Contemporary Mathematics
Volume 45, 1985

Some consequences of the classification of finite simple groups

William M. Kantor*

This paper surveys some recent results obtained by assuming

CSG: Every finite nonabelian simple group is either an alternating group, a Chevalley group, or one of the 26 sporadic groups.

My aim is to avoid well-known consequences of **CSG**, such as the Schreier conjecture. I will also avoid some of the topics mentioned by Feit or Fried at the 1979 Santa Cruz group theory conference [17,20]. Many of the applications of **CSG** mentioned here involve permutation groups; in part, this reflects my own bias. Somewhat technical consequences are not described.

Many of the examples given are not stated precisely. The flavor and potential of applications seem more important in the present context than do comprehensive lists. Of course, there is no theory of applications of **CSG**; there is only a growing collection of techniques available for the solution of both old and new problems.

I hope that some of the following results will eventually be proved without the use of **CSG**. Many of them certainly do not look as if **CSG** should be involved at all.

MR classification: 20D05

*Supported in part by NSF Grant MCS 7903130.

Example 1. Probably the deepest and most potentially important of the examples described here are taken from a series of papers by Seitz [43-46]. All that can be described in a brief, non-technical manner amounts to the tip of the iceberg of at least two major projects.

(A) *Let G be a classical group over $GF(q)$, where $q > 11$ and $(6,q) = 1$. Let T be a maximal torus (not necessarily split). Then there is a precise description of all subgroups of G containing T but contained in no parabolic subgroup [44].* This description is in terms of the underlying vector space. There is also a good description in the case of all the remaining Chevalley groups, in terms of the corresponding algebraic group [43].

The proof requires **CSG**, and involves a remarkable interplay between **CSG** and algebraic groups. The next two results involve a similar interplay, but require only a few of the results obtained in the proof of **CSG**, rather than the full force of **CSG** itself.

(B) *If G is a Chevalley group over $GF(q)$, where q is odd and $q > 3$, and if X is any p-group, then any proper subgroup of G containing $N_G(X)$ is contained in a proper parabolic subgroup.*

(C) *Let G be a full classical subgroup of $GL(V)$, where V is a vector space over $GF(q)$ and q is odd and $q > 3$. Let $\overline{G}$ be the appropriate classical group defined on the corresponding vector space $\overline{V}$ over the algebraic closure of $GF(q)$. If $S \subset G$ is any set of p-elements, then the following are equivalent:*

$$G' \leq \langle C_G(s) \mid s \in S \rangle$$
$$SL(V) \leq \langle C_{GL(V)}(s) \mid s \in S \rangle$$
$$\overline{G}' \leq \langle C_{\overline{G}}(s) \mid s \in S \rangle$$
$$SL(\overline{V}) \leq \langle C_{GL(\overline{V})}(s) \mid s \in S \rangle.$$

Moreover, if all of these fail then there is a proper subspace W of V

such that each of the above centralizers leaves W or $\overline{W}$ invariant [46]. A similar result for sets of p′-elements is proved in [43] using (A).

Example 2 [18]. *Let T be the Brauer tree associated to a p-block with a nontrivial cyclic defect group of a group algebra $R[G]$, where R is the ring of integers in a finite extension of the p-adics. Then T is isomorphic to the union of several copies of a tree T_0 that are disjoint except that they have a certain vertex of T_0 identified. Moreover, either T_0 has at most 248 edges, or T_0 is a chain.* This implies that most trees do not arise as Brauer trees. In [18] it is noted that, without the help of **CSG**, no tree has yet been shown not to arise in this manner.

Example 3. A recent issue of the Journal of Algebra (Vol. 77, No. 1) contains very clear indications that there will be a rapidly expanding collection of "purely" group theoretic applications of **CSG**. In [2] it is shown that, for any finite group G, there is a solvable subgroup S and an element g of G such that $G = \langle S, S^g \rangle$. In [1] it is shown that, if G is a group of order $2^a 3^b m$, $(6,m) = 1$, then G is solvable if and only if it has subgroups of order $2^a m$ and $3^b m$ (compare Example 5 below). Finally, [23] contains results concerning the centralizer in Aut G of a Sylow p-subgroup of a group G, where $O_{p'}(G) = 1$ and $p > 2$. It does not seem feasible to survey (at this point in time) the growing literature in this direction.

