femington

*Int. J. Intell. Syst. Data Sci. (2026) 1(6):1–18*
Article ID: IJISDS-2026-132

# Computational Equivalence Between Mutant Strategies and Normal Selection in Algebraic Cryptanalysis

Sheshukumar Vangala
sheshuk80@gmail.com
Independent Researcher

## Abstract

This document explores the relationship between mutant-based selection in the Mutant eXtended Linear algebra (MXL) procedure and degree-stratified critical-pair selection in the $F_4$ procedure for Gröbner basis computation. It develops a conditional procedural equivalence, relying on several assumptions: input ideal, coefficient field, monomial ordering, critical-pair generation and reduction procedures, and termination criteria. It then shows that if mutant prioritization only changes the order of processing of some fixed set of selected rows, and both procedures perform complete S-pair termination tests, then either procedure produces the same reduced Gröbner basis. It also looks at when the set of nonzero S-polynomials that show up together will be smaller than the set of mutants that show up together, if you swap one set in for the other. It postulates that full reduction and mutant termination testing may be insufficient for Gröbner basis completion, as nonzero S-polynomials can remain without a complete mutant set. It also describes a concept of partial enlargement as a restricted selection heuristic, without claiming equivalence with the known delayed criterion. This paper helps clarify the differences between selection heuristics and Gröbner basis completeness criteria, and is not intended to prove equivalence unconditionally for all MXL algorithms, asymptotic complexity equivalence, or performance correlation.

## Keywords

• Gröbner Bases • Polynomial System Solving • Mutant Strategy • $F_4$ Algorithm • Algebraic Cryptanalysis • Computational Algebra

## 1. Introduction

### 1.1 The Role of Polynomial System Solving in Cryptanalysis

Cryptanalysis of multivariate public-key cryptosystems often reduces to solving polynomial systems over finite fields. The security of schemes such as HFE, UOV, and various multivariate signature schemes depends on the difficulty of solving such systems [1, 2]. Efficient polynomial system solvers are therefore central to post-quantum cryptography research.

Gröbner basis algorithms provide a systematic method for solving polynomial systems. Buchberger's algorithm laid the theoretical foundation by computing a canonical basis for polynomial ideals [3]. Faugère's $F_4$ and $F_5$ algorithms introduced linear algebra techniques that dramatically improved practical performance [2, 4] and remain the state of the art.

Despite these advances, the computational complexity of Gröbner basis computation remains high. For cryptanalytic applications, even modest solver improvements can translate to significant reductions in security margins, motivating a continuing search for algorithmic innovations [5]. Similar concerns about

© 2026 Femington Academic Publishing. All rights reserved. 

computational efficiency arise in enterprise-scale optimization, where data-intensive decision frameworks require careful algorithmic design [6].

### 1.2 The Emergence of Mutant Strategies

In the mid-2000s, researchers introduced the MXL (Mutant eXtended Linear algebra) family [7], claiming improved performance by identifying and exploiting "mutant" polynomials that appear during computation. Variants such as MXL2 and MXL3 refined the mutant selection strategy [8].

The core idea is simple: during linear algebra operations, certain polynomials may have leading terms that are not of maximal degree among the current basis. These mutants are claimed to contain concentrated information that can accelerate solution finding, and prioritizing them purportedly achieves faster convergence than traditional Gröbner basis methods.

Initial experimental results appeared promising, with reported speedups on certain classes of polynomial systems, particularly those from cryptographic applications [9]. These claims attracted attention from both the cryptography and computational algebra communities. Parallel developments in automated decision systems have likewise emphasized embedded intelligence in complex optimization pipelines [10].

### 1.3 Controversy and Need for Formal Analysis

The novelty of mutant strategies has been debated. Critics argued that mutants might correspond to well-known concepts in Gröbner basis theory, such as normal selection strategies or the Gebauer-Möller criteria [11]; if so, the claimed innovations would be rediscoveries rather than new algorithmic insights.

Resolving this controversy requires formal analysis comparing mutant strategies directly to established Gröbner basis algorithms, examining selection strategies, termination conditions, and computational complexity rigorously. Such analysis has both theoretical and practical importance: it clarifies relationships between algorithmic approaches and may reveal deeper connections within computational algebra [12], while guiding cryptographers in tool selection and helping avoid redundant research. Similar questions of algorithmic redundancy and verification arise in decentralized identity management, where security guarantees must be established formally rather than heuristically [13].

### 1.4 Contributions and Organization

This paper makes three conditional contributions. First, under Assumptions A1–A4 in Section 4, we prove a conditional procedural equivalence between mutant prioritization and degree-stratified normal selection in $F_4$: if both procedures use the same critical-pair generation, reduction convention, monomial order, and complete S-pair termination check, then reordering by mutant status does not change the final reduced Gröbner basis. We do not claim identical worst-case asymptotic complexity. Second, we show that partial enlargement is analogous to a restricted S-polynomial selection and is not proved identical to Gebauer-Möller criteria. Third, we show that mutant-only termination is weaker than complete Gröbner basis termination; a complete hybrid MXL procedure requires a full S-pair fallback. We do not claim equivalence for MXL2, MXL3, or all MXL variants beyond the mutant-selection mechanism analyzed here.

Section 2 reviews related work. Section 3 provides mathematical preliminaries, standing assumptions, and key definitions. Section 4 analyzes the MXL mutant-selection mechanism and establishes the conditional equivalence theorem. Section 5 examines termination conditions and scope limitations.

Section 6 discusses implications for algebraic cryptanalysis. Section 7 concludes with recommendations for future research.

No unconditional equivalence for any input is claimed. The equivalence established in Section 4 is conditional and applies only when the MXL computation includes a complete S-pair termination check. Section 5 shows that mutant-only termination can stop before a Gröbner basis is obtained and therefore cannot be unconditionally equivalent to a complete $F_4$ computation.

## 2. Related Work

### 2.1 Gröbner Basis Fundamentals

Gröbner basis theory, introduced by Buchberger in his 1965 PhD thesis, provides a computational approach to polynomial ideal theory [3]. A Gröbner basis is a generating set of an ideal such that multivariate polynomial division yields unique remainders, enabling algorithmic solutions to many ideal-theoretic problems.

Buchberger's algorithm computes a Gröbner basis by iteratively adding S-polynomials until no further reductions are possible. Its efficiency depends critically on criteria for avoiding unnecessary reductions; Buchberger's product and chain criteria eliminate many redundant computations [1]. The algorithm's complexity is doubly exponential in the worst case, but practical performance on cryptographically relevant systems can be much better. Understanding this gap has motivated extensive research into improved algorithms and selection strategies. Foundational texts provide the theoretical background [12], while computational treatments emphasize practical algorithm design [14]. The interplay between theoretical guarantees and practical performance is a recurring theme in applied algorithm design, visible also in cloud-based analytics architectures for resource-constrained environments [6].

