Parity and Correlation in Probabilistic Group Theory

Abstract. This is the Master's Thesis of Tai Kaufman at UCI Irvine, June 2001, directed by Professor Michael Fried. Group theory arises with symmetry investigations of data. When groups of symmetries are (almost) simple, there is an interesting phenomenon: Two randomly selected elements selected among those symmetries can, with high probability, generate the whole group. If the group is simple, that probability is close to 1. This holds for the symmetric group on n letters, S_n, or its index two alternating subgroup, no matter the size of n. We take as a hypothesis, that two elements generate S_n. Then, we consider how they generate S_n. We call this more subtle aspect of generation the correlation between the generators. Our concentration is on the special case $n = 8$. This value is big enough to produce interesting relations with such famous problems as (2,3)-generation from the literature. It is small enough to pose questions on whether human perception can detect the phenomenon of parity of permutations.

Contents

CHAPTER 1

INTRODUCTION

We investigate the first group that arises in probabilistic group theory, the group of permutations of all integers $1, 2, \ldots, n$. Mathematicians denote this S_n, where the letter S stands for symmetric. To get insight on the group of all permutations, we chose to focus on the case $n = 8$ – permutations of just eight objects. This might seem like arbitrary choice. We found, however, that the number eight was just large enough to pose combinatorial variability and yet just small enough that our limited group theory backgrounds could handle applying mathematics to it. Prof. Fried is not a group theorist, though he uses group theory in his work, and this thesis clearly uses much of his technical expertise.

We will raise and answer several questions about this group. For example, which pairs of elements of S_8 can generate all of S_8? Can we visualize S_8 in some simple way? Such questions may appear overwhelming, since S_8, having order $8! = 40,320$, appears large. I found, however, I could greatly simplify these problems using subjects from my algebra classes at UCI, like subgroups, conjugacy classes, and orders of elements; and topics from my complex variables classes, like Möbius transformations.

This paper researches a substantial problem in group theory and relates the mathematics to practical situations and the value of elementary group theory in secondary school mathematics. Thus it will be of interest to students and teachers of group theory, math researchers, and high school math teachers. We assume the reader knows the basic definitions behind group theory, but may need reminders of some definitions and conventions. Since the groups in this thesis are explicit, we don't require much from the reader's background.

In this first chapter, after declaring our goals and previewing our mathematical results we begin by illustrating commutative and noncommutative operations in everyday life. Then, we show how noncommutativity produces complexity and lends mystery to our research questions, which we state at the end of the chapter. We also discuss group theory basics and probabilistic group theory results germane to our questions. Then we approach our research questions in two parts, first treating a specific case in Chap. 2, then the more general case in Chap. 3. We find the latter to require some theory of *primitive groups*, which we treat in Chap. 4. In Chap. 5 we conclude with pedagogical aspects of our work and visualization of the problems with BASIC programs.

1. OVERVIEW GOALS

Prof. Fried and I to answer a question that many students ask: What is the group theory of a first-year graduate student for? Is it possible to explain its relation to high school mathematics and its value to many high school teachers or students? Is is possible to show that operations generating groups do appear naturally in

everyday life? We consider these hard tasks, not finished here. Still, we hope a high school teacher hearing our efforts to make these connections could say he now has a better idea of group theory being more than just a subtle topic suitable for separating graduate students according to their technical abilities.

1.1. Noncommuting operations. Pairs of invertible operations on sets arise in everyday life, for the display of physical objects, and generation of data. There is a major difference between commuting and noncommuting operations. In the former case such a pair will usually generate only a small pair of total operations. This thesis explores the latter case: How to decide the maximal group of operations two noncommuting operations can generate. A major phenomenon in group theory is that two elements randomly chosen from even some large complicated groups can generate the group with high probability. One condition guaranteeing this is the group has large order and is a member of a sequence of simple groups. To consider how two elements generate a group we introduce a statistic we call the *correlation*. The correlation of two elements x and y of a group G is $\langle (x, y), (y, x) \rangle$, a new group inside $G \times G$.

The idea that the order is large requires considering natural series of groups. The classification of finite simple groups includes many such series. Still, there are other series, like the symmetric groups that aren't simple, and are even more likely to have applications. We explore that for these the probability of generation for a random pair (assuming the order is large) approaches some fixed number smaller than 1. We intensively investigate the case $G = S_8$, describing the possible correlations. One case comes out especially interesting. That was where two elements were in the same conjugacy class. The correlation then depends on the element giving the conjugation between them.

1.2. Proof versus computer program. Further, we compare the software program GAP with pure mathematical proof. We find that proof is immensely more efficient and revealing about what is causing certain phenomena. Sometimes, however, an expeditious use of GAP showed there was something to find. Since finding proofs requires great training, using GAP gave surprising motivation in acquiring that training.

We also wrote BASIC programs to visualize the groups and problems in question. These programs confirm for even small values of n results about the distribution of the number of cycles and orders of elements in S_n discovered by Erdös and Turán. These results drove much of modern research in probabilistic group theory.

1.3. Seeing group structures. Finally, we argue the value of introducing geometric situations from group theory into high school mathematics. Algebra and geometry have different domains in most high school classes. Understanding the effect of composing simple geometric operations benefits from geometric visualization. Having command of the total possible geometric operations generated by any two requires the algebra of conjugacy classes in groups, and a more modern form of proof than that of geometry. We claim a problem similar to ours, combined with a treatment of probability and statistics in Algebra II courses, would effectively reveal how groups generated by noncommuting operations belong in high school. In the present system both geometric and algebraic use of function composition (called change of variables) is a great hurdle for most students in several variables

calculus. This topic runs any higher use of mathematics in applications. Yet, the curriculum crams it in such a small place, few ever master it.

The notion of two sets being in parity appears in our visual discussion of the correlation of two banks of lights §3. We would not expect someone viewing the visual displays illustrating correlation between generators to catch that behind this lay the alternating group of degree 8 and that its essential property is from Galois' Theorem that it is a simple group. Yet, the *only* constraint on the displays from the two banks of lights is that they will always be in parity. This is essentially equivalent to the special case of Galois' Theorem. So, if a viewer of these displays could detect that parity agreement is the only constraint, this might mean that simple groups can reveal themselves visually. It is actually a psychology experiment we haven't, though could have, performed: *Can the human eye (perception system) detect parity agreement?*

2. SUMMARY OF TECHNICAL CONTRIBUTIONS

We make contributions to a conjecture that two randomly chosen elements from S_n generate all of S_n has probability tending to $3/4$ as $n \mapsto \infty$ (Chap. 1 Conj. 6.1).

Much of this thesis is about understanding how someone works with groups, their subgroups and conjugacy classes. We apply this to computations in S_8. Two results in the paper call for determining subgroups in challenging situations generated by two elements x and y. We denote the subgroup by the notation $\langle x, y\rangle$. Key notions are *transitive* and *primitive* subgroup. Given specific elements x and y it is usually obvious when $\langle x, y\rangle$ is a transitive subgroup. The case of Chap. 3 Lem. 9.3 is where x has order four and cycle type $(2)(2)(4)$ acting on the integers $\{1, \ldots, 8\}$ and y is the conjugation of x by an element β of order two. The result is a characterization of this situation so that $\langle x, y\rangle$ is a primitive group, from which we deduce it is S_8. This produces cases that achieve the most interesting of the correlation groups $\mathrm{Cor}(x, y)$.

Chap. 4 Prop. 5.3 produces the one primitive proper subgroup of S_8 that is not in A_8, and so it completes our classification of primitive subgroups of S_8, a key to deciding when $\langle x, y\rangle = S_8$. The group in this case is $\mathrm{PGL}_2(\mathbb{F}_7)$ which is like the group of Möbius transformations in complex variables, except the functions $z \mapsto \frac{az+b}{cz+d}$ (with $ad - bc \neq 0$) have a, b, c, d in the finite field $\mathbb{F}_7$ instead of in the complex numbers. This group and certain of its subgroups play appear in the problem of (2,3)-generation that motivated many results from [**Sh01**].

Chap. 4 Prop. 1.1 shows that A_8 is not (2,3)-generated. We explain why this is an interesting borderline to Miller's Theorem. It was especially interesting to us, because it corroborated that our intuitive choice of using S_8 as our explicit focus group revealed many historically interesting mathematical phenomena.

Chap. 4 Prop. 5.4 gives the other significant proper primitive subgroup of S_8, the group generated by translations by elements in the vector space $(\mathbb{Z}/2)^3 = V$ and the matrix operations of $G = \mathrm{GL}_3(\mathbb{Z}/2)$, invertible 3×3 matrices acting on V.

Finally, we tried to show that our investigations fit nicely with an advanced research topic, on probabilistic generation of finite simple groups. The recently proved Main Conjecture in that area is Thm. 4.1.

3. COMMUTING AND NONCOMMUTING OPERATIONS

We recall the definition of commutativity. Call an operation on any finite set S *invertible* if its range includes each point of S. It is then automatic that no pair of distinct points goes to the same point. A common use for the word operation is a *function* from S to S. Then, the invertible operations $\mathrm{Aut}(S)$ form a *group* by using composition of two such as *multiplication*. We say two elements $g_1, g_2 \in \mathrm{Aut}(S)$, *commute* if for $s \in S$, the effect of g_1 on $g_2(s)$ gives the same result as the effect of g_2 on $g_1(s)$. In mathematical notation $g_2 \circ g_1 = g_1 \circ g_2$, where $\circ$ means *compose*.

It may surprise even those who have had traditional group theory course how little information one must give to create a very big group from only a few of its elements if the elements are far from commuting. This group itself is a measure of the meaning of what it means to be *far from commuting*.

In everyday life we often come upon commuting operations. For example: If a lazy Susan set of shelves contains books or art objects for a display, people will look at the items in the shelves by turning the lazy Susan an appropriate number of degrees. The display of the shelves by a turning of θ_1 degrees, followed by someone else turning it θ_2 degrees leads to a total turn of $\theta_1 + \theta_2$ degrees, the exact same result for the two people turning the shelves in the opposite order.

Less common, though still present in everyday life, we see noncommuting operations. For example: Suppose a globe has two rods, called R_1 and R_2, through the center sticking a short way out of it, at an angle (in their plane) of 90 degrees. Suppose further you can choose either one of the rods and you can rotate the globe any desired angle around either rod. The purpose might be to rotate the globe to display part of the surface. Then, the operation of rotating through an angle of θ_1 degrees around R_1 followed by rotating through θ_2 degrees around R_2 might not lead to the same show of the globe's surface as first rotating θ_2 degrees around R_2, then rotating through θ_1 degrees around R_1.

In our main example — closely related to our research questions — we picture the operations A and B as a way of getting a variable display of colored lights. The eight numbers 1 through 8 might correspond to an even spacing of eight colors on bulbs, from red to violet, with two banks Bank_1 and Bank_2 of such lights. Then, A corresponds to switching the colors on the first two lights of Bank_1 and shifting the colors to the right on Bank_2 (wrapping the last light around to first position). Then, B corresponds to doing the same thing with the two banks of lights switched. The goal here is to offer an interesting display of great variability in the colors in the two banks of lights through the simple device of having a somewhat random choice each second of whether it is A or B that goes into effect.

