TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 303, Number 2, October 1987

SQUARES OF CONJUGACY CLASSES IN THE INFINITE SYMMETRIC GROUPS

MANFRED DROSTE

ABSTRACT. Using combinatorial methods, we will examine squares of conjugacy classes in the symmetric groups S_ν of all permutations of an infinite set of cardinality $\aleph_\nu$. For arbitrary permutations $p \in S_\nu$, we will characterize when each element $s \in S_\nu$ with finite support can be written as a product of two conjugates of p, and if p has infinitely many fixed points, we determine when all elements of S_ν are products of two conjugates of p. Classical group-theoretical theorems are obtained from similar results.

1. Introduction. We will deal with the symmetric group S_ν of all permutations of an infinite set of cardinality $\aleph_\nu$. The normal subgroups of S_ν are known since 1933 from Schreier and Ulam [**25**] in the countable case (i.e. for $\nu = 0$) and from Baer [**3**] in the general case. They form a well-ordered chain

$$\{1\} \subseteq A_\nu \subseteq S_\nu^0 \subseteq S_\nu^1 \subseteq \cdots \subseteq S_\nu^\nu \subseteq S_\nu^{\nu+1} = S_\nu,$$

where S_ν^τ is the group of all elements of S_ν moving less than $\aleph_\tau$ symbols ($0 \leq \tau \leq \nu + 1$) and A_ν is the infinite alternating group in S_ν^0. The result that the factor groups $H_\nu^\tau = S_\nu^{\tau+1}/S_\nu^\tau$ ($0 \leq \tau \leq \nu$) are simple has recently been sharpened in two directions.

First, Moran [**21**, **22**] and Arad, Chillag and Moran [**1**] have shown that for any non-unit conjugacy class C in H_ν^τ ($0 \leq \tau \leq \nu$), in fact $H_\nu^\tau = C^2$ if $\nu > 0$, and $H_\nu^\tau = C^3$ if $\nu = 0$. Secondly, Droste and Göbel [**13**] (and Bertram [**5**] if $\nu = 0$) showed that whenever $p \in S_\nu$ satisfies $|p| = \aleph_\tau$, then each element of $S_\nu^{\tau+1}$ is a product of four conjugates of p, i.e. $S_\nu^{\tau+1} = [p]^4$; here $|p|$ denotes the cardinality of the support of p and $[p]$ is the conjugacy class of p in S_ν. Indeed, here we even have $S_\nu^{\tau+1} = [p]^3$ if $\tau < \nu$ or if $\tau = \nu$ and p is not a fixed-point-free involution, see [**11**].

It is the aim of this paper to study which conjugacy classes C in the groups $S_\nu^{\tau+1}$ satisfy $S_\nu^{\tau+1} = C^2$. In the literature, several authors [**6**, **17**, **20**] have already proposed this problem for $\tau = \nu$, and various conjugacy classes C in S_ν have been found satisfying $S_\nu = C^2$, cf. [**4–6**, **10–14**, **17**, **19**, **23**]. Here, we first wish to characterize when C^2 contains S_ν^0, the group of all permutations with finite support. Because of work done in [**10**], we can assume that no $p \in C$ has an infinite orbit. Let us call $(k, l, m) \in \mathbf{N}^3$ an *additive triple*, if $k + l = m$. For $p \in S_\nu$ let $S_\infty(p) = \{n \in \mathbf{N};\ p \text{ has infinitely many orbits of length (cardinality) } n\}$. Using

Received by the editors September 26, 1986.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 20B30; Secondary 20E32.
Key words and phrases. Infinite symmetric groups, finite symmetric groups, permutations, conjugacy classes, orbits, fixed points.

covering results of Boccara [7] and Dvir [16] for finite symmetric groups, we will show

THEOREM 1. *Let $p \in S_\nu$ have no infinite orbit. Then the following are equivalent:*

(1) $S_\nu^0 \subseteq [p]^2$.

(2) $(S_\infty(p))^3$ *contains an additive triple.*

In fact, here condition (2) is also equivalent to the statement that $[p]^2$ contains a transposition; this was observed by G. Moran. Hence, if $[p]^2$ contains a transposition, then it contains every permutation of the underlying set with finite support. Using Theorem 1 as well as results of Moran [21] and of [10, 11], we can now characterize when $S_\nu = [p]^2$, provided the permutation $p \in S_\nu$ has infinitely many fixed points.

THEOREM 2. *Let $p \in S_\nu$ have infinitely many fixed points. Then $S_\nu = [p]^2$ if and only if $|p| = \aleph_\nu$ and at least one of the following two conditions holds:*

(1) *p has an infinite orbit.*

(2) *$(S_\infty(p))^3$ contains an additive triple, and, if $\nu = 0$, p has also infinitely many finite orbits of length ≥ 3.*

We will also give a simple characterization of when a permutation $p \in S_\nu$ ($\nu > 0$) with at least one infinite orbit satisfies $S_\nu = [p]^2$, see Theorem 5.2. These results generalize various theorems of the literature, cf. Bertram [4, 5], Boccara [6], Droste and Göbel [13, 14], Gray [17], Moran [19], and [10, 11]. As a consequence, we will obtain for each $0 \leq \tau < \nu$ a complete characterization of all conjugacy classes C in $S_\nu^{\tau+1}$ with $S_\nu^{\tau+1} = C^2$:

COROLLARY 3. *Let $0 \leq \tau < \nu$, and let $p \in S_\nu$. Then the following are equivalent:*

(1) $S_\nu^{\tau+1} = [p]^2$.

(2) $|p| = \aleph_\tau$ *and* $[p]^2$ *contains a transposition.*

(3) $|p| = \aleph_\tau$ *and either p has an infinite orbit or $(S_\infty(p))^3$ contains an additive triple.*

We just note here that if $\tau = 0$ or if τ is a limit-ordinal with $0 < \tau \leq \nu$, clearly there is *no* conjugacy class C in S_ν^τ with $S_\nu^\tau = C^2$, and the same applies to the group A_ν.

The proof of Theorem 1 is contained in §3. We prove Theorem 2 in the countable case in §4 and derive from this the uncountable case and Corollary 3 in §5; this section also contains further related group-theoretical results.

2. Notation and remarks. Let $\dot{\bigcup} A_i$ denote a *disjoint* union; $\mathbf{N} = \{1, 2, \dots\}$, the set of all positive integers, and $\mathbf{N}_\infty = \mathbf{N} \dot{\cup} \{\aleph_0\}$. For any group G we let $[g] = \{x^{-1} \cdot g \cdot x; x \in G\}$, the conjugacy class of $g \in G$, and $A \cdot B = \{a \cdot b; a \in A, b \in B\}$ for subsets $A, B \subseteq G$. Mappings operate from the right on elements; so the composition of mappings is from left to right.

