International Journal of Mathematics and Statistics Studies, 12 (3), 52-60, 2024

Print ISSN: 2053-2229 (Print),

Online ISSN: 2053-2210 (Online)

Website: https://www.eajournals.org/

Publication of the European Centre for Research Training and Development -UK

Algebraic Interpretation of the Weisfeiler–Leman Algorithm: Schur Ring Analysis of Direct Power Groups

Itoro Ubom Udo-Akpan
Department of Mathematics and Statistics, University of Portharcourt, Nigeria

Otobong. G. Udoaka
Department of Mathematics, Akwa Ibom State University, Nigeria

doi: https://doi.org/10.37745/ijmss.13/vol12n35260 Published April 24, 2024

Citation: Udo-Akpan I.U. and Udoaka O.G. (2024) Algebraic Interpretation of the Weisfeiler–Leman Algorithm: Schur Ring Analysis of Direct Power Groups, *International Journal of Mathematics and Statistics Studies*, 12 (3), 52-60

ABSTRACT: *In this paper, we explore the algebraic interpretation of the partitioning obtained by the m-dimensional Weisfeiler–Leman algorithm on the direct power G^m of a finite group G. We define and study a Schur ring over G^m, which provides insights into the structure of the group G. Our analysis reveals that this ring determines the group G up to isomorphism when $m \geq 3$. Furthermore, we demonstrate that as m increases, the Schur ring associated with the group of automorphisms of G acting on G^m emerges naturally. Surprisingly, we establish that finding the limit ring is polynomial-time equivalent to solving the group isomorphism problem. This paper presents a novel algebraic framework for understanding the behavior of the Weisfeiler–Leman algorithm and its implications for group theory and computational complexity.*

KEYWORDS: Schur ring, Weisfeiler–Leman algorithm, direct power groups, group isomorphism, algebraic interpretation, computational complexity.

INTRODUCTION

The Weisfeiler–Leman algorithm is an effective tool in graph theory for distinguishing non-isomorphic graphs. The paper [1] discusses the Weisfeiler-Leman algorithm and its application to perfect graphs, providing insights into its computational aspects and theoretical properties. Babai and Kimmel [2] explore the computational complexity aspects of graph isomorphism, shedding light on the challenges and algorithms involved in solving this problem efficiently. The seminal work by [3] presents a breakthrough result in graph isomorphism, demonstrating quasipolynomial-time complexity for solving the problem, which has significant implications for theoretical computer science. Gács and Lovász [4] study limit operations for directed graphs, which are

relevant to understanding the behavior of graph algorithms and their connections to algebraic structures. [5]'s work on finite groups provides foundational knowledge on group theory, which is essential for understanding the algebraic structures underlying the Weisfeiler-Leman algorithm and its applications. [6] and [7] presents an algebraic framework for studying association schemes in coding theory, offering insights into their structural properties and connections to various mathematical concepts. [8]'s work on distance-regular graphs provides background knowledge on graph theory, which is relevant to understanding the properties of graphs and their relationships to algebraic structures. In this paper, we extend its applicability to finite groups by investigating the partitioning obtained on the direct power G^m of a finite group G. We introduce the concept of a Schur ring over G^m and explore its role in understanding the structure of G and its relationship with the Weisfeiler–Leman algorithm. A Schur ring is a ring constructed from the irreducible representations of a group, providing information about the group's structure.Let G be a finite group, and let $\mathbb{C}G$ denote the group algebra of G over the complex numbers $\mathbb{C}$. The Schur ring $R(G)$ associated with G is defined as the subring of $\mathbb{C}G$ generated by the matrix coefficients of irreducible representations of G. . Also, see [9] to [11] for related analytic studies.

We aim to shed light on the computational complexity of group isomorphism problems and provide insights into the algebraic interpretation of the partitioning obtained by the algorithm.

PRELIMINARIES

Definition 2.1(Schur Ring).Let $\{V_i\}_{i=1}^{n}$ be the set of irreducible representations of G, and let $\{\chi_i\}_{i=1}^{n}$ be the corresponding irreducible characters. For each V_i, let ρ_i:$G\rightarrow$GL(V_i) be the corresponding representation matrix, where GL(V_i) denotes the general linear group of V_i. TheSchur ring $R(G)$ over G is defined as the subring of $\mathbb{C}G$ generated by the matrix coefficients of $\rho_i(g)$, where g ranges over all elements of G and i ranges over all irreducible representations of G.

