JOURNAL OF ALGEBRAIC STATISTICS
Volume 9, No. 1, 2018, p. 88-93
https://publishoa.com
ISSN: 1309-3452
DOI: https://doi.org/10.52783/jas.v9i1.1443

Symmetric Generation for Homomorphic Image

Ashok Singh Bhandari
Department of Mathematics, Graphic Era Hill University, Dehradun, Uttarakhand, India 248002

Abstract

Inherent combinatorial structure is seen in the extremely symmetric generating sets of many groups. Theoretically, such generating sets may provide novel existence proofs for groups, and practically, they can give us concise ways of describing elements of groups. Here, we provide a review of the research done on symmetric generating sets. Consistent with previous overviews, we place special emphasis on the ad hoc simple groupings. To create finite homomorphic pictures of infinite semidirect products, we introduce the method of double coset enumeration. In this study, we survey the many ways that symmetric generating sets may be made larger. One may talk about the function f from G to H as "mapping" G to H if it represents a relationship between elements of two algebraic systems. The underlying combinatorial structure of the generating sets of many groups is high symmetry. Theoretically, such generating sets may provide novel existence proofs for groups, and practically, they can give us concise ways of describing elements of groups.

Keywords: Symmetric Generation, Homomorphic, Image, Finite Group, Isomorphism

Introduction

The set im(f) of elements of H to which at least one element of G is transferred is called the image of the homomorphism. It is not necessary for im(f) to equal all of H. The set ker(f) of all items of G that map to the identity element of H is called the kernel of the homomorphism. It's possible that a special relationship, called a homomorphism, exists between the members of two algebraic systems. When two systems are homomorphic, conclusions on one system generally apply just as well to the other, even though the components and operations seem to be completely different. Hence, if a new system can be proven to be homomorphic to an existing one, then certain aspects of the existing system may be transferred to the new one, making the analysis of the new system easier.

When two systems undergo a homomorphism, the interactions between pairs of related elements are remarkably similar. Take the groups G and H as an example. Elements of G undergo a number of operations.

New constructions and presentations for many different finite groups, including the sporadic simple groups, have been made possible using the methods of symmetric generation. The use of symmetric generating sets has proved helpful in the quest to make group computing easier. The main program of allows for the multiplication of ·0 items represented in this way, making this method of representation useful in practice. Finding symmetric generating sets for big groups is quite interesting because of all the practical uses for them.

If G is a symmetric group, then T is a symmetric generating set for G. The subset N is considered the control group.

After satisfying these two conditions, we can say that G is a homomorphic image of its infinite progenitor m*n:N, which is the free product of n copies of the cyclic group Cm extended by N, for any natural number m. G may be defined further by adding relations of the type π =w(t1,t2,..tn), where n ∈N and w is a word in the symmetric generators. Hence, for n = 3, 4, 5,..., m = 2.

$$\frac{2^{*n} : N}{\pi_1 w_1, \ldots, w_s w_s} \cong \left\langle N, T \middle| t_i^2 = 1, \quad t_i^{\pi} = t_{\pi(i)}, \quad \pi_1 w_1 = \ldots = \pi_s w_s = 1 \right\rangle$$

it is possible to provide relations for more ancestors as well.

The coset Ntitj will be represented by I the coset Nti, ij, and so on. Each permutation involving an element of G may be found on the left, thanks to the fact that iπ = $\pi\pi^{-1}$i π= πi^{π}. This indicates that each element of G may be written in terms

JOURNAL OF ALGEBRAIC STATISTICS
Volume 9, No. 1, 2018, p. 88-93
https://publishoa.com
ISSN: 1309-3452
DOI: https://doi.org/10.52783/jas.v9i1.1443
of a permutation in N followed by a symmetric generator word. In addition, we may write $N^i=C_N(t_i)$ for the N stabilizer with just one point, $N^i=C_N(t_i)$ for the N stabilizer with two points,

$$N^{ij} = C_N\left(\left\langle t_i, t_j \right\rangle\right)$$

Literature Review

Liang, Min (2013) Can you do computations with encrypted data without first decrypting them? Blind computing and homomorphic encryption have been used to this problem. Each enciphered state of size n qubits is amenable to any unitary transformation under this method. The QFHE technique boasts unbreakable security when compared to traditional homomorphic encryption.