S_M denotes the symmetric group of all permutations of a set M, $A_M \subseteq S_M$ the alternating group if M is finite, and id_M (or id, if there is no ambiguity) the identity permutation of M. Now let $p \in S_M$. Then $D(p) = M$, the domain of p. An orbit of p is a minimal p-invariant subset of M. The length of an orbit is its

cardinality, and an orbit is nontrivial if it has length ≥ 2. The type of $p \in S_M$ is the function $\bar{p}$ from $\mathbf{N}_\infty$ into $\{c; 0 \leq c \leq |M|\}$ defined by

$$\bar{p}(n) = |\{X; X \text{ orbit of } p \text{ of length } n\}| \qquad (n \in \mathbf{N}_\infty).$$

Hence $\bar{p}(1)$ is the cardinality of the set of all fixed points of p. The support of p is the set $\{x \in M; x^p \neq x\}$; its cardinality will be denoted by $|p|$. Hence $|p| = \sum_{n\geq 2} n \cdot \bar{p}(n)$. The following fact is well known (e.g. [**26**, 11.3.1]) and will be used throughout this paper without mentioning it again:

Whenever $p, q \in S_M$, then $[p] = [q]$ if and only if $\bar{p} = \bar{q}$. In particular, p^{-1} is conjugate to p, and hence $\mathrm{id}_M = p \cdot p^{-1} \in [p]^2$ for any permutation $p \in S_M$.

If $M = \dot{\bigcup}_{i\in I} M_i$ is a partition, $p_i \in S_{M_i}$ and $p \in S_M$ satisfy $p|_{M_i} = p_i$ $(i \in I)$, then we also write $p = \bigoplus_{i\in I} p_i$. Clearly, in this case $\bar{p}(n) = \sum_{i\in I} \overline{p_i}(n)$, and if also $q_i \in S_{M_i}$ $(i \in I)$ and $q = \bigoplus_{i\in I} q_i$, then $p \cdot q = \bigoplus_{i\in I}(p_i \cdot q_i)$.

3. Proof of Theorem 1. This section is devoted to the proof of Theorem 1. We will also derive a necessary condition for permutations $p \in S_\nu$ to satisfy $A_\nu \subseteq [p]^2$. One of the main tools for the proofs of this paper is the *splitting-argument-technique* which may be best described by an example. Let $s, p \in S_0$ and suppose we wish to show that s is a product of two conjugates of p. Assume that it is possible to decompose $s = s_1 \oplus s_2$ and $p = p_1 \oplus p_2$ such that the domains of s_1, s_2, p_1, p_2 are all infinite. Now if, for $i = 1, 2$, we can find permutations q_i, r_i of the domain $D(s_i)$ of s_i such that $s_i = q_i \cdot r_i$ and $\overline{q_i} = \overline{r_i} = \overline{p_i}$, then $q = q_1 \oplus q_2$ and $r = r_1 \oplus r_2 \in S_0$ satisfy $\bar{q} = \bar{r} = \bar{p}$, hence are conjugate to p, and $s = s_1 \oplus s_2 = (q_1 \cdot r_1) \oplus (q_2 \cdot r_2) = q \cdot r \in [p]^2$, establishing our goal. Now we give the formal statement of the technique which is only a bit more general than the above example.

(3.0) THE SPLITTING-ARGUMENT-TECHNIQUE. *Let M, M_i be sets and $s_i, q_i, r_i \in S_{M_i}$ such that $s_i \in [q_i] \cdot [r_i]$ in S_{M_i} for each $i \in I$. Let $s, q, r \in S_M$ satisfy $\bar{s}(n) = \sum_{i\in I} \overline{s_i}(n)$, $\bar{q}(n) = \sum_{i\in I} \overline{q_i}(n)$, $\bar{r}(n) = \sum_{i\in I} \overline{r_i}(n)$ for each $n \in \mathbf{N}_\infty$. Then $s \in [q] \cdot [r]$ in S_M.*

A proof of this result is contained, for instance, in [**11**]. Now we turn to the proof of Theorem 1. Let M be a fixed finite set with $|M| = n \in \mathbf{N}$ and $n \geq 3$. Our argument for Theorem 1 rests on results of Boccara [**7**] and Dvir [**16**] characterizing when a cycle in S_M is a product of two elements of S_M belonging to prescribed conjugacy classes. We follow mainly the version of Dvir [**16**].

If $q \in S_M$, let $c(q)$ denote the number of orbits of q. For each $3 \leq i \leq n$ let C_i denote the conjugacy class of all cycles of length i in S_M, i.e. of all $s \in S_M$ such that $\bar{s}(i) = 1$ and $\bar{s}(j) = 0$ if $j \neq 1, i$. Now let $q, r \in S_M$ and $T = (q, r)$. We put $r(T) = 2n + 1 - c(q) - c(r)$ and let $i(T) = \min\{i; 3 \leq i \leq n, C_i \subseteq [q] \cdot [r]\}$ provided such i exists. Then we have

LEMMA 3.1 (DVIR [**16**, THEOREM 6.1]). *Let $q, r \in S_M$, $T = (q, r)$, and $3 \leq l \leq n$. Assume that $i(T)$ exists. Then $C_l \subseteq [q] \cdot [r]$ if and only if $i(T) \leq l \leq r(T)$ and $l \equiv i(T) \bmod 2$.*

Note that if $q \in S_M$ is neither the identity nor a fixed-point-free involution and if $T = (q, q)$, then $i(T) = 3$, as follows from Boccara [**7**, Théorème 4.3] or from the

identities

$$(1\ 2\ 3) = (1\ 2)(3) \cdot (1\ 3)(2),$$
$$(1\ 2\ 3) = (1\ 3\ 2) \cdot (3\ 2\ 1),$$
$$(1\ 2\ 3)(4) \cdots (k) = (1\ 3\ 2\ 4\ 5 \cdots k) \cdot (k \cdots 4\ 3\ 2\ 1) \quad \text{if } 4 \leq k \leq n.$$

Therefore the following result is immediate by Lemma 3.1 (or by Boccara [**7**, 4.3, 4.12]).

LEMMA 3.2. *Let $3 \leq n \in \mathbf{N}$, $|M| = n$, and $s \in A_M$ such that s has precisely one nontrivial orbit. Let $p \in S_M$ have only orbits of length ≥ 3. Then $s \in [p]^2$.*

Next we show

LEMMA 3.3. *Let $(k,l,m) \in \mathbf{N}^3$ be an additive triple, $n = j \cdot m$ for some $j \in \mathbf{N}$, and $|M| = n$. Let $s \in S_M \backslash A_M$ have precisely one nontrivial orbit. Then there are $q, r \in S_M$ such that $s = q \cdot r$ and the following two conditions hold:*

(i) $\bar{q}(m) = j$, *i.e. q has only orbits of length m.*

(ii) $\bar{r}(m) = j - 1$, $\bar{r}(k) = \bar{r}(l) = 1$ *if $k \neq l$, and $\bar{r}(k) = 2$ if $k = l$, i.e. r has $j - 1$ orbits of length m, one orbit of length k, and another one of length l.*

PROOF. If s is a transposition, the result is clear by the identity

$$(1 \quad k+1) = (m \quad m-1 \quad \cdots \quad 2\ 1) \cdot (1 \quad 2 \quad \cdots \quad k)(k+1 \quad k+2 \quad \cdots \quad m).$$

Hence let now the nontrivial orbit of s have length ≥ 4. By Lemma 3.1 it suffices to prove the result for the case that the nontrivial orbit of s has length precisely 4. This follows from the subsequent identities where we assume without loss of generality that j is minimal with respect to $n = j \cdot m \geq 4$.