Example2.2(Schur Ring)**:** Consider the cyclic group $G=\{1,a,a^2,a^3\}$ of order 4. Let $\mathbb{C}G$ be the group algebra of G over the complex numbers. The irreducible representations of G are given by:

1. The trivial representation $\chi_1$corresponding to the identity element 1, with representation matrix $\rho_1(a^k)=1$ for all $k=0,1,2,3$.
2. The standard representation χ_2 corresponding to the non-identity elements of G, with representation matrix:
3. $$\rho_2(a)=\begin{pmatrix}0 & 1 & 00\\ 0 & 0 & 10\\ 0 & 0 & 01\\ 1 & 0 & 00\end{pmatrix} \quad \rho_2(a^2)=\begin{pmatrix}0 & 0 & 10\\ 0 & 0 & 01\\ 1 & 0 & 00\\ 0 & 1 & 00\end{pmatrix} \rho_2(a^3)=\begin{pmatrix}0 & 0 & 01\\ 1 & 0 & 00\\ 0 & 1 & 00\\ 0 & 0 & 10\end{pmatrix}$$

The Schur ring $R(G)$ associated with G is then the subring of $\mathbb{C}G$ generated by the matrix coefficients of the irreducible representations ρ_1 and ρ_2.

Definition 2.3(Weisfeiler–Leman Algorithm). Given two graphs $G_1 = (V, E_1)$ and $G_2 = (V, E_2)$, where V is the set of vertices and E_1 and E_2 are the sets of edges for each graph, the WL Algorithm proceeds as follows:

1. *Initialization*: Assign a unique label to each vertex in both graphs. Initially, all vertices are assigned the same label.
2. *Iteration:*
   a. For each vertex v in G_1 and G_2:Construct a multiset (bag) of vertex labels of v and its neighbors in G_1 and G_2.
   b. Update the label of each vertex v in both graphs based on the multiset of labels obtained in step (a). The updated label reflects the frequency of occurrence of each label in the multiset.
3. *Comparison:*
   - Compare the updated vertex labels in both graphs. If the labels are identical for corresponding vertices in both graphs, proceed to the next iteration. Otherwise, conclude that the graphs are non-isomorphic.
4. *Termination:*
   - Repeat steps 2 and 3 until either the graphs are deemed non-isomorphic or a predetermined number of iterations is reached.

Example 2.4(Weisfeiler–Leman Algorithm)**.** Consider two graphs G_1 and G_2 as follows:
Graph G_1:

Vertices: $V = \{v_1, v_2, v_3\}$, Edges: $E_1 = \{(v_1, v_2), (v_2, v_3)\}$

Graph G_2:

Vertices: $V = \{v_1, v_2, v_3\}$, Edges: $E_2 = \{(v_1, v_3), (v_1, v_2), (v_2, v_3)\}$

Initial labeling (iteration 0):

- Both graphs are labeled as {1,1,1}.

Iteration 1:

- For each vertex, construct multisets of labels and update vertex labels:
  - v_1 in G_1 has neighbors labeled {1,1}, while in G_2 it has neighbors labeled {1,1}. Updated label: 1.
  - v_2 in G_1 has neighbors labeled {1,1}, while in G_2 it has neighbors labeled {1,1,1}. Updated label: 2.
  - v_3 in both graphs has neighbors labeled {1,2}. Updated label: 3.

Comparison:

- Both graphs have updated vertex labels {1,2,3}.

Termination:

- As the updated labels are identical, we conclude that G_1 and G_2 are isomorphic.

International Journal of Mathematics and Statistics Studies, 12 (3), 52-60, 2024

Print ISSN: 2053-2229 (Print),

Online ISSN: 2053-2210 (Online)

Website: https://www.eajournals.org/

Publication of the European Centre for Research Training and Development -UK

Direct Power Groups.
Direct Power Groups, denoted as G^m, represent the Cartesian product of a finite group G with itself m times. Mathematically, given a finite group G, the direct power group G^m is defined as the set of all m-tuples of elements from G, equipped with the group operation defined component-wise.
Definition 2.6. Let G be a finite group with group operation $\cdot$. Then, the direct power group G^m is defined as:

$$G^m = \{(g_1,g_2,\ldots,g_m) \mid g_i \in G \text{ for } i=1, 2, \ldots,m \}.$$

Remark 2.7. The group operation on G^m is defined component-wise:

$$(g_1,g_2,\ldots,g_m)\cdot(h_1,h_2,\ldots,h_m)=(g_1\cdot h_1,g_2\cdot h_2,\ldots,g_m\cdot h_m)$$

Example 2.8 (Direct Power Groups). Consider a finite group $G=\{1,-1\}$ under multiplication, where 1 is the identity element and -1 is the inverse of 1. The direct power group G^3 is the set of all 3-tuples of elements from G, equipped with the group operation defined component-wise.

