International Journal of Scientific Engineering and Research (IJSER)
ISSN (Online): 2347-3878
SJIF (2025): 8.036

A Linear Algebraic Approach to the Conjugacy Search Problem in Matrix Groups over Finite Fields

Rameshwar Pandurang Maghade

Department of Mathematics, Dnyanopasak Shikshan Mandal's Arts, Commerce and Science College, Jintur-431509
Dist. Parbhani, India
Email: *rameshwarmaghade[at]gmail.com*

Abstract: ***The Conjugacy Search Problem has been proposed as a foundation for several non-commutative cryptographic protocols. In this paper, we investigate the computational complexity of this problem in matrix groups over finite fields, specifically $GL(n, \mathbb{F}_q)$. We demonstrate that the conjugacy search problem in this setting reduces to solving a homogeneous linear system derived via tensor (Kronecker) products. This reduction enables efficient recovery of conjugating elements using standard linear algebra techniques. We provide both theoretical justification and computational evidence, implemented in SageMath, showing that conjugators can be recovered with high success rate across a wide range of parameters. Our results indicate that matrix groups over finite fields are unsuitable for cryptographic schemes based on conjugacy hardness.***

Keywords: Cryptography, Conjugacy Search Problem, Matrix Groups, Finite Fields, Linear Algebra, Cryptrographic Security, Kronecker Product, Conjugacy-Based Cryptography, Non-Abelian Cryptography, SageMath.

1. Introduction

Group-based cryptography has emerged as an alternative to classical number-theoretic cryptography, aiming to construct secure systems based on computational problems in non-abelian algebraic structures. Among these, the conjugacy search problem has received considerable attention due to its apparent asymmetry: while conjugation is computationally straightforward, recovering the conjugating element is presumed difficult in certain groups.

Formally, given a group G and elements $g, h \in G$ such that $h = xgx^{-1}$ for some unknown $x \in G$, the goal is to determine x. This problem has been proposed as the basis for key exchange protocols and public-key cryptosystems in various non-commutative settings.

However, the security of such constructions critically depends on the hardness of the underlying problem in the chosen group. In this work, we focus on matrix groups over finite fields, particularly $GL(n, \mathbb{F}_q)$, due to their rich algebraic structure and computational accessibility.

The main contribution of this paper is to show that, the conjugacy search problem in these groups is efficiently solvable. By translating the problem into a system of linear equations using tensor algebra, we obtain a practical and deterministic method for recovering conjugators. Our approach combines theoretical analysis with extensive computational experiments.

1.1 Related Work

The conjugacy search problem has been extensively studied within group-based cryptography, particularly in braid groups and other non-commutative algebraic structures. Early public-key constructions based on algebraic groups were proposed by Anshel, Anshel, and Goldfeld, while later work by Birman, Ko, Lee, Shpilrain, and Ushakov investigated algorithmic properties of conjugacy problems in various groups.

For matrix groups, conjugacy corresponds to matrix similarity, whose algebraic structure has long been understood through rational and Jordan canonical forms. Furthermore, the vectorization identity

$$vec(AXB) = (B^T \otimes A)\, vec(X)$$

is a classical result in matrix analysis and numerical linear algebra, where it is frequently employed for solving Sylvester-type matrix equations.

The present work does not claim novelty in these underlying linear algebraic identities. Instead, it demonstrates that combining these classical tools yields a practical polynomial-time algorithm for recovering conjugating matrices in finite general linear groups, thereby providing additional evidence that such groups are unsuitable for cryptographic constructions relying on conjugacy hardness.

2. Preliminaries

Let $\mathbb{F}_q$ denote a finite field with q elements. The general linear group $GL(n, \mathbb{F}_q)$ consists of all invertible $n \times n$ matrices over $\mathbb{F}_q$.

2.1 Conjugacy in Groups

Two elements $g, h \in G$ are said to be conjugate if there exists $x \in G$ such that:

$$h = xgx^{-1}$$

This defines an equivalence relation on G, partitioning it into conjugacy classes.

2.2 Matrix Representation

In $GL(n, \mathbb{F}_q)$, conjugacy corresponds to similarity of matrices. That is, two matrices represent the same linear transformation under different bases.

2.3 Canonical Forms

The structure of conjugacy classes is governed by canonical forms such as the Jordan Canonical Form, which describes matrices up to similarity over algebraically closed fields. Over finite fields, analogous classifications are given by rational canonical forms.

2.4 Problem Statement

Given $g, h \in GL(n, \mathbb{F}_q)$ such that $h = xgx^{-1}$, determine x.

3. Conjugacy in Matrix Groups

In matrix groups, conjugacy reflects structural equivalence. Specifically:

- Conjugate matrices share the same characteristic polynomial
- They have identical minimal polynomials
- Their invariant subspace structure coincides

Thus, conjugacy is determined by intrinsic algebraic properties rather than arbitrary relationships.

Importantly, if g and h are conjugate, then there exists a matrix X satisfying:

$$Xg = hX$$

This equation forms the basis of our computational approach.