Mella, Silvia & Susella, Ruggero. (2013) In order to better understand the properties of homomorphic evaluation according to the BGV scheme, Several symmetric cryptographic primitives' homomorphic computability is analyzed this year (2013). Specifically, we evaluate AES using the standards developed by Gentry, Halevi, and Smart. We next enhance it and evaluate the homomorphic computation of many distinct families of cryptographic methods. We then detail the results of our performance investigation of the primitives we included using the recently released HElib. In order to draw a generalization about the homomorphic evaluation of symmetric cryptographic primitives, we explain our results for the various primitives we have investigated in the conclusion section.

Vizár, Damian & Vaudenay, Serge. (2015) Homomorphic encryption has exploded in popularity since since Gentry's seminal work was published in 2009. The fundamental contribution of Gentry's thesis was the demonstration that a completely homomorphic encryption method is feasible to construct. Despite how revolutionary Gentry's breakthrough was, designs using the bootstrapping approach have extremely poor performance in key generation and homomorphic assessment of circuits. In an effort to avoid the bootstrapping step, several writers have attempted to devise methods that can assess homomorphic circuits with an arbitrary number of inputs. This study defines symmetric homomorphic encryption and evaluates the safety of four alternative ideas for symmetric homomorphic encryption that have been previously published in three other studies. We show that all of these systems are vulnerable to a known plaintext key-recovery attack.

Vankudoth, Biksham & Vasumathi, D. (2017) Fully Homomorphic Encryption (FHE) is a cutting-edge area of cryptography research that, as of 2017, empowers the untrusted server to conduct calculations on encrypted data, addressing security and privacy concerns associated with new technologies like cloud computing. After Craig Gentry's initial creation of FHE in 2009, other more FHE systems were created, each of which relies on bootstrapping and squashing for security. Since it relies on perfect lattices, it is more difficult to implement and would incur a high computational cost if used in practice, although it is theoretically viable. In this work, For the Somewhat Homomorphic scheme, we provide a lightweight Fully Homomorphic Encryption scheme based on the GV system that uses matrices in place of integers. We drastically reduce the size of the key by adding the Reduced Approximate GCD issue. The scheme's semantic security has also been shown under Approximate GCD, and a novel technique for key creation and refreshment before each calculation has been proposed.

Recent Development in the Symmetric Generation Of Groups

Symmetric Generation

We will define numerous terms crucial to this examination here as we outline the overarching theory of symmetric generation. Involutions of order n produce a free group denoted by 2^{*n}. For a collection of random number generators for this free good, we use the notation {t1, t2,.., tn}. This free product, undergoes an automorphism when the generators are $\hat{\pi}$ permuted according to the sequence $\pi \in$ Sn.

$$t_i^{\hat{\pi}} := \pi^{-1} t_i \pi = t_{\pi(i)}, \quad (1)$$

JOURNAL OF ALGEBRAIC STATISTICS
Volume 9, No. 1, 2018, p. 88-93
https://publishoa.com
ISSN: 1309-3452
DOI: https://doi.org/10.52783/jas.v9i1.1443
By applying this operation to the group $N \leq S_n$, we get the semi-direct product $P:= 2^{\star n}: N$.

P is a progenitor of N when N behaves in a transitive manner. Using the symmetric generators, any element in P may be expressed as a relator of the form w, where $\pi \in N$ and πw is a word (1). As a result, the expression $H := \langle w1\pi 1, \ldots, wr\pi r \rangle$ for any r may be used to describe every finitely formed subgroup of P. The remainder after dividing P by H's normal closure, H^P, will be written as

$$\frac{2^{\star n}: N}{w_1\pi_1, \ldots, w_r\pi_r} := G$$

We state that the relations $w1\pi 1, \ldots, wr\pi r$ factor the progenitor P. Because the relation $w\pi = id$ is implicit whenever we write a relator $w\pi$, we will only ever use the term "relation" when we mean "relator" sensu stricto. G denotes the intended audience. In many cases, these relationships may be expressed in a shorter form by writing $(\pi w)^d$, where d is an integer positive. The author thinks it's clearest to call both t P and its mirror counterpart in G symmetric generators. Similarly, it is clear that either $N \leq P$ or its mirror counterpart in G may be referred to as the control group. The number of symmetric generators in a relation is what we call its length.

From here, whenever we refer to a generator of size $2^{\star n}$ in P or its homomorphic counterpart in G, we will somewhat misuse notation by using ti for both. We'll use the letter N for the P-group norm and the G-group homomorphism. Once again, in the author's view, there should be no misunderstanding.

The problem of determining whether or not G is finite arises immediately. Specifically, in G, we tally up all the cosets of N. Let $g \in G$. We may infer this since gN NgN. Therefore, counting double cosets of type NgN in G is much easier than counting single cosets of type gN in G. The following definition will do the trick. The subgroup described by for every word w in the symmetric generators is what we call the coset stabilizing subgroup.