Triple $(1,1,2)$: $(1\ 2\ 3\ 4) = (1\ 2)(3\ 4) \cdot (1\ 3)(2)(4)$.

Triple $(1,2,3)$: $(1\ 2\ 3\ 4) = (1\ 2\ 5)(6\ 4\ 3) \cdot (1\ 5\ 3)(4\ 6)(2)$.

Triple $(2,2,4)$: $(1\ 2\ 3\ 4) = (4\ 3\ 2\ 1) \cdot (1\ 3)(2\ 4)$.

Triple $(k,l,k+l)$ with $k,l \in \mathbf{N}$, $l \geq 3$:

$$(k+1 \quad 1 \quad k+2 \quad k+3) = (k+l \quad k+l-1 \quad \cdots \quad 3 \quad 2 \quad 1) \cdot (1 \quad 2 \quad 3 \quad \cdots \quad k)(k+1 \quad k+3 \quad k+4 \quad \cdots \quad k+l \quad k+2).$$

We will also need the following result communicated to us by G. Moran.

PROPOSITION 3.4. *Let $p \in S_\nu$ have no infinite orbit. Then $[p]^2$ contains a transposition if and only if $(S_\infty(p))^3$ contains an additive triple.*

PROOF. It rests on the well-known observation that if $s \in S_\nu^0$ is a transposition and $r \in S_\nu$ is any permutation, then the orbits of $q = s \cdot r$ and r differ only in that either one orbit of r is the union of two distinct orbits of q, or vice versa. Hence, if $[p]^2$ contains a transposition, then $(S_\infty(p))^3$ contains an additive triple. The converse is immediate by the first identity given in the proof of Lemma 3.3, and a splitting-argument.

Now we can give the

PROOF OF THEOREM 1. (1) $\rightarrow$ (2). Immediate by Proposition 3.4.

(2) $\rightarrow$ (1). By an easy splitting-argument, it suffices to show that $s \in [p]^2$ for each $s \in S_\nu^0$ which has precisely one nontrivial orbit. Since any permutation is a

product of two involutions, we can also assume that $\bar{p}(m) = \aleph_0$ for some $m \geq 3$. Now the result follows from Lemmas 3.2 and 3.3.

Next we give a necessary condition for a permutation $p \in S_\nu$ such that $[p]^2$ contains the infinite alternating group A_ν; recall that A_ν is the group of all elements of S_ν^0 which, if restricted to their support, are even. This result partially generalizes Moran [**19**, Corollary 2.5].

THEOREM 3.5. *Let $p \in S_\nu$ satisfy $A_\nu \subseteq [p]^2$. Then at least one of the following three conditions holds*:

(1) *p has at least one infinite orbit.*

(2) *p has infinitely many fixed points and infinitely many orbits of length 2.*

(3) *p has infinitely many finite orbits of length ≥ 3.*

PROOF. Assume that $A_\nu \subseteq [p]^2$ but neither of conditions (1)–(3) holds. Thus p has no infinite orbit, only finitely many orbits of length $\neq 2$, and infinitely many orbits of length 2. Choose $s \in A_\nu$ such that all the nontrivial orbits of s have different lengths and s has more than $2 \cdot \sum_{n \neq 2} n \cdot \bar{p}(n)$ nontrivial orbits. We claim $s \notin [p]^2$.

Assume that $s = q \cdot r$ for some conjugates q, r of p. There is a nontrivial orbit T of s such that each $t \in T$ belongs to some orbit of length 2 of q and to some orbit of length 2 of r. Let $Q(R)$ be the set of all orbits of length 2 of $q(r)$, respectively. We may assume $T \subset \mathbf{Z}$. Suppose first that $i^q \in T$ for some $i \in T$. Let $j = i^q$ and assume without loss of generality $i < j$. Hence $s|_T$ is a cyclic permutation of T of the form

$$s|_T = (\cdots \quad i \quad i+1 \quad \cdots \quad j-1 \quad j \quad \cdots).$$

Since $\{i, j\} \in Q$, we get $j^r = i+1$ and $\{i+1, j\} \in R$. Thus $(j-1)^q = i+1$, and so $\{i+1, j-1\} \in Q$. By induction, $\{i+k, j-k\} \in Q$ for each $k \in \mathbf{N}$ with $i+k < j-k$, and $\{i+1+k, j-k\} \in R$ for each $k \in \mathbf{N}$ with $i+1+k < j-k$. It follows that for some $m \in T$ with $i \leq m \leq j$, either $m^q = m$ or $m^r = m$, a contradiction.

Now assume that $i^q \in T^*$ for some $i \in T$ and some orbit $T^* \neq T$ of s. We may assume that $T = \{1, \ldots, j\}$, $T^* = \{1^*, \ldots, j^*\}$,

$$s|_{T \cup T^*} = (1 \quad 2 \quad \cdots \quad j)(1^* \quad \cdots \quad j^*), \quad \text{and} \quad 1^q = 1^*.$$

Then $\{1, 1^*\} \in Q$, thus $1^{*r} = 2$ and $1^r = 2^*$. Hence $\{1^*, 2\}, \{1, 2^*\} \in R$ and so $j^{*q} = 2$, $j^q = 2^*$. Thus $\{2, j^*\}, \{2^*, j\} \in Q$. Now $j^{*r} = 3$, so $\{3, j^*\} \in R$ and thus $(j-1)^{*q} = 3$, $\{3, (j-1)^*\} \in Q$. Hence $\{2, j^*\}, \{3, (j-1)^*\}, \ldots, \{j, 2^*\} \in Q$, which implies $j = j^*$, a contradiction.

By Bertram [**4**, Theorem 2.1] (cf. the subsequent Lemma 4.8), condition (1) of Theorem 3.5 is also sufficient to imply that $A_\nu \subseteq [p]^2$. The same applies to condition (2) by Moran [**19**, Corollary 2.4] (cf. Lemma 4.7). However, this is not true for condition (3). For, if $s \in A_0$ has only one orbit of length 2 and one orbit of length 4 (and no others) and if $p \in S_0$ has only orbits of length 3, then $s \notin [p]^2$, as can be easily checked; this example was communicated to us by G. Moran.

