\}\}$, if $A = \{1,2\}$, $A \subseteq X$, $\underline{R}A = \{1\}$ and $\overline{R}A = \{1,2,3\}$.

Exact set $= \{(1), (2,3), (1,2,3)\}$, Rough set $= \{(2), (3), (1,2), (1,3)\}$, so $ID(X) = \emptyset$ and $ED(X) = \emptyset$.

4.2 Construction and Classification in $GF(2^3)$

To construct the field $GF(2^3)$, we utilize the irreducible poly ring $\mathrm{f}(u) = u^3 + u + 1$ over $\mathbb{Z}_2$, where its elements are the remainders of division by $f(u)$, resulting in $2^3 = 8$ distinct elements:

$$\{0, 1, u, u+1, u^2, u^2+1, u^2+u, u^2+u+1\}.$$

This structure forms the finite field $GF(2^3)$, where addition is defined modulo 2 and multiplication is performed modulo $f(u)$. By applying the conjugacy relation R while excluding the zero element, and form the equivalence classes that serve as the topological basis for the space (X, R).

To distinguish between the four types of sets in the approx. space over $GF(2^3)$, we examine the power set $P(A)$, the power set $P(A)$ contains $2^7 = 128$ subsets. We demonstrate that these subsets are either exact or rough, while verifying that internally and externally R-definable sets are empty.

Example 4.2: Let $X = \{1,2,3,4,5,6,7\}$ be a finite field, R is an equivalence relation:

$$R = \{(1,1), (2,2), (2,5), (3,3), (3,7), (4,4), (4,6), (5,2), (5,5), (6,4), (6,6), (7,3), (7,7)\}.$$

The equivalence classes derived from this relation are:

$$[u] = \{\{1\}, \{2,5\}, \{3,7\}, \{4,6\}\},$$

and the B is a base of τ,

$$B = \{\varphi, \{1\}, \{2,5\}, \{3,7\}, \{4,6\}\},$$

$$\tau = \{\varphi, X, \{1\}, \{2,5\}, \{3,7\}, \{4,6\}, \{1,2,5\}, \{1,3,7\}, \{1,4,6\}, \{2,3,5,7\}, \{2,4,5,6\}, \{3,4,6,7\}, \{1,2,3,5,7\}, \{1,2,4,5,6\}, \{1,3,4,6,7\}, \{2,3,4,5,6,7\}\}.$$

$A = \{1,5,7\}$, $A \subseteq X$, $\underline{R}A = \{1,2,3,5,7\}$ and $\overline{R}A = \{1\}$.

$$\mathit{Exact\ set} = \{(1), (2,5), (3,7), (4,6), (1,2,5), (1,3,7), (1,4,6), (2,3,5,7), (2,4,5,6), (3,4,6,7), (1,2,3,5,7), (1,2,4,5,6), (1,3,4,6,7), (2,3,4,5,6,7), (1,2,3,4,5,6,7)\}.$$

Since the power set contains 128 elements, 112 elements are rough sets, and with the exact sets and the empty set, the total becomes 128 elements, so $ID(X) = ED(X) = \emptyset$.

5 ROUGH MEMBERSHIP FUNCTION (ACCURACY OF THE ELEMENT)

The formal foundation of the rough membership function is attributed to the works of Pawlak and Skowron [14], with earlier contributions by Wong and Ziarko [15] and Pawlak et al. [16], while Yao and Wong [17] enriched this field with valuable contributions. This function is defined as a mathematical measure of the degree of belonging of an element to $A \subseteq X$, where the equivalence class $[u]_R$ partitions the rough space (X, R) over $GF(2^n)$, and the function measures the overlap between A and $[u]_R$ containing x, and is defined by the following formula:

$$\mu_A^R : X \to [0,1],$$

where:

$$\mu_A^R(u) = \frac{|[u]_R \cap A|}{|[u]_R|}. \quad (2)$$

5.1 Interpretation of Results

The resulting value of the rough membership function ranges between 0 and 1:

- When the result is 1: The set A is considered an exact set with respect to that element.

- When the value is between 0 and 1: The set A is considered a rough set.
- When the result is 0: The element is completely outside the set A.