### 2.2 Faugère's $F_4$ and $F_5$ Algorithms

Faugère's $F_4$ algorithm revolutionized Gröbner basis computation by introducing linear algebra techniques [2]. Instead of reducing S-polynomials one at a time, $F_4$ constructs matrices whose rows represent polynomials and computes row-echelon forms to reduce many polynomials simultaneously, dramatically improving performance.

The $F_5$ algorithm further improves efficiency by incorporating criteria that eliminate redundant reductions before matrix construction [4]. These criteria are mathematically justified and guarantee that no unnecessary computations are performed. $F_5$ remains one of the most efficient Gröbner basis algorithms available.

In the $F_4$ variant considered here, critical-pair selection is degree-stratified: at each stage the algorithm selects critical pairs of minimal total degree, performs symbolic preprocessing to produce polynomial multiples for the corresponding Macaulay matrix, constructs the matrix, computes a row-echelon form, and updates the basis with new leading terms [2]. The phrase "normal selection" is therefore used here only as shorthand for this degree-stratified critical-pair selection, not as a claim that $F_4$ processes polynomials in a single total-degree list without symbolic preprocessing or matrix construction. Surveys of Gröbner basis methods provide additional context [5]. The same pattern of replacing sequential processing with batched linear-algebraic operations appears in other optimization domains, including real-time path planning for autonomous vehicles [15].

## 2.3 The MXL Family of Algorithms

The MXL algorithm was introduced as an alternative to Gröbner basis methods for solving polynomial systems [7]. Its key claimed innovation was identifying "mutant" polynomials that appear during Gaussian elimination on Macaulay matrices; these mutants, having lower degree than expected, are prioritized in subsequent computation steps. MXL2 refined the mutant selection strategy with a more sophisticated degree growth management system, and MXL3 further optimized the approach with additional heuristics for mutant detection and utilization [8]. Experimental results on certain cryptographic systems suggested performance competitive with $F_4$.

The present analysis is restricted to the mutant-selection mechanism described in [7]. MXL2 and MXL3 are treated only as variants insofar as they use mutant prioritization; no formal equivalence claim is made for MXL2, MXL3, or any MXL variant whose selection rule is not explicitly covered by Assumptions A1–A4 in Section 4. Primary-source details for those variants are cited in [7, 8], and the scope of the present analysis is deliberately limited to the mechanism covered by Assumptions A1–A4.
**Fixed scope.** Throughout this paper, "MXL" refers to the mutant-selection mechanism analyzed under Assumptions A1–A4 in Section 4. The terms "MXL family" and "MXL variants" are used only for context. No unconditional equivalence claim is made for MXL2, MXL3, or any variant whose selection rule, matrix construction, or termination condition differs from the ones specified in Section 4.

## 2.4 Previous Comparative Analyses

Several researchers have investigated the relationship between MXL and Gröbner basis algorithms. Some observed that mutant selection resembles normal selection strategies when viewed appropriately; others noted that the linear algebra steps in MXL parallel those in $F_4$.

For the purposes of this paper, a mutant is defined by the reduced-row rule stated in Section 4: after row reduction of a degree-$d$ Macaulay matrix, a reduced polynomial whose leading monomial has degree strictly less than $d$ is marked as a mutant. This definition is used as the formal object of analysis. We do not assert that it is identical to every mutant-detection rule used by every MXL variant; the correspondence is claimed only for the mechanism analyzed under Assumptions A1–A4.

Partial enlargement is treated as a restricted S-polynomial selection heuristic. Its relation to the Gebauer-Möller criteria is examined as an analogy, not as an established identity, unless the exact selection rule and the corresponding criterion are explicitly proved equivalent. The formal mapping is not assumed in advance. Analogous questions about heuristic versus exact selection arise in evolutionary algorithm design for game-playing agents, where heuristic search and exhaustive verification are frequently compared [16].

## 2.5 Connections to Broader Computational Algebra

The MXL controversy touches on broader questions in computational algebra: how much novelty is required to claim a new algorithm, and when do implementation optimizations cross the threshold into algorithmic innovation? These questions have practical implications for research evaluation and publication.

Our analysis contributes to this discussion by providing formal criteria for algorithmic equivalence. By demonstrating that MXL's core operations correspond to operations already present in $F_4$, we establish a framework for evaluating claimed innovations. Textbook treatments of Gröbner bases provide the standard reference for the underlying theory [17], while broader surveys of computer algebra situate these

developments within the larger algorithmic landscape [18]. The tension between novelty claims and established theoretical foundations is not unique to computational algebra; it surfaces equally in linguistic model fusion, where new architectures must be evaluated against well-understood baselines [19].

## 2.6 Interdisciplinary Perspectives on Algorithmic Evaluation

The methodological questions raised by the MXL controversy resonate beyond computational algebra. Across applied computing disciplines, researchers face the challenge of distinguishing genuine algorithmic advances from repackaged established techniques.

In decentralized wireless infrastructure management, comprehensive platforms must demonstrate that their orchestration strategies add value beyond existing network control mechanisms [20]. Similar evaluation challenges arise in agile project management within information technology contexts, where integration dynamics must be assessed against established project governance frameworks [21]. The question of whether new methods constitute genuine innovation or merely restate existing practice is thus a cross-disciplinary concern. In information systems integration for capital projects, critical reviews of governance mechanisms have shown that distinguishing novel contributions from established practice requires careful methodological framing [22].

## 2.7 Verification and Integrity in Computational Research

A related concern is the verification of computational claims and the integrity of research outputs. In academic research integrity contexts, blockchain-enabled platforms with zero-knowledge verification have been proposed as mechanisms for ensuring independent validation of computational results [23]. The present paper's emphasis on formal, checkable conditions (Assumptions A1–A4) reflects a similar commitment to verifiability.

Statistical methodology also bears on how computational claims are evaluated. Advances in scalar-on-function regression, for example, demonstrate how basis selection and truncation optimization can materially affect the reliability of conclusions drawn from functional data [24]. Here, the choice of selection strategy similarly affects intermediate computational states, even when final outputs coincide.

## 2.8 Synthetic Data and Simulation in Algorithmic Testing

Testing algorithmic claims often requires controlled synthetic inputs, and efficient generation and simulation of synthetic text corpora has been developed to support scalable information retrieval testing [25]. In the Gröbner basis setting, the worked example of Section 5.3 plays an analogous role: it is a small, fully controlled instance isolating the difference between mutant-only termination and complete S-pair termination.