Finally, we note that if $\nu = 0$ and $[p]^2$ contains a permutation s which has only one (infinite) orbit, then again p satisfies condition (3.5)(3), as shown in [**11**, Theorem 4.1].

4. Proof of Theorem 2 (the countable case). In this section we wish to prove Theorem 2 in the countable case, i.e. for $\nu = 0$. We will also derive from it a few consequences on squares C^2 of conjugacy classes C in S_0. Since Theorem 1 characterizes when C^2 contains S_0^0, here we first derive a sufficient condition for permutations $p \in S_0$ such that $[p]^2$ contains all elements s of S_0 with infinite support. In [**10**] we characterized the sets $[p]^2$ if $p \in S_0$ has at least one infinite orbit; so here we can assume that p has infinite support, but $\bar{p}(\aleph_0) = 0$. Then, of course, p has infinitely many nontrivial finite orbits. Let us first consider the case that $s \in S_0$ has also no infinite orbit. Our main tool for this case will be the following recent result of G. Moran.

LEMMA 4.1 (MORAN [**21**, PROPOSITION 5.1, THEOREM 3]). *Let $s, q, r \in S_0$ each have infinite support but no infinite orbit such that s and q have no fixed points, r has precisely one fixed point, and all nontrivial orbits of q and r have length at least 4. Then $s \in [q] \cdot [r]$.*

It is clear by an easy splitting-argument that the assumptions on the fixed points of q, r in Lemma 4.1 can be weakened to the effect that either q or r has at least one fixed point. This will be used in the following without mentioning it again. Next we show

LEMMA 4.2. *Let $s, p \in S_0$ have infinite support but no infinite orbit such that p has infinitely many fixed points and infinitely many orbits of length ≥ 4. Then $s \in [p]^2$.*

PROOF. Clearly s has infinitely many nontrivial finite orbits. We distinguish between three cases.

Case 1. Assume that s has infinitely many orbits of length 2.

Split $s = s_1 \oplus s_2$ such that $|D(s_1)| = 4 \cdot (\bar{p}(2) + \bar{p}(3))$, s_1 has only orbits of length 2, and $D(s_2)$ is infinite. The following formulas,

$$(1\ 2)(3\ 4) = (1\ 2)(3)(4) \cdot (1)(2)(3\ 4),$$
$$(1\ 2)(3\ 4) = (1\ 2\ 3)(4) \cdot (1\ 4\ 3)(2),$$

show that there are permutations q_1, r_1 of $D(s_1)$ such that $s_1 = q_1 \cdot r_1$, $\overline{q_1}(i) = \overline{r_1}(i) = 0$ for each $i \geq 4$, and $\overline{q_1}(i) = \overline{r_1}(i) = \bar{p}(i)$ for $i = 2, 3$. By Lemma 4.1, there are permutations q_2, r_2 of $D(s_2)$ such that $s_2 = q_2 \cdot r_2$, $\overline{q_2}(i) = \overline{r_2}(i) = \bar{p}(i)$ for each $i \neq 2, 3$, and $\overline{q_2}(i) = \overline{r_2}(i) = 0$ for $i = 2, 3$. Hence $q = q_1 \oplus q_2$, $r = r_1 \oplus r_2 \in S_0$ are conjugate to p and thus $s = q \cdot r \in [p]^2$.

Case 2. Assume that s has infinitely many orbits of length 3.

Here we proceed completely analogously to Case 1. Only split $s = s_1 \oplus s_2$ such that $|D(s_1)| = 3 \cdot (\bar{p}(2) + \bar{p}(3))$, s_1 has only orbits of length 3, and $D(s_2)$ is infinite. Then use the formulas

$$(1\ 2\ 3) = (1\ 2)(3) \cdot (1\ 3)(2),$$
$$(1\ 2\ 3) = (1\ 3\ 2) \cdot (1\ 3\ 2),$$

to obtain the required number of orbits of lengths 2 or 3 of p. Again $s \in [p]^2$ follows by Lemma 4.1.

Case 3. Assume that s has infinitely many orbits of length ≥ 4.

We split $s = s_1 \oplus s_2 \oplus s_3$ such that s_1, s_2, s_3 each have infinite support and s_1 contains all orbits of s of length at most 3. Hence s_2, s_3 each have infinitely many

orbits of length ≥ 4, but no orbits of length ≤ 3. Next split $p = p_1 \oplus p_2 \oplus p_3$ such that p_1, p_2, p_3 each contain infinitely many orbits of length ≥ 4 of p, and p_1 has infinitely many fixed points, but no orbits of length 2 or 3.

By Lemma 4.1, there are permutations q_1, r_1 of $D(s_1)$ such that $s_1 = q_1 \cdot r_1$ and $\overline{q_1} = \overline{r_1} = \overline{p_1}$. Again by Lemma 4.1, we can find permutations q_2, r_2 of $D(s_2)$ such that $q_2 = s_2 \cdot r_2^{-1}$, $\overline{q_2}(i) = \bar{p}(i)$ and $r_2(i) = 0$ for $i = 2, 3$, and $\overline{q_2}(i) = \overline{r_2}(i) = \overline{p_2}(i)$ for each $i \geq 4$. Similarly, there are permutations q_3, r_3 of $D(s_3)$ such that $r_3 = q_3^{-1} \cdot s_3$, $\overline{r_3}(i) = \bar{p}(i)$ and $\overline{q_3}(i) = 0$ for $i = 2, 3$, and $\overline{q_3}(i) = \overline{r_3}(i) = \overline{p_3}(i)$ for each $i \geq 4$.

Now let $q = q_1 \oplus q_2 \oplus q_3$ and $r = r_1 \oplus r_2 \oplus r_3$. Then $q, r \in S_0$, $\bar{q} = \bar{r} = \bar{p}$, and $s = q \cdot r \in [p]^2$. The result follows.

Next we deal with permutations $s \in S_0$ having at least one infinite orbit. Here our considerations rest on the following result proved in [**11**].

LEMMA 4.3 [**11**, PROOF OF LEMMA 4.2]. *Let $p_1, p_2 \in S_0$ each have infinitely many nontrivial finite, but no infinite orbits such that*

$$\overline{p_1}(1) = \sum_{n \geq 3} (n-2) \cdot \overline{p_2}(n) \quad \text{and} \quad \overline{p_2}(1) = 1 + \sum_{n \geq 3} (n-2) \cdot \overline{p_1}(n).$$

Let $\{P_i; i \in \mathbf{N}\}$ ($\{P^i; i \in \mathbf{N}\}$) be an enumeration of the set of all nontrivial orbits of p_1 (p_2), respectively, and let $s \in S_0$ have precisely one (infinite) orbit.

Then there are permutations $q \in [p_1]$, $r \in [p_2]$ whose nontrivial orbits can be enumerated as $\{Q_i; i \in \mathbf{N}\}$, $\{R_i; i \in \mathbf{N}\}$, respectively, such that $s = q \cdot r$ and $|Q_i| = |P_i|$, $|R_i| = |P^i|$, and $Q_i \cap R_i \neq \emptyset$ for each $i \in \mathbf{N}$.