Example 5.1: Let $X = \{1,2,3\}$ be finite field, and the equivalence classes be $[u]_R = \{\{1\},\{2,3\}\}$. For a subset $A = \{2,3\}$, we calculate the rough membership values $\mu_A^R(u)$ for each element as follows:

- $\mu_A^R(1) = \frac{|\{1\}\cap\{2,3\}|}{|\{1\}|} = \frac{0}{1} = 0.$
- $\mu_A^R(2) = \frac{|\{2,3\}\cap\{2,3\}|}{|\{2,3\}|} = \frac{2}{2} = 1.$
- $\mu_A^R(3) = \frac{|\{2,3\}\cap\{2,3\}|}{|\{2,3\}|} = \frac{2}{2} = 1.$

Since $\mu_A^R(u) \in \{0,1\}$ for all $u \in X$, the set $A = \{2,3\}$ is an exact set.

Example 5.2: Let $X = \{1,2,3,4,5,6,7\}$ be finite field, and the equivalence classes be $[u]_R = \{\{1\},\{2,5\},\{3,7\},\{4,6\}\}$. For a subset $A = \{1,5,7\}$, we calculate the rough membership values $\mu_A^R(u)$ for each element as follows:

- $\mu_A^R(1) = \frac{|\{1\}\cap\{1,5,7\}|}{|\{1\}|} = \frac{1}{1} = 1.$
- $\mu_A^R(2) = \frac{|\{2,5\}\cap\{1,5,7\}|}{|\{2,5\}|} = \frac{1}{2} = 0.5.$
- $\mu_A^R(3) = \frac{|\{3,7\}\cap\{1,5,7\}|}{|\{3,7\}|} = \frac{1}{2} = 0.5.$
- $\mu_A^R(4) = \frac{|\{4,6\}\cap\{1,5,7\}|}{|\{4,6\}|} = \frac{0}{2} = 0.$
- $\mu_A^R(5) = \frac{|\{2,5\}\cap\{1,5,7\}|}{|\{2,5\}|} = \frac{1}{2} = 0.5.$
- $\mu_A^R(6) = \frac{|\{4,6\}\cap\{1,5,7\}|}{|\{4,6\}|} = \frac{0}{2} = 0.$
- $\mu_A^R(7) = \frac{|\{3,7\}\cap\{1,5,7\}|}{|\{3,7\}|} = \frac{1}{2} = 0.5.$

Since $\mu_A^R(u) \notin \{0,1\}$ for some $u \in X$, the set $A = \{1,5,7\}$ is a rough set.

6 CONCLUSIONS

The research succeeded in building a bridge connecting algebraic and topological structures. We have constructed an approx. space derived from the Galois field $GF(2^n)$ generated through poly rings, and we also proved that the conjugacy relation that is an equivalence relation, and by applying the equivalence classes derived from the irreducible poly $(u^n + u + 1)$, we formed a mathematical basis for constructing the approx. space. The membership function provides a quantitative classification of the elements of subsets and its results are confined between 0 and 1. The membership function allows the classification of the sets of the approx. space into rough sets and exact sets. Consequently, the approx. space generated by $GF(2^n)$ contains only exact and rough sets, while the internally and externally defined sets are empty sets.

The computational results obtained from the application of the conjugacy relation on GFs $GF\ (2^2)$ and $GF\ (2^3)$ lead to several pivotal conclusions:

