MATHEMATICS OF COMPUTATION, VOLUME 33, NUMBER 146
APRIL 1979, PAGES 812–814

The Nonabelian Simple Groups $G, |G| < 10^6$— Minimal Generating Pairs

By John McKay and Kiang-Chuen Young

Abstract. Minimal (k, m, n) generating pairs and their associated presentations are defined for all nonabelian simple groups G, $|G| < 10^6$, excepting the family $\mathrm{PSL}(2, q)$. A complete set of minimal $(2, m, n)$ generating permutations of minimal degree is tabulated for these G. The set is complete in the sense that any minimal generating pair for G will satisfy the same presentation as exactly one of the listed pairs.

Introduction. This paper is one of a series on the simple groups of order up to 10^6. In another paper [1] we exhibit certain presentations, known as minimal (k, m, n) presentations, for all simple groups of order up to 10^5 excepting most members of a family $\mathrm{PSL}(2, q)$. Here we give the permutations corresponding to these presentations for all simple groups (with the same exceptions) of order up to 10^6.

Notation. G is a nonabelian simple group, which is identified with its group of inner automorphisms.

A is the group of automorphisms of G.

$|x|$ is an abbreviation for $|\langle x \rangle|$.

$C_A(x)$ is the centralizer of x in A.

$x \overset{A}{\sim} y$ means $x = y^t$, $t \in A$.

Definitions. Let $S = \{u \mid \langle u, v \rangle = G \text{ for some } v\}$, and let $k = k(G) = \min_{u \in S}\{|u|\}$. For $a \in S$ of order k, a *minimal* (k, m, n) *generating pair (for* G*) with respect to* a is an ordered pair (x, y) such that

(1) $\langle x, y \rangle = G$,

(2) $x \in a^A$,

(3) if $\langle x, z \rangle = G$, then $|z| \geqslant |y| = m$,

(4) $|xy| = n$.

A minimal (k, m, n) generating pair (x, y) satisfies a *minimal* (k, m, n) *presentation for* G:

$$\langle x, y; x^k = y^m = (xy)^n = 1, \{r_i(x, y)\}_{i \in I} = 1 \rangle .$$

Useful Results. A minimal generating pair with respect to a is a minimal generating pair with respect to any element of a^A, since the above properties are invariant under the action of automorphisms in A.

Received September 16, 1976; revised April 4, 1978.

AMS (MOS) subject classifications (1970). Primary 20–04, 20B99, 20D05, 20F05.

Key words and phrases. Finite simple groups, permutation groups, generating permutations.

Let A act on $G \times G$ as

$$(x, y)^t \longmapsto (x^t, y^t), \qquad t \in A.$$

The transitivity sets are the orbitals of A. Denote the orbital containing (x, y) by $O_{x,y}$.

PROPOSITION 1. $|O_{x,y}| = |A|/|C_A(x) \cap C_A(y)|$. *If, further,* $\langle x, y \rangle \cong G$ *then* $|O_{x,y}| = |A|$.

Let $P_G(x, y)$ mean that (x, y) satisfies a presentation P_G of G, where $\langle x, y \rangle = G$.

THEOREM 1. *Suppose* $P_G(a, b)$, *then* $P_G(x, y)$ *if and only if* $\exists\, t \in A$ *such that* $a^t = x$ *and* $b^t = y$.

Proof. Sufficiency is immediate. For necessity we may construct a map t': $G \longrightarrow G$ such that $a^{t'} = x$ and $b^{t'} = y$. The map t' is surjective and preserves the defining relations (and hence all relations); therefore, $t' \in A$. □

LEMMA 1.

$$|\{(x^t, y) \,|\, P_G(x^t, y), t \in A\}| = |C_A(y)|.$$

Proof. Use Theorem 1 and Proposition 1, restricting the action of A to $C_A(y)$. □

This result can be used in counting arguments [3], [4], [7] to count the number of orbitals of minimal generating pairs for G when the class structure constants [5] and the maximal subgroups [2] are known. We can also estimate the probability that a pair of elements chosen at random from their conjugacy classes should generate G or satisfy a given presentation [1].