We use Lemma 4.3 to show

LEMMA 4.4. *Let $p_1, p_2 \in S_0$ each have no infinite orbit, but infinitely many fixed points and infinitely many orbits of length ≥ 4. Let $s \in S_0$ have at least one infinite orbit. Then $s \in [p_1] \cdot [p_2]$.*

PROOF. By a usual splitting-argument, it suffices to consider the case that s has precisely one infinite orbit. Because of Lemma 4.3, we can also assume that s has at least one finite orbit. We first consider the case that s has precisely one finite orbit and then later show how to deal with the general case.

So let U denote the infinite and V the finite orbit of s. Let $k = |V| \in \mathbf{N}$; we may assume that $V = \{1, 2, \ldots, k\}$ and $s|_V = (1 \quad 2 \quad \cdots \quad k)$. Put $r = k/2$ if k is even, and $r = (k+1)/2$ if k is odd. Next let $\{P_i; i \in \mathbf{N}\}$ ($\{P^i; i \in \mathbf{N}\}$) be an enumeration of the set of all nontrivial orbits of p_1 (p_2), respectively, such that the set $I = \{i \in \mathbf{N}; |P_i| \geq 4, |P^i| \geq 4\}$ is infinite. Choose a subset $I^* \subseteq I$ with $|I^*| = r$ and here, in the present case, put $K = I^*$. Enumerate $I^* = \{1^*, 2^*, \ldots, r^*\}$.

Now by Lemma 4.3 there are permutations q, r of U each having infinitely many fixed points such that $s|_U = q \cdot r$ and the nontrivial orbits of q (r) can be enumerated as $\{Q_i; i \in \mathbf{N}\}$ ($\{R_i; i \in \mathbf{N}\}$), respectively, such that the following five conditions hold:

(1) $|Q_i| = |P_i|$ and $|R_i| = |P^i|$ for each $i \in \mathbf{N} \backslash K$;

(2) $|Q_i| = |P_i| - 2$ for each $i \in I^*$, provided that k is even;

(3) $|Q_i| = |P_i| - 2$ if $i \in I^* \backslash \{r^*\}$, and $|Q_i| = |P_i| - 1$ if $i = r^* \in I^*$, provided that k is odd;

(4) $|R_i| = |P^i| - 2$ if $i \in I^* \backslash \{1^*\}$, and $|R_i| = |P^i| - 1$ if $i = 1^* \in I^*$;

(5) $Q_i \cap R_i \neq \emptyset$ for each $i \in \mathbf{N}$.

Note that we have indeed $|Q_i|, |R_i| \geq 2$ for all $i \in \mathbf{N}$ and that $|Q_i|, |R_i| \geq 4$ for infinitely many $i \in \mathbf{N}$, in fact for all $i \in I \backslash K$. For each $i \in I^*$ choose some $b_i \in Q_i \cap R_i$ and let $a_i = b_i{}^{q^{-1}} \in Q_i$, $c_i = b_i{}^r \in R_i$.

Now we define two permutations q^*, r^* of $M = U \dot{\cup} V$ as follows. First put $x^{q^*} = x^q$ ($x^{r^*} = x^r$) whenever either $x \in U$ and x is a fixed point of $q\,(r)$, or $x \in Q_i$ ($x \in R_i$) for some $i \in \mathbf{N} \backslash K$, respectively. Now let $Q^* = \dot{\bigcup}_{i \in I^*} Q_i$ and $R^* = \dot{\bigcup}_{i \in I^*} R_i$. Then we have

$$q|_{Q^*} = (\cdots a_1 \cdot b_1 \cdot \cdots)(\cdots a_2 \cdot b_2 \cdot \cdots) \cdots (\cdots a_r \cdot b_r \cdot \cdots),$$
$$r|_{R^*} = (\cdots b_1 \cdot c_1 \cdot \cdots)(\cdots b_2 \cdot c_2 \cdot \cdots) \cdots (\cdots b_r \cdot c_r \cdot \cdots).$$

Now we distinguish between two cases.

Case 1. Assume that k is even, i.e. $k = 2r$.

We put

$$q^*|_{Q^* \dot{\cup} V} = (\cdots a_1 \cdot \quad 1 \quad 2r \quad b_1 \cdot \cdots)(\cdots a_2 \cdot \quad 2 \quad 2r-1 \quad b_2 \cdot \cdots)$$
$$\cdots (\cdots a_r \cdot \quad r \quad r+1 \quad b_r \cdot \cdots),$$

that is, we let $x^{q^*} = x^q$ if $x \in Q_i \backslash \{a_i\}$ ($i \in I^*$) and $a_j \cdot {}^{q^*} = j$, $j^{q^*} = 2r + 1 - j$, $(2r+1-j)^{q^*} = b_j \cdot$ for each $j \in \{1, \ldots, r\}$.

Similarly, let

$$r^*|_{R^* \dot{\cup} V} = (\cdots b_1 \cdot \quad 1 \quad c_1 \cdot \cdots)(\cdots b_2 \cdot \quad 2r \quad 2 \quad c_2 \cdot \cdots)$$
$$(\cdots b_3 \cdot \quad 2r-1 \quad 3 \quad c_3 \cdot \cdots) \cdots (\cdots b_r \cdot \quad r+2 \quad r \quad c_r \cdot \cdots)(r+1).$$

This includes

$$q^*|_{Q^* \dot{\cup} V} = (\cdots a_1 \cdot \quad 1 \quad 2 \quad b_1 \cdot \cdots)$$

and

$$r^*|_{R^* \dot{\cup} V} = (\cdots b_1 \cdot \quad 1 \quad c_1 \cdot \cdots)(2)$$

if $r = 1$.

It follows that q^*, r^* are permutations of $M = U \dot{\cup} V$ with $x^{q^* \cdot r^*} = x^{q \cdot r} = x^s$ for each $x \in Q^*$, and $x^{q^* \cdot r^*} = x^s$ for each $x \in V$. Therefore we obtain $s = q^* \cdot r^*$, and $\overline{q^*} = \overline{p_1}, \overline{r^*} = \overline{p_2}$ are straightforward. Hence $s \in [p_1] \cdot [p_2]$.

Case 2. Assume that k is odd, i.e. $k = 2r - 1$.

