BULL. AUSTRAL. MATH. SOC.
VOL. 22 (1980), 113-124.

20B35, 20B99, 20G40

TWO-GENERATOR GROUPS II

J.L. BRENNER AND JAMES WIEGOLD

Let n be an odd integer greater than 9. It is proved that the alternating group A_n has spread 3 in the sense that for any non-trivial elements x_1, x_2, x_3 of A_n, there is an element y in A_n such that $\langle x_i, y\rangle = A_n$ for $i = 1, 2, 3$.

1. Introduction

This article is a continuation of [2], to which the reader is referred for motivation and background material. We recall the principal definition.

DEFINITION 1.1. A finite group G is said to have *spread* r if for every set $\{x_1, \ldots, x_r\}$ of non-trivial elements of G there is an element y such that $\langle x_i, y\rangle = G$ for $i = 1, 2, \ldots, r$. The set of all finite groups having spread r is denoted by Γ_r.

Thus each Γ_r is a set of two-generator groups, and $\Gamma_r \supseteq \Gamma_{r+1}$ for all $r \geq 1$. In [2] (see also Binder [1] for an independent proof), we showed that $A_{2n} \in \Gamma_4 \backslash \Gamma_5$ for $n \geq 4$, and various analogous results for the groups $\mathrm{PSL}(2, q)$. On the other hand, it turned out that A_{19} has enormous spread, more than 6,000,000,000 or so. This is due to the scarcity of transitive subgroups of A_{19}, and we indicate here (in §4) a similar result for alternating groups A_p, whenever p is a prime for

Received 19 December 1979.

which A_p displays the same scarcity of transitive subgroups. This result, and general considerations, lead us to believe that A_n has spread that tends to infinity with n, for odd n. We are unable to prove anything like this. Combinatorial methods like those in [2] are used to prove (in §2) that $A_n \in \Gamma_3$ if n is odd and at least 11. There is no doubt that similar arguments would prove that $A_n \in \Gamma_4$ for sufficiently large n, or even $A_n \in \Gamma_5$ and so on, but the extra combinatorial complication is hardly worth indulging in, given our belief that the spread of A_n is unbounded for large odd n.

For odd composite n, we give a very simple proof in §3 that A_n does *not* have spread C_{d-1}^{n-1}, where d is the smallest prime divisor of n. This is very easy. Quite possibly the following problem will have an affirmative answer, but it will be exceedingly difficult to prove.

PROBLEM 1.2. For n odd and composite, with d the smallest prime factor, does A_n have spread close to $C_{d-1}^{n-1} - 1$?

We have been unable to resolve this even in the simplest case, namely for A_9. Finally, in §3, we sketch a proof of the (special but new) result that PSL(3, 4) cannot be generated by an element of order 2 and one of order 3. The context is the following. In [2] we defined $\Gamma_1^{(k)}$ to consist of those groups G in Γ_1 such that every non-trivial element a belongs to a generating pair $\{a, b\}$ such that one of a, b has order k. Thus $\mathrm{PSL}(3, 4) \notin \Gamma_1^{(2)}$. In an interesting doctoral dissertation [4], Langer filled more of the gaps in [2] by establishing that, for $q \neq 2, 9$, the group $\mathrm{PSL}(2, q)$ belongs to $\Gamma_1^{(k)}$ whenever it has an element of order k.

2. Alternating groups of odd degree

We mentioned in [2] that $A_5 \in \Gamma_2 \backslash \Gamma_3$. It is easy to prove that A_7

https://doi.org/10.1017/S0004972700006389 Published online by Cambridge University Press

and A_9 lie in Γ_2, and we shall omit the proof. The reader will see how to do it by examining the methods employed in this section.

Wherever possible we shall use "standard elements" as supplementary generators.

DEFINITION 2.1. Let $n = 2k + 1$, $k > 2$. A *standard type* is the type $k^1(\frac{1}{2}(k+1))^2$ if k is odd; $(k+1)^1(\frac{1}{2}k)^2$ if k is even. The elements in A_n of standard type are called *standard elements*.

