12-1991

Undergraduates, the Right Questions, and Cayley Produce Results

Gary J. Sherman
Rose-Hulman Institute of Technology

MSTR 91-07

UNDERGRADUATES, THE RIGHT QUESTIONS AND CAYLEY PRODUCE RESULTS

Gary J. Sherman

MS TR 91-07

December 1991

Department of Mathematics
Rose-Hulman Institute of Technology
Terre Haute, IN 47803

FAX(812) 877-3198 **Phone: (812) 877-8391**

UNDERGRADUATES, THE RIGHT QUESTIONS AND CAYLEY PRODUCE RESULTS

Gary J. Sherman*
Department of Mathematics
Rose-Hulman Institute of Technology
Terre Haute, IN 47803 USA
SHERMAN@ROSEVC.ROSE-HULMAN.EDU

ABSTRACT: During the summers of 1989, 1990 and 1991 eighteen undergraduates participated in a National Science Foundation Research Experiences for Undergraduates program at Rose-Hulman for which the author was the principal investigator. This paper provides some examples of the mathematics discovered during these three summers and discusses the philosophy, environment and process which made these discoveries possible.

Introduction

Can the computer revolutionize the teaching of undergraduate mathematics? Some say yes. Others say no. The question is broad, the data is soft and the protagonists are emotional - so who knows? I have taken either position depending on whom I'm trying to antagonize.

Can the computer enable bright, well-prepared, motivated undergraduates to do research in finite group theory? Some say "Finite group theory, are you kidding?" Others say "Finite group theory, are you kidding?" I say yes – proof by example is the point of this paper.

Many of my analyst friends are from the 'The only examples we ever saw in graduate school were S_3, D_4 and $\mathbb{Z}_n$' school of group theory. They are analysts, so maybe that's not so bad — or maybe it's one of the reasons they are analysts. I'm am algebraist, so I

---

*Work supported by NSF grant numbers DMS-890057, 8922674, 9100509
AMS Subject Classification Number: 20D60

was more sophisticated: I could also wheel and deal with the quaternion group of order eight and I had memorized just about every proof in Marshall Hall's book [11]. But, if somebody would have asked me a specific question about one of the nonabelian groups of order 32, I would have fainted or been on the way to my grandmother's funeral. Not so with the students who participate in my National Science Foundation Research Experiences for Undergraduates (NSF-REU) program at Rose-Hulman. Each summer, less than a week into the progam, they know more gritty facts about specific groups than I knew after five years in a PhD program. Indeed, the group-theoretic banter in our work-room crackles with the energy, the enthusiasm and the detail students usually reserve for discussions of sports or sex. What generates this mathematical energy, enthusiasm and detail? Bright, motivated undergraduates, the 'right' questions and the computer algebra system CAYLEY [13].

The students

Each summer six students participate in Rose-Hulman's NSF-REU program for which the author is the principal investigator. The participants are selected from among applicants (70 for 1991) who meet the National Science Foundation's eligibility requirements

-US citizenship-

-Fulltime undergraduate status in the fall of the succeeding year-

and the academic prerequisites that I set.

-A rigorous modern algebra course to include the Sylow theorems-

-Experience with a high level programming language-

Given that an applicant satisfies these prerequisties, I use data from an application form, a transcript and two letters of recommendation to select a subset of the applicants to call on the phone. The six participants are selected after the phone conversations. Not only do I want bright, motivated students but I want students who are capable of collaborating (willingly and productively) with me and with their fellow participants. And, to guarantee that the group (no pun intended) has enough social spice to keep it alive for seven weeks, I want women and men from small liberal arts colleges and major research universitys with varied non-mathematical interests. Thus far six women (Sarah Marie Belcastro, Cheryl Grood, Sharon Kineke, Judy Leavitt, Jeanne Nielsen, and Catherine Sugar) and twelve men (Joel Atkins, Stewart Burns, Jordan Ellenberg, Steve Knox, John O'Bryan, Kevin O'Bryant, David Patrick, Lawren Smithline, Tom Tucker, Mark Walker, Marty Wattenberg and Eric Wepsic) have represented Brown University, Carnegie-Mellon University, the College of Wooster, Duke University, Harvard University, Haverford College, New Mexico State University, Pomona College, Rose-Hulman Institute of Technology, the University of Chicago and the University of Michigan in the program. Of the participants who have graduated, all are in Ph.D. programs in mathematics (Berkeley, Duke, Illinois, Michigan and Stanford).