Here we put

$$q^*|_{Q^* \dot{\cup} V} = (\cdots a_1 \cdot \quad 1 \quad 2r-1 \quad b_1 \cdot \cdots)(\cdots a_2 \cdot \quad 2 \quad 2r-2 \quad b_2 \cdot \cdots)$$
$$\cdots (\cdots a_{(r-1)} \cdot \quad r-1 \quad r+1 \quad b_{(r-1)} \cdot \cdots)(\cdots a_r \cdot \quad r \quad b_r \cdot \cdots)$$

and

$$r^*|_{R^* \dot{\cup} V} = (\cdots b_1 \cdot \quad 1 \quad c_1 \cdot \cdots)(\cdots b_2 \cdot \quad 2r-1 \quad 2 \quad c_2 \cdot \cdots)$$
$$(\cdots b_3 \cdot \quad 2r-2 \quad 3 \quad c_3 \cdot \cdots) \cdots (\cdots b_r \cdot \quad r+1 \quad r \quad c_r \cdot \cdots).$$

This includes $q^*|_{Q^* \dot{\cup} V} = (\cdots a_1 \cdot \quad 1 \quad b_1 \cdot \cdots)$ and $r^*|_{R^* \dot{\cup} V} = (\cdots b_1 \cdot \quad 1 \quad c_1 \cdot \cdots)$ if $r = 1$.

Again we have $x^{q^* \cdot r^*} = x^s$ for each $x \in M$, and thus q^*, r^* are permutations of M with $s = q^* \cdot r^*$ and $\overline{q^*} = \overline{p_1}, \overline{r^*} = \overline{p_2}$. Hence $s \in [p_1] \cdot [p_2]$ as claimed.

Finally, let us assume that s has more than one finite orbit. We proceed quite similarly as before. Let $\{V_j; j \in J\}$ be an enumeration of the finite orbits of s. For

each $j \in J$ let $k_j = |V_j|$, and put $r_j = k_j/2$ if k_j is even, and $r_j = (k_j+1)/2$ if k_j is odd. If the set I is defined as before, choose a system $(I_j)_{j\in J}$ of pairwise disjoint subsets of I such that $|I_j| = r_j$ for each $j \in J$ and such that $I\backslash K$ is still infinite, where $K = \dot{\bigcup}_{j\in J} I_j$. Now continue as above, dealing simultaneously with each set I_j $(j \in J)$ as before with I^*. Then the result follows.

As a first consequence of our results, we obtain a sufficient condition for permutations $p \in S_0$ with no infinite orbit such that $[p]^2$ contains all elements of S_0 with infinite support.

THEOREM 4.5. *Let $p \in S_0$ have no infinite orbit, but infinitely many fixed points and infinitely many orbits of length ≥ 4. Then $S_0\backslash S_0^0 \subseteq [p]^2$.*

PROOF. Immediate by Lemmas 4.2 and 4.4.

Now we give an example to show that the assumptions of Theorem 4.5 (and, in fact, of Lemma 4.2) cannot be arbitrarily weakened.

EXAMPLE 4.6. *Let $s, p \in S_0$ such that s is an involution with precisely one fixed point and p has only orbits of length 3. Then $s \notin [p]^2$.*

PROOF. Suppose that $s = q \cdot r$ for some conjugates q, r of p. Let us assume that the underlying set is $\mathbf{N} \cup \{0\}$, s has the following form:

$$s = (0)(1\ 2)(3\ 4)(5\ 6)(7\ 8)\cdots,$$

and $1^q = 0$. Then $0^q \neq 2$, for otherwise we get $2^q = 1$ and 1 must be a fixed point of r, a contradiction. Therefore assume $0^q = 3$ and hence $3^q = 1$. Then $0^r = 1^{q\cdot r} = 1^s = 2$ and, similarly, $3^r = 0$ and $1^r = 4$. Thus $2^r = 3$, which implies $4^q = 2$. We may assume that $5^q = 4$. Then $2^q = 5$, which shows $5^r = 1$ and hence $4^r = 5$. But this implies $6^q = 4$, a final contradiction.

We will also need the following two results from [**10**, **11**] which characterize for two conjugacy classes C in S_0 when $S_0 = C^2$.

LEMMA 4.7 [**11**, THEOREM 2b]. *Let $p \in S_0$ have no infinite orbit, but infinitely many fixed points and infinitely many orbits of length 2.*

(a) *If p has infinitely many orbits of length ≥ 3, then $S_0 = [p]^2$.*

(b) *If p has only finitely many orbits of length ≥ 3, then $[p]^2 = \{s \in S_0;\ s$ has infinitely many orbits$\}$.*

LEMMA 4.8 [**10**, THEOREM 1]. *Let $p \in S_0$ have at least one infinite orbit. If p has either at least two infinite orbits or, for some $n \in \mathbf{N}$, infinitely many finite orbits of length n, then $S_0 = [p]^2$. In the other case, $[p]^2 = (S_0\backslash S_0^0)\,\dot{\cup}\, A_0$.*

Now we can give the

PROOF OF THEOREM 2 IN THE COUNTABLE CASE (I.E. $\nu = 0$). First suppose $S_0 = [p]^2$. Clearly p has infinite support. If condition (1) is violated, by Theorem 1 there exists an additive triple (k, l, m) in $(S_\infty(p))^3$. If $m \geq 3$, condition (2) of Theorem 2 is immediate, and if $m = 2$, it follows from Lemma 4.7(b).

Conversely, assume that condition (1) or (2) holds. In the first case, we get $S_0 = [p]^2$ by Lemma 4.8. Secondly, let p have no infinite orbit, but let (k, l, m) be an additive triple in $(S_\infty(p))^3$. Then we obtain $S_0 = [p]^2$ by Lemma 4.7(a) if $m \leq 3$, and by Theorem 1 and Theorem 4.5 if $m \geq 4$.

It remains open whether condition (2) of Theorem 2 is also sufficient to imply that $S_0 = [p]^2$ if $p \in S_0$ is assumed to have only a finite number of fixed points. The assertions of Theorem 2 in the uncountable case will be proved in §5. As a consequence of Theorems 1 and 2 we now show that if $p \in S_0$ has infinitely many fixed points and $[p]^2$ contains both a transposition and some $s \in S_0$ with only finitely many orbits (and hence at least one infinite orbit), then $S_0 = [p]^2$.

COROLLARY 4.9. *Let $p \in S_0$ have infinitely many fixed points such that $[p]^2$ contains a transposition. Then either $[p]^2 = \{s \in S_0;\ s$ has infinitely many orbits$\}$ or $S_0 = [p]^2$.*

PROOF. If p has an infinite orbit, the result is clear by Lemma 4.8. If p has no infinite orbit, $(S_\infty(p))^3$ contains an additive triple by Theorem 1. Now the result is immediate by Theorem 2 and Lemma 4.7.

Finally we wish to sharpen Theorem 4.5 and show, in view of the result of Lemma 4.8, that there are also many conjugacy classes $[p]$ in S_0 where p has no infinite orbit, but $[p]^2$ contains precisely all elements of S_0 which either have infinite support of have finite support and are even. The following result from the corresponding theory for finite symmetric groups has found various generalizations, cf. [**7**, **16**] and the references mentioned there.