Thus for odd k, a standard element is a product of a k-cycle and two $\frac{1}{2}(k+1)$-cycles, and similarly for even k. This is the vital property of standard elements:

THEOREM 2.2. *For odd $n > 5$, the only transitive subgroup of A_n containing a standard element is A_n itself.*

Proof. Any subgroup H containing a standard element contains a k-cycle if k is odd and a $(k+1)$-cycle if k is even. Since k and $k + 1$ are prime to $2k + 1$, this means that H is primitive if it is transitive. Now use a theorem of Williamson ([7]; see also [2]): if a primitive group G of degree n contains a t-cycle, $1 < t < n$, then $G \supseteq A_n$ unless $t > (n-t)!$.

To prove that every three elements of A_n have a common "mate", we may assume at the outset that they are of prime order. In the proof of the theorem that follows, we do not go into every detail, to save space and to spare the reader. In all cases where this is possible, we use a standard element as common mate: when it is not possible, an n-cycle always works. Indeed, one of the things that makes the odd-degree case so difficult to contend with is that sometimes we are *forced* to use an n-cycle as common mate; for example, only an n-cycle will mate each of $(1, 2)(3, 4)$, $(1, 3)(2, 4)$, $(1, 4)(2, 3)$ simultaneously.

THEOREM 2.3. *Let x_1, x_2, x_3 be elements of prime order in A_n, n odd and greater than 9, with the order of x_i greater than or equal to the order of x_j if $i \leq j$. Then there is a standard element y such that $\langle x_i, y\rangle = A_n$ for $i = 1, 2, 3$, except in the following cases:*

https://doi.org/10.1017/S0004972700006389 Published online by Cambridge University Press

(1) x_1, x_2 *are* 3*-cycles moving exactly* 2 *symbols in common, say* $x_1 = (1, 2, 3)$, $x_2 = (1, 2, 4)$, *and* x_3 *is of the form* $(3, 4, \gamma)$ *or* $(3, 4)(\alpha, \beta)$;

(2) x_1, x_2 *are* 3*-cycles moving exactly one symbol in common, say* $x_1 = (1, 2, 3)$, $x_2 = (1, 4, 5)$, *and* x_3 *is of the form* $(2, 3)(4, 5)$, $(2, 4)(3, 5)$ *or* $(2, 5)(3, 4)$;

(3) x_1, x_2, x_3 *are all of order* 2 , *and move exactly the same four symbols, say* $x_1 = (1, 2)(3, 4)$, $x_2 = (1, 3)(2, 4)$, $x_3 = (1, 4)(2, 3)$.

In each of the exceptional cases, there is an n*-cycle that is a common mate for* x_1, x_2, x_3 .

Proof. We split the proof up into several cases. Recall that each cycle in every standard element moves at least 3 symbols, since $n \geq 11$.

CASE 1. x_1, x_2 have odd order.

Case 1A. Suppose that there is an orbit Ω_1 of $\langle x_1 \rangle$ and an orbit Ω_2 of $\langle x_2 \rangle$ with subsets $T_1 \subseteq \Omega_1$, $T_2 \subseteq \Omega_2$ such that $T_1 \cap T_2 = \emptyset$ and $|T_1| = |T_2| = 3$. For simplicity write $T_1 = \{1, 2, 3\}$, $T_2 = \{4, 5, 6\}$. Thus 1, 2, 3 occur in the same cycle of x_1 , and 4, 5, 6 in the same cycle of x_2 , and by Theorem 2.2 any standard element

$$y = (1, \alpha_1, \ldots)(2, \alpha_2, \ldots)(3, \alpha_3, \ldots) ,$$

where α_1, α_2, α_3 are 4, 5, 6 in some order, will be a common mate for x_1 and x_2 , since $\langle x_1, y \rangle$ and $\langle x_2, y \rangle$ are transitive. Clearly, if x_3 has odd order, then three symbols from the same cycle of x_3 can be disposed, one in each of the three cycles in one of the six choices of y ; and this choice will be a common mate for all three elements however the remaining symbols are distributed. The same sort of reasoning applies if x_3 is of order 2 .

https://doi.org/10.1017/S0004972700006389 Published online by Cambridge University Press