Would the arrays that come up in each bank then appear purely random? Also, would there be other special properties, like a correlation between the colors seen on Bank_1 versus those on Bank_2?

As a final example, it is also possible to describe biological processes as the result of two disparate though related operations on the state of an organism. The operations could lead to the organism either orienting itself to its environment or displaying itself for sexual attraction in an interesting way.

4. PROBABILISTIC GROUP THEORY PUZZLES

The bank of lights example was interesting to us, for it displayed through mathematics that two operations, because they were noncommuting, could generate

so many visual possibilities as total possible operations on the two banks of lights. When we saw [**Sh01**], we realized that more than a century of mathematical papers had topics closely related to our curiosity about selecting elements randomly from a group. Our topic of investigating the possibility of making something from the group theory of a simple master's level course was close to doing serious research in mathematics.

The most fundamental notion of group theory is the subgroup, and distinguished in the topic of subgroups is that of a *normal* subgroup (§5). There is no particularly useful classification of all finite groups. There is, however, a classification of all groups having no proper normal subgroups: the *simple* groups. This, one of the biggest theorems in Twentieth Century mathematics, is called the *classification of finite simple groups*. This theorem is very difficult to understand. I understand few mathematicians can even state it precisely. Still, group theorists have found it extremely useful, and among its corollaries is the following (explained in [**Sh01**]). For a set S use the notation $|S|$ for its cardinality.

THEOREM 4.1. *Suppose G is a finite group and L_G is the number of pairs $(x, y) \in G \times G$ such that x and y generate G (see below; $\langle x, y\rangle = G$). Then, if G is simple, $P_G = \frac{L_G}{|G|^2}$ approaches 1 as $|G|$ gets large.*

Since the set of simple groups is large and complicated, this theorem is a qualitative expression of how two simple noncommuting processes generate many complicated processes by iteration. There are reasons for considering other series of groups, not necessarily simple, such as the symmetric groups, for they are likely to be the actual groups that appear in applications.

A near corollary of Thm. 4.1 is our Conj. 6.1: That for n large, roughly three out of four times, when you select two elements x and y from S_n, these elements will generate the whole group of permutations. Another way to put this: Given any small positive number ϵ, there exists a number N such that if n is greater than N, then for a random pair $(x, y) \in S_n \times S_n$, the smallest subgroup of S_n containing both x and y is just S_n with probability $\frac{3}{4} - \epsilon$. The *near proof* uses only the case of Thm. 4.1 for the subset of simple groups called the alternating groups (§5).

Galois discovered the alternating groups and the series of simple groups called $\mathrm{PSL}_2(\mathbb{F}_q)$ by 1830. It wasn't until the 1950s that the list of simple groups extended much beyond Galois' knowledge of them. We use only those simple groups he knew.

It is usually not obvious what is the the smallest subgroup containing a given x and y. We denote this subgroup by $\langle x, y\rangle$, and think of it as *group closure* in the way that topology thinks of the closure of a set. Chap. 3 §4 illustrates it takes nontrivial ideas to figure what is $\langle x, y\rangle$ even for subgroups of S_8.

5. GROUP BASICS FOR INVESTIGATING S_8

We review some basics and declare our terminology and notation. First, *disjoint cycle notation* will be useful. To illustrate it, suppose $n = 16$, and g is given by

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 16 & 12 & 9 & 8 & 1 & 3 & 2 & 5 & 6 & 10 & 11 & 7 & 4 & 13 & 14 & 15 \end{pmatrix}.$$

The notation indicates g maps 9 to 6. Disjoint cycle notation for g represents g as a product of disjoint cycles of integers. It requires fewer symbols than the complete permutation notation. Also, it shortens computations in S_n by parsing the group

action into memorable pieces. The disjoint cycle representation for g is

$$(1\,16\,15\,14\,13\,4\,8\,5)(2\,12\,7)(9\,6\,3).$$

Within each cycle, $g(i)$ is placed to the right of i; the order of the disjoint cycles is unimportant. That is, $g(1) = 16$ appears to the right of 1, and the cycle closes at 5 because $g(5)$ is 1, at the beginning of the cycle. Further, exclude the cycles of length 1 ($g(10) = 10$ gives a cycle (10)) for efficiency. An element of S_n is a *k-cycle*, $k > 1$ if it has one and only one cycle —of length k —of length bigger than 1.

EXAMPLE 5.1 (Noncommuting). Suppose $g \in S_n$. If g is an n-cycle, written as $(i_1, \ldots, i_n)$. Then the only elements h that commute with g are the powers of g. More generally we will use, in some computations, that it is easy to write down the collection of elements in S_n commuting with any particular $g' \in S_n$ —called the *centralizer* of g' —if we have a practical display of its disjoint cycle decomposition. For example, in Ex. 7.1 we write down the centralizer of an element in S_8 having disjoint cycle shape (2)(2)(4). That centralizer appears in the examples using elements of that shape.

Often the crucial property we ask for a subset $S \subset S_n$ is this: Is S closed under composing its permutations? That is, for $g, g' \in S$, is $gg' \in S$? This is the necessary and sufficient condition that S is a *subgroup* of S_n.

The most important subgroup of S_n is the *alternating group* A_n. This is the subset of permutations one can write as products of an even number of 2-cycles.

For any two elements g, h in a group, a key operation is that of conjugation of h by g. This produces the element ghg^{-1}. For any set S, denote the result of conjugating every element in S by g by ${}^gS$. If S is a group in S_n, then ${}^gS$ will be also. So, assume $G = S$ is a group. The effect of conjugating G by $g \in S_n$ is to consider G as exactly the same elements, though regarded as permutations of $\{1', 2', \ldots, n'\}$ where j' is the integer $g(j)$. That is, we have merely renamed the integers $\{1, 2, \ldots, n\}$. In looking at subgroups G of S_n, for many tasks there would be no point in distinguishing the groups G and gGg^{-1}.

A subgroup H of another group G is called *normal* if for each $h \in H$ and each $g \in G$, $hgh^{-1} \in H$. That is, H is closed under conjugations by elements from G. A group G is called *simple* if it has no normal subgroups except itself and $\{1\}$. Galois (1840) proved that A_n is a simple group if $n \geq 5$. We use that A_8 is a simple group in every aspect of our examples.

Cyclic groups are those generated by a single element. The cardinality of a cyclic group is called the *order* (of the element generating it). Cyclic groups look easy and very understandable to us. They appear in many undergraduate courses under the title of *generalizations of clock arithmetic*. If the order of a cyclic group is a prime number, the cyclic group is also simple. It has no proper subgroups at all! These, however, are the trivial simple groups, and we exclude them from now on when referring to simple groups.

6. DIXON'S 1969 CONJECTURE [D69]

Dixon proposed that two randomly chosen elements of a finite simple group G generate G with probability approaching 1 as $|G| \mapsto \infty$. [**KL90**] and [**LiSh95**] have since shown this. This theorem can be applied to the sequence of alternating groups $\{A_n\}_{n=5}^{\infty}$, since since they are (finite) simple groups. In combinatorial practice,

operations are from groups that contain simple subgroups properly. We confined our thinking to the example of S_n and we made the following conjecture.

CONJECTURE 6.1. The probability that two randomly chosen elements from S_n generate all permutations tends to $3/4$ as $n \mapsto \infty$.

PROOF DEPENDING ON A HYPOTHESIS. Suppose there is a fixed integer N and N words $w_1, \ldots, w_N$ in the letters x and y so the following holds.

(6.1a) For each i, and $(x, y) \in (S_n \setminus A_n) \times A_n$, $w_i(x, y) \in A_n$.
(6.1b) For some $i_{x,y} \in \{1, \ldots, N\}$,

$$2|\{w_{i_{x,y}}(x, y), y)\}_{(x,y)\in(S_n\setminus A_n)\times A_n}|/(n!)^2 \mapsto 1 \text{ as } n \mapsto \infty.$$

There are four cases to consider: $(x, y) \in A_n \times A_n$, (x, y) or (y, x) in $(S_n \setminus A_n) \times A_n$ or $(x, y) \in (S_n \setminus A_n) \times (S_n \setminus A_n)$. In the first case the probability is 0 that $\langle x, y\rangle = S_n$. We want to show, in each of the other cases, that the probability of $\langle x, y\rangle = S_n$ approaches 1 for large n. Assume the second case holds.

Apply Dixon's Conjecture to the case of the alternating groups. By hypothesis (6.1), with probability 1 for n large, there is a choice of i so that $\langle w_i(x, y), y\rangle = A_n$. Since $xA_n = S_n \setminus A_n$, we get $\langle x, y\rangle = S_n$ with probability 1.

We don't need an extra hypothesis when both x and y are in $S_n \setminus A_n$ because $\langle x, xy\rangle = \langle x, y\rangle$ and (x, xy) is appropriate for hypothesis (6.1). Hence, for n large, $3/4$ of the time we will be able to write all elements of S_n as words in x and y. □

We give an example of two elements x and y generating S_n.

LEMMA 6.2. *Let* $x = (1\,k)$ *and* $y = (1 \ldots n)$ *with* $(k-1, n) = 1$. *Then* $\langle x, y\rangle = S_n$.

PROOF. First do the case when $k = 2$. Note that $z = xy = (2 \ldots n)$. The conjugate of x by z^j is $z^j x z^{-j}$. This is a 2-cycle that permutes 1 and $j+2$: $(1\,j+2)$. Conjugating 2-cycles of form $(1\,k)$ by powers of y gives all possible 2-cycles in S_n. Therefore $\langle x, y\rangle = S_n$.

Now consider the general case when $(k-1, n) = 1$, and let ℓ be an integer so that $\ell(k-1) \equiv 1 \mod n$. Then, $\langle y^\ell\rangle = \langle y\rangle$, so $\langle x, y^\ell\rangle = S_n$. If we write y^ℓ as $(1' \ldots n')$ by changing the names of the integers so that $1 = 1'$, then 2 is renamed to k. The general case now follows from the particular case. □

7. OUR QUESTIONS

Some subtler questions have not been investigated by probabilistic group theory to our knowledge. This thesis introduces terminology and notation in what we call the correlation between (or of) x and y. It is the group generated in $S_n \times S_n$ by the two elements $A = (x, y)$ and $B = (y, x)$. Denote this $\mathrm{Cor}(x, y)$. Our questions below show points of interest in computing $\mathrm{Cor}(x, y)$. We use conjugacy classes under S_n of two element sets $\{x, y\}_{x,y\in S_8}$. In Chap. 2 we then focus on the case $n = 8, x = (1\,2)$ and $y = (1\,2\,3\,4\,5\,6\,7\,8)$. Then Chap. 3 addresses general pairs $\{x, y\}$ when $n = 8$.

We carefully inspect answers to these questions:

(7.1a) For a given n and a given pair x and y, what are the possible elements in $\mathrm{Cor}(x, y)$?

(7.1b) If the answer to (7.2a) indicates a certain element should be in $\mathrm{Cor}(x, y)$, how can we construct it as a product of a string of the elements $A = (x, y)$ and $B = (y, x)$?

More difficult for us are the following questions, to which this investigation provide clues.