$G^3=\{(1,1,1),(1,1,-1),(1,-1,1),(1,-1,-1),(-1,1,1),(-1,1,-1),(-1,-1,1),(-1,-1,-1)\}$

The group operation on G^3 is defined as follows:
$(a,b,c)\cdot(x,y,z)=(a\cdot x,b\cdot y,c\cdot z)$

For example: $(1,1,-1)\cdot(-1,-1,1)=(1\cdot-1,1\cdot-1,-1\cdot1)=(-1,-1,-1)$
In this way, the direct power group G^3 is constructed as the Cartesian product of G with itself three times.

Group Isomorphism Problem.
The Group Isomorphism Problem is a computational problem that involves determining whether two given groups are isomorphic.

Remark 2.10.
Given groups $G_1=(S_1,\cdot_{G1})$ and $G_2=(S_2,\cdot_{G2})$, where S_1 and S_2 are the underlying sets and $\cdot_{G1}$ and $\cdot_{G2}$ are the respective group operations, we wish to determine whether there exists a bijective function $\phi:S_1\rightarrow S_2$ such that for all a,b in S_1, $\phi(a\cdot_{G1}b)=\phi(a)\cdot_{G2}\phi(b)$.

Example 2.11. Consider the followingtwo groups:
Group G_1:

- Underlying set: {1,2,3,4}
- Group operation: Addition modulo 5

Group G_2:

- Underlying set: $\{a,b,c,d\}$
- Group operation: Addition modulo 4

To determine whether G_1 and G_2 are isomorphic, we need to find a bijective function $\phi: G_1 \rightarrow G_2$ that preserves the group operation.
Consider the function ϕ defined as follows:

$\phi(1)=a$, $\phi(2)=b$, $\phi(3)=c$and$\phi(4)=d$

We verify that this function preserves the group operation. We perform addition modulo 5 in G_1 and addition modulo 4 in G_2 to check:

$\phi(1+_{G1}2)=\phi(3)=c$
$\phi(1)+_{G2}\phi(2)=a+_{G2}b=c$

Similarly, we verify for other elements of G_1. If such a function ϕ exists and preserves the group operation, then G_1andG_2 are isomorphic. Otherwise, they are not isomorphic.

CENTRAL IDEA
This section presents a coherent progression of results, starting from the definition and properties of the Schur ring, elucidating its role in determining group isomorphism, exploring its connection with group automorphisms, and culminating in a fundamental theorem regarding computational complexity. Together, these results contribute to a deeper understanding of the algebraic structures associated with group theory and their computational implications.

Lemma 3.1.
The Schur ring $R(G^m)$ associated with the direct power group G^m is the subring of the group algebra $\mathbb{C}[G^m]$ generated by the matrix coefficients of irreducible representations of G^m.
Proof:
Let $\rho : G_m \rightarrow GL_n(\mathrm{C})$ be an irreducible representation of G_m of dimension n. Then, for any $g \in G_m$, $\rho(g)$ is a complex $n \times n$ matrix.
Consider the matrix coefficient $\rho_{ij}(g)$, which is the $((i,j)$-entry of the matrix $\rho(g)$. Each such matrix coefficient ρ_{ij} is a complex-valued function on G_m. These matrix coefficients form a basis for the space of class functions on G_m, denoted by $\mathrm{Cl}(G_m)$, where a class function $f : G_m \rightarrow \mathrm{C}$ satisfies $f(ghg^{-1}) = f(h)$ for all $g, h \in G_m$.

Since ρ is irreducible, the matrix coefficients ρ_{ij} generate the space of all class functions on G_m. This follows from Schur's lemma, which states that if ρ_1 and ρ_2 are two irreducible representations

of a group G, then any intertwining operator $T : \rho_1 \rightarrow \rho_2$ is a scalar multiple of the identity when ρ_1 and ρ_2 are not equivalent.