Example 4. Let L and K be fields with $L \supset K$. The **relative Brauer group** B(L/K) consists of all Brauer classes of finite-dimensional central simple K-algebras split by L.

(A) *If K is a finitely generated extension of a global field* and L is*

---

*An algebraic number field or an algebraic function field in one variable over a finite field.

a nontrivial extension of K, then B(L/K) is infinite. This is proved in [16]; the case in which K is itself a global field was obtained earlier in [15]. Since B(L/K) is an abelian group, it is surprising that (A) is a consequence of

(B) *If G is a transitive permutation group on X, where $|X| > 1$, then there is a prime p such that some p-element fixes no point of X (see [15]).* It seems ridiculous to have proved this using **CSG**. There should be a character-theoretic proof. On the other hand, the special case of (A) in which K is a global field is actually "equivalent" to (B) [15,39].

The group G in (B) is a suitable Galois group. (If L is separable over K and N is the normal closure of L/K, then $G = \mathrm{Gal}(N/K)$ and $G_x = \mathrm{Gal}(N/L)$.) The p-element in (B) is used to construct infinitely many K-algebras.

Almost all subsequent examples also concern a permutation group G on a set X. If $x \in X$ then G_x is the stabilizer of x. Frequently, G will be primitive on X; that is, G will be transitive on X and G_x will be a maximal subgroup of G. In this situation, it is sometimes possible to reduce to the case of more or less simple groups, using the following result.

O'Nan-Scott Theorem [40,8,3]. Assume that G is primitive on X, and that the subgroup N generated by all the minimal normal subgroups of G is not a regular normal elementary abelian subgroup. Then $N = T_1 \times \cdots \times T_m$, with the T_i isomorphic nonabelian simple groups. Moreover, one of the following holds.

(i) *$T_1 \leq G_1$ for a primitive group G_1 of degree n_1, $n = n_1^m$, and $G \leq G_1 wr S_m$.*

(ii) $N_x = D_1 \times \cdots \times D_\ell$, *where* $m = k\ell$, D_i *is a diagonal subgroup of* $T_{(i-1)k+1} \times \cdots \times T_{ik}$, *and* $n = |T_1|^{(k-1)\ell}$.

(iii) $N_x = 1$ *and* $n = |T_1|^m$.

The original statement of the above theorem omitted possibility (iii); see [3].

The first application of this result is a fairly simply one.

Example 5. *All primitive groups G can be essentially classified for which* $|X|$ *is a power of a prime p and such that G has no regular normal subgroup.* The word "essentially" refers to the use of the O'Nan-Scott Theorem: (i) holds there, m is arbitrary, and an arbitrary transitive group of degree m can be permuting the factors T_i. The case $m = 1$ is due to myself (see [34]); when G is simple, the result was recently rediscovered independently by Arad and Fisman and by Guralnick. Our methods are the same, and very straightforward. The idea is as follows.

After reducing to the case $m = 1$, one reduces to the situation in which G has a normal Chevalley subgroup T of characteristic r. If $p \neq r$ then T_x contains a Sylow r-subgroup U of T, and a lemma of Tits applies. If $p = r$ then U is transitive on X, so that $T = UT_x$ and Seitz's flag-transitive theorem [41] applies if T has rank ≥ 2.

Of course, Example 5 trivializes the many difficult results on permutation groups of prime degree (as does the next example). Another type of application is found in [34].

Example 6. *All 2-transitive groups have been determined.* This determination falls into several parts, depending upon the nature of a minimal normal subgroup N of G: $N = A_n$, handled in 1895 [37]; N Chevalley [14]; N sporadic is simply folklore; and N elementary abelian [29,25,26,28].

