Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 43 Issue: 08-2024
DOI: 10.5281/zenodo.13354384

FINITE GROUPS, SIMPLE GROUPS, AND THE CLASSIFICATION OF FINITE SIMPLE GROUPS WITH APPLICATIONS IN CRYPTOGRAPHY AND CODING THEORY

RITU
BKN Public School Kharkara (Meham). Email: malikritu079@gmail.com

Abstract

Finite groups and simple groups are fundamental structures in algebra that play critical roles in various fields, including cryptography and coding theory. The classification of finite simple groups is one of the most significant achievements in modern mathematics, providing a comprehensive list of building blocks for all finite groups. This paper explores the properties of finite groups and simple groups, details the classification of finite simple groups, and highlights their applications in cryptography and coding theory.

1. INTRODUCTION

Finite groups are mathematical structures with a finite number of elements that follow specific algebraic rules. Simple groups, a subset of finite groups, have no nontrivial normal subgroups and serve as the building blocks for all finite groups.

The classification of finite simple groups, completed in the late 20th century, has profound implications for various mathematical and practical fields, particularly cryptography and coding theory (Arezoomand ET AL., 2024).

This paper aims to provide an overview of finite groups and simple groups, discuss the classification of finite simple groups, and explore their applications in cryptography and coding theory.

2. FINITE GROUPS

A finite group **G** is a set with a finite number of elements equipped with a binary operation that satisfies the group axioms: closure, associativity, identity, and invertibility (Starkovich & Starkovich 2021).

Definition 1: A group **G** is finite if it has a finite number of elements, called the order of **G**, denoted by |**G**|.

Example 1: The Symmetric Group S_3

The symmetric group (S_3) consists of all permutations of three elements. It has 6 elements:

S_3 = {e, (12), (13), (23), (123), (132)}

where e is the identity permutation, (12) swaps elements 1 and 2, (13) swaps elements 1 and 3, (23) swaps elements 2 and 3, (123) is the cycle that sends 1 to 2, 2 to 3, and 3 to 1, and (132) is the cycle that sends 1 to 3, 3 to 2, and 2 to 1.

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 43 Issue: 08-2024
DOI: 10.5281/zenodo.13354384

3. SIMPLE GROUPS

Simple groups are finite groups with no nontrivial normal subgroups.

Definition 2: A group (G) is simple if its only normal subgroups are the trivial subgroup {e} and (G) itself (Craven, 2023).

Example 2: The Alternating Group A_5

The alternating group A_5 consists of all even permutations of five elements. It has 60 elements and is simple. The group A_5 can be thought of as the group of rotations of a regular icosahedron (Kerber, 2006).

4. CLASSIFICATION OF FINITE SIMPLE GROUPS

The classification theorem for finite simple groups states that every finite simple group belongs to one of the following categories: (Almuhaimeed, 2018)

1. Cyclic groups of prime order.
2. Alternating groups A_n for $n \geq 5$.
3. Groups of Lie type.
4. The 26 sporadic simple groups.

Theorem (Classification of Finite Simple Groups): Every finite simple group is isomorphic to one of the following (Dona et al., 2024)

- A cyclic group of prime order.
- An alternating group A_n for $n \geq 5$.
- A simple group of Lie type.
- One of the 26 sporadic groups.

Example 3: Cyclic Groups of Prime Order

The cyclic group C_p of prime order p consists of $\{e, a, a^2, \ldots, a^{p-1}\}$, where a is a generator of the group. This group is simple because it has no nontrivial normal subgroups

Example 4: Alternating Groups

The alternating group A^5 has 60 elements and is a simple group $n \geq 5$. It can be represented by the even permutations of five elements.

Example 5: Sporadic Groups

The Monster group M is the largest sporadic simple group, with approximately 8 times 10^{53} elements. It plays a role in various areas of mathematics, including string theory.

5. APPLICATIONS IN CRYPTOGRAPHY

Cryptography is the science of secure communication. Group theory, particularly the properties of finite and simple groups, underpins many cryptographic protocols (Battarbee., 2023).

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 43 Issue: 08-2024
DOI: 10.5281/zenodo.13354384

5.1 Public-Key Cryptography

Public-key cryptographic systems, such as RSA and ECC, rely on the difficulty of certain mathematical problems in finite groups (Imam et al., 2021).

Example 6: RSA Encryption

RSA encryption uses the multiplicative group of integers modulo n, where n is a product of two large primes. The security of RSA is based on the difficulty of factoring large composite numbers (Sharma et al., 2023).

Solution:

1. Choose two large prime numbers p and q.
2. Compute n = pq and ϕ (n) = (p−1) (q−1).
3. Choose an integer e such that 1 < e < ϕ (n) and gcd (e, ϕ (n) = 1.
4. Compute d such that ed =1 (mod ϕ (n)).
5. The public key is (n, e) and the private key is (n, d).