Case 1B. If the condition imposed on the orbits in Case 1A does not hold, then for every orbit Ω_1 of $\langle x_1 \rangle$ and every orbit Ω_2 of $\langle x_2 \rangle$, every three-element subset of Ω_1 intersects every three-element subset of Ω_2. This imposes severe restrictions on Ω_1, Ω_2. A moment's thought shows that one of three things must happen:

(i) $|\Omega_1| = |\Omega_2| = 3$ and $\Omega_1 \cap \Omega_2 \neq \emptyset$;

(ii) $|\Omega_1| = 5$, $|\Omega_2| = 3$ and $\Omega_2 \subseteq \Omega_1$, or symmetrically $|\Omega_1| = 3$, $|\Omega_2| = 5$, $\Omega_1 \subseteq \Omega_2$;

(iii) $\Omega_1 = \Omega_2$ and $|\Omega_1| = 5$.

Since these conditions hold for *every* pair of orbits, x_1 and x_2 must have very restricted forms. If x_1 has order more than 3, then it follows that x_1 is a 5-cycle and x_2 is a 5-cycle or a 3-cycle with support contained in that of x_1. In other words, x_1 is of the form $(1, 2, 3, 4, 5)$ say, and x_2 is either a 5-cycle on the same letters or a 3-cycle on three of them, say on 1, 2, 3 with no loss of generality. In this case a standard element

$$y = (1, \ldots)(2, \ldots)(3, \ldots)$$

will be a mate for x_1 and x_2. Clearly, whatever x_3 is, y can be fleshed out to be a mate for x_3 too.

Thus we may now suppose that x_1 and x_2 have order 3, and that every cycle in x_1 intersects every cycle in x_2. This can happen in very few ways. Neither element can move more than 9 symbols, and we may assume that $9 \geq |\mathrm{supp}(x_1)| \geq |\mathrm{supp}(x_2)|$.

If x_1 moves 9 symbols, the situation is typified by

$$x_1 = (1, 2, 3)(4, 5, 6)(7, 8, 9),$$

$$x_2 = (1, 4, 7) \ldots,$$

https://doi.org/10.1017/S0004972700006389 Published online by Cambridge University Press

in which case any standard element

$$y = (1, \ldots)(4, \ldots)(7, \ldots)$$

is a common mate for x_1 and x_2, and it can be fleshed out to be a mate for x_3, whatever x_3 may be other than $(1, 4, 7)^{\pm 1}$. If x_3 is $(1, 4, 7)^{\pm 1}$, we can assume that x_2 has a further 3-cycle in its decomposition, say $(2, 5, 8)$ or its like, and argue from there.

If x_1 moves 6 symbols, one has cases like

$$x_1 = (1, 2, 3)(4, 5, 6), \quad x_2 = (1, 4, \alpha)(2, 5, \beta),$$

$$x_1 = (1, 2, 3)(4, 5, 6), \quad x_2 = (1, 4, \alpha).$$

In these cases a standard element

$$(1, \ldots)(4, \ldots)(\alpha, \ldots) \quad \text{if } \alpha \in \{2, 3, 5, 6\},$$

$$(1, \ldots)(4, \ldots)(\alpha, \gamma, \ldots) \quad \text{if } \alpha \notin \{2, 3, 5, 6\},$$

for any $\gamma \in \{2, 3, 5, 6\}$, is a common mate for x_1, x_2. Clearly, whatever x_3 may be, there is room to accommodate x_3 as well.

Lastly, if $|\mathrm{supp}(x_1)| = 3$, then both x_1 and x_2 are 3-cycles, and problematical cases are typified by

$$x_1 = (1, 2, 3), \quad x_2 = (1, 2, 4),$$

$$x_1 = (1, 2, 3), \quad x_2 = (1, 4, 5),$$

the case $x_1 = x_2^{\pm 1}$ being trivial.