LEMMA 4.10 (GLEASON [**18**, PROPOSITION 4, p. 172]). *Let M be a finite set with $|M| \geq 5$, and let $p \in S_M$ have only one orbit (which is, hence, of length $|M|$). Then $A_M = [p]^2$ in S_M.*

Now we can show

COROLLARY 4.11. *Let $p \in S_0$ have infinitely many fixed points and finite orbits of arbitrarily large lengths. Then $(S_0 \backslash S_0^0) \cup A_0 \subseteq [p]^2$, and equality holds if and only if p has no infinite orbit and, for each $n \in \mathbf{N}$, only finitely many orbits of length $2n$.*

PROOF. If p has an infinite orbit, we have $S_0 = [p]^2$ by Lemma 4.8. Hence let us assume now that $\bar{p}(\aleph_0) = 0$. By Theorem 4.5 we have $S_0 \backslash S_0^0 \subseteq [p]^2$, and $A_0 \subseteq [p]^2$ follows by a splitting-argument from Lemma 4.10. The final statement of the corollary is now immediate by Moran [**20**, Theorem 3] which characterizes when a permutation $p \in S_0$ satisfies $[p]^2 \cap S_0^0 \subseteq A_0$.

5. From the countable to the uncountable. In this section we will prove Theorem 2 in the uncountable case and Corollary 3. We will also obtain a simple characterization of when a permutation $p \in S_\nu$ $(\nu > 0)$ with at least one infinite orbit satisfies $S_\nu = [p]^2$, using the result contained in Lemma 4.8 for the countable case.

Let us start with a few preliminary remarks. Recall that $S_\nu^\tau = \{s \in S_\nu; |s| < \aleph_\tau\}$ $(0 \leq \tau \leq \nu + 1)$. First note that any two permutations $q, r \in S_\nu^\tau$ are conjugate in S_ν^τ if and only if they are conjugate in S_ν. Next, if $s, p \in S_\nu$ and $s \in [p]^2$, then clearly $|s| \leq 2 \cdot |p|$. This shows that if $\tau = 0$ or if τ is a limit-ordinal, there is *no* conjugacy class C in S_ν^τ with $S_\nu^\tau = C^2$. Also, it is easy to see that if $p \in S_\nu$ has infinite support, then $[p]^2$ contains some permutation $s \in S_\nu$ with $|s| = |p|$ (in fact, by [**10**, Lemma 4.9] and a splitting-argument $[p]^2$ contains each permutation $s \in S_\nu$ which has $|p|$ orbits of length $\aleph_0$, no nontrivial finite orbits, and infinitely many

fixed points). Consequently, each permutation $p \in S_\nu$ with $S_\nu^{\tau+1} = [p]^2$ satisfies $|p| = \aleph_\tau$ $(0 \leq \tau \leq \nu)$. Finally note that if $p \in S_\nu$ and $\nu > 0$, there exists $n \in \mathbf{N}_\infty$ such that p has uncountably many orbits of length n.

Let us call an element $p \in S_\nu$ a *nice permutation* if it has, for each $n \in \mathbf{N}_\infty$, either no or infinitely many orbits of length n. In particular, such a permutation has either infinite support or is the identity. The following result, which will be crucial for this section, is essentially contained in Moran [**21**] and can be shown in the same way as Theorem 2 in [**21**] is derived from Lemmas 3 and 4 of [**21**].

LEMMA 5.1 (MORAN [**21**]). *Let s, p be nice permutations of an infinite set M with $|s| \leq |p|$. Then $s \in [p]^2$.*

Now we apply Lemma 5.1 to obtain the following result which shows, in particular, that if $p \in S_\nu$ $(\nu > 0)$ satisfies $|p| = \aleph_\nu$ and has at least one infinite orbit, then $S_\nu = [p]^2$. This generalizes Theorem 2 of Droste and Göbel [**14**].

THEOREM 5.2. *Let $\nu > 0$ and let $p \in S_\nu$ have at least one infinite orbit. Then, for any $0 \leq \tau \leq \nu$, $S_\nu^{\tau+1} = [p]^2$ if and only if $|p| = \aleph_\tau$.*

PROOF. As noted above, it suffices to show that if $|p| = \aleph_\tau$ and $s \in S_\nu$ satisfies $|s| \leq |p|$, then $s \in [p]^2$. First choose $n \in \mathbf{N}_\infty$ such that $\bar{p}(n) \geq \aleph_0$. Next decompose $s = s_1 \oplus s_2$ and $p = p_1 \oplus p_2$ such that $|D(s_1)| = |D(p_1)| = \aleph_0$, p_1 has at least one infinite orbit and infinitely many orbits of length n, and s_2, p_2 are nice permutations with $|s_2| \leq |p_2|$. By Lemma 4.8, there are two permutations q_1, r_1 of $D(s_1)$ with $s_1 = q_1 \cdot r_1$ and $\overline{q_1} = \overline{r_1} = \overline{p_1}$. Since $|D(s_2)| = |D(p_2)| = \aleph_\nu$, by Lemma 5.1 we can find permutations q_2, r_2 of $D(s_2)$ with $s_2 = q_2 \cdot r_2$ and $\overline{q_2} = \overline{r_2} = \overline{p_2}$. Then $q = q_1 \oplus q_2$ and $r = r_1 \oplus r_2$ satisfy $q, r \in S_\nu$, $\bar{q} = \bar{r} = \bar{p}$, and $s = q \cdot r \in [p]^2$.

Now we turn to the proof of Theorem 2 and Corollary 3. In a very similar way as for Theorem 5.2 we show

PROPOSITION 5.3. *Let $\nu > 0$ and $0 \leq \tau \leq \nu$, and let $p \in S_\nu$ have infinitely many fixed points such that $|p| = \aleph_\tau$ and $(S_\infty(p))^3$ contains an additive triple. Then $S_\nu^{\tau+1} = [p]^2$.*

PROOF. Let $s \in S_\nu^{\tau+1}$. Split $s = s_1 \oplus s_2$ and $p = p_1 \oplus p_2$ such that $|D(s_1)| = |D(p_1)| = \aleph_0$, s_1 has infinitely many orbits, p_1 has infinitely many fixed points, $(S_\infty(p_1))^3$ contains an additive triple, and s_2, p_2 are nice permutations with $|s_2| \leq |p_2|$. By Corollary 4.9 and Theorem 1, there are two permutations q_1, r_1 of $D(s_1)$ such that $s_1 = q_1 \cdot r_1$ and $\overline{q_1} = \overline{r_1} = \overline{p_1}$. By Lemma 5.1, there exist permutations q_2, r_2 of $D(s_2)$ with $s_2 = q_2 \cdot r_2$ and $\overline{q_2} = \overline{r_2} = \overline{p_2}$. Hence $q = q_1 \oplus q_2$ and $r = r_1 \oplus r_2$ satisfy $q, r \in S_\nu$, $\bar{q} = \bar{r} = \bar{p}$, and $s = q \cdot r \in [p]^2$.

