Properties of Generating Sets of Finite Groups

by

Paul Apisa and R. Keith Dennis

We now provide a few more details about the prerequisites for the REU in group theory, where to find additional information about the mathematics and a little about the mechanics and goals of our program. In addition, we give a detailed version of the topics and types of questions that will be considered.

Further Information

Students in the project should have a solid background in basic linear algebra and abstract algebra. For example, the first six chapters of the textbook by Dummit and Foote, *Abstract Algebra*, 3rd edition, Wiley, would be more than adequate for the required background in group theory. For example, section 5.2 defines the term *elementary divisors* which appears below and in one standard description of the decomposition of finite abelian groups as direct products of cyclic groups. The same book also has several chapters on linear algebra (Chapters 10, 11, 12) but they're at a level higher than we expect most students to have seen.

The basic ideas for some of the specific topics we discuss below are worked out in detail in the 2010 Cornell Senior Thesis of Daniel J. Collins. See

`http://www.math.cornell.edu/Research/SeniorTheses/2010/collinsThesis.pdf`

In particular, references for most of the other topics discussed can be found in the thesis as well.

Basic Goals and Mechanics

During the summer students will learn several topics in group theory they've probably not seen before by directly working with these new ideas, both theoretically and computationally. In fact, one usually finds that writing programs helps one understand the mathematics in a much more concrete way than ones does when only trying to prove theorems. Conversely even small theoretical gains many times have substantial consequences computationally which in return allows the study of even larger and more complicated examples. This makes it much more likely that one is getting a true picture of what is going on rather than only seeing the parts of the subject which are small enough and simple enough to do by hand or with unsophisticated tools.

Those students accepted to participate in the program will receive further information including a set of notes by Dan Collins covering most of the needed background in group theory as well as a development of some of the topics described below.

Previous programming experience will be an advantage as we study these topics by experimenting computationally. Many explicit examples in a number of different situations can be given this way. Tutorials on programming will be given and a number of example programs will be provided. The computer algebra systems GAP and Magma will be our main tools. GAP is freely available for all operating systems. See

`http://www.gap-system.org/`

for further information as well as to get your own copy of the program. Magma is not free, but will be available via a license provided by the Cornell Mathematics Department.

A separate computer lab containing Linux workstations will be available for Cornell REU students. The students in this project will have access to a number of machines including remotely accessing larger machines. The largest have 64G, 128G, and 192G of memory, with the last two having 16 CPUs and 12 CPUs, respectively. GAP does have a facility for parallel computation so students with a strong interest in computations might find that of interest.

We'll start this project with a small collection of computational tools, theorems, and questions. Our goal is to significantly enlarge the contents of each of these collections. The research program will not be fixed, but will develop according to the interests and skills of the participants. An abundance of problems at many different levels of difficulty will be considered. This is a relatively new area of study with a real possibility of progress on problems at the edges of current research. New discoveries are likely to lead to publication.

A Brief Description of the Mathematics

Let G be a finite group. Any subset $s = \{g_1, ..., g_n\}$ of G generates a subgroup H. We say s is *irredundant* (or independent) if every proper subset of s generates a proper subgroup of H. Let $r(G)$ be the smallest size of a generating set of G, $m(G)$ the largest size of an irredundant generating set, and $i(G)$ the largest size of any irredundant set. Clearly $r(G) \leq m(G) \leq i(G)$.

Exercise 1. Use the elementary divisor and primary decompositions of an abelian group to calculate $r(G)$, $m(G)$, and $i(G)$ for a finite abelian group G. Determine precisely when $r(G) = m(G)$ for G a finite abelian group?

Exercise 2. Construct a group G where $m(G) < i(G)$ as follows. Let $q = p^n$ for p a prime. Let $\mathbb{F}_q$ be a finite field with q elements. Recall that the multiplicative group $\mathbb{F}_q^*$ is cyclic of order $r = q - 1$. Take $G = {\mathbb{F}_q}^+ \rtimes {\mathbb{F}_q}^*$ be the semi-direct product where the multiplicative group acts on the additive group by multiplication. Show that $r(G) = 2$. Show that the additive group is a simple ${\mathbb{F}_q}^*$-module (i.e., considered as a module over the group ring $\mathbb{F}_p[{\mathbb{F}_q}^*]$; that is, it has no proper non-trivial submodules). Suppose r is a prime (e.g., $q = 32$, $r = 31$). Show that $m(G) = 2$ as well. Note that $i(G) = n$ (at least n is clear; use that the module is simple to show it is exactly n). Conclude that it is not necessarily the case that any irredundant set can be extended to an irredundant generating set. Next try to compute $m(G)$ and $i(G)$ in general.