To encrypt a message m:

$c = m^e \pmod{n}$

To decrypt the ciphertext c:

$m = c^e \pmod{n}$

5.2 Elliptic Curve Cryptography (ECC)

ECC uses the group structure of elliptic curves over finite fields to create secure cryptographic systems (Liu et al., 2024).

Example 7: Elliptic Curve over Fp

Consider the elliptic curve E defined by the equation $y^2=x^3+ax+b$ over the finite field Fp.

Solution:

1. Define the elliptic curve E over Fp with parameters a and b.
2. Choose a base point P on the curve.
3. Select a private key d, a randomly chosen integer.
4. Compute the public key Q = dP.
5. To encrypt a message point M on the curve, choose a random integer k and compute $C_1 = kP$ and $C_2 = M + kQ$.
6. To decrypt the ciphertext (C_1, C_2), compute $M = C_2 – dC_1$.

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 43 Issue: 08-2024
DOI: 10.5281/zenodo.13354384

6. APPLICATIONS IN CODING THEORY

Coding theory deals with the design of error-correcting codes for reliable data transmission and storage. Finite groups play a crucial role in constructing these codes (Garani et al., 2023).

6.1 Linear Codes

Linear codes are a type of error-correcting code constructed using the group structure of vector spaces over finite fields (Vanstome et al., 2013).

Example 8: Reed-Solomon Code

The Reed-Solomon code is a linear code that uses the structure of finite fields to detect and correct errors in data transmission.

Solution:

1. Let Fq be a finite field with q elements.
2. Define the message polynomial m(x) of degree less than k.
3. Encode the message by evaluating m(x) at n distinct points in Fq.

To decode, use polynomial interpolation to recover m(x) from the received codeword, correcting errors up to a certain bound.

6.2 Group Codes

Group codes use the algebraic structure of groups to design error-correcting codes with specific properties.

Example 9: Binary Golay Code

The binary Golay code is a group code based on the Mathieu group M_{24}, one of the sporadic simple groups.

Solution:

1. The binary Golay code G_{23} is a [23, 12, 7] code, meaning it encodes 12-bit messages into 23-bit codewords with a minimum distance of 7.
2. Construct the code using the generator matrix derived from the Mathieu group M_{24}.

7. CONCLUSION

Finite groups, simple groups, and the classification of finite simple groups form the backbone of modern algebra with significant implications for cryptography and coding theory. Understanding these structures enables the development of secure cryptographic protocols and robust error-correcting codes. The classification of finite simple groups not only represents a monumental mathematical achievement but also provides essential tools for practical applications in technology and communication.

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 43 Issue: 08-2024
DOI: 10.5281/zenodo.13354384

References

1) Arezoomand, M., Iranmanesh, M. A., Praeger, C. E., & Tracey, G. (2024). Totally 2-closed finite groups with trivial Fitting subgroup. *Bulletin of Mathematical Sciences*, *14*(01), 2350004..

2) Starkovich, S. P., & Starkovich, S. P. (2021). Groups. *The Structures of Mathematical Physics: An Introduction*, 25-52.

3) Craven, D. A. (2023). The maximal subgroups of the exceptional groups F 4 (q), E 6 (q) and E 6 2 (q) and related almost simple groups. *Inventiones mathematicae*, *234*(2), 637-719.

4) Kerber, A. (2006). *Representations of Permutation Groups I: Representations of Wreath Products and Applications to the Representation Theory of Symmetric and Alternating Groups* (Vol. 240). Springer.

5) Dona, D., Maróti, A., & Pyber, L. (2024). Growth of products of subsets in finite simple groups. *Bulletin of the London Mathematical Society*.

6) Almuhaimeed, A. (2018). *Group Actions on Rings*. The University of Manchester (United Kingdom).

7) Battarbee, C. (2023). *Analysis and Applications of Two Group-Theoretic Problems in Post-Quantum Cryptography* (Doctoral dissertation, University of York).

8) Imam, R., Areeb, Q. M., Alturki, A., & Anwer, F. (2021). Systematic and critical review of rsa based public key cryptographic schemes: Past and present status. *IEEE access*, *9*, 155949-155976.

9) Sharma, S., Ramkumar, K. R., Kaur, A., Hasija, T., Mittal, S., & Singh, B. (2023). Post-quantum cryptography: A solution to the challenges of classical encryption algorithms. *Modern Electronics Devices and Communication Systems: Select Proceedings of MEDCOM 2021*, 23-38.

10) Liu, M., Kultinov, K., & Wang, C. (2024). The Implementations and Applications of Elliptic Curve Cryptography. *Proceedings of 39th International Confer*, *98*, 89-102.

11) Garani, S. S., Nadkarni, P. J., & Raina, A. (2023). Theory behind quantum error correcting codes: An overview. *Journal of the Indian Institute of Science*, *103*(2), 449-495.

12) Vanstone, S. A., & Van Oorschot, P. C. (2013). *An introduction to error correcting codes with applications* (Vol. 71). Springer Science & Business Media.