$N^{(w)} := \{\pi \in N | Nw\pi = Nw\}$

The double coset $|N: N^{(w)}|$ contains the right cosets of $N^{(w)}$, hence it is evident that this is a subgroup of N.

Double Coset Enumeration

As mentioned before, a double coset enumeration is often used to confirm a symmetric presentation of a finite group. Early instances of symmetric presentations included groups small enough that counting cosets could be done by hand. Nevertheless, current focus has shifted to bigger groups, making automation of the process to enumerate double cosets a need.

Some General Lemmata

Relationships of frequently considerable importance arise spontaneously as we follow the following lemmata. In particular, these lemmata are unexpectedly helpful in pointing us in the direction of relevant linkages to think about.

Lemma 1:

$\langle ti , tj \rangle \cap N \leq C_N (Stab_N (i, j))$

This lemma has a natural induction that allows it to be generalized to an infinite set of symmetric generators. This lemma, despite its stunning simplicity, turns out to be quite potent. The actual length of this word is unknown; however, Those members of the control group who are likely to appear in a relation factoring a progenitor are those for whom the above lemma holds. The following lemma shows to be helpful in resolving this issue.

Lemma 2:

JOURNAL OF ALGEBRAIC STATISTICS
Volume 9, No. 1, 2018, p. 88-93
https://publishoa.com
ISSN: 1309-3452
DOI: https://doi.org/10.52783/jas.v9i1.1443
Let N be a perfect control group, and let P:= $2^{\star n}$: N be a progenitor. Thus, Every homomorphic image of a perfect group P is also perfect or has a perfect subgroup up to index 2. If w is a member of the set of odd-length symmetric generators, then the image makes sense.

$$\frac{2^{\star n} : N}{\pi w}$$

is perfect.

Generation of S_6 Over S4

A symmetric presentation of the infinite semidirect product descended from 3^{*4}:S4 is considered.

< x,y,t | x^4, y^2, $(y*x)^3$, t^3, (t,y) , (t^x,y) >

factoring in the connections,

t_0^3= [(012) t_0] ^{5}, [(0l)t_0]^4, [(012) $t_0t_1^{-1}$] ^{2}

Thus

$$G \cong \frac{3^{*4} : S_4}{((0,1,2)t_0)^5,\ ((0,1)t_0)^4,\ \left((0,1,2)t_0t_1^{-1}\right)^2}$$

$$\cong\langle N, T \mid N\cong S_4,\ t_i^{\pi}=t_{\pi(i)},\ t_0^3=[(012)t_0]^5=[(01)t_0]^4=[(012)t_0t_1^{-1}]^2=1\rangle$$

The homomorphic image is isomorphic to S6 according to a table in Bray. First, we'll prove that |G|=720, and then we'll prove the more definitive assertion that G ≅ S6. On the symmetric generators, the control group S4 = <x, y> acts as follows:

$$x\sim(0,1,2,3) \text{ and } y\sim(2,3).$$

$((0,1,2)t_0)^5$ translates to $((x^{-3}yxyx^2)t)^5$,

$((0,1)t_0)^4$ translates to $((x^{-2}yx^2t)^4$,

$((0,1,2)t_0t_1^{-1}))^2$ translates to $((x^{-3}yxyx^2)tt^{-x})^2$

In the case when π=(0,1,2) we may expand $(\pi t_0)^5$=1 to yield

$$\pi t_0\pi t_0\pi t_0\pi t_0\pi t_0 = \pi^2 t_0^{\pi} t_0 t_0^{\pi^2} t_0^{\pi} t_0 = \pi^2 t_1 t_0 t_2 t_1 t_0 = 1$$

$$\pi^2 t_1 t_0 t_2 = t_0^{-1} t_1^{-1}$$ (Relation 1)

Assuming that π=(0,1), we may expand $(\pi t_0)^4$=1, which yields

$$\pi t_0\pi t_0\pi t_0\pi t_0 = t_0^{\pi} t_0 t_0^{\pi} t_0 = t_1 t_0 t_1 t_0 = 1$$

$$\Rightarrow \quad t_1 t_0 = t_0^{-1} t_1^{-1}$$ (Relation 2)