A finite dimensional vector space G over the integers mod p where p is prime (the unique field with p elements, $\mathbb{F}_p = \mathbb{Z}_p$) is just an elementary abelian p-group, and an irredundant generating set is just a basis. Some properties in this case are:

(1) any two bases have the same number of elements,

(2) every irredundant set is contained in some basis,

(3) every generating set contains some basis,

(4) for any basis and any non-trivial element of G, there is some element of the basis that can be replaced by the given element to yield a new basis for G,

(5) every element of a basis has prime order,

(6) given two ordered bases there exists a unique automorphism of G that takes one to the other; so $|\mathrm{Aut}(G)|$ is the number of distinct bases of G.

Irredundant generating sets for arbitrary finite groups have very few of these properties in the general case.

Exercise 3. All but one of these 6 properties fail to hold for some finite group G. Find examples for the 5 that fail. For the one remaining property that always holds, give a proof. These are easy to do.

Nevertheless for a given group, a study of how closely irredundant generating sets are to having these properties provides a useful framework to guide their study. We list here a few general results.

Tarksi's Theorem

For example the first theorem in the subject, due to Tarski, asserts that there are no gaps between the sizes of irredundant generating sets: For any k, $r(G) \leq k \leq m(G)$, there exists an irredundant generating set with k elements.

One interesting problem is to determine the numbers $r(G)$, $m(G)$, and $i(G)$. In 1936 P. Hall gave a method of computing $r(G)$ using the Möbius function of the lattice of subgroups of the finite group G. This method turns out to be fairly efficient and works well computationally for groups of small size. More recently D. Collins found a formula for $m(G)$ in terms of the Möbius function. However, computationally the formula turns out to be quite inefficient. The formulas of Hall and Collins actually determine more, namely the number of irredundant generating sequences of a specific length. It's thus conceivable that there might be simpler methods to determine $r(G)$ and $m(G)$ without determining how many there are of the given length at the same time. For solvable groups there is an alternate method to compute $m(G)$ in terms of a chief series for G that is also efficient computationally. As yet no such method is known for determining $m(G)$ for non-solvable groups in terms of a chief series for the group. As yet there is no easy way to determine $i(G)$.

Several other results can be obtained from Tarski-like arguments, which are very simple: Given a fixed irredundant generating set, one just measures distances between elements, sets, sequences, etc. in a group by counting the number of operations (multiplications by single elements of the given generating set) used to go from one to the other. Explicitly, given an irredundant generating set B and an element $g \in G$ write g as a product of elements of B but use only positive exponents on the elements of B. For this particular representation of g as a product, the sum of the exponents is called the *length* of g (with respect to this representation as a product). We then define $\ell_B(g)$ to be the minimum of the lengths of g taken over all possible ways of representing g as a product as just described. One can then use this function ℓ to define distances between elements, sets of elements, or sequences of elements in G, but in several different ways. In Tarski's original paper he uses the same kind of idea to define the notion of distance, but in yet another way. However all methods are based on counting the number of multiplications used. It seems very likely that there are other results which may be proven by using variations on Tarski's original idea. This is certainly an area which deserves further study.

The Frattini Subgroup

The Frattini subgroup, $\Phi(G)$, of a group G is the set of elements that are non-generators (that is, can be removed from any set that generates yielding a set that still generates). This subgroup can also be described as the intersection of all maximal subgroups of the group. In many situations it plays a trivial role, that is, it is straightforward to describe what happens for G in terms of what happens for $G/\Phi(G)$. Sometimes below we describe what happens in the Frattini-free case (i.e., $\Phi(G) = 1$) to simplify the statements. Section 6.1 of the book of Dummit and Foote and in particular the exercises (page 199) provide a lot of information on the properties of the Frattini subgroup. If one also knows something about ring theory, then one should see the analogy between the behavior of the Frattini subgroup and the Jacobson radical.