(7.2a) Suppose the answer to (7.1a) predicts that a certain element, C, should be in $\mathrm{Cor}(x, y)$. Assume on the jth trial we randomly select an operator O_j from $\{A, B\}$, and form the words

$$O_1 = w_1,\ O_1O_2 = w_2, \ldots,\ O_1O_2O_3 \cdots O_j = w_j,\ \ldots$$

With what frequency does C appear within k trials for k large?

(7.2b) Given again a certain element C of $\mathrm{Cor}(x, y)$, if we systematically generate elements of $\mathrm{Cor}(x, y)$ by multiplying longer and longer strings in A and B (like binary numbers), after how many trials will that given element of $\mathrm{Cor}(x, y)$ appear?

(7.2c) What is the distribution of those randomly generated elements?

(7.2d) What is the expectation profile for hitting elements by all products of length $\leq k$?

(7.2e) Given x and y (and so A and B giving the correlation) that generate S_n, suppose k is large and even. Will the distributions of elements that are exactly k products from $\{A, B\}$ be the same as that for $k + 2$?

CHAPTER 2

FIRST INVESTIGATIONS FOR $n = 8$

This chapter answers (7.1) when $n = 8$, $x = (1\,2)$ and $y = (1\,2\,3\,4\,5\,6\,7\,8)$.

0.1. ANSWERS TO (7.1a)**.** We already know from Chap. 1 Lem. 6.2 that x and y generate S_8. The generators A and B are both (odd,odd) elements. Denote the subgroup of $S_8 \times S_8$ consisting of pairs (g_1, g_2) with $g_1 g_2^{-1} \in A_8$ by $S_8 \times_* S_8$.

LEMMA 0.1. *For x and y in our special case, let K be the subgroup of* $\mathrm{Cor}(x, y)$ *consisting of elements of the form* $(1\,k)$*. Then, K contains* $(1, (1\,5)(2\,6)(3\,7)(4\,8)) = (1, h)$*,* $(1, h^*) = (1, (2\,5)(1\,6)(3\,7)(4\,8))$ *and* $(1, hh^*) = (1, (1\,2)(5\,6))$*. Conclude that* $\mathrm{Cor}(x, y) = S_8 \times_* S_8$*.*

PROOF. Notice K contains $(x, y)^4 = (1, h)$. To see K is a normal subgroup of $\mathrm{Cor}(x, y)$, note that for any $g = (a, b) \in S_n \times S_n$ and any $(1, k) \in K$,

$$g(1, k)g^{-1} = (aa^{-1}, bkb^{-1}) = (1, bkb^{-1})$$

is still in K. So, K also contains $B(1, h)B^{-1} = (1, h^*)$. Notice that K is isomorphic to a subgroup of S_8 via the projection $(1\,k) \mapsto k$. Since K is normal in $\mathrm{Cor}(x, y)$, its image in S_8 is also normal in S_8. The image of K in S_8 is nontrivial because it contains $(x, y)(x, y) = (1, yy)$.

Further, as two (odd,odd) elements generate $\mathrm{Cor}(x, y)$, all elements in $\mathrm{Cor}(x, y)$ have the form (even,even) or (odd,odd). So, $(1, k)$ has the form (even, even). Therefore the image of K is a subgroup of S_8 inside of A_8, the alternating group on eight elements. By Galois' theorem, A_8 is a simple group and so K must equal the set of elements of the form $(1, u)$ with $u \in A_8$. Similarly, the set of all (even, 1) is another subgroup of $\mathrm{Cor}(x, y)$. So, $\mathrm{Cor}(x, y)$ contains all (even, even) elements.

As the generators of $\mathrm{Cor}(x, y)$ have the form (odd, odd), we conclude $\mathrm{Cor}(x, y)$ also contains all (odd, odd) elements. Since $\mathrm{Cor}(x, y)$ must be a subset of (odd,odd) $\cup$ (even,even), this implies $\mathrm{Cor}(x, y)$ is precisely all (odd,odd) and (even,even) permutations of $S_8 \times S_8$. □

1. USING THE PROOF

We look first at a specific case. Since (x, x) has the form (odd,odd), our answer to (7.1a) shows it belongs in $\mathrm{Cor}(x, y)$. How can we express (x, x) as a word in $A = (x, y)$ and $B = (y, x)$?

My first approach to this was to multiply some short strings of A and B to try to produce (x, x). I reasoned that such a simple element should be expressible as a product of a very short string. After trying repeatedly without success, I turned to writing a QBASIC program (see Program 1 Chap. A), "S8S8CAL2," to systematically search through all string products to find it. Yet, S8S8CAL2 computed the products of all $A - B$ strings from length 1 through length 10 and failed to generate (x, x).

I thought that the proof of Lem. 0.1 would not tell me how to generate a specific element. When Prof. Fried challenged this assumption, I started to look for something in the proof indicating how to generate (x, x).

So here is how I used the proof to generate it. The proof builds elements of $\mathrm{Cor}(x, y)$ from the subgroup, K, of elements of the form $(1, k)$. Use Lem. 0.1 and the elements $(1, (1\,5)(2\,6)(3\,7)(4\,8)) = (1, h)$, $(1, (2\,5)(1\,6)(3\,7)(4\,8)) = (1, h^*)$ and $(1, hh^*) = (1, (1\,2)(5\,6))$ to produce (x, x). For example, if $(1, xy)$ appears, then we can produce $(x, x) = (1, xy)(x, y)^{-1} = (1, xy)A^{-1}$. Note that $xy = (1\,3\,4\,5\,6\,7\,8)$.

Conjugating $(1, k)$ by A (resp. B) is the same as replacing k by conjugation by x (resp. y). This conversation gets the result from the following lemma about computing words $w(x, y)$ (or strings) in x and y that achieve particular conjugations from the one element $hh^* = z$. Write $u = z_1z_2z_3$ with $z_1 = z$, $z_2 = (2\,3)(5\,7)$ and $z_3 = (2\,4)(1\,6)$, so $u = (1\,3\,4\,2\,6\,7\,5)$. We are using that it is easy to form whatever shape in A_8 we want by multiplying conjugates having the shape $(2)(2)$.

LEMMA 1.1. *An explicit word $w_i(x, y)$ conjugates z to z_i, $i = 2, 3$. Finally, an explicit word $w_4(x, y)$ conjugates u to z. Putting this together gives (x, x) as a specific word in A and B.*

PROOF. Conjugation by $\beta = (1\,3)(6\,7)$ takes z to z_2. So, if we write β as a word in x and y that gives the word w_2. The proof of Chap. 1 Lem. 6.2 is explicit in finding words in x and y that give any two cycle in S_8. So we easily get $(1\,3)$ and $(6\,7)$ as words in x and y. Then multiply these to get the word $w_2(x, y)$. The other cases are essentially the same. □

This demonstrates how two proofs apply to write any element of $\mathrm{Cor}(x, y)$ as a word in A and B. Keeping track of all the intermediate words that are useful in writing x and y as products of conjugates of hh^* makes it look like a formidable process, though it all comes from recognizing how to use that all elements in S_8 of the same shape are conjugate.

2. LESSONS LEARNED FROM A PROOF

Our answer to (7.1b) used our proof of Lem. 0.1. It told what elements are in $\mathrm{Cor}(x, y)$, *and* it showed how to get a particular choice like (x, x). Though our proof did not explicitly say how to produce each given element of the group, it gave clues. There are several lessons I learned from this. It shows that proof is a powerful analytical tool. The proof was far more powerful than random guessing or a computer program in showing how to generate a specific element of the group.

Previously I thought of proofs as non-constructive, whereas this one does give a construction. I suspect many algebra proofs do give clues on how to construct objects that they declare to exist, though the amount and obviousness of the clues varies from proof to proof. For example, in contrast to this proof which gave only subtle clues, our proof of Lem. 6.2 explicitly shows how to get any 2-cycle. So it produces all permutations that it claims to exist in the group.

The proof of Lem. 0.1 and the construction in §1 also taught me something about groups which I had not understood from my graduate abstract algebra courses. It vividly reinforced that normal subgroups and isomorphisms are powerful tools in analyzing groups. For example, the proof used the normal subgroup K and an isomorphism between K and A_8. It showed that in examining S_n, the

alternating subgroup and the parity of permutations are important ideas. Furthermore, it showed the value of conjugation in constructing desired elements (as in our construction of (x, x)).

CHAPTER 3

COMPUTING CORRELATIONS IN S_8

In answering our questions in the more general case, at first it appears there are many choices to take for elements x and y —so many choices that it is prohibitive to try all pairs. *Conjugation*, however, diminishes the work of many computations.

1. USING CONJUGATION IN S_n

Suppose we start with a particular x and y and then take any element $g \in S_n$ to form a new pair $\{gxg^{-1}, gyg^{-1}\}$, the conjugate of $\{x, y\}$ by g. This new pair will have the same properties as did the old pair for most questions.

So, with no loss it makes sense to look at only one pair $\{x, y\}$ in each conjugacy class. Here are the questions we would ask.

(1.1a) How to list all conjugacy classes of pairs $\{x, y\}$ that generate S_8.
(1.1b) How to figure the group $\mathrm{Cor}(x, y)$ as we run over these conjugacy classes.
(1.1c) How to interpret the data we get.

We again concentrate on the case $n = 8$.

2. LISTING S_8 CONJUGACY CLASSES

Before answering which classes of pairs generate S_8, first consider how to list all classes of pairs. To represent the conjugacy classes of single elements in S_8, we can write all permutations as products of disjoint cycles of decreasing length. Example: $(1\,2\,3)(4\,5)$. Denote the cycle description of this element by $(3, 2; 3)$ meaning a 3-cycle, followed by a 2-cycle, followed by three 1-cycles. Then conjugacy classes correspond to partitions of the integer 8 via the following notation:

$$(n_1, \ldots, n_m; 8 - (n_1 + \cdots + n_m)), \quad n_1 \geq n_2 \geq \cdots \geq n_m > 1, n + 1 + \cdots + n_m \leq 8.$$

Thus the conjugacy classes in S_8 are

[cycle lengths larger than 1 ; number of fixed elements]
$[8; 0]$
$[7; 1]$
$[6, 2; 0]$ $[6; 2]$
$[5, 3; 0]$ $[5, 2; 1]$ $[5; 3]$
$[4, 4; 0]$ $[4, 3; 1]$ $[4, 2, 2; 0]$ $[4, 2; 2]$ $[4; 4]$
$[3, 3, 2; 0]$ $[3, 3; 2]$ $[3, 2, 2; 1]$ $[3, 2; 3]$ $[3; 5]$
$[2, 2, 2, 2; 0]$ $[2, 2, 2; 2]$ $[2, 2, ; 4]$ $[2; 6]$
$[; 8]$

Our goal is to list pairs $\{x, y\}$, up to the conjugation action of S_8 where $\langle x, y\rangle = S_8$. Using conjugation by S_8, we keep the first element, x, in simplest form, filling in its cycles with the numbers 1 through 8 in order. Then, systematically vary the possibilities for the second element y. For example, pairs of elements from

the conjugacy classes having the form $[5,2;0]$ and $[7;1]$ include such classes as $((1\,2\,3\,4\,5)(6\,7),(1\,2\,3\,4\,5\,6\,7))$ and $((1\,2\,3\,4\,5)(6\,7),(1\,2\,3\,4\,5\,6\,8))$.