Some 'right' questions (and answers)

The fundamental theorem for finite abelian groups (each is a direct product of cyclic groups of prime-power order) and the basic classification scheme for groups (labeling a group as abelian, nilpotent, supersolvable, solvable or simple indicates, at least in a qualitative sense, the degree of commutativity the group enjoys) reflects the importance of the notion of commutativity in understanding group structure. How does one get beginning abstract algebra students ($xy = yx$ as far as they are concerned) to deal with the subtleties of the commutativity issue? I do it directly and quantitativley by asking them

What is the probablility that two elements of a finite group commute? (1)

A sample of our NSF-REU results ([1], [2], [7],.[10], [14], [15], [19], [20], [23].), consisting of three theorems each having its roots in mathematics motivated by this question, follows.

The formal answer to (1),

$$Pr_2(G) = |\{ (x,y) \mid xy = yx \}| / |G|^2,$$

raises another question:

How many ordered pairs of elements of a finite group commute? (2)

The answer to (2), orginally due to Erdos and Turan [8], is $k|G|$, where k is the number of conjugacy classes in G.

Thus, the useful answer to (1) is

$$Pr_2(G) = k/|G|.$$

Fortunately, $Pr_2(G) = 1$ if, and only if, G is abelian . Surprizingly, $Pr_2(G) \leq 5/8$ [9] if, and only if, G is nonabelian; i.e., there is a probablility 'gap' between nonabelian groups and abelian groups. Moreover, $Pr_2(G) = 5/8$ if, and only if, $G/Z \cong Z_2 \oplus Z_2$; i.e., 'abelianess' has a threshold and we know which groups occupy the threshold.

Rewriteabililty. Commutativity is a special case of rewriteability [3]. An n-tuple of a finite group G is n-rewriteable if

$$x_1 x_2 \cdots x_n = x_{\sigma(1)} x_{\sigma(2)} \cdots x_{\sigma(n)}.$$

for some nontrivial permutation $\sigma \in S_n$, the symmetric group on n symbols. The proportion of n-tuples from G which are n-rewriteable is denoted by $Pr_n(G)$ and G is said to be n-rewriteable if $Pr_n(G) = 1$. The 2-rewriteable groups are precisely the abelian groups. Both 4-rewriteable groups [16] and 3-rewriteable groups [6] have been characterized. The characterization of 4-rewriteable groups is long and technical, encompassing eight subclasses of groups. The Cliff's Notes version might go something like G is 4-rewriteable if (just about), and only if (just about), G has an abelian subgroup of index two or a derived group of order at most eight. The characterization of 3-rewriteable groups is much sharper. Each of the following conditions is equivalent to 3-rewriteability.

i) The order of the derived group of G is at most 2 [6]. Recall that the derived group of is the subgroup of G generated by commutators: $< x^{-1}y^{-1}xy \mid x,y \in G >$.

ii) Each conjugacy class is of order one or two [6]. Recall that the conjugacy class of x is $\{ y^{-1}xy \mid y \in G \}$.

iii) The probabililty of two elements commuting is greater than 1/2; i.e., $Pr_2(G) > 1/2$ [15].

Have you anticipated the question?

Does there exit a '5/8-like bound' for n-rewriteability? (3)

For general n, we think the answer is yes [15]. For n = 4, we 'know' the answer is yes and we will soon prove it. For n=3, the answer is yes – and the bound is 17/18. This result was first conjectured in [15], a paper which grew out of our work in the 1989 NSF-REU. Walker, who participated in the 1989 NSF-REU between his junior and senior years, proved (in his senior thesis for a degree in mathematics at New Mexico State University) that if G is not 3-rewriteable, then $Pr_3(G) \leq 971/972$. Ellenberg, who participated in the 1990 NSF-REU between his freshman and sophmore years at Harvard, finished it off with the following theorem.

Theorem 1 [7]. *A finite group G is not 3-rewriteable if, and only if, $Pr_3(G) \leq 17/18$. $Pr_3(G) = 17/18$, if and only if, G modulo its center is isomorphic to the symmetric group on three symbols.*

The proof is elementary – but hard and subtle – and makes use of a classic technique (assume there is a counter example and derive a contradiction about a minimal counter example) in conjunction with i), ii) and iii) above.