Now we give the

PROOF OF THEOREM 2 IN THE UNCOUNTABLE CASE (I.E. $\nu > 0$). If $S_\nu = [p]^2$, clearly $|p| = \aleph_\nu$, and Theorem 1 implies that condition (1) or (2) holds. The converse is immediate by Theorem 5.2 and Proposition 5.3.

With this, the proof of Theorem 2 is complete. To the best of our knowledge, Theorem 2, Lemma 4.8, and Theorem 5.2 contain all conjugacy classes C in S_ν $(\nu \geq 0)$ presently known satisfying $S_\nu = C^2$. Next we obtain the

PROOF OF COROLLARY 3. (1) $\rightarrow$ (2). Obvious.

(2) $\rightarrow$ (3). Immediate by Theorem 1.

(3) → (1). Apply Theorem 5.2 and Proposition 5.3.

In [**10**] we showed that any infinite group G can be embedded into a simple group H of the same cardinality satisfying $H = C^2$ for each nonunit conjugacy class C in H. Here we wish to sharpen this result. For background information and a variety of recent theorems in this area we refer the reader to [**1**, **2**, **16**, **21**, **22**]. We will use the following result related to Lemma 5.1.

LEMMA 5.4 (MORAN [**21**, LEMMA 3]). *Let $s, q, r \in S_\nu$ be permutations each having $\aleph_\nu$ nontrivial orbits of the same length, and no others. Then $s \in [q] \cdot [r]$.*

Now we show

THEOREM 5.5. *Every infinite group G can be embedded into a simple group H of the same cardinality which satisfies $H\backslash\{1\} \subseteq C_1 \cdot C_2$ for all nonunit conjugacy classes C_1, C_2 in H.*

PROOF. Let $|G| = \aleph_\nu$. We show that there is a group H_1 of cardinality $\aleph_\nu$ containing G such that for all $a, b, c \in G\backslash\{1\}$, we have $a = b' \cdot c'$ for some conjugates b', c' of b, c in H_1, respectively. Let $\varphi\colon G \hookrightarrow G \times \{1\} \subseteq G \oplus G \hookrightarrow S_\nu$ be the composition of the canonical embedding and Cayley's right-regular representation. We identify G with its image under φ in S_ν. Then, if $g \in G$ has order n ($n \in \mathbf{N}_\infty$), g has in S_ν precisely $\aleph_\nu$ orbits of length n, and no others. Hence by Lemma 5.4 there exists a subgroup H_1 of S_ν with the required properties. Now a straightforward induction implies the result.

For other group-theoretical consequences of similar covering theorems as considered, we refer the reader to [**1**, **8**–**9**, **12**–**15**, **21**–**22**, **27**].

REFERENCES

1. Z. Arad, D. Chillag and G. Moran, *Groups with a small covering number*, Products of Conjugacy Classes in Groups (Z. Arad and M. Herzog, eds.), Lecture Notes in Math., vol. 1112, Springer, Berlin, 1985, pp. 222–244.
2. Z. Arad, M. Herzog and J. Stavi, *Powers and products of conjugacy classes in groups*, Products of Conjugacy Classes in Groups (Z. Arad and M. Herzog, eds.), Lecture Notes in Math., vol. 1112, Springer, Berlin, 1985, pp. 6–51.
3. R. Baer, *Die Kompositionsreihe der Gruppe aller eineindeutigen Abbildungen einer unendlichen Menge auf sich*, Studia Math. **5** (1934), 15–17.
4. E. A. Bertram, *Permutations as products of conjugate infinite cycles*, Pacific J. Math. **39** (1971), 275–284.
5. ———, *On a theorem of Schreier and Ulam for permutations*, J. Algebra **24** (1973), 316–322.
6. G. Boccara, *Sur les permutations d'un ensemble infini dénombrable, dont toute orbite essentielle est infinie*, C. R. Acad. Sci. Paris Sér. A **287** (1978), 281–283.
7. ———, *Cycles comme produit de deux permutations de classes donnees*, Discrete Math. **38** (1982), 129–142.
8. J. L. Brenner and R. C. Lyndon, *Nonparabolic subgroups of the modular group*, J. Algebra **77** (1982), 311–322.
9. ———, *The orbits of the product of two permutations*, European J. Combin. **4** (1983), 279–293.
10. M. Droste, *Products of conjugacy classes of the infinite symmetric groups*, Discrete Math. **47** (1983), 35–48.
11. ———, *Cubes of conjugacy classes covering the infinite symmetric group*, Trans. Amer. Math. Soc. **288** (1985), 381–393.
12. ———, *Classes of universal words for the infinite symmetric groups*, Algebra Universalis **20** (1985), 205–216.

13. M. Droste and R. Göbel, *On a theorem of Baer, Schreier and Ulam for permutations*, J. Algebra **58** (1979), 282–290.
14. ____, *Products of conjugate permutations*, Pacific J. Math. **92** (1981), 47–60.
15. M. Droste and S. Shelah, *On the universality of systems of words in permutation groups*, Pacific J. Math. **127** (1987), 321–328.
16. Y. Dvir, *Covering properties of permutation groups*, Products of Conjugacy Classes in Groups (Z. Arad and M. Herzog, eds.), Lecture Notes in Math., vol. 1112, Springer, Berlin, 1985, pp. 197–221.
17. A. B. Gray, *Infinite symmetric and monomial groups*, Ph.D. Thesis, New Mexico State Univ., Las Cruces, New Mexico, 1960.
18. D. H. Husemoller, *Ramified coverings of Rieman surfaces*, Duke Math. J. **29** (1962), 167–174.
19. G. Moran, *The product of two reflection classes of the symmetric group*, Discrete Math. **15** (1976), 63–77.
20. ____, *Parity features for classes of the infinite symmetric group*, J. Combin. Theory Ser. A **33** (1982), 82–98.
21. ____, *Of planar Eulerian graphs and permutations*, Trans. Amer. Math. Soc. **287** (1985), 323–341.
22. ____, *The products of conjugacy classes in some infinite simple groups*, Israel J. Math. **50** (1985), 54–74.
23. ____, *Conjugacy classes whose square is an infinite symmetric group* (to appear).
24. O. Ore, *Some remarks on commutators*, Proc. Amer. Math. Soc. **2** (1951), 307–314.
25. J. Schreier and S. Ulam, *Über die Permutationsgruppe der natürlichen Zahlenfolge*, Studia Math. **4** (1933), 134–141.
26. W. R. Scott, *Group theory*, Prentice-Hall, Englewood Cliffs, N. J., 1964.
27. W. W. Stothers, *Subgroups of infinite index in the modular group*, Glasgow Math. J. **19** (1978), 33–43.

FACHBEREICH 6-MATHEMATIK, UNIVERSITÄT GHS ESSEN, 4300 ESSEN 1, FEDERAL REPUBLIC OF GERMANY