In the first case, a standard common mate for x_1, x_2 has to be of a form like

$$(1, \ldots)(2, \ldots)(3, \ldots, 4, \ldots).$$

This will not mate any elements $(\alpha, \beta)(3, 4)$ nor $(3, 4, \gamma)^{\pm 1}$, but it can be fleshed-out to mate anything else. We have thus come to our first exceptions, and we must provide our n-cycle common mate. Evidently, the

https://doi.org/10.1017/S0004972700006389 Published online by Cambridge University Press

essentially different possibilities for $x_3 = (\alpha, \beta)(3, 4)$ are $(1, 2)(3, 4)$, $(1, 5)(3, 4)$, $(5, 6)(3, 4)$; in all cases $(1, 2, \ldots, n)$ is a common mate for $(1, 2, 3)$, $(1, 2, 4)$, $(\alpha, \beta)(3, 4)$. Similarly, the essentially different cases for $x_3 = (3, 4, \gamma)^{\pm 1}$ are $(2, 3, 4)^{\pm 1}$ and $(3, 4, 5)^{\pm 1}$; and again $(1, 2, \ldots, n)$ is a common mate. The necessary calculations are routine, and we omit them.

In the second case, a standard common mate for x_1, x_2 must take one of these forms

$$g = (1, \ldots)(2, \ldots, 4, \ldots)(3, \ldots, 5, \ldots) ,$$

$$h = (1, \ldots)(2, \ldots, 5, \ldots)(3, \ldots, 4, \ldots) ,$$

and only $(2, 3)(4, 5)$, $(2, 5)(3, 4)$, $(2, 4)(3, 5)$ cannot be mated by one of g, h . But yet again, $(1, 2, \ldots, n)$ is a common mate in all problematical cases.

We have now finished the case in which x_1, x_2 have odd order.

CASE 2. x_1 has odd order, x_2, x_3 have order 2 .

Case 2A. Suppose that there are 3 entries in a cycle of x_1 , say 1, 2, 3 , different from the entries in two cycles of x_2 , say 4, 5, 6, 7 ; so

$$x_1 = (1, \ldots, 2, \ldots, 3, \ldots) \ldots ,$$

$$x_2 = (45)(67) \ldots .$$

There are essentially four distributions of 1, 2, 3, 4, 5, 6, 7 among the three cycles of a standard element y that ensures that it mates x_1 and x_2 . Here are the four with 1, 2, 3 in a given order:

$$(1, 4, 6, \ldots)(2, 5, \ldots)(3, 7, \ldots) ,$$

$$(1, 4, 7, \ldots)(2, 5, \ldots)(3, 6, \ldots) ,$$

$$(1, 4, \ldots)(2, 5, 6, \ldots)(3, 7, \ldots) ,$$

$$(1, 4, \ldots)(2, 5, 7, \ldots)(3, 6, \ldots) .$$

https://doi.org/10.1017/S0004972700006389 Published online by Cambridge University Press

Clearly, whatever element of order two x_3 might be, one of the 24 possibilities for y can be fleshed out so as to mate it.

Case 2B. Suppose that the condition assumed in Case 2A is false. As in Case 1B, we get strong restrictions on the possibilities for x_1, x_2. For a start, x_1 has order less than or equal to 5; if it has order 5 it is a 5-cycle and both x_2, x_3 have support of order 4 intersecting every three-element subset of $\mathrm{supp}(x_1)$. In other words, x_1 is something like $(1, 2, 3, 4, 5)$, and each of x_2, x_3 something like $(1, 2)(3, 4)$ or $(1, 2)(3, 6)$. This case is easy; just start with a tentative common mate for x_2, x_3 and flesh it out to accommodate x_1.

Suppose finally that x_1 has order 3, say

$$x_1 = (1, 2, 3) \ldots .$$

Obviously, x_2 $[x_3]$ (being even) cannot move more than 8 symbols; for if it did, it would have ≥ 6 transpositions, and some pair of them would fail to involve any of 1, 2, 3. It is possible for x_2 $[x_3]$ to have support of cardinal 8, but then x_1 has support of cardinal less than or equal to 6; and the usual sort of argument can be pushed through to find a standard common mate.

CASE 3. x_1, x_2, x_3 are all of order 2.

By now the plot should be clear. One first considers the case where x_1, x_2 have forms like

$$x_1 = (1, 2)(3, 4) \ldots ,$$

$$x_2 = (5, 6)(7, 8) \ldots .$$

The symbols 1, 2, 3, 4, 5, 6, 7, 8 can then be disposed in 32 essentially different ways in a "standard shape", so that any fleshing-out is a common mate for x_1, x_2. In all cases there is enough flexibility to accommodate x_3 as well.