3.1 Theorem

Let $g, h \in GL(n, \mathbb{F}_q)$ such that $h = xgx^{-1}$ for some invertible matrix x. Then a conjugating matrix can be recovered in deterministic polynomial time by solving the homogeneous linear system

$$(I \otimes g^T - h \otimes I)\, vec(X) = 0$$

followed by selecting any invertible element from the solution space.

Proof: The equation

$$Xg = hX$$

is equivalent to

$$(I \otimes g^T - h \otimes I)\, vec(X) = 0$$

The coefficient matrix has size

$$n^2 \times n^2$$

Gaussian elimination computes its kernel in field operations.

$$O(n^6)$$

Since $h = xgx^{-1}$

The true conjugator x belongs to the kernel, ensuring that the kernel is nontrivial.

Testing invertibility of candidate matrices requires operations.

$$O(n^3)$$

Hence the overall algorithm runs in polynomial time.

4. Linear Algebraic Attack

This section presents our main method for solving the conjugacy search problem.

4.1 Reformulations as a Linear System

Starting form:

$$Xg = hX$$

we rewrite this equation using vectorization. Let $vec(X)$ denote the vector obtained by stacking the columns of X. Then:

$$(I \otimes g^T - h \otimes I)\, vec(X) = 0$$

where $\otimes$ denotes the Kroncker product.

This yields a homogeneous linear system in n^2 variables.

4.2 Solution Space

The set of solutions forms a vector space:

$$S = \{X \mid Xg = hX\}$$

Since a valid conjugator exists, S is non-trivial.

4.3 Extracting Invertible Solutions

Not all solutions are invertible. However, by sampling linear combinations of basis vectors of S, one can efficiently find an invertible matrix X such that:

$$XgX^{-1} = h$$

4.4 Algorithm

- Construct matrix:
$$A = I \otimes g^T - h \otimes I$$
- Compute kernel of A
- Generate random linear combinations of kernel basis
- Test invertibility and verify conjugacy

5. Computational Results

We implemented the above algorithm in SageMath and conducted experiments for:

- $n = 2, 3, 4$
- $q = 2, 3, 4$
- 50 trials per parameter set

5.1 Result Summary

n	q	Success Rate	Avg Time (s)
2	2	1.0	0.0045
2	3	1.0	0.0044
2	5	1.0	0.0040
3	2	1.0	0.0052
3	3	1.0	0.0063
3	5	1.0	0.0059
4	2	1.0	0.0093
4	3	1.0	0.0104
4	5	1.0	0.0143

5.2 Observations

The computational experiments demonstrate that the proposed linear algebraic attack is highly effective for solving the conjugacy search problem in matrix groups over finite fields. In every tested case, the algorithm successfully recovered a valid conjugating matrix X, resulting in a success rate of 100%.

It was observed that the running time increases gradually with the matrix dimension n, which is expected due to the larger linear systems involved. However, the growth remained computationally manageable and consistent with polynomial-time behaviour.

Another important observation is that increasing the field size q did not significantly affect the success of the attack. The algorithm remained efficient across all tested finite fields. Furthermore, the attack succeeded even for non-diagonalizable matrices, indicating that the method does not rely on spectral decomposition or eigenvalue computations.

Overall, the experiments strongly suggest that conjugacy in matrix groups possesses exploitable linear structure, making the problem computationally tractable.

5.3 Interpretation

The experimental results indicate that the conjugacy search problem in matrix groups is fundamentally linear algebraic in nature. Although conjugacy is defined through noncommutative group operations, the relation

$$Xg = hX$$

transforms the problem into a homogeneous linear system over finite fields.

This reduction explains the consistent success of the proposed attack. Standard linear algebra methods are sufficient to recover conjugators efficiently, which significantly weakens the cryptographic hardness assumption associated with these groups.

The findings also demonstrate that noncommutativity alone does not guarantee cryptographic security. In matrix groups, the existence of underlying linear representations introduces structural weaknesses that can be exploited algorithmically.

5.4 Limitations

The present work focuses exclusively on finite general linear groups.

The conclusions do not extend automatically to braid groups, Thompson groups, or other non-commutative groups where the conjugacy search problem may remain computationally difficult.

Future work will investigate whether similar linearization techniques exist for broader classes of algebraic groups.

6. Cryptographic Implications

The results of this work have important implications for conjugacy-based cryptography. Since the conjugacy search problem in $GL(n, \mathbb{F}_q)$ can be reduced to linear algebra computations, matrix groups over finite fields do not provide a secure foundation for cryptographic protocols based on conjugacy hardness.

The vulnerability identified in this paper is structural rather than implementation-specific. Consequently, increasing parameter sizes alone is unlikely to restore security. Any cryptographic construction relying on conjugacy hardness in low-dimensional matrix groups may therefore be susceptible to efficient algebraic attacks.

These findings highlight the necessity of carefully analyzing algebraic representations before selecting groups for cryptographic applications.

6.1 Lack of Hardness

A secure cryptographic primitive requires a computationally hard problem. However, our results show:

$$Conjugacy\ Search\ in\ GL(n, \mathbb{F}_q) \in P$$

Thus, it is unsuitable for cryptographic use.