The Replacement Property

An irredundant generating sequence s satisfies the *replacement property* if for any element g not equal to 1, there exists some element of s which when replaced by g, gives a new generating set s' for G. The group G satisfies the *replacement property for* k if all irredundant generating sets of size k satisfy the replacement property. If G satisfies the replacement property, then it's easy to see that $\Phi(G) = 1$.

For vector spaces a standard result (appearing in developments of linear algebra in earlier years) called the Steinitz Exchange Property asserts that for any basis B of a vector space V and any independent subset S of V, there exists a subset of B which when replaced by S yields a basis for V. Our replacement property differs in two ways: we replace only one element, and the resulting new set generates G but isn't necessarily irredundant.

Using the same (Tarski) type of argument, one can show that there may be a weak version of the Steinitz Exchange Property, but only for sets of size $m(G)$: If G has the replacement property for all irredundant generating sets of size k, then $k = m(G)$.

Many groups have the replacement property for $m(G)$: vector spaces, Frattini-free abelian groups, the symmetric groups and many small non-abelian simple groups. However, many solvable groups do not, with the Frobenius group of order 20 ($\mathrm{Aut}(\mathbb{Z}_5) = \mathbb{Z}_5 \rtimes \mathbb{Z}_4$) being the smallest. One can give an explicit characterization of the solvable groups having the replacement property, but very little is known about the non-solvable case. An example of a simple group where the replacement property does not hold is $PSL(2, \mathbb{Z}_{17})$.

Geometry

One can determine the behavior of these functions on the direct product of groups. Both m and i are additive, that is, $m(G \times H) = m(G) + m(H)$. A theorem of Gaschütz gives a simple but more complicated formula for $r(G \times H)$. For two groups which are relatively prime (no common non-trivial homomorphic images) all three are easily shown to be additive. If further, both groups satisfy the replacement property, then the irredundant generating sets of length $m(G) + m(H)$ are obtained by taking the union of the images (under the natural maps) of irredundant generating sets of maximal length for G and H. Only in special cases (e.g., direct products of simple groups or solvable groups) is this formula known more generally. This will be one of the problems we study.

The behavior of these functions under semi-direct products or more complicated extensions is not understood very well, especially in the non-solvable case. Examples of specific questions are

- Find a nice description for length-$m(G)$ irredundant generating set in A_n,
- Determine $m(G)$ exactly and find a nice description for length-$m(G)$ irredundant generating sets in various $PSL(n, q)$,
- Determine $m(G)$ in other simple group families (or for sporadic groups), and find nice description for length-$m(G)$ irredundant generating sets there.
- Determine a recursive way to find and count length-$m(G)$ irredundant generating sets for solvable groups.

Until recently, it would have been very difficult to make much progress on problems of this type without a great deal of background in group theory. However, a new approach which in essence is geometric in nature provides computationally very efficient ways to quickly determine all irredundant generating sequences of any length for any finite group. It seems likely that such ideas will also provide efficient means for proving theorems, but much is still to be worked out. For example, it is now easy to prove the previously unknown $m(M_{11}) = 5$ where M_{11} denotes the smallest sporadic simple Mathieu group. Such arguments are given by relating $m(G)$ to $i(M)$ for all maximal subgroups M of G as is suggested by the work of Whiston:

$$m(G) \leq 1 + \max\{\, i(M) \mid M \text{ maximal in } G \,\} .$$

Thus, computationally at least, one should determine both $m(G)$ and $i(G)$ together recursively. We develop a more subtle version of the preceding inequality that depends on the existence of certain families of $m(G)$ maximal subgroups of G which are in what is called *general position.* The latter is in essence a geometric condition and will be one of the main topics of study. Results for small groups suggests that one conceivable interpretation of the computation is that it gives an explicit version of the Möbius function computation: the terms have been grouped togather in a natural way so that all of the cancellations from the negative values of the Möbius functions have already occurred and what is left is a sum of positive terms.

Homogeneous Covers

If one considers universal mapping properties such as are possessed by bases of vector spaces (the last property in our original list), bases of groups do not have that property in general. Let G be any finite group and n an integer with $n \geq r(G)$. Define the *n-th homogeneous cover* of G to be the group $H(n,G) = F_n/K$ where K is the intersection of all of the kernels of the surjective homomorphisms from the free group of rank n onto G. Note that each generating sequence of G of length n gives rise to such a kernel. The groups $H = H(n,G)$ that arise by this construction are called *homogeneous of rank n*. They can be described in several equivalent ways:

- H satisfies a certain universal mapping propery,
- $\mathrm{Aut}(H)$ acts transitively on the set of generating sequences of H of length n,
- the presentations for H with respect to any basis of size n are identical.