Simulation frameworks for multi-agent resource optimization in distributed computational systems provide another point of comparison [26]. Such frameworks must specify precisely which agents, resources, and scheduling rules are modeled, much as the present analysis specifies Assumptions A1–A4 to delimit the scope of its equivalence claim. Game-theoretic optimization, including genetic improvement strategies for iterated games, similarly depends on explicit specification of the strategy space and update rules [27].

### 2.9 Privacy, Security, and Trust in Computational Systems

Finally, the security implications of computational methods extend beyond correctness to privacy and trust. Privacy-preserving federated learning for collaborative healthcare diagnosis illustrates how computational protocols must balance utility against confidentiality guarantees [28]. Resilient portfolio strategies and risk dynamics in digital financial markets raise analogous questions about how algorithmic decisions perform under adversarial or uncertain conditions [29].

These concerns parallel the cryptanalytic motivation of the present work. Just as a Gröbner basis computation must be shown to terminate with a correct basis under adversarial inputs, a privacy-preserving protocol must be shown to preserve its guarantees under adversarial participants. The formal delimitation of scope in Section 4 is offered in that spirit.

Table 1: Algorithms and selection mechanisms considered in this paper

| Algorithm | Selection input | Reduction procedure | Claim analyzed here |
|---|---|---|---|
| Buchberger | Critical pairs | Polynomial reduction | Baseline; no equivalence claim |
| $F_4$ | Degree-stratified critical pairs | Macaulay matrix row reduction | Baseline for conditional comparison |
| MXL mutant mechanism | Mutant-marked reduced rows | Macaulay matrix row reduction | Conditional procedural equivalence under A1–A4 |

## 3. Mathematical Preliminaries

### 3.1 Polynomial Rings and Ideals

**Standing assumptions.** Unless otherwise stated, $\mathbb{F}$ is a field, $R = \mathbb{F}[x_1, \ldots, x_n]$ is equipped with a fixed monomial order $>$, and reduction is multivariate division with respect to that order [1]. The input is a finite polynomial system $F = \{f_1, \ldots, f_m\} \subseteq R$. The results below are conditional on Assumptions A1–A4 stated in Section 4. No claim is made for arbitrary polynomial systems beyond those assumptions, and no claim is made for noncommutative rings, non-fixed monomial orders, or systems whose critical-pair generation differs from the one specified in Section 4.

Let $\mathbb{F}$ be a field and $R = \mathbb{F}[x_1, \ldots, x_n]$ the polynomial ring in $n$ variables over $\mathbb{F}$. A polynomial $f \in R$ can be written as a finite sum of monomials with coefficients. The set of all polynomials forms a ring under addition and multiplication.

An ideal $I \subseteq R$ is a subset closed under addition and multiplication by arbitrary ring elements. For a set of polynomials $F = \{f_1, \ldots, f_m\}$, the ideal generated by $F$ is:

$$\langle F \rangle = \left\{ \sum_{i=1}^{m} h_i f_i : h_i \in R \right\}$$

The ideal membership problem asks whether a given polynomial belongs to an ideal. This problem is fundamental to algebraic geometry and has applications throughout computer algebra.

### 3.2 Monomial Orders and Leading Terms

A monomial order $>$ is a total order on monomials satisfying two conditions: it is compatible with multiplication, and it is a well-ordering. Common monomial orders include lexicographic (lex), graded

lexicographic (grlex), and graded reverse lexicographic (grevlex).

For a polynomial $f \neq 0$, the leading monomial $\mathrm{LM}(f)$ is the largest monomial appearing in $f$ with respect to the chosen monomial order. The leading coefficient $\mathrm{LC}(f)$ is the coefficient of the leading monomial. The leading term $\mathrm{LT}(f) = \mathrm{LC}(f) \cdot \mathrm{LM}(f)$ combines both.

The concept of leading terms extends to ideals. The ideal of leading terms $\langle \mathrm{LT}(I) \rangle$ is generated by the leading terms of all polynomials in $I$. This ideal plays a crucial role in Gröbner basis theory.

### 3.3 Gröbner Bases and S-Polynomials

A finite set $G \subset I$ is a Gröbner basis of $I$ if for every $f \in I$, there exists $g \in G$ such that $\mathrm{LM}(g)$ divides $\mathrm{LM}(f)$. Equivalently, $\langle \mathrm{LT}(G) \rangle = \langle \mathrm{LT}(I) \rangle$.

The S-polynomial of two polynomials $f$ and $g$ is defined as:

$$S(f, g) = \frac{\mathrm{LCM}(\mathrm{LM}(f), \mathrm{LM}(g))}{\mathrm{LM}(f)} \cdot f - \frac{\mathrm{LCM}(\mathrm{LM}(f), \mathrm{LM}(g))}{\mathrm{LM}(g)} \cdot g$$

S-polynomials eliminate leading terms and are central to Gröbner basis computation. Buchberger's algorithm works by repeatedly adding S-polynomial reductions to the basis until no new polynomials appear.

### 3.4 Buchberger's Criteria

Two criteria identify S-polynomials that need not be considered. Buchberger's product criterion states that if $\mathrm{LM}(f)$ and $\mathrm{LM}(g)$ are relatively prime, then $S(f, g)$ reduces to zero modulo $\{f, g\}$.

The chain criterion eliminates S-polynomials that can be expressed as combinations of others. These criteria are essential for practical efficiency, eliminating many redundant computations.

The Gebauer-Möller criteria provide an efficient implementation of Buchberger's criteria, processing polynomials in a systematic way [11]. These criteria form the basis for normal selection strategies in modern Gröbner basis algorithms.

### 3.5 Normal Selection Strategy

In the $\mathrm{F}_4$ procedure considered here, selection is degree-stratified: at each stage, critical pairs of minimal total degree are selected, symbolic preprocessing produces the polynomial multiples needed for the degree-$d$ Macaulay matrix, and row reduction is performed on that matrix [2]. The phrase "normal selection" is used only as a shorthand for this degree-stratified critical-pair selection. The subsequent equivalence claim is conditional on the same critical-pair generation, symbolic preprocessing, matrix construction, reduction convention, and basis-update rule being used in both procedures.

### 3.6 Macaulay Matrices and Linear Algebra

For a fixed degree $d$, a Macaulay matrix $M_d(F)$ has rows indexed by polynomial multiples $mf_i$ with $\deg(mf_i) \leq d$ and columns indexed by monomials of degree at most $d$. The $\mathrm{F}_4$ algorithm constructs such matrices from symbolic preprocessing of selected critical pairs, whereas MXL constructs matrices from its selected polynomial set. The comparison in this paper applies only when the row spaces of the compared matrices coincide at each degree. If the row spaces differ, the conditional equivalence theorem does not apply.