These pairs represent distinct classes since only the latter moves the element 8.

3. S_8 ACTION ON UNORDERED PAIRS

Fixing x still allows conjugating y by elements in S_8 commuting with x. It is easy to figure out the elements that commute with a given x (see Lem. 3.1 for examples). We call this group $Z_{S_8}(x)$. So the problem of computing the S_8 conjugacy classes on pairs is straightforward. Still, computationally it is worth checking how hard it is to list the resulting pairs.

For simplicity, stay only with those pairs $\{x,y\}$ that could possibly generate S_8 (this will be explained below). In answering the question of which classes of pairs generate S_8, we now investigate some particular cases. From this point we extensively use the notion of primitivity from Chap. 4 §4. We use that S_8 (and A_8) are primitive groups in their action on $\{1,\dots,8\}$.

LEMMA 3.1. *The centralizer of any n-cycle w in S_n consists of the group of powers of w. Let $x=(1\,2\,3\,4\,5\,6\,7\,8)$ (representing the form $[8;0]$). Then, up to S_8 conjugacy, pairs of form $\{x,y\}$ with y of form $[2;6]$ generate S_8 if and only if $y=(1\,j)$ with $j\in\{2,4\}$.*

PROOF. If $x=(1\,2\,3\,4\,5\,6\,7\,8)$ then $Z_{S_8}(x)=\langle x\rangle$. To see this, let $z\in S_8$ be an element that commutes with x. If $z(1)=k$, replace z by $x^{-(k-1)}z=z'$, another element that commutes with x, but this one takes 1 to 1. Use $z'x=xz'$ to inductively conclude that $z'(t)=t$ for each integer $t\in\{1,\dots,8\}$. Example: $z'x(1)=z'(2)=xz'(1)=x(1)=2$. The same idea works for an n-cycle in S_n.

Given any 2-cycle $(i\,j)$, we have already computed how conjugation by powers of x works (proof of Chap. 1 Lem. 6.2). The result allows replacing $(i\,j)$ by $(i+k\,j+k)$ for any integer $k \mod 8$. So, choose k so the distance between $i+k$ and $j+k$ is at most 4, and one of the integers is 1. The result is $y=(1\,j')$.

Chap. 1 Lem. 6.2 shows that if j' is even, since $j'-1,8)=1$, such x and y do generate S_8.

If, however, j' is odd, then x and y induce an action on the two sets $U_1=\{1,3,5,7\}$ and $U_2=\{2,4,6,8\}$. That is they generate a group that is not primitive (§4) and so it cannot be S_8.

□

The next easy lemma essentially appears in the proof of Chap. 1 Lem. 6.2.

LEMMA 3.2. *Among the pairs of the form ($[7;1]$, $[2;6]$) take $x=(1\,2\,3\,4\,5\,6\,7)$. Up to S_8 conjugacy, if $\langle x,y\rangle=S_8$, then $y=(1\,8)$.*

We may also eliminate $\{x,y\}$ if both elements are in A_8. This allows us to assume one of x or y is in $S_8\setminus A_8$. For simplicity we assume from this point the following conditions.

(3.1a) $x\in S_8\setminus A_8$.

(3.1b) $\langle x,y\rangle$ acts primitively on the integers 1,..., 8.

LEMMA 3.3. *Among the pairs of the form $\{(1\,2\,3\,4\,5\,6\,7),[2,2,2;2]\}$, up to S_8 conjugation assume $y=(1\,8)(i_1\,i_2)(j_1\,j_2)$. The $\frac{1}{2}\frac{6!}{2!2!2!}=3^2\cdot 5$ choices of y give pairs of distinct S_8 conjugacy classes. Each of these S_8 classes $\{x,y\}$ automatically has $\langle x,y\rangle$ primitive. Then, $\langle x,y\rangle$ contains a 2-cycle exactly when $\langle x,y\rangle=S_8$.*

PROOF. For $\langle x, y\rangle$ to be primitive on $\{1, \dots, 8\}$ requires y to include 8 in the support of one of its 2-cycles. Write $y = (k\,8)(i_1\,i_2)(j_1\,j_2)$. By conjugating y by x^j we leave 8 fixed, and replace k by $k + j \mod 7$. This allows us to assume $k = 1$. The centralizer of x in S_8 consists of the powers of x. Suppose $y = (1\,8)(i_1\,i_2)(j_1\,j_2)$ and $y' = (1\,8)(i_1'\,i_2')(j_1'\,j_2')$. For any power of x, $x^j y x^{-j}$ conjugates the 2-cycle $(1\,8)$ to $(1 + j\,8)$ (with $1 + j$ regarded $\mod 7$). So, it does not move y to an allowable element unless $j \equiv 0 \mod 7$. Conclude: $\{x, y\}$ and $\{x, y'\}$ are conjugate if and only if $y = y'$.

The elements in $\langle x, y\rangle$ that fix 8 include x, which is transitive on the remaining integers. From Lem. 5.2, this implies $\langle x, y\rangle$ is primitive.

If $\langle x, y\rangle$ is S_8, then it contains all 2-cycles. Suppose, conversely that $\langle x, y\rangle$ contains a 2-cycle $u = (i\,i')$. Then, apply Lem. 3.2 to conclude $\langle x, y\rangle = S_8$. □

4. $\langle x, y\rangle$ FOR ((7),(2)(2)(2))

Consider the pairs $\{x, y\}$ in Lem. 3.3, up to S_8 conjugacy: $x = (1\,2\,3\,4\,5\,6\,7)$ and $y = (1\,8)(i_1\,i_2)(j_1\,j_2)$. Chap. A §2 shows output from the program TAIJOB1.BAS. Like Lem. 3.3, its output shows some 2-cycle is in $\langle (1\,2\,3\,4\,5\,6\,7), (4\,5)(6\,7)(1\,8)\rangle$, so that this group is S_8. This is a simple case where we can compare proof with a program. We discuss a subtler case, where the results of a program led us deeper into using proofs.

See Chap. 3 §3 for how the computer program **GAP** works. Here is the result of applying **GAP**. Of the 45 different S_8 conjugacy classes $\{x, y\}$, only twice does $\langle x, y\rangle = S_8$ not hold. Chap. 4 Prop. 5.3 explains, without using **GAP**, the group of order 336 that appears in the remaining two cases. There is exactly the right number of pairs $\{x, y\}$ (two) representing S_8 conjugacy classes from Lem. 3.2 as to give the list below. We use x for the 7-cycle $(1\,2\,3\,4\,5\,6\,7)$.

5. Cor(x, y) FOR ((7),(2)(2)(2))

To compute the corrolation in this case, we first give it to **GAP**. The result in the case of the first item from Table 4 is the following.

```
h:=Group((1,2,3,4,5,6,7)(16,9)(12,13)(14,15),
(8,1)(4,5)(6,7)(9,10,11,12,13,14,15));
[ [ 2, 14 ], [ 3, 4 ], [ 5, 2 ], [ 7, 2 ] ]
```

The group these generate is $S_8 \times S_8$. The mathematical argument is as previously similar to that of Lem. 0.1.

LEMMA 5.1. *All $\{x, y\}$ from Table 4 have* Cor$(x, y) = S_8 \times S_8$.

PROOF. The key property is that the group Cor(x, y) projects onto each factor to be S_8. That is, Cor(x, y) is isomorphic to S_8 via $(g, g') \mapsto (g, 1)$ and via $(g, g') \mapsto (1, g)$. Further, in this case, Cor(x, y) is not contained in the pairs (g, g') such that $g'g^{-1} \in A_8$, because x is odd and y is even. Following the argument of Lem. 0.1, we must show there is a nontrivial element of the form $(1, g)$ in Cor(x, y). To get such just take $(x, y)^2$. □

6. OTHER POSSIBILITIES FOR Cor(x, y)?

There are some difficult cases we have not considered, though many ingredients are ready. From the computations of §4, we must inspect those S_8 conjugacy classes pairs $\{x, y\}$ from S_8 where $\langle x, y\rangle = S_8$. While it is not always easy to list those cases

where the group is primitive, we do this efficiently enough to reduce the problem to the following consideration. Do x and y both lie in a subgroup of S_8 conjugate to the group appearing in Chap. 4 Prop. 5.3, called $\mathrm{PGL}_2(\mathbb{F}_7)$. Otherwise, according to Chap. 4 Prop. 5.3 and Prop. 5.4, they cannot lie in a (proper) maximal subgroup of S_8. So, $\langle x, y\rangle = S_8$.

TABLE 1. ((7),(2)(2)(2))

```
h:=Group(x,(8,1)(4,5)(6,7)); # S_8
(Group h, generated by two displayed elements, is S_8)
h:=Group(x,(8,1)(4,2)(6,7)); # S_8 h:=Group(x,(8,1)(4,3)(6,7)); # S_8
h:=Group(x,(8,1)(3,2)(6,7)); # 336    [[2,4], [3,1],[7,1]]
(Prime factorization of  336, the group's order)
h:=Group(x,(8,1)(2,5)(6,7)); # S_8  h:=Group(x,(8,1)(3,5)(6,7)); # S_8

h:=Group(x,(8,1)(4,2)(5,7)); # S_8 h:=Group(x,(8,1)(4,3)(5,7)); # S_8
h:=Group(x,(8,1)(2,3)(5,7)); # S_8 h:=Group(x,(8,1)(6,2)(5,7)); # S_8
h:=Group(x,(8,1)(3,6)(5,7)); # S_8 h:=Group(x,(8,1)(4,6)(5,7)); # S_8

h:=Group(x,(8,1)(3,2)(4,7)); # S_8 h:=Group(x,(8,1)(5,2)(4,7)); # 336
h:=Group(x,(8,1)(2,6)(4,7)); # S_8 h:=Group(x,(8,1)(3,5)(4,7)); # S_8
h:=Group(x,(8,1)(3,6)(4,7)); # S_8 h:=Group(x,(8,1)(5,6)(4,7)); # S_8

h:=Group(x,(8,1)(4,2)(3,7)); # S_8 h:=Group(x,(8,1)(5,2)(3,7)); # S_8
h:=Group(x,(8,1)(2,6)(3,7)); # S_8 h:=Group(x,(8,1)(4,5)(3,7)); # S_8
h:=Group(x,(8,1)(4,6)(3,7)); # S_8 h:=Group(x,(8,1)(5,6)(3,7)); # S_8

h:=Group(x,(8,1)(4,3)(2,7)); # S_8 h:=Group(x,(8,1)(5,3)(2,7)); # S_8
h:=Group(x,(8,1)(3,6)(2,7)); # S_8 h:=Group(x,(8,1)(4,5)(2,7)); # S_8
h:=Group(x,(8,1)(4,6)(2,7)); # S_8 h:=Group(x,(8,1)(5,6)(2,7)); # S_8

h:=Group(x,(8,1)(4,2)(5,6)); # S_8 h:=Group(x,(8,1)(4,3)(5,6)); # S_8
h:=Group(x,(8,1)(2,3)(5,6)); # S_8

h:=Group(x,(8,1)(3,2)(4,6)); # S_8 h:=Group(x,(8,1)(5,2)(4,6)); # S_8
h:=Group(x,(8,1)(3,5)(4,6)); # S_8

h:=Group(x,(8,1)(4,2)(3,6)); # S_8 h:=Group(x,(8,1)(5,2)(3,6)); # S_8
h:=Group(x,(8,1)(4,5)(3,6)); # S_8

h:=Group(x,(8,1)(4,3)(2,6)); # S_8 h:=Group(x,(8,1)(5,3)(2,6)); # S_8
h:=Group(x,(8,1)(4,5)(2,6)); # S_8

h:=Group(x,(8,1)(2,3)(4,5)); # S_8 h:=Group(x,(8,1)(2,4)(3,5)); # S_8
h:=Group(x,(8,1)(4,3)(2,5)); # S_8
```

There is one nontrivial point in the argument for computing Cor(x, y) in Lem. 0.1. We know from that lemma of two possible outcomes: Cor(x, y) is either $S_8 \times S_8$ or the index two subgroup of pairs $(g_1, g_2) \in S_8 \times S_8$ where $g_1 g_2^{-1} \in A_8$: $S_8 \times_* S_8$.