Centralizers. Another measure of commutativity for a finte group is the number of distinct centralizers the group possesses. Recall that the centralizer of x in G, denoted by C(x), is the subgroup of G consisting of all elements which commute with x; i.e., $C(x) = \{y \in G \mid xy = yx\}$. Let Cent(G) denote the number of distinct centralizers in G; i.e.,

$$\mathrm{Cent}(G) = |\{ C(x) \mid x \in G\}|.$$

Clearly, G is abelian if, and only if, Cent(G) = 1.

What can we say about Cent(G) for nonabelian groups? (4)

It turns out that there is a centralizer 'gap' for nonabelian groups anlagous to the probability 'gap' between 1 and 5/8: if Cent(G) $\neq$ 1, then Cent(G) is at least 4. The fact that Cent(G) is neither two nor three follows from an old Putnam problem [18].

> *Show that a finite group can not be the union of two of its proper subgroups. Does the statement remain true if "two" is replaced by "three"?*

The statement does not remain true if "two" is replaced by "three". The dihedral group on four symbols and the quaternion group of order eight can each be written as the union of three proper subgroups. But, in a sense, these are the only such groups because a group is the union of three proper subgroups if, and only if, $G/N \cong Z_2 \oplus Z_2$, where N in the intersection of these three subgroups [4]. It turns out that if G has only four centralizers, then N is the center, Z, of G (i.e., the intersection of all of the centralizers of G). Thus, Cent(G) = 4 if, and only if, $G/Z \cong Z_2 \oplus Z_2$. Now, S_3 has five centralizers and S_3 is a very special group, so here is a result that just has to be true: Cent(G) = 5 if, and only if, $G \cong S_3$. Sarah Marie Belcastro, who participated in the 1990 REU between her junior and senior years at Haverford, used the following theorem to say, "Well, not quite."

Theorem 2 [2]. *Cent(G) = 5 if, and only if,* $G/Z \cong S_3$ *or* $G/Z \cong Z_3 \oplus Z_3$.

The proof is elementary and makes incessant use of Lagrange's theorem, the fact that

$$|AB| \geq |A||B|/|A \cap B|$$

for subgroups and spirit of the Putnam problem.

Normality. Each subgroup of an abelian group is normal; i. e., Hx = xH for each element of G and each subgroup of G. However, this 'commutativity' condition does not characterize the class of abelian groups: The quaternion group of order eight, Q, is a nonabelian group in which each subgroup is normal. But, in a sense it is the only such group.

> *Each subgroup of G is normal if, and only if, G is abelian or G is the direct product of Q, an abelian group in which each element of order two and an abelian group in which each element has odd order* (see [11], pages 190-192).

Such groups are said to be Dedekind. The nonabelian Dedekind groups are referred to as Hamiltonian groups.

There are several ways to measure 'Dedekindness'[23]. Here's one. Let D(G) denote the proportion of subgroups of G which are normal. Clearly, G is Dedekind if, and only if, D(G) = 1.

How Dedekind can a finite group be?

At one time I thought there was a '5/8-like' bound for measures such as D(G) [22]. In the spring of 1988, Mark Leonard, Scott Krutsch (students in my abstract algebra course at the time) and I began to suspect that I was wrong. In the summer of 1989, Walker, Tucker, who participated in the 1989 NSF-REU between his sophomore and junior years at Harvard, and I proved that I was wrong — very wrong.

Theorem 3 [23]. *For each $r \in [0,1]$ there exists a sequence of groups $\{G_n\}$ such that $D(G) \to r$ as $n \to \infty$.*

Indeed, there are three other natural measures of 'Dedekindness' for which this result holds. And, for each of the four measures the proof of the theorem is constructive; i.e., the proof constructs a group such that $| D(G) - r | < \varepsilon$ where r is your favorite number between zero and one and epsilon is as small as you like.