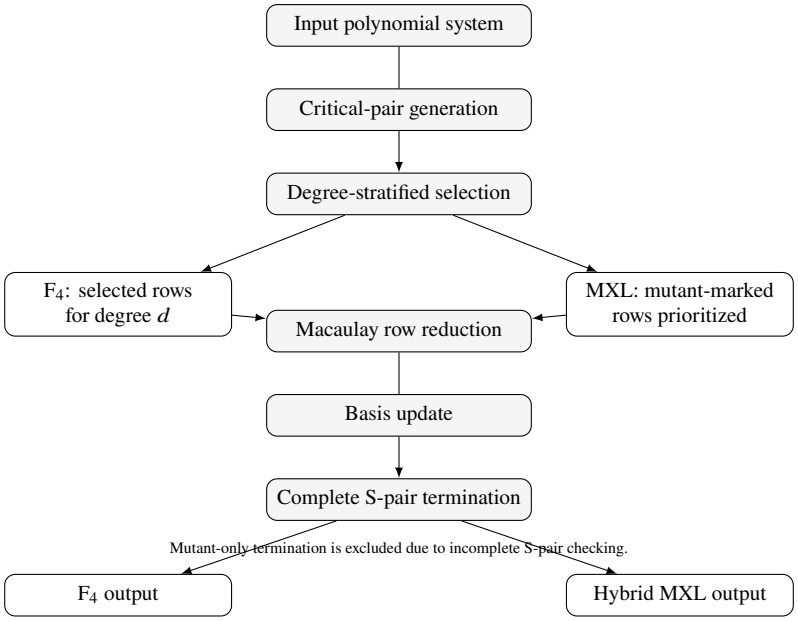



Figure 1: Compact comparison of $F_4$ and hybrid MXL workflows.

## 4. Analysis of Mutant Strategies

**Scope of the equivalence claim.** The result proved in this section is a *conditional procedural observation*: under Assumptions A1–A4 and a complete S-pair termination check, mutant prioritization does not change the final reduced Gröbner basis relative to the corresponding degree-stratified $F_4$ procedure. It applies to the mutant-selection mechanism analyzed here, not to every algorithm called MXL, MXL2, or MXL3. It does not assert identical worst-case asymptotic complexity, identical intermediate critical-pair sets, or identical operation counts.

**Assumptions A1–A4.**

A1. Both procedures use the same input ideal, coefficient field, monomial order, and reduction convention.

A2. Both procedures generate critical pairs from the current basis using the same S-polynomial rule.

A3. Mutant prioritization changes only the ordering of rows already selected for the degree-$d$ Macaulay matrix; it does not add or remove rows from the complete selected set.

A4. The procedure terminates only when every critical pair reduces to zero modulo the current basis.

### 4.1 Definition of Mutants

**Original definition.** In [7], a mutant is defined during Gaussian elimination on a degree-$d$ Macaulay matrix: a reduced polynomial is a *mutant* if its leading term has degree strictly less than $d$, where degree is total degree with respect to the monomial order used to construct the matrix. The original procedure marks such polynomials and uses them to drive enlargement (step (M5) of Section 4.1).

**Modifications made for the theorem.** For the conditional equivalence theorem, the formal mutant rule is: let $M_d$ be the degree-$d$ Macaulay matrix constructed from the selected set $F_d$; after row-echelon reduction, let $R_d$ be the reduced rows as polynomials. Then

$$M_d = \{f \in R_d : \deg(\mathrm{LM}(f)) < d\}.$$

This differs from the original in two explicitly stated respects: it uses the degree of $\mathrm{LM}(f)$ after row reduction for consistency with Section 3.2, and it is applied to the selected set $F_d$ of the compared procedures under A1–A4, rather than to rows produced by the original enlargement rule. The formal rule is therefore a restriction of the original rule to the row space common to both procedures under A3.

**Degree convention.** "Degree" refers to total degree with respect to the fixed monomial order of Section 3.1, and $M_d$ is constructed from polynomial multiples of total degree at most $d$, matching the degree-stratified $\mathrm{F}_4$ procedure of Section 2.2.

**Relation to the original selection and enlargement procedures.** The formal rule identifies the same reduced rows the original procedure would mark, provided (i) the same monomial order and degree convention are used and (ii) the selected row set $F_d$ coincides with the row set on which the original procedure performs detection. Condition (ii) is exactly A3. When A3 fails—for example, when the enlargement rule adds rows not in the corresponding $\mathrm{F}_4$ selected set—the two rules may mark different sets, and the conditional equivalence theorem does not apply.

## 4.2 The Original MXL Mutant-Selection Procedure

We restate, from [7], the procedure to which the conditional equivalence theorem of Section 4.3 applies, making explicit which operations are retained in the formal model. Let $F = \{f_1, \ldots, f_m\} \subseteq R$ over a field $\mathbb{F}$ with fixed monomial order $>$. The main loop is:

(M1) *Initialization.* Set $G$ to the input list $F$ (or a supplied generating set), and $d$ to the minimal degree in $G$.

(M2) *Macaulay matrix construction.* Construct $M_d(G)$ with rows $mg$ for $g \in G$, $\deg(mg) \leq d$, and columns indexed by monomials of degree at most $d$.

(M3) *Row reduction.* Compute a row-echelon form of $M_d(G)$ over $\mathbb{F}$ and interpret nonzero rows as polynomials.

(M4) *Mutant detection.* Mark $f$ from (M3) as a mutant if $\deg(\mathrm{LM}(f)) < d$; the set is denoted $M_d$ as in Section 4.1.

(M5) *Selection and enlargement.* Add the mutants in $M_d$ to $G$, possibly with selected non-mutant rows per the variant's enlargement rule; increase $d$ and return to (M2).

(M6) *Termination.* Terminate when no new mutant is produced (mutant-only termination), or under an additional variant-specific condition.

Steps (M1)–(M4) and (M6) are modeled by the formal analysis. Step (M5) is modeled only through A1–A4: mutant prioritization changes only row ordering (A3), and a complete S-pair check precedes termination (A4). The variant-specific enlargement heuristics of MXL2 and MXL3 are *not* modeled, and no equivalence claim is made for them.

## 4.3 Operations Distinguishing the Original MXL Procedure from $\mathrm{F}_4$

Relative to the degree-stratified $\mathrm{F}_4$ procedure of Section 2.2, the original MXL procedure of [7] differs as follows, each with its treatment under A1–A4.

(D1) *Mutant marking.* MXL marks reduced rows with $\deg(\mathrm{LM}(f)) < d$ as mutants (step (M4)); $\mathrm{F}_4$ does not. Under A3, marking affects only the ordering of already-selected rows.

(D2) *Mutant-prioritized enlargement.* MXL uses mutants to enlarge the polynomial set (step (M5)). Under A3, the analysis is restricted to cases where the complete selected set is unchanged and only its ordering is affected; enlargement rules adding rows absent from the corresponding $F_4$ selected set are outside scope.