One of these two must happen (dependent on whether $xy \in S_8$ or in A_8), assuming that Cor(x, y) contains an element of form $(1, g)$ with $g \neq 1$. This last was automatic if x and y have different orders. We have not dealt with the case x and y have the same order.

PROPOSITION 6.1. *Suppose there is an automorphism α of S_8 having order two that takes x to y. If $\langle x, y\rangle = S_8$, then* Cor$(x, y)$ *is the subgroup of $S_8 \times S_8$ isomorphic to S_8 given by $S_{8,\alpha} = \{(g, \alpha(g)) \mid g \in S_8\}$. Otherwise,* Cor$(x, y)$ *is $S_8 \times S_8$ or $S_8 \times_* S_8$.*

PROOF. Suppose there is such an automorphism α of order 2. Then the group $S_{8,\alpha}$ contains $(x, \alpha(x))$ and $(\alpha(x), \alpha^2(x)) = (y, x)$ and so it equals Cor(x, y).

Now assume the general case. Suppose Cor(x, y) contains two elements (g, h_1) and (g, h_2) with $h_1 \neq h_2$. Then, it contains $(g, h_1)(g, h_2)^{-1} = (1, h_2 h_2^{-1})$, and we already know what is Cor(x, y). The negation of this situation is that for each $(g, h) \in$ Cor(x, y), the map $g \mapsto h$ is a one-one map. This map must therefore be an automorphism: $g_1 g_2 \mapsto h_1 h_2$. Call this automorphism α.

We show α has order 2. Under the assumptions, since $(x, y) \in$ Cor(x, y), $y = \alpha(x)$. Since $(y, x) \in$ Cor(x, y), $x = \alpha(y)$. Apply α to both sides of this last equation, to conclude $\alpha(x) = y = \alpha^2(y)$ and, similarly, $x = \alpha^2(x)$. Since $\langle x, y\rangle = S_8$, we know α^2 from its effect on x and y. Therefore α^2 is the identify automorphism. This concludes the proof of the proposition. □

The following result is in [**Isa94**, 79-80].

LEMMA 6.2. *The automorphisms α of S_n having order 2 are either conjugations by an element of order 2, or $n = 6$.*

7. Cor(x, y) WITH ORDERS OF x AND y THE SAME

We now investigate the possibility the orders of (x, y) are integers (n, n) with $1, \leq n \leq 8$. We need, however, that at least one of x or y (assume x for certain) in $S_8 \setminus A_8$. So, n odd is out. So is $n = 2$ out: Two elements of order 2 generate a *dihedral group* (rigid motions of a regular polygon) of order $2k$ where k is the order of xy.

For each of $n = 4, 6, 8$ we discuss the subcases for determining Cor(x, y). For each such n consider elements by their cycle type. For the pairs x and y we use combinatorics around the centralizer subgroup of x to to assure the group they generate is primitive (Chap. 4 §4). Then we need only show x and y are not both in a proper primitive subgroup of S_8 containing an element of $S_8 \setminus A_8$. The only possibilities are that some conjugate of PGL$(\mathbb{F}_7)$ contains x and y.

EXAMPLE 7.1 (Illustration of (x, y) cycle type). ((2)(2)(4),(4)(4)) means x has cycle type (2)(2)(4) and y has cycle type (4)(4). Conjugation of x and y by an element of S_8 allows us to assume $x = (1\,2)(3\,4)(5\,6\,7\,8)$. Conjugating y by any element in the centralizer, $Z_{S_8}(x)$, of x does not change the problem, so for $\langle x, y\rangle$ to be primitive, y is determined only up to conjugation by $\langle (5\,6\,7\,8), (1\,3\,2\,4), (1\,2)\rangle$. Conclude: If $\langle x, y\rangle = S_8$, then Cor$(x, y) = S_8 \times S_8$ since the possibility of $S_{8,\alpha}$ requires that x and y have the same cycle type.

According to Prop. 6.1, we know the outcome unless y is the conjugate to x by an element of order 2.

8. THE CASE $n = 8$

The case $n = 8$ is especially easy for y must also be an 8-cycle. So y is conjugate to $x = (1\,2\,3\,4\,5\,6\,7\,8)$. Further, $\langle x, y\rangle$ primitive means the 8-cycle for y must move some even integer to an even integer. With no loss, by conjugating by x, assume y either has the effect $2 \mapsto 4$ or $2 \mapsto 6$. (6,6) (and (8,8) (both eight cycles). The following shows $\langle x, y\rangle = S_8$ for certain.

LEMMA 8.1. *The group* $\mathrm{PGL}(\mathbb{F}_7)$ *contains no element of order 8.*

PROOF. An element of order 8 would be in a 2-Sylow subgroup of such a group. A 2-Sylow of $\mathrm{PSL}_2(\mathbb{F}_7)$ is a subgroup of A_8 and all its elements of 2-power order have order 2. So, the biggest order of a 2-power element in $\mathrm{PGL}(\mathbb{F}_7)$ is four. □

We summarize the result of all of this.

PROPOSITION 8.2. *Consider any $h \in S_8$ that maps some odd integer to an even integer and some even integer to an even integer. If h has order two, then with the automorphism α_h given by conjugation by h, $\mathrm{Cor}(x, hxh^{-1}) = S_{8,\alpha_h}$. If, however, $h \in S_8$ does not have order 2, then $\mathrm{Cor}(x, hxh^{-1}) = S_8 \times_* S_8$. This gives a complete description of all possibilities for $\mathrm{Cor}(x, y)$ where x and y both have order 8.*

9. THE CASE $n = 4$

Suppose x has the shape in Ex. 7.1. A set of imprimitivity must have cardinality 2 or 4. If $\langle x, y\rangle$ is transitive, with no loss we may assume a set of imprimitivity contains any a priori integer.

LEMMA 9.1. *Suppose $\langle x, y\rangle$ is transitive, but not primitive. If a set of imprimitivity has cardinality 2, we may assume it is $\{5, 7\}$ (or $\{6, 8\}$).*

If a set of imprimitivity I has cardinality 4, then with no loss we may assume I contains $\{5, 7\}$.

PROOF. Assume the set of imprimitivity has cardinality 2 and it contains the integer 5. If the set is a subset of $\{5, 6, 7, 8\}$, then use that for n-cycle, $(1\,2\,\ldots\,n)$, the group generated by this has only the sets of imprimitivity consisting of the integers $\equiv a \mod k$ for some integer a and divisor k of n. If the set is not a subset of $\{5, 6, 7, 8\}$, then by apply x^2 to the set you find it also contains 7, and so has four elements.

If a set of imprimitivity has cardinarily 4, then x^2 maps this set into itself: Either it fixes at least one integer in the set or the set consists of $\{5, 6, 7, 8\}$. So, the set contains $\{5, 7\}$. □

Here are examples where x has the shape in Ex. 7.1 and $\langle x, y\rangle$ is primitive. Recall the centralizer of x is $\langle(5\,6\,7\,8), (1\,3\,2\,4), (1\,2)\rangle$.

We comment on this table. Guaranteeing that $\langle x, y\rangle$ is primitive is trickier with an irregular shape. For example with $y = (1\,5)(2\,6)(3\,4\,7\,8)$, $\{5, 7, 3, 6\}$ is a set of imprimitivity for $\langle x, y\rangle$.

Apply Lem. 9.1 to 4_1 to inspect a possible set of imprimivity I containing $\{5, 7\}$. Square y to see $4 \in I$. If any other integer from $\{1, 2, 3, 6\}$ is in I another integer from this set would have to be in there too. So, $\langle x, y\rangle$ is primitive in 4_1. Apply the

TABLE 2. Cases $n = 4$

n	shape pair	y	$\mathrm{Cor}(x, y)$
4_1	((2)(2)(4),(4)(4))	(1 2 3 6)(5 8 4 7)	$S_8 \times S_8$
4_2	((2)(2)(4),(2)(4))	(2 3)(4 6 7 8)	$S_8 \times S_8$
4_3	((2)(2)(4),(2)(2)(4))	(1 5)(2 3)(6 7 4 8)	$S_8 \times_* S_8$
4_4	((2)(2)(4),(2)(2)(4))	(7 2)(8 4)(6 5 1 3)	$S_{8,(1\,7)(3\,8)(5\,6)}$

same thinking to $y = (1\,5)(2\,3)(6\,7\,4\,8)$ (4_3 in the table). A set of imprimitivity I must contain $\{5, 7, 8\}$, and so it contains 6, and then 4. So 4_3 is primitive.

For 4_2, a set I of imprimitivity containing $\{5, 7\}$ would also contain 4 (from applying y which fixes 5). To add another integer, it would have to be in $\{1, 2, 3\}$. Since x takes 5 to 7, if $1 \in I$ (or $2 \in I$), then 2 (or 1) would be also. This leaves only the possibility $3 \in I$, which implies x maps I to I, a contraction. So, 4_2 is primitive.

It is easy to get y that is conjugation of x by an element, β, of order 2. For example try $y = (1\,5)(3\,6)(2\,4\,7\,8)$, conjugation of x by $(2\,5)(4\,6)$. The problem is that $\langle x, y\rangle$ has $\{2, 3, 5, 7\}$ as a set of imprimitivity. The explanation of 4_4 in Table 9 is in Lem. 9.3 which considers the case of conjugating x by a product of three disjoint 2-cycles. The minimum number of 2-cycles necessary to assure $\langle x, y\rangle$ is transitive is two. Conjugating β by an element of the centralizer of x doesn't change the problem. Lem. 9.2 shows we can't take β a product of two disjoint 2-cycles. The case where β is a product of four disjoint 2-cycles breaks up into cases similarly, so we didn't write it out.