6.2 Structural Weakness

The primary weakness of matrix groups arises from their inherent linear structure. Although the groups themselves are noncommutative, matrix representations satisfy algebraic relations that can be expressed through systems of linear equations.

The equation $Xg = hX$

directly exposes this vulnerability by transforming the conjugacy problem into a tractable linear algebra problem. This structural property enables efficient attacks independent of brute force or exhaustive search methods.

As a result, the weakness is intrinsic to the algebraic representation of the group rather than a flaw in a particular cryptographic implementation.

6.3 Negative Result

The results obtained in this paper provide a negative cryptographic result for matrix-group-based conjugacy systems. Specifically, the experiments and theoretical analysis show that the conjugacy search problem in $GL(n, \mathbb{F}_q)$ is computationally feasible and therefore unsuitable as a hardness assumption for secure public-key cryptography.

This does not imply that all noncommutative cryptographic systems are insecure. Rather, it demonstrates that matrix groups over finite fields fail to provide sufficient resistance against linear algebraic attacks. Future research should therefore focus on alternative algebraic structures where conjugacy-related problems remain computationally difficult.

7. Conclusion

This paper examined the Conjugacy Search Problem (CSP) in the general linear group $GL(n, \mathbb{F}_q)$ and demonstrated that it can be efficiently solved by reducing it to a homogeneous system of linear equations using classical vectorization and Kronecker-product techniques. The proposed algorithm was implemented in SageMath, and computational experiments confirmed its effectiveness across various matrix dimensions and finite fields. These results show that the CSP in finite matrix groups is solvable in deterministic polynomial time, providing further evidence that such groups are unsuitable for cryptographic schemes based on the assumed hardness of conjugacy search. Future work may extend this approach to other non-commutative groups and investigate whether similar linearization techniques can be applied to broader classes of algebraic structures.

References

[1] Kalka, A., Teicher, M., and Tsaban, B., “Short Expressions of Permutations as Products and Cryptanalysis of the Algebraic Eraser,” *Advances in Applied Mathematics*, vol. 49, no. 1, pp. 57–76, 2012.
[2] Anshel, I., Anshel, M., and Goldfeld, D., “An Algebraic Method for Public-Key Cryptography,” *Mathematical Research Letters*, vol. 6, no. 3–4, pp. 287–291, 1999.
[3] Shpilrain, V., and Ushakov, A., “Thompson’s Group and Public Key Cryptography,” *ACM SIGSAM Bulletin*, vol. 39, no. 1, pp. 15–32, 2005.
[4] The Sage Developers, “SageMath, the Sage Mathematics Software System (Version 9.3),” 2024.
[5] Birman, J. S., Ko, K. H., and Lee, S. J., “A New Approach to the Word and Conjugacy Problems in the Braid Groups,” *Advances in Mathematics*, vol. 139, no. 2, pp. 322–353, 1998.
[6] Horn, R. A., and Johnson, C. R., *Topics in Matrix Analysis*, Cambridge University Press, Cambridge, 1991.
[7] Gantmacher, F. R., *The Theory of Matrices*, Vols. 1–2, Chelsea Publishing Company, 1959.
[8] Golub, G. H., and Van Loan, C. F., *Matrix Computations*, 4th Edition, Johns Hopkins University Press, 2013.
[9] Magnus, J. R., and Neudecker, H., *Matrix Differential Calculus with Applications in Statistics and Econometrics*, Wiley, 1999.
[10] Horn, R. A., and Johnson, C. R., *Matrix Analysis*, 2nd Edition, Cambridge University Press, 2012.
[11] Bhatia, R., *Matrix Analysis*, Springer, 1997.
[12] Tian, Y., "Rank Equalities and Inequalities for Kronecker Products of Matrices with Applications," *Applied Mathematics and Computation*, **150** (2004), 129–137.
[13] Koning, R. H., Neudecker, H., and Wansbeek, T. J., "Block Kronecker Products and the VECB Operator," *Linear Algebra and its Applications*, **149** (1991), 165–184.
[14] Menezes, A. J., van Oorschot, P. C., and Vanstone, S. A., *Handbook of Applied Cryptography*, CRC Press, Boca Raton, FL, 1996.
[15] Stallings, W., *Cryptography and Network Security: Principles and Practice*, 8th Edition, Pearson, 2023.
[16] Roman, S., *Advanced Linear Algebra*, 3rd Edition, Springer, New York, 2008.
[17] Lidl, R., and Niederreiter, H., *Finite Fields*, 2nd Edition, Cambridge University Press, Cambridge, 1997.
[18] Rotman, J. J., *An Introduction to the Theory of Groups*, 4th Edition, Springer, New York, 1995.
[19] Myasnikov, A., Shpilrain, V., and Ushakov, A., *Group-Based Cryptography*, Advanced Courses in Mathematics CRM Barcelona, Birkhäuser, 2008.
[20] Hoffstein, J., Pipher, J., and Silverman, J. H., *An Introduction to Mathematical Cryptography*, 2nd Edition, Springer, 2014.