JOURNAL OF ALGEBRAIC STATISTICS
Volume 9, No. 1, 2018, p. 88-93
https://publishoa.com
ISSN: 1309-3452
DOI: https://doi.org/10.52783/jas.v9i1.1443
Assuming $(\pi t_0 t_1^{-1})^2=1$, expanding $\pi=(0,1,2)$

$$\pi t_0 t_1^{-1} \pi t_0 t_1^{-1} = \pi^2 \left(t_0 t_1^{-1}\right)^{\pi} t_0 t_1^{-1} = (0,2,1) t_1 t_2^{-1} t_0 t_1^{-1} = 1$$

$$(0,2,1) t_1 t_2^{-1} = t_1 t_0^{-1}$$

(Relation 3)

That's a weaker claim than $Nt_1t^{-1}_2 = Nt_1t_0^{-1}$

Proof of Isomorphism

Since

$$\frac{|N|}{|N|} + \frac{|N|}{|N^{(0)}|} + \frac{|N|}{|N^{(00)}|} + \frac{|N|}{|N^{(01)}|} + \frac{|N|}{|N^{(011)}|} + \frac{|N|}{|N^{(001)}|} +$$

$$\frac{|N|}{|N^{(0110)}|} = \frac{24}{24} + \frac{24}{6} + \frac{24}{6} + \frac{24}{2} + \frac{24}{6} + \frac{24}{6} + \frac{24}{24} = 30$$

There is a limit of 30 to N's index in G. Hence, the maximum order of the G group of images is |N| *30 = 24*30 = 720.

By treating G as a subgroup of S_{30} operating on the 30 symbols, we are able to prove that |G| =720. We do this by calculating the effect of t on the 30 cosets, as well as the action of the control group N.

Conjugation by Wand shows that

i. |<x,y,t>| = 720,

ii. <x,y>≅ S_4, and

iii. t has precisely four conjugates.

iv. Extra relations exist between the variables (x,y,i).

It has been shown that | <x,y,t>| = 720. N = <x,y> ≅S_4. Since the order of xy equals 3.

Conclusion

We point out that the symmetric presentations we've spoken about so far are the most "elegant" symmetric presentations of random simple groups found since. It has been shown that many additional symmetric formulations of ad hoc groups are harder to motivate for different reasons. Algebra, number theory, algebraic geometry, and (algebraic) combinatorics are only few of the domains where the MAGMA computer algebra system's software environment may be put to use. In this thesis, it was used to study how various representations of finite groups, such as the orbits of their double cosets, are organized and interpreted. When two systems undergo a homomorphism, the interactions between pairs of related elements are remarkably similar. It is only reasonable to look for ways to generalize symmetric generating sets for small groups to big groups given the success of symmetric generating set approaches with small groups.

References

1. Liang, Min. (2013). Symmetric quantum fully homomorphic encryption with perfect security. Quantum Information Processing. 12. 10.1007/s11128-013-0626-5.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 9, No. 1, 2018, p. 88-93
https://publishoa.com
ISSN: 1309-3452
DOI: https://doi.org/10.52783/jas.v9i1.1443
2. Mella, Silvia & Susella, Ruggero. (2013). On the Homomorphic Computation of Symmetric Cryptographic Primitives. 10.1007/978-3-642-45239-0_3.
3. Vizár, Damian & Vaudenay, Serge. (2015). Cryptanalysis Of Chosen Symmetric Homomorphic Schemes. Studia Scientiarum Mathematicarum Hungarica. 52. 288-306. 10.1556/012.2015.52.2.1311.
4. Vankudoth, Biksham & Vasumathi, D. (2017). An efficient symmetric based algorithm for data security in cloud computing through homomorphic encryption scheme. International Journal of Applied Engineering Research. 12. 10477-10484.
5. Mushtaq, Qaiser & Rafiq, Ayesha. (2013). Adjacency Matrices of PSL(2,5) and Resemblance of Its Coset Diagrams with Fullerene C60. Algebra Colloquium. 20. 10.1142/S1005386713000515.
6. Aslam, M. & Ahmad, Rehan. (2013). Some results on homomorphic images of Δ(2,3,13). Journal of Mathematics. The Punjab University. 45.
7. Baccari, Kevin J., "Homomorphic Images and Related Topics" (2015). Electronic Theses, Projects, and Dissertations. 224.
8. Nebe, Gabi & Parker, Richard & Rees, Sarah. (2016). A method for building permutation representations of finitely presented groups.
9. Koch, Robert & Ramgoolam, Sanjaye. (2011). Strings from Feynman Graph counting: without large N. Physical Review D. 85. 10.1103/PhysRevD.85.026007.
10. Hartung, René. (2011). Coset enumeration for certain infinitely presented groups. International Journal of Algebra and Computation. 21. 10.1142/S0218196711006637.