THEOREM 2. *The pair* (x, y), *where* $x \in a^A$ *and* $y \in b^A$, *is a minimal generating pair for* G *with respect to* a *if and only if*

$$(x, y) \overset{A}{\sim} (a^{u_i}, b),$$

where $A = \bigcup_i C_A(a) u_i C_A(b)$ *and* $\langle a^{u_i}, b \rangle = G$.

Proof. Let $(x, y) = (a^s, b^t)$, where $s, t \in A$. Then for some $\alpha \in C_A(a)$ and $\beta \in C_A(b)$, we have

$$(x, y) \overset{A}{\sim} (a^{st^{-1}}, b) = (a^{\alpha u_i \beta}, b) = (a^{u_i \beta}, b) \overset{A}{\sim} (a^{u_i}, b). \quad \square$$

We deduce from this result that for a complete set of minimal generating pairs we need choose for a and b only those representatives of conjugacy classes in A whose orders satisfy the minimality conditions. The set is complete in the sense that for any minimal generating pair (x, y), there is some $t \in A$ such that $(x, y)^t = (a, b)$ for exactly one listed pair (a, b). We have listed a representative pair (a, b) from each orbital containing a minimal (k, m, n) pair. We find, as conjectured for all finite nonabelian simple groups by Steinberg [6], that $k(G) = 2$ for all groups G listed. It is an old conjecture that all finite simple groups require at most two generators. This result is proved in [6] for groups of Lie type.

The Tables. The first line for each group G gives its name, order, minimal degree as a permutation group, and the order of its outer automorphism group. This is followed by the conjugacy classes and their cycle types and the orders of centralizers of elements. When there is more than one conjugacy class of generators of a cyclic subgroup, the notation identifies the classes by letters following their period, e.g., $10AB$ denotes two classes of period 10.

The generating pairs of permutations are displayed in image form. Each pair is identified by number, e.g., 20.5 denotes the fifth generating pair of the twentieth group. The notation $(2, m, n; s)$ denotes the relations $a^2 = b^m = (ab)^n = (a^{-1}b^{-1}ab)^s = 1$; the names of the conjugacy classes of a and b are given as well. Additional relators sufficient to distinguish the generating pair uniquely are given on the same line where needed.

The permutations are given in pairs (a, b); when only a is given, the generator b is taken to be the one last printed in full. When (a, b^{-1}) is a distinct minimal generating pair, this is denoted by $b \longrightarrow b^{-1}$.

One word of warning–for purposes of distinguishing minimal generating pairs it is the conjugacy class in Aut(G) that matters, and it is possible for elements to have distinct cycle types and yet be conjugate in Aut(G), e.g., classes $2A$ and $2B$ are conjugate in Aut(Sp(4, 4)) but have differing cycle types.

Although great care has been taken in preparing these tables, the authors will be grateful to hear of any errors found in them. (The tables are located in the microfiche section at the end of this issue.)

Acknowledgements. The authors acknowledge the support of the National Research Council of Canada.

Special thanks are due to Robin Rohlicek for his help in preparing these tables for publication.

Department of Computer Science
Concordia University
1455 Maisonneuve W.
Montreal, Quebec, Canada

Department of Mathematics
Vanier College
Montreal, Quebec, Canada

1. J. J. CANNON, J. MCKAY & K. C. YOUNG, "The non-abelian simple groups G, $|G| < 10^5$. Presentations." (To appear.)

2. J. FISCHER & J. MCKAY, "The non-abelian simple groups G, $|G| < 10^6$. Maximal subgroups," *Math. Comp.*, v. 32, 1978, pp. 1293–1302.

3. J. MCKAY, "Computing with finite simple groups," *Proc. Second Internat. Conf. Theory of Groups*, Lecture Notes in Math., vol. 372, Springer-Verlag, Berlin, New York, 1974, pp. 448–452.

4. J. MCKAY, "Subgroups and permutation characters," *Computers in Algebra and Number Theory*, SIAM-AMS Proceedings, vol. 4, 1970, Amer. Math. Soc., Providence, R. I., 1971, pp. 177–181.

5. J. MCKAY, "The non-abelian simple groups G, $|G| < 10^6$. Character tables." (To appear.)

6. R. STEINBERG, "Generators for simple groups," *Canad. J. Math.*, v. 14, 1962, pp. 277–283.

7. K. C. YOUNG, *Computing with Finite Groups*, Ph. D. thesis, McGill University, Montreal, Canada, 1975.