CAYLEY

CAYLEY is a high level programming language (which can be used interactively or in batch mode), designed around the algebraic concepts of structure, set and mapping containing a large run-time library (of algebraic, geometric and combinatorial algorithms), an extensive data base (group theoretic and geometric knowledge) and a deduction engine. What distinguishes CAYLEY from other computer algebra packages is that it allows the user to define the structure in which he or she wishes to compute and to extract global information about the structure (in addition, of course, to information about individual elements). For example, if G is a 'small' (order less than 20,000) finitely presented group then one can compute complete structural information for G (conjugacy classes, subgroup lattice, normal subgroups and automorphism group). Some CAYLEY commands are provided below (in context) to illustrate how easy CAYLEY is to use and to hint at its power. For more information on CAYLEY see [13].

Roles

The student's role is to 'do' mathematics. My role includes providing the 'right' questions – easy for me to say, but hardest of my roles to fulfill. The examples I have given exhibit the spirit of my approach: view the major theorems and concepts of elementary group theory from a quantitative point of view. This approach generates questions that lend themselves to an empirical analysis of example after example. Enter CAYLEY: CAYLEY enables undergraduates (or analysts or me), who might otherwise by restricted to S_3, D_4 and $\mathbb{Z}_n$, to make and test interesting, significant conjectures by providing a (virtually) boundless inventory of examples and the facility to compute in those examples. Fortunately, good students working on the 'right' question with CAYLEY tend to suggest more 'right' questions ([1], [2], [10], [14], [15], [19], [23], [24]).

Here's how CAYLEY played its role in the development of the theorems mentioned above.

Theorem 1. If one views rewriteability as a generalization of commutativity and if one is familiar with the 5/8 bound for commutativity and other '5/8-like' bounds ([17],

[21], [22]), then one is compelled to ask if there is a '5/8-like' bound for rewriteability. My intuition told me the bound existed and I told my REU students to find it for 3-rewriteability. Their response – direct, computational and impossible without CAYLEY – was to pass group after group to the following CAYLEY procedure that counts the number of rewriteable 3-tuples in a group G. (CAYLEY commands are capitalized throughout the paper.)

```
COUNT = 0;
    FOR EACH X IN G DO
        FOR EACH Y IN G DO
            FOR EACH Z IN G DO
                IF X*Y*Z EQ X*Z*Y THEN GOTO 1;
                IF X*Y*Z EQ Y*X*Z THEN GOTO 1;
                IF X*Y*Z EQ Y*Z*X THEN GOTO 1;        (5)
                IF X*Y*Z EQ Z*X*Y THEN GOTO 1;
                IF X*Y*Z EQ Z*Y*X THEN GOTO 1;
                LOOP;
                1: COUNT = COUNT + 1;
            END;
        END;
    END;
PRINT COUNT;
```

How does one get groups into the machine? Some are already there. For example,

symmetric groups: G = SYMMETRIC(26); ,

alternating groups: G = ALTERNATING(48); , dihedral groups: G = DIHEDRAL(10); .

Others can be defined using a permutation representation or generators and relations. For example,

G: PERMUTATION GROUP(9);

G. GENERATORS: A = (1,2,3,4,5,6,7,8,9),

B = (2,8,5)(3,6,9);

and

G: FREE(A,B);

G. RELATIONS: A↑9 = B↑3 = B*A*(B↑2)*(A↑4) = 1;

both give access to the same group nonabelian group of order 27:

$$G = < a,b \mid a^9 = b^3 = e \text{ and } bab^{-1} = a^4 >. \quad (6)$$

The 'direct, computational and impossible without CAYLEY' approach and $|G|$ interact to slow the computation of $Pr_3(G)$ as $|G|$ increases. Our solution was statistical: obtain a confidence interval for $Pr_3(G)$ by sampling G x G x G (yes, RANELT(G) selects a random element of G). This technique, which proves useful accross the whole genre of problems we consider, quickly 'established' the 3-rewriteability bound as 17/18 and motivated Walker and Ellenberg to go after the proof with a vengeance.

Theorem 2. As I noted earlier my intuition on the centralizer problem was wrong. How did Belcastro know it was wrong? She wrote a CAYLEY procedure that counts the centralizers in a group (yes, CENTRALIZER(G, x) will give you the centralizer of x in G). Passing this procedure each non-ableian group of order up to 100 (yes, they are all available in CAYLEY) produced the case I overlooked in my original conjecture. Our proof of the theorem simply reflects the understanding we gleaned from examining examples using CAYLEY.