When N is a Chevalley group, the proof is based on the following simple idea. Assume for simplicity that $G = N$. If $1_{G_x}^G$ is not contained in 1_B^G (where B is a Borel subgroup of G), then Seitz's flag-transitive theorem [41] applies. Since $1_{G_x}^G - 1_G$ is irreducible, the only other possibility is that $1_{G_x}^G \subset 1_B^G$. In general, the characteristic p of G divides the degree of any irreducible constituent of $1_B^G - 1_G$. Thus, $|G:G_x| \equiv 1 \pmod p$, G_x contains a Sylow p-subgroup of G, and a lemma of Tits can then be applied.

When N is elementary abelian of order p^d, G_x is a subgroup of GL(d,p) transitive on the nontrivial elements of N. If $d > 2$ and $q^d \neq 2^6$, there is an element of prime order acting irreducibly on N, and it follows that G_x has at most one nonabelian composition factor [24]. If G_x is solvable, see [29]. If G_x is nonsolvable, reduce to the case in which $G_x/Z(G_x)$ has a normal Chevalley subgroup of characteristic r. If $p = r$, standard results concerning the representations of a Chevalley group in its own characteristic eliminate most cases. If $p \neq r$, each irreducible representation of G_x in characteristic r has relatively large degree [33]; this can then be played off against the transitivity of G_x, which forces d to be small.

Corollary. *If $n = |X|$, all primitive groups G of degree n having an n-cycle can be determined.* (Namely, $G \geq A_n$, $G \trianglerighteq PSL(d,q)$ and $n = (q^d - 1)/(q - 1)$, $n = 11$ or 23 and G is PSL(2,11), M_{11} or M_{23}, or n is prime and G has a normal Sylow n-subgroup. In fact, if we exclude the last possibility, then classical results of Burnside and Schur yield the 2-transitivity of G.)

Some number-theoretic consequences of the determination of all 2-transitive groups are given in [19,20] and [13]. An application to logic is found in [12]. (However, a non-group-theoretic proof of this application has

also been obtained [51].)

Example 7. Assume that G is primitive on X, and has rank 3 (i.e., G has exactly 3 orbits on X × X). The following are the only cases left to classify: G has a normal exceptional Chevalley subgroup over a field of moderately small size (no more than $(1.8)^{10^{18}}$); or G has a regular normal elementary abelian subgroup. (In the latter case, the problem seems to be to find a suitably nice prime divisor of $|G_x|$.)

Let N be as in the O'Nan-Scott Theorem, and assume that N is nonabelian. Then $m \leq 2$ [8]; and if $m = 2$ then G is contained in $G_1 wr Z_2$ for a 2-transitive group G_1. This leaves the case $m = 1$. If N is sporadic, the desired result is again folklore. If N is alternating, see [5]. If N is an exceptional Chevalley group, see [42] (or the next example). Finally, if N is a classical group the desired classification appears in [31]; 1_B^G is used somewhat as in the preceding example.

As time goes on, the last two examples seem less interesting to me. More general types of results are needed. One possible direction is towards asymptotic results, as in the next five examples.

Example 8 [5,30,42]. *Given $r \geq 2$, there are only finitely many unknown primitive rank r permutation groups G,X such that G has a simple normal subgroup.* Here, the "known" permutation representations are as follows: $G \geq A_n$, X consists of all k-sets; G has a normal Chevalley subgroup, X is class of maximal parabolic subgroups; or G has a normal classical subgroup, and G_x is reducible.

When G has a normal Chevalley subgroup of characteristic p, and the Weyl group is fixed, the result was proved [42] by playing off 1_U^G against the permutation character $1_{G_x}^G$. (Namely, when the field is large it was shown that U must be contained in G_x.) This settles the case of exceptional

Chevalley groups, among other things (compare Example 7).

The remaining situations were dealt with in an entirely different manner. If $1 \neq g \in G$, it is easy to show that there is a G_x-orbit on $X - \{x\}$ of size $\leq |g^G|$, and then that $|G:G_x| \leq |g^G|^r$ (see [5]). In each case, g is chosen so that $|g^G|$ is minimized. On the other hand, a lower bound on $|X| = |G:G_x|$ can also be obtained. When G is symmetric or alternating, such a lower bound has been known for about a century, and sufficed for the result [5]. When G is a classical group, new lower bounds had to be found [30].