If x_1, x_2 do not have shapes as indicated, there are clearly strong restrictions, and the whole argument goes through to provide a standard common mate except when x_1, x_2, x_3 have forms like $(1, 2)(3, 4)$, $(1, 3)(2, 4)$, $(1, 4)(2, 3)$ respectively. In that case $(1, 2, \ldots, n)$ is a common mate, as is easy to check.

We can thus state:

COROLLARY 2.4. *A_n has spread 3 for $n \geq 11$.*

3. The case of odd composite n

Here is the simple result mentioned in the introduction.

THEOREM 3.1. *Let n be an odd composite integer, and d its smallest proper divisor. Then A_n does not have spread $z = C_{d-1}^{n-1}$.*

For each choice of $d - 1$ symbols out of the $n - 1$ symbols $2, 3, \ldots, n$, we construct a d-cycle moving 1 and these $d - 1$ chosen symbols. There are z such d-cycles, and we claim that no common mate exists. Firstly, a common mate must be an n-cycle, since any element with more than one cycle in its canonical decomposition generates an intransitive subgroup with one of our d-cycles. However, every n-cycle generates an imprimitive group with one of them.

This is an inadequate sort of result, but it is the best we can do. For the remainder of the section we sketch a proof that $\mathrm{PSL}(3, 4)$ cannot be generated by an element of order 2 and one of order 3.

The following argument has been kindly supplied by Professor A. Sinkov; it replaces our original argument, which was longer. Since $\mathrm{PSL}(3, 4)$ has no element of order greater than 7, two elements of orders 2, 3 in $\mathrm{PSL}(3, 4)$ must generate $(2, 3, n; p)$ with $n \leq 7$ and $p \leq 7$ [7]. All these groups are known. In fact $(2, 3, 7; 7)$ has order 1092; see [3]. This shows that $\mathrm{PSL}(3, 4)$ cannot in fact be generated by elements of orders 2, 3.

4. The spread of A_p, p prime

In this section we show that for certain primes p, the spread of A_p

https://doi.org/10.1017/S0004972700006389 Published online by Cambridge University Press

is huge. We call p a good prime if the only insoluble transitive groups of degree p are A_p and S_p. Neumann and Ligler [5] listed 19 such primes, and reported the existence of many others. (19 is one of the good primes.) Undoubtedly the consensus now is that the good primes are in the majority.

Let p be a good prime, and q a prime dividing $\frac{1}{2}(p-1)$. The group A_p contains $(p-1)!$ p-cycles that lie in $(p-2)!$ cyclic groups $\langle v_\nu \rangle = T_\nu$ of order p, the Sylow p-subgroups of A_p. In the symmetric group S_p, there is a $(p-1)$-cycle w_ν that transforms v_ν into its gth power, where g is a primitive root mod p. Thus the normalizer N_ν of T_ν in A_p is an extension of T_ν by a cyclic group $\langle u_\nu \rangle$ of order $\frac{1}{2}(p-1)$. This normalizer contains elements of order q. Each such element x is the product of $(p-1)/q$ q-cycles, and we need to know the number $r = r(p, q)$ of Sylow p-normalizers N_ν that contains a particular element x of this shape $q^{(p-1)/q}$.

The total number of elements in A_p that have the same cycle-structure as x is $p!/s(p, q)$, where $s(p, q) = q^{(p-1)/q}\big((p-1)/q\big)!$. Of these, $p(q-1)$ lie in each of the $(p-2)!$ Sylow p-normalizers N_ν. This establishes the relation

$$p(q-1)(p-2)! = r(p, q)\cdot p!/s(p, q) , \tag{4.1}$$

from which the value of $r(p, q)$ is determined. It is easily checked that for fixed p, $r(p, q)$ is maximal when q is the smallest prime divisor of $\frac{1}{2}(p-1)$.

THEOREM 4.2. *If p is a good prime, then A_p has spread $t_p - 1$, where*

$$t_p = (p-1)!/\big(s(p, q)(q-1)\big) ,$$

and q is the smallest prime divisor of $\frac{1}{2}(q-1)$.