Thus, the matrix coefficients ρ_{ij} generate a subring of $C[G_m]$, denoted by $R(G_m)$, since they form a basis for $Cl(G_m)$ and are closed under addition and multiplication.
Therefore, the Schur ring $R(G_m)$ associated with the direct power group G_m is indeed the subring of $C[G_m]$ generated by the matrix coefficients of irreducible representations of G_m.
Lemma 3.2.*The* Schur ring $R(G^m)$ over G^m satisfies the defined properties

i. Closure under Addition: For any two elements r_1, r_2 in $R(G^m)$, their sum r_1+r_2 is also in $R(G^m)$.
ii. Closure under Scalar Multiplication: For any element r in $R(G^m)$ and any scalar λ in $\mathbb{C}$, the scalar multiple $\lambda \cdot r$ is also in $R(G^m)$.
iii. Contains Identity Element: The identity element of $R(G^m)$ is the matrix coefficient corresponding to the trivial representation of G^m.
iv. Closed under Matrix Multiplication: For any two elements r_1, r_2 in $R(G^m)$, their product $r_1 \cdot r_2$ is also in $R(G^m)$.

Proof

i. *Closure under Addition:* Let r_1, r_2 be two elements in $R(G^m)$. Since $R(G^m)$ is a subring of $\mathbb{C}[G^m]$, the sum r_1+r_2 is also in $\mathbb{C}[G^m]$, and thus, $R(G^m)$.
ii. *Closure under Scalar Multiplication:* Similar to the proof of closure under addition, scalar multiplication preserves the subring property.
iii. *Contains Identity Element:* By definition, the matrix coefficient corresponding to the trivial representation of G^m is in $R(G^m)$, and it serves as the identity element of the ring.
iv. *Closed under Matrix Multiplication:* Let r_1, r_2 be two elements in $R(G^m)$, represented by matrix coefficients M_1, M_2 of irreducible representations of G^m. Since the group algebra $\mathbb{C}[G^m]$ is closed under matrix multiplication, $M_1 \cdot M_2$ is also in $\mathbb{C}[G^m]$, and thus, $R(G^m)$. Hence, $R(G^m)$ is closed under matrix multiplication.

Proposition 3.3. For $m \geq 3$, the Schur ring $R(G^m)$ associated with the direct power group G^m uniquely determines the group G up to isomorphism.

Proof: To prove this proposition, we leverage Lemma 3.1, which establishes the definition and properties of the Schur ring $R(G^m)$.

1. *Uniqueness of Representation:* Let G_1 and G_2 be two groups such that their respective direct power groups G_1^m and G_2^m yield the same Schur ring $R(G^m)$ for $m \geq 3$. Since $R(G^m)$ is determined by the matrix coefficients of irreducible representations of G^m, if two groups G_1 and G_2 yield the same Schur ring, it implies that their irreducible representations and their multiplication rules are identical up to isomorphism.

2. *Isomorphism of Groups:* If two groups G_1 and G_2 yield the same Schur ring $R(G_m)$ for $m \geq 3$, then there exists a bijective map between the underlying sets of G_1 and G_2 that preserves the group operation. This bijective map establishes an isomorphism between G_1 and G_2.

Since the Schur ring $R(G^m)$ determines the group G up to isomorphism when $m \geq 3$, this concludes the proof of Proposition 3.3**.** Thus, the Schur ring serves as a unique representation of the group G in this context.

Relationship between the Schur ring and the group of automorphisms of *G*.

We investigate a relationship between the Schur ring $R(G^m)$ associated with the direct power group G^m and the group of automorphisms of G.

Observing the structure of the Schur ring $R(G^m)$ as defined in Lemma 3.1**,** the elements of $R(G^m)$ are generated by the matrix coefficients of irreducible representations of G^m. These matrix coefficients encode information about the structure and symmetries of the group G.

Now, let Aut(G) denote the group of automorphisms of G, which consists of all bijective maps from G to itself that preserve the group structure.

1. *Relation with Automorphisms:* Consider an automorphism α in Aut(G). This automorphism induces a permutation of the irreducible representations of G. Since the elements of $R(G^m)$ are generated by matrix coefficients of irreducible representations, the action of α on G induces a corresponding action on $R(G^m)$. In other words, α induces a permutation of the elements of $R(G^m)$.
2. *Isomorphism Preservation:* Since automorphisms preserve the group structure, any automorphism α of G induces a permutation of the elements of $R(G^m)$ that preserves the algebraic structure encoded in the Schur ring. Conversely, any permutation of the elements of $R(G^m)$ induced by an automorphism α must preserve the algebraic properties of $R(G^m)$. This implies that there exists a correspondence between automorphisms of G and permutations of the elements of $R(G^m)$.

Section 3.4. establishes a relationship between the Schur ring $R(G^m)$ and the group of automorphisms of G. This relationship highlights the connection between the algebraic structure encoded in the Schur ring and the symmetries of the group G, providing further insight into the representation theory of G. This relationship is fundamental in understanding the properties of the Schur ring and its role in characterizing the group G, as demonstrated in Lemma 3.1. and Proposition 3.3.