Example 9 [8]. *There is a constant c such that, if G,X is a primitive permutation group of degree n having no regular normal elementary abelian subgroup, then either G,X is known or* $|G| < n^{c \log \log n}$. This is proved using the O'Nan-Scott Theorem, **CSG**, and the aforementioned lower bounds on |X|. The constant c is less than 10.

Stronger bounds on |G| are obtained in [4], on the assumption that the composition factors of G are somewhat restricted.

Example 10 [9]. *For almost all n, if G is a primitive subgroup of* S_n *then* $G \geq A_n$.

More precisely, let E be the set of all n such that there is a primitive subgroup G of S_n such that $G \not\geq A_n$. Then

$$|E \cap [1,x]| = 2\pi(x) + (1 + \sqrt{2})x^{\frac{1}{2}} + O(x^{\frac{1}{2}}/\log x).$$

(Here, $\pi(x)$ is the number of primes $p \leq x$. The first term corresponds to integers n of the form $n = p$ or $p + 1$; the second term corresponds to the cases $n = k^2$ or $\binom{k}{2}$.) The proof uses the O'Nan-Scott Theorem, **CSG**, and Example 8.

Example 11 [10]: the Sims conjecture. *There is a function $f(d)$ such that, if G is primitive on X and G_x has an orbit on $X - \{x\}$ of size d, then $|G_x| \leq f(d)$.*

It had been known [48,50] that there is a function g(d) and a prime p such that $|G_x/O_p(G_x)| \leq g(d)$. (In fact, $g(d) = d!\{(d-1)!\}^2$ works.) Thus, the problem was to bound $|O_p(G_x)|$. This was first reduced to the case in which G has a simple normal subgroup N (using the O'Nan-Scott Theorem), and then to the case in which N is a Chevalley group of characteristic r (using **CSG**, of course). If $p = r$ a standard result of Borel and Tits applies; if $p \neq r$, detailed knowledge of properties of maximal tori was required.

Example 12 [38]. *There is a constant c such that the number of isomorphism classes of groups of order n is less than $n^{c(\log_2 n)^2}$.* The proof uses the following consequence of **CSG**: the number of simple groups of order n is small (that number never exceeds 2).

Example 13. There should be many nontrivial applications of **CSG** to combinatorial questions. For example, no finite group is yet known not to be capable of acting on a finite projective plane. Nevertheless, some results in this direction are obtained in [27,47].

Technical applications of **CSG** in coding theory are found in [21,22].

In [6], **CSG** was used to determine all graphs such that any isomorphism between induced subgraphs on at most 4 vertices is the restriction of an automorphism of the whole graph. (The corresponding result with 5 in place of 4 was handled in [7] using a purely combinatorial approach.)

A graph is called *distance-transitive* if it is connected and if, whenever x, y, x′, y′ are vertices and d(x,y) = d(x′,y′), there is an automorphism sending x to x′ and y to y′; its *valence* is the number of vertices joined to

a given one. In [10] it is shown that, *for each* $k > 2$, *there are only finitely many distance-transitive graphs of valence* k. The proof rests heavily on Example 11.

Next, consider a graph whose automorphism group is transitive on s-arcs (i.e., ordered sequences $(x_0, x_1, \cdots, x_s)$ of vertices such that $x_i \neq x_{i+2}$ and x_i is joined to x_{i+1} for all i). In [49] it is shown that $s \leq 7$. The proof depends on Example 6: if $s \geq 2$ then the stabilizer of a vertex x is z-transitive on the vertices joined to x.

Example 14. *Algorithms.* Assuming that we are given permutations generating a subgroup G of S_n, we wish to find properties or subgroups of G in time a polynomial in the input length.

(A) *A composition series for G can be found in polynomial time [36].*

(B) *If p is a prime dividing* $|G|$ *then an element of order p can be found in polynomial time [32].* (A fundamental algorithm due to Sims determines $|G|$ in polynomial time.)