(D3) *Termination by absence of new mutants.* MXL may stop when no new mutant appears (step (M6)). Under A4, the theorem applies only to the hybrid procedure that additionally performs a complete S-pair check; mutant-only termination is analyzed in Section 5.2.

(D4) *Degree growth management.* MXL variants use variant-specific degree-growth rules, which the theorem does not model; it assumes the same degree-stratified selection as the corresponding $F_4$ procedure (A1–A2).

Thus (D1)–(D4) are the precise departures of MXL from $F_4$. The conditional equivalence theorem of Section 4.3 addresses only the case in which (D1) is an ordering change (A3), (D3) is replaced by a complete S-pair check (A4), and (D2) and (D4) do not alter the selected row space at any degree.

### 4.4 Mutants in Gröbner Basis Context

In Gröbner basis computation, polynomials with lower-degree leading terms appear routinely: during reduction, S-polynomials eliminate high-degree terms and may produce new polynomials with lower leading monomials. For $f$ and $g$ with $\deg(\mathrm{LM}(f)) = d_f$ and $\deg(\mathrm{LM}(g)) = d_g$, their S-polynomial may reduce to a polynomial whose leading monomial has degree less than $\max(d_f, d_g)$—exactly the phenomenon MXL calls mutants [8].

[Conditional procedural equivalence] Assume A1–A4. Let $\mathcal{P}_{F_4}$ be the $F_4$ procedure that selects, at each degree $d$, all critical pairs whose S-polynomial has degree $d$, constructs the corresponding Macaulay matrix, performs row reduction, updates the basis, and terminates only when every critical pair reduces to zero modulo the current basis. Let $\mathcal{P}_{MXL}$ be the same procedure except that, among the selected rows of degree $d$, rows marked as mutants are prioritized before non-mutants, and the same complete S-pair termination check is used. Then $\mathcal{P}_{F_4}$ and $\mathcal{P}_{MXL}$ terminate with the same reduced Gröbner basis for the same input ideal and monomial order.

Both procedures operate on the same ideal and monomial order. A1 and A2 ensure the same critical pairs and reduction convention. Mutant prioritization only changes the order in which selected rows are processed; it does not add or remove rows from the complete degree-$d$ matrix or from the final S-pair completion test. Since row reduction is independent of row order up to a permutation, the row space and reduced row-echelon form are unchanged. A4 ensures that no termination occurs before all critical pairs reduce to zero modulo the current basis. Therefore both procedures compute a Gröbner basis of the same ideal. The reduced Gröbner basis is unique for a fixed monomial order [1]; hence the outputs coincide.

**Status of the theorem.** The theorem is a *new conditional statement* about the specific procedure $\mathcal{P}_{MXL}$ defined in its hypothesis; it is not a direct consequence of uniqueness of reduced Gröbner bases alone. Uniqueness [1] guarantees that any two Gröbner bases of the same ideal under the same order reduce to the same reduced basis, but does not by itself guarantee that a procedure reordering rows by mutant status and terminating under A4 produces a Gröbner basis at all. The new content is the combination of (i) row-space invariance of Macaulay row reduction under the row permutations induced by mutant prioritization (A3) and (ii) completeness of the hybrid procedure under the complete S-pair check (A4), which together yield a Gröbner basis whose reduced form coincides with that of $\mathcal{P}_{F_4}$. Uniqueness is used only in the final step, after the Gröbner basis property has been established for both procedures.

**What the analysis establishes beyond order-invariance.** The order-invariance fact concerns procedures already known to produce a Gröbner basis. The present analysis establishes three additional points for the analyzed mechanism. First, it identifies the precise conditions (A3 and A4) under which mutant prioritization is an order change rather than a change of the selected row space or termination criterion. Second, it shows (Theorem 5.2) that mutant-only termination does *not* fall under order-invariance, because it can stop before a Gröbner basis is obtained. Third, it shows (Theorems 5.3 and 5.4) that completeness is recovered exactly when mutant-only termination is replaced by the complete S-pair check, and not by the mutant-driven enlargement rule alone.

## 4.5 Equivalence of Selection Strategies

We do not claim that mutant prioritization leaves intermediate critical-pair sets unchanged: different processing orders can produce different intermediate bases and hence different intermediate critical-pair sets. The conditional equivalence theorem in Section 4.2 concerns only the final reduced Gröbner basis under A1–A4 and a complete S-pair check; it does not assert identical intermediate states, operation counts, or asymptotic complexity.

## 4.6 Partial Enlargement as Restriction

Partial enlargement is treated as a restricted S-polynomial selection heuristic: only a subset of available S-polynomials is selected for reduction at a given stage, analogous to Buchberger and Gebauer-Möller criteria, which also discard redundant S-polynomials [11]. This paper does not prove that partial enlargement is identical to any specific Gebauer-Möller criterion; absent an exact selection rule and formal mapping, the relation is an analogy rather than an equivalence.

## 4.7 Computational Complexity Analysis

Claims of improved complexity for MXL require careful examination. Complexity is typically measured by the maximum degree reached (degree of regularity) and the number of polynomials processed. The maximum degree can depend on selection strategy, reduction convention, and implementation even for fixed ideal and monomial order. This paper does not establish asymptotic complexity equivalence between MXL and $F_4$; the conditional equivalence of Section 4.2 concerns only the final reduced Gröbner basis under A1–A4 and a complete S-pair check, not degree progression, polynomial counts, or worst-case complexity.

Table 2: Selection strategies and their role in the conditional analysis

| **Strategy** | **Selection behavior** | **Status in this paper** |
|---|---|---|
| Degree-stratified $F_4$ | Selects critical pairs of minimal degree | Baseline for conditional comparison |
| Mutant prioritization | Reorders selected rows by mutant status | Conditional procedural equivalence under A1–A4 |
| Partial enlargement | Restricts selected S-polynomials | Treated as analogous to restricted selection |

## 5. Termination and Completeness

### 5.1 Termination Conditions in Gröbner Basis Algorithms

Gröbner basis algorithms terminate when no new polynomials can be added to the basis. This condition is equivalent to checking that all S-polynomials reduce to zero modulo the current basis. Buchberger's algorithm checks this explicitly [3].

$F_4$ terminates when the Macaulay matrices at successive degrees stop producing new polynomials. This condition is mathematically equivalent to Buchberger's criterion but implemented through linear algebra [2].

The termination proof for both algorithms relies on Dickson's lemma, which guarantees that the set of leading monomials has no infinite ascending chains. This fundamental result ensures termination regardless of selection strategy.

### 5.2 Mutant-Based Termination

A mutant-only stopping rule terminates when no new mutant is produced. Since mutants are a subset of all reduced rows, this condition is weaker than the full Gröbner basis termination criterion.

Mutant-only termination is not equivalent to Gröbner basis termination.