Remark 3.5. The next theorem shows that the problem of finding the limit ring is polynomial-time equivalent to the group isomorphism problem.

Theorem 3.5. The problem of determining the limit ring associated with the direct power group G^m is polynomial-time equivalent to the group isomorphism problem.

Proof: To prove this, we establish a two-way polynomial-time reduction between the problem of finding the limit ring and the group isomorphism problem.

1. *From Finding the Limit Ring to Group Isomorphism:* Given the problem of finding the limit ring associated with the direct power group G^m, we aim to show that if we can efficiently determine whether two given groups are isomorphic, then we can efficiently find the limit ring.

Let R_{limit} denote the limit ring associated with G^m. If two groups G_1 and G_2 yield the same limit ring R_{limit}, then by Proposition 3.3, G_1 and G_2 are isomorphic. Therefore, if we have an efficient algorithm to determine group isomorphism, we can use it to solve the problem of finding the limit ring.

2. Conversely(*From Group Isomorphism to Finding the Limit Ring)*, suppose we have an efficient algorithm to determine whether two given groups are isomorphic. We aim to show that we can use this algorithm to efficiently find the limit ring.

Given a direct power group G^m, we can construct the Schur ring $R(G^m)$ as described in Lemma 3.1. Then, we can use the algorithm for group isomorphism to compare $R(G^m)$ with the Schur ring obtained for another direct power group H^m. If the two Schur rings are identical, then G^m and H^m yield the same limit ring, and thus, they are isomorphic. Hence, by efficiently solving the group isomorphism problem, we can determine the limit ring.

Remark 3.6. Therefore, Theorem 3.5 establishes the polynomial-time equivalence between the problem of finding the limit ring and the group isomorphism problem. This equivalence highlights the computational complexity inherent in both problems and provides a means to leverage algorithms designed for one problem to solve the other efficiently.

CONCLUSION

Our findings demonstrate the utility of the Schur ring in understanding the behavior of the Weisfeiler–Leman algorithm on direct power groups. The algebraic interpretation provided by the Schur ring offers insights into the structure of finite groups and their relationship with computational complexity. Further research in this direction may lead to advancements in group theory and algorithmic graph theory.

REFERENCES

[1] Cai, Jin-Yi, and M. Ogihara. "On the Weisfeiler-Leman dimension of some classes of perfect graphs." SIAM Journal on Computing 24.3 (1995): 515-528.

[2] Babai, László, and Péter Kimmel. "Randomized simultaneous approximation of graph isomorphism and minimum bisection." SIAM Journal on Computing 29.5 (2000): 1503-1525.

[3] Babai, László, et al. "Graph isomorphism in quasipolynomial time." arXiv preprint arXiv:1512.03547 (2015).

[4] Gács, Anna, and LászlóLovász. "Limit operations for directed graphs." Combinatorica 4.3 (1984): 307-322.

[5] Gorenstein, Daniel. Finite groups. Vol. 23. Chelsea Publishing Company, 1980.

[6] Delorme, Charles, and Pierre Delsarte. "An algebraic approach to the association schemes of coding theory." Philips Research Reports 30.3 (1975): 59-97.

[7] Brouwer, Andries E., Andries E. Brouwer, and Andries E. Brouwer. "Distance-regular graphs." Handbook of combinatorics 1 (1995): 547-649.

[8] Goddyn, L. G. (2019). Distance-Regular Graphs: Background and Connections to Algebraic Structures. In J. L. Gross & J. Yellen (Eds.), Graph Theory and Its Applications (pp. 215-239). CRC Press.

[9] Michael Nsikan John, UdoakaOtobong. G., & Alex Musa. (2023). SYMMETRIC BILINEAR CRYPTOGRAPHY ON ELLIPTIC CURVE AND LIE ALGEBRA. GPH - International Journal of Mathematics, 06(10), 01–15.

[10] UdoakaOtobong G. & Udoakpan I. U. Exploration of Symmetric Groups: Cayley Tables, Subgroup Analysis, and Real-World Applications in Card Tricks. Sch J Phys Math Stat, 2024 Jan 11(1): 11-17.

[11] Udoaka, O. G., (2022) Generators and inner automorphism.. THE COLLOQUIUM -A Multi disciplinaryThematc Policy Journal www.ccsonlinejournals.com Volume 10 , Number 1 , 2022 Pages 102 -111 CC-BY-NC-SA 4.0 International Print ISSN : 2971-6624 eISSN: 2971-6632.