For (A) and (B), the algorithms given in [36] and [32] require **CSG** in order to prove their validity. The difficulty is, of course, the polynomial restriction. For example, standard proofs of Cauchy's theorem require exponential time if p is fairly large.

On the other hand, it is not known whether a Sylow p-subgroup of G can be found in polynomial time -- even if G is assumed to be solvable. (However, if G is simple and p is a prime dividing $|G|$ then a Sylow p-subgroup of G can be found in polynomial time [32]. The proof uses **CSG**.) Whether centralizers of elements of G can be found in polynomial time is even harder; it may be relevant to the very difficult $P \neq NP$ problem of theoretical computer science.

It must be emphasized that the above results are of a theoretical, not practical nature. The polynomial restriction is quite different from the criteria for speed used in the computer construction and study of finite groups. Those criteria depend on probabilistic arguments, whereas (A) and (B) are concerned with absolute success in all situations. The difference can be seen using Cannon's Santa Cruz paper [11]. He states that finding centralizers and finding intersections of subgroups are cheap (i.e., can be done quickly and efficiently); finding Sylow subgroups requires medium cost; and testing simplicity and finding a regular normal subgroup of a primitive group are expensive. Yet, these expensive questions can be answered in polynomial time; finding Sylow subgroups is an open question; and the remaining questions are relevant to the $P \neq NP$ and graph isomorphism problems [35].

References

[1] Z. Arad and M. B. Ward, New criteria for the solvability of finite groups. J. Algebra 77 (1982) 234-246.

[2] M. Aschbacher and R. Guralnick, Solvable generation of groups and Sylow subgroups of the lower central series. J. Algebra 77 (1982) 189-201.

[3] M. Aschbacher and L. L. Scott, Maximal subgroups of finite groups (to appear).

[4] L. Babai, P. J. Cameron and P. P. Pálfy, On the orders of primitive groups with restricted nonabelian composition factors (to appear in J. Algebra).

[5] E. Bannai, Maximal subgroups of low rank of finite symmetric and alternating groups. J. Fac. Sci. Univ. Tokyo 18 (1972) 475-486.

[6] J. M. J. Buczak, Finite group theory. D. Phil. Thesis, Oxford U. 1980.

[7] P. J. Cameron, 6-transitive graphs. J. Combinatorial Theory (B) 28 (1980), 168-179.

[8] P. J. Cameron, Finite permutation groups and finite simple groups. Bull. LMS 13 (1981) 1-22.

[9] P. J. Cameron, P. M. Neumann and D. N. Teague, On the degrees of primitive permutation groups. Math. Z. 180 (1982) 141-149.

[10] P. J. Cameron, C. E. Praeger, J. Saxl and G. M. Seitz, On the Sims conjecture and distance transitive graphs to appear in Bull. LMS.

[11] J. Cannon, Effective procedures for the recognition of primitive groups. Proc. Symp. Pure Math. 37 (1980) 487-493.

[12] G. Cherlin, L. Harrington and A. Lachlan, $\aleph_0$-categorical $\aleph_0$-stable structures (to appear).

[13] A. M. Cohen and H. Zantema, A computation concerning doubly transitive permutation groups (to appear).

[14] C. W. Curtis, W. M. Kantor and G. M. Seitz, The 2-transitive

permutation representations of the finite Chevalley groups. TAMS 218 (1976) 1-57.

[15] B. Fein, W. M. Kantor and M. Schacher, Relative Brauer groups, II. J. reine angew. Math. 328 (1981) 39-57.

[16] B. Fein and M. Schacher, Relative Brauer groups, III (to appear).

[17] W. Feit, Some consequences of the classification of finite simple groups. Proc. Symp. Pure Math. 37 (1980) 175-181.

[18] W. Feit, Possible Brauer trees (to appear).

[19] W. Feit, M. Fried and L. L. Scott, Applications of the classification of simple groups to monodromy (to appear).

[20] M. Fried, Exposition on an arithmetic-group theoretic connection via Riemann's existence theorem. Proc. Symp. Pure Math. 37 (1980)571-602.