Theorem 3. Once upon a time I claimed a '5/8-like' bound existed for D(G) [22]. Then, I got realistic: even if I 'knew' the bound I could not 'prove' the bound because, in general, very little is known, or is likely to be known, about the denominator of D(G); i.e., the number of subgroups of G. On the other hand, if the '5/8-like' bound for D(G) doesn't exist, proving it doesn't exist might require control of the denominator of D(G) only for some 'tractable' class of groups. A year in industy doing operations research finally pays off: look for a solution where, given that a solution exists, the probability of finding it is not zero.

My role also includes knowing where 'where' might be. I suggested that Tucker and Walker look at metacyclic groups like the group appearing in (6):

$$G(p,n) = < a,b \mid a^{p^{n-1}} = b^p = e \text{ and } bab^{-1} = a^{p^{n-2}+1} >, \tag{7}$$

where p is a prime and n is a positive interger. They used CAYLEY to determine the number of normal subgroups (yes, NORMAL SUBGROUPS(G) will provide a list of all the normal subgroups of G) for lots of G(p,n)'s. The data they compiled and a formula, in terms of p and n, for the number of subgroups of G(p,n) [5] suggested that

$$D(G) \rightarrow \begin{cases} (n-2)/(n-1) \text{ as } p \rightarrow \infty. \\ 1 \qquad \text{as } n \rightarrow \infty. \end{cases}$$

Where did Theorem 3 come from? CAYLEY-play. Tucker and Walker, after convincing themselves that the bound didn't exist (no proof yet of course) began looking at direct products of G(p,n)'s with CAYLEY and noticed that they could push D(G) around at will. The construction, which comprises the proof of Theorem 3, is a mathematical summary of this CAYLEY-play.

If you have access to CAYLEY and would like to see CAYLEY-play in action, take another look at (5). If CAYLEY can count the number of 3-tuples which are rewriteable (in at least one nontrivial way), then it can certainly count the number, r_i, of 3-tuples which are rewriteable in exactly i ($0 \leq i \leq 5$) nontrivial ways. Have it do this for various groups and record the counts, (r_0, r_1, r_2, r_3, r_4, r_5), until you 'know' a theorem.

The monster (and I don't mean a sporadic simple group) will appear while you are doing the exercise in the previous paragraph. I have seen it at bicycle races. It always tries to hide behind weak legs which are clad in $150 riding shorts and wrapped around a $3000 hi-tech bicycle. It came to my home in the form of an electric nail-gun when we were adding a room to our house. My wife had to pull the plug early the first morning I had the gun because I was driving nails into any thing that didn't move – just because I could do it. The monster appears whenever a new tool is available for an old job. Its name is Falling-in-love-with-the-tool-and-forgetting-the-job.

Computers and mathematics are especially attractive to the Monster. If your department is implementing or considering the implementation of compter algebra systems, say in calculus, differential equations or discrete mathematics, you have met, or will soon meet, the monster. It manifests itself in the form of faculty and students becoming emotionally involved with Maple or Mathematica or whatever and forgetting that the point is mathematics, not pulling the trigger on their software package. As Paul Halmos said in a recent article [12],

> *"You push buttons, and things happen instantaneously and spectacularly, and if that's not what you wanted to know, you can make it go away and push another button. The reason cats and little children like to play with ping pong balls is that a tiny effort instantaneously produces a large result – very satisfying."*

Another of my roles is to stand in the middle of the workroom, early and often in the program, point at the monster and scream – much in the fashion of an extra in a 50's horror movie. I'm proud to say that this summer's NSF-REU students refer to their workstations and CAYLEY as their nail-guns.

Why does it work?

I'm assuming, of course, that this interaction of students, questions and CAYLEY does work. My definition of 'work' is that the mix produces mathematics – examples, constructions and theorems – not just computer printout. The hard evidence includes five refereed publication, four papers that are currently being refereed, five papers that are in preparation, and eighteen talks at local, regional and national meetings.

So, why does it work? In my opinion, it is some complicated interaction among the following factors.