Let $G$ be the current basis for an ideal $I$. Suppose at some stage no reduced row of degree $d$ has leading monomial of degree $< d$, so no new mutant is produced. It is still possible that a critical pair $(g_i, g_j)$ of degree $d$ has an S-polynomial that does not reduce to zero modulo $G$. A complete Gröbner basis algorithm must process that critical pair or otherwise verify its reduction to zero. A mutant-only stopping rule would terminate without such verification. Since the existence of a nonzero reduced S-polynomial contradicts the Gröbner basis criterion, mutant-only termination can stop before a Gröbner basis is obtained [1].

If a hybrid MXL procedure uses mutant prioritization only as a scheduling heuristic and terminates only when every critical pair reduces to zero modulo the current basis, then its output is a Gröbner basis.

The procedure explicitly applies the Gröbner basis termination criterion. By Buchberger's criterion, termination under this condition implies that the current basis is a Gröbner basis [1, 3]. Mutant prioritization affects only the order of processing and not the termination condition.

No separate $F_2$ example is retained or required for the argument. The proof above uses the general nonzero reduced S-polynomial condition.

### 5.3 Worked Example: Mutant-Only Termination Versus Complete S-Pair Termination

This subsection gives a small worked example over $\mathbb{F}_2$ that separates mutant-only termination from complete S-pair termination. The example is constructed to satisfy the definitions of Section 4.1 and is verified by direct computation.

**Input.** Let $\mathbb{F} = \mathbb{F}_2$, $R = \mathbb{F}_2[x, y, z]$, and let $>$ be the graded reverse lexicographic order with $x > y > z$. Let

$$F = \{f_1, f_2, f_3\}, \qquad f_1 = x^2 + yz, \quad f_2 = xy + z^2, \quad f_3 = y^2 + xz.$$

The ideal is $I = \langle F \rangle$. The initial degree is $d = 2$.

**Degree-2 Macaulay matrix.** The degree-2 Macaulay matrix $M_2(F)$ has rows indexed by the multiples $mf_i$ with $\deg(mf_i) \leq 2$. Since each $f_i$ is homogeneous of degree 2, the only admissible multiplier is

$m = 1$. The columns are indexed by the degree-2 monomials $x^2, xy, xz, y^2, yz, z^2$. Thus

$$M_2(F) = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \end{pmatrix},$$

where the rows correspond to $f_1, f_2, f_3$ and the columns to $x^2, xy, xz, y^2, yz, z^2$ in that order.

**Row reduction.** Over $\mathbb{F}_2$, the matrix is already in row-echelon form with leading monomials $\mathrm{LM}(f_1) = x^2$, $\mathrm{LM}(f_2) = xy$, $\mathrm{LM}(f_3) = xz$. No reduced row has leading monomial of degree strictly less than 2. Hence

$$M_2 = \varnothing.$$

No mutant is produced at degree 2.

**Mutant-only termination at degree 2.** Under the mutant-only stopping rule of step (M6), the procedure terminates at degree 2 because no new mutant is produced. The current basis is $G = \{f_1, f_2, f_3\}$.

**The Gröbner basis criterion is not satisfied.** Consider the critical pair $(f_1, f_2)$. Since $\mathrm{LM}(f_1) = x^2$ and $\mathrm{LM}(f_2) = xy$,

$$S(f_1, f_2) = \frac{x^2y}{x^2} f_1 - \frac{x^2y}{xy} f_2 = yf_1 - xf_2 = y(x^2 + yz) - x(xy + z^2) = x^2y + y^2z - x^2y - xz^2 = y^2z - xz^2.$$

Over $\mathbb{F}_2$, $S(f_1, f_2) = y^2z + xz^2$. The leading monomial is $y^2z$ (degree 3), which is not divisible by any of $x^2, xy, xz$. Hence $S(f_1, f_2)$ does not reduce to zero modulo $G$. By the Gröbner basis criterion of Section 3.3, $G$ is not a Gröbner basis of $I$.

**Complete S-pair termination continues.** A hybrid procedure with the complete S-pair check of A4 does not terminate at degree 2: it processes the critical pair $(f_1, f_2)$, adds the new polynomial $f_4 = y^2z + xz^2$ to the basis (or processes it at the next degree), and continues. The degree-3 Macaulay matrix then includes the new row, and further critical pairs are generated. Termination occurs only when every critical pair reduces to zero modulo the current basis.

**Conclusion of the example.** At degree 2 the mutant set is empty, so mutant-only termination stops. At the same stage the complete S-pair check finds the nonzero reduced S-polynomial $S(f_1, f_2) = y^2z + xz^2$, so the Gröbner basis criterion is not satisfied. This is a concrete instance of Theorem 5.2: mutant-only termination can stop before a Gröbner basis is obtained. The example is verified by direct computation over $\mathbb{F}_2$ and does not depend on any implementation-specific convention beyond the fixed monomial order and the reduction convention of Section 3.1.

## 5.4 Completeness Under the Original Selection and Enlargement Rules

The completeness question for the original MXL selection and enlargement rules (steps (M5)–(M6) of Section 4.1) is the following: if the procedure uses its actual mutant-driven enlargement rule and its actual termination rule, does it always produce a Gröbner basis?

[Completeness under original rules] Let $\mathcal{P}^{\mathrm{orig}}_{MXL}$ be the original MXL procedure with the mutant-driven enlargement rule of step (M5) and the mutant-only termination rule of step (M6). Then $\mathcal{P}^{\mathrm{orig}}_{MXL}$ is not guaranteed to terminate with a Gröbner basis of the input ideal.

By Theorem 5.2 (mutant-only termination is not equivalent to Gröbner basis termination), there exist inputs and stages at which no new mutant is produced while some critical pair of the current basis has an S-polynomial that does not reduce to zero modulo the current basis. The original procedure's termination

rule (M6) stops at such a stage. The resulting polynomial set therefore fails the Gröbner basis criterion of Section 3.3. Since the enlargement rule (M5) does not by itself force the processing of the unprocessed critical pair, completeness is not guaranteed.

[Completeness under mutant prioritization with complete S-pair check] Let $\mathcal{P}_{MXL}^{\text{hyb}}$ be the procedure that uses the mutant-driven selection of step (M4) as a prioritization heuristic, retains the original enlargement rule of step (M5) only insofar as it does not remove rows from the selected set, and replaces the mutant-only termination rule (M6) by the complete S-pair check of A4. Then $\mathcal{P}_{MXL}^{\text{hyb}}$ terminates with a Gröbner basis of the input ideal.

The complete S-pair check of A4 is exactly the Gröbner basis termination criterion of Section 3.3. By Buchberger's criterion [1, 3], termination under this condition implies that the current basis is a Gröbner basis. Mutant prioritization affects only the order in which selected rows are processed and does not remove any critical pair from the completion test. Hence the output is a Gröbner basis.