[21] S. M. Gagola, Jr., Weight enumerators of normalized codes (to appear in SIAM J. Alg. Disc. Methods).

[22] S. M. Gagola, Jr., Weight enumerators of normalized codes, II. The hermitian case (to appear in SIAM J. Alg. Disc. Methods).

[23] F. Gross, Automorphisms which centralize a Sylow p-subgroup. J. Algebra 77 (1982) 202-233.

[24] C. Hering, Zweifach transitive Permutationsgruppen, in denen 2 die maximale Anzahl von Fixpunkten von Involutionen ist. Math. Z. 104 (1968) 150-174.

[25] C. Hering, On linear groups which contain an irreducible subgroup of prime order. Proc. Int. Conf. Projective Planes, Washington State U. Press, 1973, 99-105.

[26] C. Hering, Transitive linear groups and linear groups which contain irreducible subgroups of prime order. Geom. Ded. 2 (1974) 425-460.

[27] C. Hering, On the structure of finite collineation groups of projective planes. Abh. Hamburg 49 (1979) 155-182.

[28] C. Hering, Transitive linear groups and linear groups which contain irreducible subgroups of prime order, II (to appear).

[29] B. Huppert, Zweifach transitive, auflösbare Permutations gruppen. Math. Z. 68 (1957) 126-150.

[30] W. M. Kantor, *Permutation representations of the finite classical groups* of small degree or rank. J. Algebra 60 (1979) 158-168.

[31] W. M. Kantor and R. A. Liebler, The rank 3 permutation representations of the finite classical groups. TAMS 271 (1982) 1-71.

[32] W. M. Kantor, Polynomial-time algorithms for finding elements of prime order and Sylow subgroups (submitted).

[33] V. Landazuri and G. M. Seitz, On the minimal degrees of projective representations of the finite Chevalley groups. J. Algebra 32 (1974) 418-443.

[34] R. A. Liebler and J. E. Yellen, In search of nonsolvable groups of central type. Pacific J. Math. 82 (1979) 485-492.

[35] E. M. Luks, Isomorphism of graphs of bounded valence can be tested in polynomial time, 42-49 in 21st IEEE Symp. Found. Comp. Sci., 1980.

[36] E. M. Luks (in preparation).

[37] E. Maillet, Sur les isomorphes holoédriques et transitifs des groupes symétriques ou alternés. J. Math. Pures Appl. (5) 1 (1895) 5-34.

[38] P. M. Neumann, An enumeration theorem for finite groups. Quart. J. Math. (2) 20 (1969) 395-401.

[39] M. Schacher, Applications of the classification of finite simple groups to Brauer groups (to appear).

[40] L. L. Scott, Representations in characteristic p. Proc. Symp. Pure Math. 37 (1980) 319-331.

[41] G. M. Seitz, Flag-transitive subgroups of Chevalley groups. Ann. of Math. 97 (1973) 27-56.

[42] G. M. Seitz, Small rank permutation representations of finite Chevalley groups. J. Algebra 28 (1974) 508-517.

[43] G. M. Seitz, The root subgroups for maximal tori in finite groups of Lie type (to appear in Pacif. J. Math.).

[44] G. M. Seitz, On the subgroup structure of classical groups. Comm. in Algebra 10 (1982) 875-885.

[45] G. M. Seitz, Parabolic subgroups containing the centralizer of a unipotent element (to appear in J. Algebra).

[47] G. Stroth, On Chevalley groups acting on projective planes (to appear).

[48] J. G. Thompson, Bounds for orders of maximal subgroups. J. Algebra 14 (1970) 135-138.

[49] R. M. Weiss, The nonexistence of 8-transitive graphs. Combinatorica 1 (1981) 309-311.

[50] H. Wielandt, Subnormal subgroups and permutation groups. Ohio State U., 1971.

[51] B.I. Zil'ber, Totally categorical structures and combinatorial geometries. Soviet Math. Dokl. 24 (1981) 149-151.

Department of Mathematics,
University of Oregon,
Eugene, Oregon,
OR 97403