1. The students are bright and they find the questions inherently interesting.

2. The students work with me not for me.

3. Mathematical calisthenics are eliminated: there is no short course to prepare for the research problems - the stated prerequisites are for real. The last thing a bright undergradaute needs is another course which uses mathematical revelation to reinforce mathematical passivity. Indeed, the Sunday the participants arrive they upack and come to my house for dinner, thus completing the orientation. After dinner we go to the workroom where they are introduced to their workstations, our mainframe and CAYLEY. Within an hour of these introductions they are using CAYLEY as a tool on open questions - which they met by mail three months earlier.

4. The program is intense: we eat, sleep and breath mathematics for seven weeks.

5. Interaction and collaboration, interaction and collaboration and interaction and collaboration. A common workroom makes it easy, a research theme encourages and rewards it and I insist on it. Here is a comment from a participant's evaluation of the 1990 REU: "I just didn't know that you could actually talk mathematics with people." This is from a student who was described as "the best we have seen at 'Prestigious University' in the past five years." That mathematics can be an exciting social activity

comes as an appealing, and motivating, revelation to most students. This makes it easier for me to discourage the me-and-the-problem syndrome, under which most undergraduates labor, and to encourage an us-and-the-problems attitude, under which most undergraduates flourish.

6. CAYLEY-play (always as a means and never as an end) converts students into aggressively adventurous mathematicians.

7. We keep the monster at bay.

References

1. J. E. Atkins and G. J. Sherman, Sets of typical subsample, Statistics and Probablility Letters (to appear).

2. S. M. Belcastro and G. J. Sherman, Counting centralizers in finite groups, Math. Mag. (being refereed).

3. R. D. Blyth and D. J. S. Robinson, Recent progress on rewriteability in groups, J. London Math. Soc. (to appear).

4. M. Bruckheimer, A. C. Bryan and A. Muir, Groups which are the union of three subgroups, Amer. Math. Monthly 77 (1970) 52-57.

5. W. C. Calhoun, Counting the subgroups of some finite groups, Amer. Math. Monthly 94 (1987) 54-59.

6. M. Curzio, P. Longobardi and M. Maj, Su di un problema combinatorio in teoria dei gruppi, Atti. Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) 74 (1983) 136-142.

7. J. E. Ellenberg, An upper bound for 3-rewriteability in finite groups, Rose-Hulman Math. Sci. Tech. Report 91-02.

8. P. Erdos and P. Turan, On some problems of a statistical group-theory, IV, Acta Math. Acad. Sci. Hung., 19 (1968) 413-435.

9. W. H. Gustafson, What is the probability that two group elements commute?, Amer. Math. Monthly, 80 (1973) 1031-1034.

10. C. Grood, Dihedral rewriteability, Journal of Undergraduate Mathematics (to appear).

11. M. Hall, The Theory of Groups, Macmillan (1959).

12. P R. Halmos, Is computer teaching harmful?, Notices Amer. Math. Soc., 38 (1991) 420-423.

13. D. F. Holt, The CAYLEY group theory system, Notices Amer. Math. Soc., 35 (1988) 1135-1140.

14. S. W. Knox, Fibonacci sequences in finite groups, Fibonacci Quarterly (to appear).

15. J. L. Leavitt, G. J. Sherman and M. E. Walker, Rewriteability in finite groups, Amer. Math. Monthly (to appear).

16. P. Longobardi, M. Maj and S. Stonehewer, The classification of groups in which every product of four elements can be reordered (preprint).

17. D. MacHale, Commutativity in finite rings, Amer. Math. Monthly, 83 (1976) 30-32.

18. The Mathematical Association of America, The Thirtieth William Lowell Putnam Mathematical Competition, December 6, 1969, Problem B-2.

19. J. Nielsen, Rewriteable sequencings of finite groups, Ars Combinatorica (being refereed).

20. J. T. O'Bryan and G. J. Sherman, Large nearly-abelian subgroups of symmetric groups, Amer. Math. Monthly (being refereed).

21. G. J. Sherman, What is the probability that an automorphism fixes a group element?, Amer. Math. Monthly, 82 (1975) 261-264.

22. G. J. Sherman, A probabilistic estimate of invariance for groups, Amer. Math. Monthly, 85 (1978) 361-363.

23. G. J. Sherman, T. J. Tucker and M. E. Walker, How Hamiltonian can a finite group be?, Arch. Math. (Basel), 57 (1991) 1-5.

24. G. J. Sherman and M. Wattenberg, Introducing...Cwatsets!, Math. Mag. (being refereed).