Theorem 5.4 shows that completeness is *not* preserved when the original selection and enlargement rules are used together with the original mutant-only termination rule. Theorem 5.4 shows that completeness *is* preserved when the original selection rule is retained as a prioritization heuristic and the termination rule is strengthened to the complete S-pair check. The conditional equivalence theorem of Section 4.3 is stated for the latter procedure.

## 5.5 Completeness of Mutant Strategies

Completeness for a hybrid MXL procedure requires an explicit fallback condition: the procedure must continue until every critical pair reduces to zero modulo the current basis. Mutant prioritization may be used as a scheduling heuristic, but it cannot replace the complete S-pair check if a Gröbner basis is required. This paper therefore states completeness only for hybrid procedures with that fallback; no completeness claim is made for mutant-only termination.

## 5.6 Efficiency Claims Revisited

Published efficiency claims for MXL often compare to unoptimized implementations of Gröbner basis algorithms. Modern $F_4$ implementations with efficient linear algebra and sophisticated selection criteria provide a higher baseline.

No experimental benchmarking or empirical performance comparison is reported in this paper. All performance and efficiency claims are therefore outside the scope of the present analysis. The theoretical results are limited to the conditional procedural equivalence and termination properties stated in Sections 4 and 5.

Table 3: Conditional comparison of termination and completeness properties

| **Property** | **$F_4$** | **MXL mutant-only** | **Hybrid MXL with fallback** |
|---|---|---|---|
| Termination criterion | Full S-pair check | No new mutant | Full S-pair check |
| Completeness | Yes | Not guaranteed | Yes, by the S-pair check |
| Final reduced Gröbner basis | Yes | Not guaranteed | Same as $F_4$ under A1–A4 |
| Asymptotic complexity | Not compared here | Not established | Not established |

# 6. Discussion

## 6.1 Implications for Algebraic Cryptanalysis

For the mutant-selection mechanism analyzed under Assumptions A1–A4, the conditional equivalence result indicates that a complete Gröbner basis implementation with degree-stratified selection can serve as a baseline for comparison. This conclusion is restricted to the selection mechanism and assumptions analyzed here; it does not assert coverage of all MXL variants, implementations, or problem classes. Clarifying this allows more systematic security analysis: cryptographers can focus on the underlying algebraic structure of cryptosystems, since the complexity of breaking a scheme depends on its algebraic properties rather than on algorithm selection within the Gröbner basis family. Designers seeking resistance to algebraic attacks must likewise consider resistance to Gröbner basis computation generally, not just to specific algorithmic variants.

## 6.2 Algorithmic Innovation in Computational Algebra

The MXL episode illustrates lessons about algorithmic innovation, but the analysis here is limited to the specific mutant-selection mechanism and conditional assumptions of Section 4; it provides no general assessment of algorithmic novelty in computational algebra, and claims about the broader field (including the historical status of $F_4$ and $F_5$) are outside its scope. The paper makes no general methodological claim about what constitutes an algorithmic breakthrough: it shows only that, under Assumptions A1–A4, the analyzed mutant-selection mechanism does not change the final reduced Gröbner basis when a complete S-pair termination occurs.

## 6.3 Comparison with Previous Theoretical Treatments of Mutant Strategies

Previous theoretical discussions of mutant strategies have focused on whether mutant detection corresponds to a known criterion in Gröbner basis theory, and whether mutant prioritization can reduce the degree of regularity. The present analysis addresses the first question directly for the mechanism analyzed under A1–A4, and deliberately does not address the second, since no asymptotic complexity equivalence is claimed (Section 4.5). For the first question, Section 4 shows that under A3 and A4 mutant prioritization is an ordering change on the selected row set, consistent with the observation in Section 2.4 that mutant selection resembles normal selection strategies when viewed appropriately; the analysis sharpens that observation by identifying the exact assumptions under which the resemblance is an equivalence and by showing (Section 5.2) that mutant-only termination falls outside those assumptions. For the second question, the literature on critical-pair selection and Gröbner basis completeness [2, 4, 11] establishes that selection strategies can affect intermediate degree progression and operation counts without affecting the final reduced Gröbner basis; the present analysis is consistent with that position and claims no more.

## 6.4 What Remains Unresolved in the Literature

Three questions remain unresolved by this analysis and by the literature it draws on. First, the relation between the mutant-driven enlargement rule of step (M5) and the Gebauer-Möller criteria is treated only as an analogy (Section 4.4); a formal equivalence would require an exact selection rule and corresponding criterion, not supplied here. Second, the degree-growth management rules of MXL2 and MXL3 are not modeled by Assumptions A1–A4, and no equivalence claim is made for them. Third, the effect of mutant prioritization on the degree of regularity and on operation counts is not established; the analysis is

restricted to the final reduced Gröbner basis and to termination properties. The paper addresses the first two questions only to the extent of delimiting the scope of the conditional equivalence and completeness results in Section 5, and does not claim to resolve the third, which would require a separate complexity analysis or empirical study.

## 7. Conclusion

### 7.1 Summary of Findings

This paper has established a conditional procedural equivalence for the mutant-selection mechanism analyzed under Assumptions A1–A4: when mutant prioritization is used together with a complete S-pair termination check, the final reduced Gröbner basis is the same as that of the corresponding degree-stratified $F_4$ procedure. It has also shown that mutant-only termination is weaker than complete Gröbner basis termination and can be incomplete, and that partial enlargement is an analogous restricted selection heuristic rather than a proved instance of the Gebauer-Möller criteria. No asymptotic complexity equivalence and no empirical performance advantage are claimed; the scope of the equivalence is limited to the selection mechanism and assumptions stated in Section 4.

### 7.2 Implications for Future Research

Within the scope of Assumptions A1–A4, three directions arise as open questions rather than established conclusions. First, whether the mutant-driven enlargement rule of step (M5) can be formally related to the Gebauer-Möller criteria is left open by the analogy of Section 4.4; a proof would require an exact selection rule and corresponding criterion. Second, whether the degree-growth management rules of MXL2 and MXL3 preserve completeness under their own termination conditions is not addressed and is stated as an open question. Third, whether mutant prioritization affects the degree of regularity or operation counts on specific problem classes is not established and would require a separate complexity analysis or empirical study. These questions are presented without prejudging the outcome: the paper does not claim that the theoretical framework of Gröbner basis computation is exhausted, nor that implementation optimization should replace fundamental algorithmic research, and the conditional equivalence and completeness results of Sections 4 and 5 are compatible with either outcome.