LEMMA 9.2. *If β has order 2 and is a product of two disjoint 2-cycles, then $\langle x, \beta y \beta^{-1}\rangle$ is not primitive.*

PROOF. To assure conjugation by β having order 2 gives $\langle x, y\rangle$ primitive requires assuring there is no set of imprimitivity I containing $\{5, 7\}$ and either the first and 3rd integers from $\beta(5\,6\,7\,8)\beta^{-1}$ or the second and 4th integers from this same element. Each disjoint cycle in β has an integer of $\{5, 6, 7, 8\}$ in its support. Conjugating β by the center of x assures $\beta = (1\,5)(3\,i_2)$ with $i_2 \in \{6, 7\}$. If $i_2 = 7$, then $I = \{5, 7\}$ is a set of imprimitivity.

Now consider the case $i_2 = 6$. This would add give $1 \in I$ by applying y^2. Then, we find with $4 \in I$, we get a set of imprimitivity. □

Now consider the case β is a product of three disjoint 2-cycles. Tacitly we assume $\langle x, y\rangle$ is transitive.

LEMMA 9.3. *Suppose one 2-cycle of β has support in $\{5, 6, 7, 8\}$ and no 2-cycle of β has support in $\{1, 2, 3, 4\}$. Then, modulo the centralizer of x, β is one of $\beta_1 = (1\,7)(3\,8)(5\,6)$, $\beta_2 = (1\,6)(3\,8)(5\,7)$. When $\beta = \beta_2$, $G_\beta = \langle x, \beta y \beta^{-1}\rangle$ has a set of imprimitivity of cardinality 2. When $\beta = \beta_1$, G_β is primitive.*

Suppose one 2-cycle of β has support in $\{1, 2, 3, 4\}$ and no 2-cycle of β has support in $\{5, 6, 7, 8\}$. Then, modulo the centralizer of x, β is one of $\beta_3 = (1\,3)(2\,5)(4\,6)$ or $\beta_4 = (1\,3)(2\,5)(4\,7)$. When $\beta = \beta_4$, $G_\beta = \langle x, \beta y \beta^{-1}\rangle$ has a set of imprimitivity of cardinality 2. When $\beta = \beta_3$, G_β is primitive.

Suppose one 2-cycle of β has support in $\{1, 2, 3, 4\}$ and one 2-cycle of β has support in $\{5, 6, 7, 8\}$. Then, modulo the centralizer of x, β is one of $\beta_5(i_1, i_2) =$

$(1\,3)(2\,5)(i_1\,i_2)$ *with* $i_1, i_2 \in \{6,7,8\}$. *Then,* $G_{\beta_5(6,7)}$ *and* $G_{\beta_5(7,8)}$ *are primitive, though* $G_{\beta_5(6,8)}$ *has a set of imprimitivity of cardinality 4.*

Suppose no 2-cycle of β *has support in* $\{1,2,3,4\}$ *and no 2-cycle of* β *has support in* $\{5,6,7,8\}$. *Then, modulo the centralizer of* x, β *is one of* $\beta_6(i_1,i_2) = (1\,5)(3\,i_1)(4\,i_2)$ *with* $i_1, i_2 \in \{6,7,8\}$ *and* $i_1 < i_2$. *Then,* $G_{\beta_6(6,8)}$ *is primitive, and* $G_{\beta_6(6,7)}$ *and* $G_{\beta_6(7,8)}$ *have sets of imprimitivity of cardinality 4.*

PROOF. For the case $\beta = \beta_2$, it preserves the imprimitivity set $\{5,7\}$ of cardinality two for $\langle x\rangle$. When $\beta = \beta_1$, $y = (7\,2)(8\,4)(6\,5\,1\,3)$. So a set I of imprimitivity containing $\{5,7\}$ also contains 3 (apply y^2). Now put any other integer into I and conclude there must be a 5th integer in it.

Again, $\beta = \beta_4$ preserves a cardinal two set of imprimitivity having order 2, so G_{β_4} is imprimitive. The primitiveness of G_{β_3} is similar to that of G_{β_1}.

The remaining examples are similar. □

The number of elements in S_8 with the shape (2)(2)(4) equals 8! divided by the order of the centralizer of x. So, there are $\frac{8!}{4!8} = 7\cdot 6\cdot 5$ such elements. As with the case $n = 8$, we need to know $\langle x, y\rangle$ is not in $\mathrm{PGL}(\mathbb{F}_7)$. As with $n = 8$, no elements in this group have shape (2)(2)(4).

LEMMA 9.4. *The conjugacy class of* $x = (1\,2)(3\,4)(5\,6\,7\,8)$ *does not meet* $\mathrm{PGL}(\mathbb{F}_7)$.

10. THE CASE $n = 6$

In this case x has cycle type (2)(3)(3) or (2)(3), and y has possible cycle types (2)(2)(3), (2)(3)(3) or (2)(3). This follows similar calculations to the case $n = 4$, though we will keep it brief, hitting only the differences between the two cases. One quick point is that x^3 is an order two element fixing six integers. If, however, an element of $\mathrm{PGL}_2(\mathbb{F}_7)$ fixes as many as three integers, it must be the identity.

For $x = (1\,2)(3\,4\,5)$, the centralizer of x is $\langle(1\,2)\rangle \times \langle(3\,4\,5)\rangle \times S_3$ where the last copy of S_3 is acting on the integers $\{6,7,8\}$. To see this use the argument Chap. 1 Lem. 3.1 to get the centralizer of each disjoint cycle. Then, combine this with the group permuting the integers that x fixes. The appearance of 3-cycles in x^2 and y^2 (and 2-cycles in x^3 and y^3) make it easy to assure primitivity. Analogous to the examples with $n = 4$ we give some for $n = 6$ in this table. We leave it to the reader as an exercise to fill in the chart.

TABLE 3. Cases $n = 6$

n	shape pair	y	$\mathrm{Cor}(x,y)$
6_1	((2)(3),(2)(2)(3))	$(2\,3)(4\,7)(5\,6\,8)$	$S_8 \times S_8$
6_2	((2)(3),(2)(3)(3))	$(2\,8)(1\,3\,7)(4\,5\,7)$	$S_8 \times_* S_8$
6_3	((2)(3)(3),(2)(2)(3))	$(7\,2)(8\,4)(6\,5\,1)$	$S_8 \times S_8$
6_4	((2)(3)(3),(2)(3)(3))	$(1\,3)(2\,4\,6)(5\,7\,8)$	$S_8 \times_* S_8$
6_5	((2)(3)(3),(2)(3)(3))	$(3\,6)(1\,4\,5)(2\,7\,8)$	$S_{8,\beta}$
6_6	((2)(3)(3),(2)(3))	$(1\,6)(3\,5\,7)$	$S_8 \times_* S_8$

Note: The type ((2)(3),(2)(3)) is missing. The next lemma explains that.

LEMMA 10.1. *If* (x,y) *has type ((2)(3),(2)(3)), then* $\langle x,y\rangle$ *is intransitive.*

PROOF. Three integers, $\{6, 7, 8\}$ are missing from the support of y. They must appear in the support of y to give $\langle x, y\rangle$ transitive. So, too, must one integer each from the 2 and 3-cycle in x, and then there must be a join of each 2 and 3-cycle of y to the 2 and 3-cycle of x. There aren't enough integers for this, and $\langle x, y\rangle$ is intransitive. □

CHAPTER 4

PRIMITIVE GROUPS

[**Sh01**] produces a function that probably has many interesting properties. It is akin to various so-called *zeta functions*. For a finite group G, let M denote a subgroup of G with no group properly between it and G (a *maximal* subgroup). As in Thm. 4.1 let P_G be the probability that two randomly selected elements from G will generate G. Then, $\zeta_G(s) = \sum_{M \text{ maximal}} \frac{|M|}{|G|}^s$ has this property: $1 - P_G \leq \zeta_G(2)$. So, Dixon's conjecture follows from proving that $\zeta_G(2) \mapsto 0$ as $|G| \mapsto \infty$ running over simple groups G. The papers that [**Sh01**] references use the famous classification of finite simple groups. This tells enough about maximal groups of simple groups to prove Dixon's conjecture.

In §8 and §9 we use a practical version of this. To consider what pairs $(x, y) \in S_8$ generate S_8 we must exclude those x and y that are *both* in some (proper) maximal subgroup of S_8. The results of this section about include describe the conjugacy classes of maximal subgroups of S_8. General results about arbitrary simple groups such as those of [**Sh01**] do use some form of a listing for certain maximal subgroups. Prof. Fried tells me that knowing how to use partial results in this direction is where present group theory researchers show their expertise.

1. (2,3)-GENERATION

Every group that is generated by two elements, a, b, with a having order 3 and b having order 2 is a quotient of a very famous group called $\mathrm{PSL}_2(\mathbb{Z})$: The set of functions $z \mapsto \frac{mz+n}{m'z+n'}$ with $m, m', n, n' \in \mathbb{Z}$ and $mn' - m'n = 1$. Shalev calls any such group a (2,3)-generated group [**Sh01**]. Such a group, together with (a, b), corresponds to an algebraic equation coming from classical complex variables. The tradition that a has order 3 and b has order 2 comes from complex variables. This convention will be useful for us.

Finding which finite simple groups are (2,3)-generated occurs in much literature since the late 1800s. The groups A_n have this property for $n \geq 9$, a result of Miller from 1901. For example, my advisor Prof. Fried had the group A_9 appear as part of his research with $a = (2\,1\,4)(3\,7\,8)(5\,6\,9)$ and $b = (4\,5)(3\,9)(1\,2)(8\,6)$ precisely because he was investigating a certain algebraic equation from his study of the Inverse Galois problem.

Also, A_8, the group of our investigation is not (2,3)-generated. Let $H_{a,b}$ be the group generated by a, b. In the proof of Prop. 1.1 below, we use the idea that if $\{a, b\}$ generated a normal subgroup $H_{a,b}$ of a group G, then the conjugates $\{gag^{-1}, gbg^{-1}\}$ by $g \in G$ also generate $H_{a,b}$.

PROPOSITION 1.1. *The group A_8 is not (2,3)-generated.*

The next three subsections complete the proof of Lem. 1.1. §2 considers what elements of respective orders 3 and 2 might be generators of A_8. §3 brings up how

the computer program **GAP** could show that the potential (2,3)-generators of A_8 all generate proper subgroups of it. Then, §5.3 gives a mathematical proof that shows exactly what is the group these (2,3)-generators give.

2. LIMITING (2,3)-GENERATORS OF A_8

Suppose a, b are respectively of order 3 and 2 and they generate A_8. Using conjugation, assume with no loss that $a = (1\,2\,3)(4\,5\,6)$. Now, we may conjugate b by any element of S_8 that centralizes a, and get new generators. Also, to be in A_8, b must be a product of either two or four disjoint 2-cycles. It is easy, however, to see that if b is a product of just two disjoint 2-cycles, there would be no way to get a transitive group from $\langle a, b\rangle$ on $\{1, 2, \ldots, 8\}$. Using transitivity conclude with no loss the following. Either:

(2.1a) b maps 8 to 4 and $b = (7\,1)(8\,4)(2\,5)(3\,6)$ or $b = (7\,1)(8\,4)(2\,6)(3\,5)$; or

(2.1b) b maps 8 to 2 or 3 and is one of $(7\,1)(8\,2)(3\,4)(5\,6)$ or $(7\,1)(8\,3)(2\,4)(5\,6)$.

For example, we use $b = (7\,1)(8\,4)(2\,5)(3\,6)$.