Proof. We use the same sort of argument as was used in [2] for the case $p = 19$. Let $t_p - 1$ non-trivial elements x_i be given. We shall

https://doi.org/10.1017/S0004972700006389 Published online by Cambridge University Press

find a common mate y for them, and indeed y will be a p-cycle. For any x_i that lies in no normalizer N_ν, there is considerable freedom. In fact $\langle x_i, y\rangle$ is insoluble and transitive in such a case, whatever p-cycle y is chosen to be; and thus $\langle x_i, y\rangle = A_p$ since p is a good prime. For the other elements x_i the reasoning is more delicate. If x_i is a p-cycle it lies in just one p-normalizer. If x_i has type $l \times \ldots \times l$, where l is a prime divisor of $\frac{1}{2}(p-1)$, then x_i lies in $r(p, l)$ normalizers N_ν. For fixed p, the largest value of $r(p, l)$ is taken when $l = q$, the smallest prime divisor of $\frac{1}{2}(p-1)$. By (4.1), the number of N_ν involved does not exceed

$$r(p, q)(t_p - 1) < r(p, q)t_p = \frac{p(q-1)(p-2)!s(p,q)}{p!} \frac{(p-1)!}{s(p,q)(q-1)} = (p-2)! .$$

Hence there is a p-cycle left over to play the role of y.

COROLLARY 4.3. *If there are infinitely many good primes, then the alternating groups of prime degree have unbounded spread.*

In the opposite direction, we have the following result:

THEOREM 4.4. *If $p > 5$, then A_p does not have spread $t_p + 3$.*

Proof. As above, let q be the smallest prime factor of $\frac{1}{2}(p-1)$; let z_i be a collection of t_p elements of type $q \times q \times \ldots \times q$ (that is, $(p-1)/q$ q-cycles), chosen so that each one lies in exactly $r(p, q)$ normalizers N_ν, and so every normalizer N_ν contains one of the z_i.

Further, set

$$z_{t_p+1} = (1, 2)(3, 4) , \quad z_{t_p+2} = (1, 4)(2, 3) , \quad z_{t_p+3} = (1, 3)(2, 4) .$$

If y mates z_{t_p+1}, z_{t_p+2} and z_{t_p+3}, then y is a p-cycle. But then one of the groups $\langle z_i, y\rangle$ is soluble $(i \in \{1, \ldots, t_p\})$, and so is not A_p.

It is quite possible that A_p has spread as much as $t_p + 2$ for good

https://doi.org/10.1017/S0004972700006389 Published online by Cambridge University Press

primes p , but this seems to be a very difficult result to establish.

References

[1] Г.Я. Бинбер [G.Ya. Binder], "О вдожении элементов знакопеременной группы четной степени в двухэлементный базис" [The inclusion of the elements of the alternating group of even degree in a two-element basis], *Izv. Vyšš. Učebn. Zaved. Mat.* **1973**, No. 8 (135), 15-18.

[2] J.L. Brenner and James Wiegold, "Two-generator groups, I", *Michigan Math. J.* **22** (1975), 53-64.

[3] H.S.M. Coxeter and W.O.J. Moser, *Generators and relations for discrete groups* (Ergebnisse der Mathematik und ihrer Grenzgebiete, **14**. Springer-Verlag, Berlin, Göttingen, Heidelberg, 1957).

[4] Ulrich Langer, "Erzeugende endlicher linearer Gruppen" (Dissertation, Universität Hamburg, Hamburg, 1977).

[5] Peter M. Neumann, "Transitive permutation groups of prime degree, II: a problem of Noboru Ito", *Bull. London Math. Soc.* **4** (1972), 337-339.

[6] Abraham Sinkov, "Necessary and sufficient conditions for generating certain simple groups by two operators of periods two and three", *Amer. J. Math.* **59** (1937), 67-76.

[7] Alan Williamson, "On primitive permutation groups containing a cycle", *Math. Z.* **130** (1973), 159-162.

10 Phillips Road,
Palo Alto,
California 94303,
USA;

Department of Mathematics,
University College,
Cardiff CF1 1XL,
Wales.