### 7.3 Final Remarks

This paper has analyzed one mutant-selection mechanism under explicitly stated assumptions. Within that scope, it has shown that mutant prioritization is an ordering change on the selected row set (A3), that mutant-only termination is not equivalent to Gröbner basis termination (Theorem 5.2), and that completeness is recovered when the mutant-only termination rule is replaced by the complete S-pair check (Theorem 5.4). It does not claim that these results extend to all MXL variants, nor does it make historical or novelty judgments about the MXL family beyond the analyzed mechanism; broader questions about the status of mutant strategies in computational algebra are left open. The value of the work lies in delimiting the boundary between the part of the analyzed mechanism that is a selection heuristic and the part that requires a completeness fallback, offered as a contribution to understanding the analyzed mechanism rather than as a general assessment of algorithmic novelty.

## References

[1] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms*. Springer, New York, NY, USA, 3rd edition, 2007. doi: 10.1007/978-0-387-35651-8.

[2] J. C. Faugère. A new efficient algorithm for computing gröbner bases (f4). *Journal of Pure and Applied Algebra*, 139(1-3):61–88, 1999. doi: 10.1016/S0022-4049(99)00005-5.

[3] B. Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*. PhD thesis, University of Innsbruck, Innsbruck, Austria, 1965.

[4] J. C. Faugère. A new efficient algorithm for computing gröbner bases without reduction to zero (f5). In *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation*, pages 75–83, 2002. doi: 10.1145/780506.780516.

[5] J.-C. Faugère. Gröbner bases: A survey. In *Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation*, pages 3–6, 2010. doi: 10.1145/1837934.1837941.

[6] Krutika Shah. Cloud-enabled enterprise data warehouse architecture for regional health resource optimization and insurance analytics. 2025. doi: 10.67231/y64edh20.

[7] M. S. E. Mohamed, W. S. A. E. Mohamed, J. Ding, and J. Buchmann. Mxl2: Solving polynomial equations over GF(2) using an improved mutant strategy. In *Post-Quantum Cryptography (PQCrypto 2008)*, volume 5299 of *Lecture Notes in Computer Science*, pages 203–215, Berlin, Germany, 2008. Springer. doi: 10.1007/978-3-540-88702-7_14.

[8] M. S. E. Mohamed, W. S. A. E. Mohamed, J. Ding, and J. Buchmann. Mxl3: An efficient algorithm for computing gröbner bases of zero-dimensional ideals. In *Information Security and Cryptology (ICISC 2009)*, volume 5984 of *Lecture Notes in Computer Science*, pages 87–100, Berlin, Germany, 2009. Springer. doi: 10.1007/978-3-642-14423-3_7.

[9] G. Ars, J.-C. Faugère, H. Imai, M. Kawazoe, and M. Sugita. Comparison between XL and gröbner basis algorithms. In *Proceedings of ASIACRYPT 2004*, volume 3329 of *Lecture Notes in Computer Science*, pages 338–353, Berlin, Germany, 2004. Springer. doi: 10.1007/978-3-540-30539-2_24.

[10] Fazle Hakeem Ghory. Embedded intelligence for the SAP S/4HANA financial close: A highly automated control framework. *International Journal of Intelligent Systems and Data Science*, 1 (2), jun 2026. doi: 10.67231/s0h5b367. URL `https://journals.femington.com/ijisds/article/view/447`.

[11] R. Gebauer and H. M. Möller. On an installation of buchberger's algorithm. *Journal of Symbolic Computation*, 6(2-3):275–286, 1988. doi: 10.1016/S0747-7171(88)80048-8.

[12] D. Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*. Springer, New York, NY, USA, 1995. doi: 10.1007/978-1-4612-5350-1.

[13] Sameeruddin Shaik. Leveraging blockchain technology for a decentralized public key infrastructure: A blueprint for secure digital identity management. In *2024 IEEE International Conference on ...*

[14] T. Becker and V. Weispfenning. *Gröbner Bases: A Computational Approach to Commutative Algebra*. Springer, New York, NY, USA, 1993. doi: 10.1007/978-1-4612-0913-3.

[15] Monisha Rengaraj. Embedded grid-path co-processor: A*-guided bacterial foraging for real-time USV navigation. 2025. doi: 10.67231/8s96mc67.

[16] Rayhan Khan. Development of an AI for versus tetris using evolutionary algorithms. 2025. doi: 10.67231/htp1hp30.

[17] W. W. Adams and P. Loustaunau. *An Introduction to Gröbner Bases*. American Mathematical Society, Providence, RI, USA, 1994.

[18] K. O. Geddes, S. R. Czapor, and G. Labahn. *Algorithms for Computer Algebra*. Springer, Boston, MA, USA, 1992. doi: 10.1007/b102438.

[19] Afsar Khan. Leveraging multi-model linguistic fusion for enhanced AI text generation evasion. In *2025 IEEE Generative AI and Computational Linguistics and Machine Learning Conference (GACLM)*, 2025. doi: 10.1109/GACLM67198.2025.11231821.

[20] Muskan Pawar. Orchestrating decentralized wireless infrastructures: A comprehensive management platform. 2025. doi: 10.67231/4z837x12.

[21] Ruchika Sinha. Unveiling agile integration dynamics within nigerian information technology projects. *Journal of Information Technology Project Management*.

[22] Ananya Sharma. Bridging the digital divide: A critical review of information systems integration for financial and contractual governance in capital projects. *Journal of Information Systems and Governance*.

[23] Het Rachhadiya. Information security for academic research integrity: A blockchain-enabled ai platform with zero-knowledge verification and immersive collaboration. *Journal of Academic Research Integrity*.

[24] Harish Kasireddy. Advancing scalar-on-function regression: A functional data analysis approach to basis selection and truncation optimization. *Journal of Data Analysis and Artificial Intelligence*, 4 (4), 2024. doi: 10.46632/jdaai/4/4/2. URL https://doi.org/10.46632/jdaai/4/4/2.

[25] Rohit Puranik. Efficient generation and simulation of synthetic text corpora for scalable information retrieval testing. In *2025 International Conference on Information Technology, Engineering and Intelligent Computing Systems (ICITEICS)*. IEEE, 2025. doi: 10.1109/ICITEICS64870.2025.11341224. URL https://doi.org/10.1109/ICITEICS64870.2025.11341224.

[26] Anirudh Reddy. Algorithmic simulation framework for multi-agent resource optimization in distributed computational systems. In *2025 IEEE International Conference on ...*, .

[27] Siddhant Poojary. Optimizing strategies in the iterated prisoner's dilemma using genetic improvement algorithms. In *2025 IEEE International Conference on ...*

[28] Rakesh Reddy. Information security and privacy-preserving federated learning for collaborative healthcare diagnosis. *Journal of Information Security and Privacy*, .

[29] Priyanka Muppuri. Resilient portfolio strategies and risk dynamics in digital financial markets during global uncertainty. In *Proceedings of the ...*