- Algebraic Structure Analysis: The conjugacy relation succeeded in both fields in classifying the algebraic elements into distinct and separate equivalence classes. It is worth noting that the granules of GF (2^2) are more precise and smaller, whereas the extension of GF (2^3) yielded a richer and more complex topological base. This further reinforces the validity and effectiveness of the proposed methodology as the degree of the irreducible poly increases.
- Interpretation of Ambiguity Regions and Membership: It is evident from applying the Rough Membership Function to both fields that it provides a precise quantitative measure for determining the degreeof uncertainty. It was found that the boundary regions BN(A) are closely and strictly governed by the conjugacy classes. Perhaps the most significant finding revealed by this paper is that the internally defined sets ID and the externally defined sets ED are empty sets for all tested subsets in both fields $GF\ (2^2)$ and $GF\ (2^3)$, and likewise when the degree of the field is greater than 3, the same result holds. This implies that the approx. space is perfectly partitioned, free from any undefined or vague elements.
- Distinguishing Advantages: Unlike standard rough set models, which often suffer from shortcomings in handling incomplete information systems, our algebraic model built on GF provides a precise topological structure. This is attributed to the inherent symmetry of the conjugacy relation within GF, which in contrast to standard models, leads to the isolation of non-empty ID or ED sets caused by data deficiencies.
- Practical Contribution: These results confirm the effectiveness of the topology founded on the conjugacy relation as a highly reliable framework in cryptography. The absence of ID or ED sets leads to complete certainty that every element involved in secure data transmission is either a precisely defined element (exact) or an element with clearly defined boundaries (rough), which is the fundamental requirement upon which the process of generating reliable encryption keys is based

REFERENCES

[1] Z. Pawlak, "Rough Sets," International Journal of Information and Computer Science, vol. 11, pp. 341-356, 1982, [Online]. Available: https://doi.org/10.1007/BF01001956.

[2] Z. Pawlak, Rough Sets: Theoretical Aspects of Reasoning About Data. Dordrecht: Kluwer Academic Publishers, 1991.

[3] W. Li, C. Fang, and W. Cao, "On the number of irreducible polynomials of special kinds in finite fields," AIMS Mathematics, vol. 5, no. 4, pp. 2877-2887, 2020, [Online]. Available: https://doi.org/10.3934/math.2020185.

[4] M. Abd-Ellatif and A. Ramadan, "Rough approximation of subgroup and conjugacy relation," Filomat, vol. 39, no. 18, pp. 6445-6452, 2025, [Online]. Available: https://doi.org/10.2298/FIL2518445A.

[5] A.D. Kumar, M. Vasuki, and R. Prabhakaran, "A Study on Finite Fields, Irreducible Polynomials," International Journal of Applied and Advanced Scientific Research, vol. 1, no. 1, pp. 85-93, 2016.

[6] J.B. Fraleigh, A First Course in Abstract Algebra. Pearson Education, India, 2003.

[7] G.T. Lee, Abstract Algebra: An Introductory Course. Springer, 2018.

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

[9] Y. Jiang, A Practical Guide to Error-Control Coding Using MATLAB. Norwood, MA: Artech House, 2010.

[10] T. Mora, Solving Polynomial Equation Systems. Cambridge: Cambridge University Press, 2003.

[11] D. Dikranjan and W. Tholen, Categorical Structure of Closure Operators: With Applications to Topology, Algebra and Discrete Mathematics. Dordrecht: Kluwer Academic Publishers, 1995.

[12] S. Elkhouli, A.A. Nasef, and M.A. Nasef, "Towards Pawlak Rough Approximations Theory with Applications," Journal of Contemporary Technology and Applied Engineering, vol. 3, no. 2, pp. 55-62, 2025, [Online]. Available: https://doi.org/10.21608/jctae.2025.354124.1040.

[13] Y.Y. Yao, "Two views of the theory of rough sets in finite universes," International Journal of Approximate Reasoning, vol. 15, no. 4, pp. 291-317, 1996, [Online]. Available: https://doi.org/10.1016/S0888-613X(96)00071-0.

[14] Z. Pawlak and A. Skowron, "Rough membership function," in Advances in the Dempster-Shafer Theory of Evidence, New York: Wiley, pp. 251-271, 1994.

[15] S.M. Wong and W. Ziarko, "Comparison of the probabilistic approximate classification and the fuzzy set model," Fuzzy Sets and Systems, vol. 21, no. 3, pp. 357-362, 1987, [Online]. Available: https://doi.org/10.1016/0165-0114(87)90135-7.

[16] Z. Pawlak, S.K.M. Wong, and W. Ziarko, "Rough sets: probabilistic versus deterministic approach," International Journal of Man-Machine Studies, vol. 29, no. 1, pp. 81-95, 1988.

[17] Y.Y. Yao, S.K.M. Wong, and P. Lingras, "A decision-theoretic rough set model," in Methodologies for Intelligent Systems, New York: Springer, pp. 17-24, 1990.