For G abelian, then $H(n,G) \approx (\mathbb{Z}_e)^n$ where $e = \exp(G)$ is the exponent of G. For $G = A_5$ we have $H(2, A_5) \approx (A_5)^{19}$. The exponent 19 occurs in the last example because there are 19 orbits of the group $\mathrm{Aut}(A_5) = S_5$ acting in the natural way on the ordered pairs of generators (i.e., ordered bases of size 2) of A_5. More generally for any non-abelian simple group S and any integer $n \geq r(S) = 2$, there exists a certain unique integer-valued function $f(n)$ (which depends on S) such that $H(n,S) \approx S^{f(n)}$. This last result is a consequence of work of P. Hall around 1936. These and related questions were investigated by Neumann and Neumann and were the motivation for the result of Gaschütz mentioned earlier. In fact, essentially the same construction appears in a standard proof that any finitely generated residually finite group is hopfian. The ordinary quaternion group Q_8 of order 8 has this property, as do all of the non-abelian p groups of order p^3 which have exponent p (that is, all non-identity elements have order p).

Exercise 4. Prove the statement about abelian homogeneous groups of rank n. Verify that the groups of order p^3 mentioned are the only non-abelian groups of this order which are homogeneous of rank 2.

The homogeneous cover of G is given as the subdirect product of a number of copies of G and hence has properties that are very much like those of G. For example, $H(n,G)$ is solvable if and only if G is solvable and they both have the same derived length. The two groups even have the same simple Jordan-Hölder components although not necessarily the same number of each type.

Many interesting questions arise from the study of these groups. For example, each of the elements of a set of n generators of such a group will have all the same properties. They all have the same exponent for example. If $n > r(G)$, that exponent is just $\exp(G)$. It is always true that the exponent of these generators divides $\exp(G)$. However, if $n = r(G)$ that is not necessarily the case. The smallest such example which has order 72 is the group $G = (\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes Q_8$ where Q_8 acts as a group of matrices sitting inside $\mathrm{GL}(2, \mathbb{Z}_3)$. The group G has $r(G) = 2$ and $\exp(H(2, G)) = 4$ whereas $\exp(G) = 12$. It appears that a prime has vanished! The groups doing the acting in the semi-direct product, e.g., Q_8 were called "secretive" in some publications. A generalization of an idea of W. Scharlau gives a way of directly determining which such groups have this "secretive" property.

An even more suble question about homogeneous groups arises in the case of p-groups: For a finite p-group G is it true that there exists an irredundant generating sequence of G of length $r(G)$ which contains an element having exponent $\exp(G)$? A group for which this property fails will also fail to satisfy the Hughes Conjecture. The Hughes Conjecture is known to be false, but the smallest counterexamples are of order 5^{48} (Havas and Vaughan-Lee); so a counterexample to our question about generators must be at least as large.

Origins

The previous discussion is the original entry point into this topic for the second author of this note. About 15 years ago, Persi Diaconis asked him if it would be possible to define a "K-theory" of finite groups based on n-tuples of group elements (instead of n-tuples of elements of a free module as in the classical case). Algebraic K-theory is a subject which is often considered to be a generalization of linear algebra from the study of vector spaces over a field to the study of modules over an arbitrary ring. The ideas of Neumann and Neumann suggest a natural way to associate with any finite group and positive integer $n \geq r(G)$ a homogeneous cover H of G having $r(H) = n$ with H being as close to G as possible (e.g., it has the same composition factors) and which has the appropriate universal mapping property which could thus be used as an analogue of "free modules". One would then take the automorphism groups of these along with natural maps to construct groups which would play the role of the general linear groups in ordinary algebraic K-theory. This remark is inserted merely for motivational purposes since we will neither be discussing nor attempting to construct such a theory. In particular, it is not necessary to have any familiarity with any of the concepts in this remark. However, this point of view and particularly trying to carry out such a construction, gives rise to a multitude of interesting questions about finite groups. Further, it suggests that any success in the current program might well have interesting consequences for the development of group theory.