3. PROOFS VERSUS GAP

Computer programs like **GAP** can take as input the generators a and b and check if the resulting group $H_{a,b}$ is A_8. The code at the command line of **GAP** would look like this. (Anything on a line following # denotes a comment.)

```
h:=Group((1,2,3)(4,5,6),(7,1)(8,4)(2,5)(3,6)); # Defining group h
h.name:="h"; # Declares the name property of the group.
Size( h ); # This computes the order of the group.
Print("The order of A8 is 2^7*3^2*5*7. The order of h is \n"); #
Collected(Factors(last)); # collects factors of last result.
```

GAP gave us following upon typing at the program command line:

```
gap> h:=Group((1,2,3)(4,5,6), (7,1)(8,4)(2,5)(3,6));
Group( (1,2,3)(4,5,6), (1,7)(2,5)(3,6)(4,8) )
gap> h.name:="h";
"h"
gap> Size( h );
24
gap> Print("A8 has order 2^7*3^2*5*7. The order of h is \n");
The order of A8 is 2^7*3^2*5*7. The order of h is
gap> Collected(Factors(last));
[ [ 2, 3 ], [ 3, 1 ] ]
```

The collected factors for A_8 are $2^7 \cdot 3^2 \cdot 5 \cdot 7$, larger than for h (with order $2^3 \cdot 3$). So **GAP** shows A_8 is not (2,3)-generated. Since, however, this computation comes from the 1800's when there was no **GAP**, we can compare **GAP** with computations using standard mathematical proof.

4. COMPLETING THAT A_8 ISN'T (2,3)-GENERATED

If H is a subgroup of G (versus just a subset) we use the notation $H \leq G$. An extra notion is that of a *primitive group*. For any transitive subgroup $H \leq S_n$, suppose I is a proper subset of $\{1, 2, \ldots, n\}$ containing more than one element. Then, I is a set of *imprimitivity* for H if either $h(I) = I$ or $h(I) \cap I = \emptyset$ for all

$h \in H$. Call H primitive if there is no such I. Since the group H is transitive, with no loss assume a set of imprimitivity contains 1. Let H_I be the subgroup of $h \in H$ such that $h(I) = I$. Then, H_I contains the subgroup $H(1)$ of elements in H that fix 1. The following is a well-known lemma from group theory.

LEMMA 4.1. *A transitive subgroup H of S_n is primitive if and only if there is no proper subgroup between H and $H(1)$.*

PROOF. If H^* is a group properly between H and $H(1)$, let I be the orbit of 1 under H^*. Then, the cosets of $H(1)$ in H^* correspond to the elements of I. Suppose $t \in h(I) \cap I$, then $t = h^*(1)$ and $h = h^*m$ with $m \in H(1)$ and so $h \in H^*$ and $h(I) = I$.

Conversely, if there is set of imprimitivity I, then the set of elements h^* with $h^*(1) \in I$ is properly between H and $H(1)$. □

Now return to considering the subgroup $H_{a,b} \leq A_8$. Suppose $H_{a,b}$ is A_8. then there is no way to divide $\{1, 2, ..., 8\}$ into disjoint collections of integers - each with at least two elements – so that each of a and b move the sets around. When $a = (1, 2, 3)(4, 5, 6)$ and $b = (7, 1)(8, 4)(2, 5)(3, 6)$, we can partition $\{1, 2, ..., 8\}$ into the subsets $X_1 = \{1, 4\}, X_2 = \{2, 5\}, X_3 = \{3, 6\}, X_4 = \{7, 8\}$. Then, both a and b move these sets around through their actions. The effect of a is $X_1 \mapsto X_2 \mapsto X_3 \mapsto X_1$ and $X_4 \mapsto X_4$, while b has the effect $X_1 \mapsto X_4$, $X_2 \mapsto X_2$, and $X_3 \mapsto X_3$

For the second possibility in (2.1a), the result is also that the group is not primitive with the sets above showing exactly that. For, however, any b in (2.1b), the group $H_{a,b}$ *is* primitive. **GAP** showed the existence of a group inside A_8, that is primitive of degree 8, that is (2,3)-generated and is not the alternating group. It didn't give any hint about what group that was, nor why when it would occur. With our description of the primitive subgroups in S_8 see what it is about.

Consider the set of 2×2 matrices with elements in the finite field $\mathbb{F}_7$ of order 7. Then, the group $\mathrm{PSL}_2(\mathbb{F}_7)$ of expressions $\frac{az+b}{cz+d}$ with $ad - bc = 1$ acts on $\mathbb{F}_7 \cup \{\infty\}$. The group with only the condition $ad - bc \neq 0$ is sharply triply transitive. So it has order $8 \cdot 7 \cdot 6$. When, however, you add the condition that $ad - bc = 1$, you exclude such actions as $z \mapsto -z$, and $\mathrm{PSL}_2(\mathbb{F}_7)$ has order $8 \cdot 7 \cdot 3$. Since this is a quotient of $\mathrm{PSL}_2(\mathbb{Z})$, a (2,3)-generated group, it is automatically (2,3)-generated. The matrix $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ represents an element of $\mathrm{PSL}_2(\mathbb{F}_7)$ having order 2. It acts on the 8 elements giving the permutation symbols by interchanging all elements (including 0 and ∞) in pairs. Since any element of odd order is in the alternating group, this means $\mathrm{PSL}_2(\mathbb{F}_7) \subset A_8$. **GAP** returned $2^3 \cdot 3 \cdot 7$ as the output for the factors for the group of (2.1b) in agreement with our deduction.

5. OTHER DEGREE 8 PRIMITIVE GROUPS

In this subsection we list the other primitive groups of degree 8.

DEFINITION 5.1. A group $G \subset S_n$ is doubly transitive if for each pair of distinct integers i, j there is $g \in G$ such that $g(i) = 1$ and $g(j) = 2$.

LEMMA 5.2. *A doubly transitive group is automatically primitive. Further, a transitive group G is doubly transitive if and only if $G(1)$ is transitive on $\{2, \ldots, n\}$. Any transitive subgroup of S_n containing a $(n-1)$-cycle is primitive.*

PROOF. Suppose G is a doubly transitive group, and let $G(1)$ be the elements in it that stabilize 1. If there is a group H properly between $G(1)$ and G, let $h \in H \setminus G(1)$. Then, $h(1) = j \neq 1$. For any integer $k \neq 1$, double transitivity implies there is $g'_k \in G(1)$ taking j to k. So, $g'_k h \in H$ takes 1 to k. By Lagrange's lemma the cosets $G(1)$ and $g'_k hG(1)$, $k = 2, \dots, n$ are distinct, and so the union of these cosets is all of G. Since they are all in H, it must be that $H = G$, or G is primitive.

Suppose $G(1)$ is transitive on $\{2, \dots, n\}$ (and G is transitive). Then, given integers $i \neq j$, use transitivity to find $g \in G$ taking i to 1. Then, $g(j) = k$ with $k \neq 1$. Choose $g' \in G(1)$ taking k to 2. Conclude $g'g(i) = 1$ and $g'g(j) = 2$, so G is doubly transitive.

Now suppose G is transitive, and it contains a $(n-1)$-cycle $g_(n-1)$. By conjugating $g_(n-1)$ by an element of G, assume with no loss that $g_(n-1)$ fixes 1. So, $g_(n-1)$ generates a subgroup transitive on $\{2, \dots, n\}$. So the previous deduction shows G is primitive; in particular, $G(1)$ is transitive on $\{2, \dots, n\}$, hence doubly transitive, hence primitive. □

The next proposition accounts for the cases in Table 4 with $\langle x, y\rangle \neq S_8$.

PROPOSITION 5.3. *Instead of* $\mathrm{PSL}_2(\mathbb{F}_7)$ *consider*

$$\mathrm{PGL}_2(\mathbb{F}_7) \stackrel{\text{def}}{=} \{\frac{az+b}{cz+d} \mid ad - bc \neq 0\}.$$

It has the following properties.

- (5.1a) *It contains* $\mathrm{PSL}_2(\mathbb{F}_7)$ *as a subgroup of index 2.*
- (5.1b) *It has generators of order* 7 *and order 2 that act, respectively, like a 7-cycle and a product of three disjoint 2-cycles on* $\{0, 1, \dots, 7, \infty\}$.
- (5.1c) *Up to conjugation in* $\mathrm{PGL}_2(\mathbb{F}_7)$ *there are just two such generating pairs.*

PROOF. If you change $\frac{az+b}{cz+d}$ to $\frac{u(az+b)}{u(cz+d)}$, the expression $ad-bc$ changes to $u^2(ad-bc)$. The map $\mathrm{PGL}_2(\mathbb{F}_7) \to \mathbb{F}_7^* \cup \{\infty\}$ by $\frac{az+b}{cz+d} \mapsto ad - bc$ up to multiplication by a square in $\mathbb{F}_7^*$ is a homomorphism with kernel those the elements of $\mathrm{PSL}_2(\mathbb{F}_7)$. Euler's Theorem says $\mathbb{F}_7^*$ is a cyclic group of order 6. So, the elements in it that are squares are exactly the elements of order 3. Conclude: The index of $\mathrm{PSL}_2(\mathbb{F}_7)$ in $\mathrm{PGL}_2(\mathbb{F}_7)$ is therefore two.

The elements $z \mapsto z + 1$ and $z \mapsto 1/z$ are easily shown to generate $\mathrm{PGL}_2(\mathbb{F}_7)$. The first gives a 7-cycle. The action of $z \mapsto 1/z$ on $\{0, 1, \dots, 7, \infty\}$ is easy to figure: it interchanges 0 and ∞, is of order 2 and fixes only 1 and -1 from $1, \dots, 7$. So, these two elements generate a transitive group containing a 7-cycle: the group is doubly transitive by Lem. 5.2.

It is easy to show any 7-cycle in $\mathrm{PGL}_2(\mathbb{F}_7)$ is conjugate to this, and any element of order 2 is conjugate to $z \mapsto 1/z$. If $a(z)$ has order 2 and it maps ∞ to $j \in \{0, 1, \dots, 7, \infty\}$, conjugate by a power of $z \mapsto z + 1$ to guarantee that $a(z)$ maps ∞ to 0. Since it has order two it switches ∞ and 0, and so it has the shape $z \mapsto c/z$. Up to a square, $c = \pm 1$, and that gives the two conjugacy classes of pairs listed in the statement of the proposition. □

We saw that $\mathrm{PSL}_2(\mathbb{F}_7)$ and $\mathrm{PSL}_2(\mathbb{F}_7)$ were two related primitive groups of degree 8 (in their action on $\{0, 1, \dots, 7, \infty\}$). There are three further primitive of degree 8 groups (related, though not related to $\mathrm{PGL}_2(\mathbb{F}_7)$).

PROPOSITION 5.4. *Let $G = \mathrm{GL}_3(\mathbb{Z}/2)$ be the group of invertible 3×3 matrices acting on $(\mathbb{Z}/2)^3 = V = V_8$. Then, from V and G you can construct a group $V \times^s G$ that has order $2^5 \cdot 3^2 \cdot 7$. By associating the elements of V with the integers $\{1, \ldots, 8\}$, this gives $V \times^s G$ acting on $\{1, \ldots, 8\}$. It has doubly transitive subgroups of order $8 \cdot 7$ and $2^4 \cdot 3 \cdot 7$. The group $V \times^s G$ (and all its subgroups) is a subgroup of A_8.*

PROOF. Write this group's elements in the form (v, g) with $g \in G$ and $v \in V$. Multiplication appears in the following form:

$$(v, g) \times (v', g') \stackrel{\text{def}}{=} (v + g(v'), gg')$$

where gg' is ordinary matrix multiplication and $g(v')$ means the matrix g acts on the vector v' as in linear algebra. The full collection of matrices takes any $v \in V \setminus \{0\}$ to any other. This says the group is doubly transitive and therefore primitive. Also, it will take any element in $V \setminus \{v, 0\}$ to any other. So, it is actually triply transitive. An element of $V \times^s G$ that fixes $\{v, v', 0\}$ with $v' \in V \setminus \{v, 0\}$. The order of G is $8 \cdot (2^3 - 1) \cdot (2^3 - 2) \cdot (2^3 - 2^2)$.

Since the elements of V_8 have order 2, and fix no element (by translation on V), they are all products of 4 disjoint 2-cycles, so they are in A_8. Since $V_8 \times I_3$ and $(0, 0, 0) \times \mathrm{GL}_3(\mathbb{Z}/3)$ generate $V \times^s G$, to see that $V \times^s G$ is in A_8 only requires showing $G = \mathrm{GL}_3(\mathbb{Z}/2)$ is in A_8.

From linear algebra, the diagonalizable elements generate G. The eigenvalues of a diagonalizable element are values in the nonzero elements of some finite extension of the field $\mathbb{Z}/2$. Let $\mathbb{F}$ be such a field extension, so $|\mathbb{F}| = 2^t$ for some integer t. The multiplicative elements of a finite field form a cyclic group. So, the orders of the eigenvalues as elements of this group are odd. Therefore, the order of a diagonalizable element is odd. Therefore G has generators of odd order. Since all odd order elements in S_n lie in A_n, the image of G in any S_n is in A_n. □

Shalev [**Sh01**] also quotes papers of Liebeck-Shalev 1996, Lübeck-Malle 1999. These say, excluding finitely many simple groups, there are three series of finite simple groups

$$\{\mathrm{PSp}_4(2^k), \mathrm{PSp}_4(3^k), \mathrm{Sz}(2^k)\}_{k=1}^{\infty}$$

that are not (2,3)-generated. This was an example of their general technique of taking a ζ-function approach and using some knowledge about the maximal subgroups of simple groups.

CHAPTER 5

WHERE THERE ARE NO GROUPS

1. GROUP THEORY IN HIGH SCHOOL

Group theory is not standard in high school mathematics though there are hints it could be. Combining a problem like the one in §2 with the treatment of probability (permutations and combinations) in Algebra II could introduce students to permutations as group elements. Introducing group theory in high school would be helpful in several ways. For example, I have witnessed in my work as a teaching assistant for calculus classes, that ideas involving composition, especially change of variables, composing fuctions, and using substition (as with the Chain Rule) are frustrating for almost all students. Yet, composition is a core element of group theory, and dealing with compositions with some group theoretical understanding would give students more power in dealing with compositions of functions in calculus, by giving them experience and more perspective of what a composition is. Statements of theorems involving composition, like the Chain Rule, would perhaps then be more readable, Generalizations to higher dimensions, as in vector calculus, would come with more experience behind them.

Composition to take *easy* functions and from them produce all the complicated functions. The above problem illustrates this, for in it a set of two elements generates a large group. Such group operations —especially inverse and conjugation —cause teaching problems not only in math, but also in biology, chemistry, engineering and physics. Many college courses would benefit if some elementary group theory were introduced earlier. For example, the geometry of rigid motions is a group theory topic, and is taught as such in many countries, though not in the US.

2. VISUALIZING $\langle x, y\rangle$ AND $\mathrm{Cor}(x, y)$

Finally, we would like to get a BASIC program to put some flashes on the screen to indicate something graphical about what elements you actually hit as we run over words in x and y, and in A and B. Is it possible that pairs of x and y that generate S_8 will reveal patterns in $\langle x, y\rangle$ and in their correlations that will be visible to someone in some graphic way?

All our programs and their outputs are in Chap. A. The pseudocode and a sample output of the S8CLASS.BAS are in Chap. A §3. This program lets us input any two permutations x and y from S_8. Then it multiplies longer and longer words in x and y, *a la* binary numbers, giving an ongoing tally and logarithmic bar graph of the conjugacy classes of the products. We ran this program with several different inputs and did not find anything surprising in the distribution of the classes as the products were generated.

The programs S8CYCLE.BAS and S8ORDER.BAS, whose outputs are sampled in Chap. A §4 and Chap. A §5, are similar to S8CLASS.BAS, but S8CYCLE.BAS

tallies the numbers of cycles in the products, while S8ORDER.BAS tallies the orders of the products. We ran both programs with several different x, y pairs. As the programs ran, the distributions of the orders and numbers of cycles seemed to roughly follow this classic result of Erdös and Turán [**Sh01**].

THEOREM 2.1 (Statistics in S_n). *Given any $\epsilon > 0$, for n large enough, most (at least $(1-\epsilon)n!$) permutations in S_n have roughly $\log n$ cycles. Further, for this large fraction of permutations, their orders divided by $n^{\frac{1}{2}} \log n$ are within ϵ of 1.*

Further, consider the function $f_n : \{1, \ldots, n\} \to \mathbb{Z}$ (resp. $g_n : \{1, \ldots, 2^n\} \to \mathbb{Z}$) that sends k to the number of permutations in S_n with precisely k cycles (resp. with precisely order k). Then, for n large, the graphs of f_n and g_n (scaled appropriately in their arguments and range) converge to Gaussian normal distributions with known variances as n tends to infinity.

It was pleasant to see this theorem confirmed visually. I believe displays like this could be valuable as a motivational and learning tool for algebra students.

Bibliography

[A95] M. Artin, *Algebra*, ISBN 0-13-004763-5, Prentice Hall, 1991.

[D69] J. D. Dixon, *The probability of generating the symmetric group*, Math. Z. **110** (1969), 199–205

[Isa94] I. M. Isaacs, *Algebra, a graduate course*, 1st ed., Brooks/Cole, Pacific Grove, California, 1994.

[KL90] W. M. Kantor and A. Lubotzky, *The probability of generating a finite classical group*, Geom. Dedicata **36** (1990), 67–87.

[LiSh95] M. W. Liebeck and A. Shalev, *The probability of generating a finite simple group*, Geom. Dedicata **56** (1995), 103–113.

[Sh01] A. Shalev, *Asymptotic Group Theory*, Notices of the AMS **April 2001**, 383–389.

APPENDIX A

BASIC PROGRAMS AND SAMPLE OUTPUTS

Each subsection has pseudocode for a program written in Basic. We ran these on a PC with a Pentium chip. While these Basic programs were nowhere so powerful as using **GAP**, they gave me my first experience with program writing. To use **GAP** required considerable knowledge of group theory. So, even for our little **GAP** programs, there was a substantial learning curve.

1. PROGRAM 1: S8S8CAL2.BAS

```
inputc:
Input permutation, C, in S_8\times S_8,
to be generated as a word in A and B,
where x=(1 2), y=(1 2 3 4 5 6 7 8), A=(x,y) and B=(y,x).

initializestring:
p = 0      'p is a string of 0's and 1's.
Goto calculate

increment:
Generate the next p in binary numbers (0, 1, 01, 10, 11, ...)

calculate:
With 0 and 1 representing A and B, multiply p out
If the product is C goto hit
Else goto increment

hit:
Print "The string p = ? generates C."
```

2. PROGRAM 2: TAIJOB1.BAS and output

```
initializestring:
p = 0      'p is a string of 0's and 1's.
Goto calculate

increment:
Generate the next p in binary numbers (0, 1, 01, 10, 11, ...)

calculate:
With 0 and 1 representing (3 4)(5 6)(7 8) and (1 2 3 4 5 6 7),
```

```
multiply p out.
If the product is a 2-cycle then goto hit
Else goto increment

hit:
Print trial number; "result"; string; product


Output excerpt:
string length                1
string length                2
... ...
string length                12
1911         result  111011101110  15342678
3003         result  110111011101  42315678
3549         result  101110111011  12745638
3822         result  011101110111  16345278
```

3. PROGRAM 3: S8CLASS.BAS and output

```
input:
Input permutations, x and y, as products of disjoint cycles.

initializestring:
p = 0      'p is a string of 0's and 1's.
Goto calculate

increment:
Generate the next p in binary numbers (0, 1, 01, 10, 11, ...)

calculate:
With 0 and 1 representing x and y, multiply p out.

matchclass:
Match the product with one of the 22 conjugacy classes.
Add to tally of class on the display, and recalculate the bar
 length in the logarithmic bar graph.
Goto increment


Sample output with input generators x=(1 2 3 4 5 6)(7 8), y=(2 7 3 5)(1 6 8):

DECIMAL TALLY OF CLASSES AND LOGARITHMIC BAR GRAPH
trial number: 32122
class number 1: 8 : ******** 4099
class number 2: 7 : ******** 4499
class number 3: 6 2 : ******** 2452
class number 4: 6 : ******** 2433
```

```
class number 5: 5 3 : ******** 2116
class number 6: 5 2 : ******** 3358
class number 7: 5 : ******* 1014
class number 8: 4 4 : ******* 1074
class number 9: 4 3 : ******** 2833
class number 10: 4 2 2 : ******* 1044
class number 11: 4 2 : ******** 1905
class number 12:  4 : ****** 430
class number 13:  3 3 2 : ******* 765
class number 14: 3 3 : ******* 1019
class number 15: 3 2 2 : ******* 1547
class number 16: 3 2 : ******* 789
class number 17: 3 : **** 85
class number 18: 2 2 2 2 : ***** 150
class number 19: 2 2 2 : ****** 264
class number 20: 2 2 : ***** 197
class number 21: 2 : **** 46
class number 22:  (identity) : * 3
```

4. PROGRAM 4: S8CYCLE.BAS output

The code for this program is very similar to that of S8CLASS.BAS

Sample output with generators x=(1 2 3 4 5 6)(7 8), y=(2 7 3 5)(1 6 8):

```
TALLY AND BAR GRAPH OF NUMBER OF CYCES
trial number: 32119
0 cycles: * 3
1 cycles: ********* 12605
2 cycles: ********** 15742
3 cycles: ******** 3619
4 cycles: ***** 150
```

5. PROGRAM 5: S8ORDER.BAS output

The code for this program is very similar to that of S8CLASS.BAS

Sample output with generators x=(1 2 3 4 5 6)(7 8), y=(2 7 3 5)(1 6 8):

```
TALLY AND BAR GRAPH OF ORDERS
trial number: 32164
order 0: * 3
order 2: ****** 657
order 3: ******* 1104
order 4: ******** 4452
order 5: ******* 1013
order 6: ********* 7985
```

```
order 7: ******** 4498
order 8: ******** 4098
order 10: ******** 3357
order 12: ******** 2833
order 15: ******** 2116
```