TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 307, Number 2, June 1988

PRODUCTS OF INVOLUTION CLASSES IN INFINITE SYMMETRIC GROUPS

GADI MORAN

ABSTRACT. Let A be an infinite set. Denote by S_A the group of all permutations of A, and let R_i denote the class of involutions of A moving $|A|$ elements and fixing i elements $(0 \leq i \leq |A|)$. The products R_iR_j were determined in **[M1]**. In this article we treat the products $R_{i_1} \cdots R_{i_n}$ for $n \geq 3$. Let INF denote the set of permutations in S_A moving infinitely many elements. We show:

(1) $R_{i_1} \cdots R_{i_n} = S_A$ for $n \geq 4$.

(2)(a) $R_iR_jR_k = \mathrm{INF}$ if $\{i, j, k\}$ contains two integers of different parity;

(b) $R_iR_jR_k = S_A$ if $i + j + k > 0$ and all integers in $\{i, j, k\}$ have the same parity.

(3) $R_0^3 = S_A \setminus E$, where $\theta \in E$ iff θ satisfies one of the following three conditions:

(i) θ moves precisely three elements.

(ii) θ moves precisely five elements.

(iii) θ moves precisely seven elements and has order 12.

These results were announced in 1973 in **[MO]**. (1) and part of (2)(a) were generalized recently by Droste **[D1, D2]**.

0. Introduction. Let S_A denote the symmetric group of all permutations of a set A. Elements of A are referred to as "symbols". In 1972 Bertram **[B]** showed that if A is countably infinite and C is any conjugacy class (coc) in S_A whose members move infinitely many symbols, then $C^4 = S_A$. He conjectured that, moreover, for such a coc C, $C^3 = S_A$. In the same year, in the course of proving the nonbireflectionality of the automorphism groups of some infinite trees **[M4]**, we were led to the study of products of involution classes in S_A and found it possible to give a description of the product of any two such classes **[M1]**, of any power of an involution class **[M2, M3]**, and, for infinite A, of any product of involution classes **[MO]**. For $0 \leq i \leq |A|$, let $R_i = R_i(A)$ denote the set of permutations φ of A satisfying $\varphi^2 = 1$, fixing i symbols and, if A is infinite, moving $|A|$ symbols. A class of particular significance is R_0, the class of fixed-point-free-involutions, which turned out to be a counterexample to Bertram's conjecture (**[MO, M1]**, and, later but independently, **[DG]**).

Our familiarity with products of cocs in the symmetric groups was significantly advanced during the 13 years since Bertram's conjecture and its counterexample (see **[B, Bo, D1, D2, Dv, M5]** where further reference is available). Recently, Droste **[D2]** combined the available data and proved the remarkable result that

Received by the editors April 17, 1986 and, in revised form, April 23, 1987.

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 20B07; Secondary 20B30, 20E34.

Supported in part by NSERC grant.

$R_0 = R_0(A)$ is in fact the *only* class in S_A violating Bertram's conjecture, as he had earlier suspected [**D1**].

While proofs of some of the "Bar Mitsva" (13 years old) results announced in [**MO**] have been published [**M1**, **M2**] and some have been significantly generalized (see, e.g., [**D1**, **D2**]), others are still without published proof. Among these is the actual value of R_0^3. It is high time for this gap to be filled, and this is the main objective of the present paper. Let us start by reviewing the content of [**MO**].

Assume in the sequel that A is an infinite set. In [**MO**] we announced three theorems, which we denote here by T1, T2, and T3.

T1 deals with the products of two factors R_iR_j in S_A. These products are determined in detail (for finite and infinite A) in [**M1**, Theorem 2.1]. T1 is then restated and proved as Corollary 2.5. (Theorem 2.1 in [**M1**] simplifies to Theorem 2.6 when A is finite.)

T2 gives the precise value of products of three factors $R_iR_jR_k$ other than R_0^3, and is restated as (2) in the abstract. Among its immediate corollaries is $R_iR_jR_kR_l = S_A$ for all $0 \leq i, j, k, l \leq |A|$, stated as (1) in the abstract. (Indeed, for any coc D and any coc $C \subseteq \mathrm{INF}$ we have $(D \cdot C) \cap \mathrm{INF} \neq \emptyset$; hence $D \subseteq C \cdot \mathrm{INF}$. Thus, (1) follows from (2) (and (3)).)

The part "$R_iR_jR_k \supseteq \mathrm{INF}$" of T2 was significantly generalized by Droste, who showed that in fact $C_1C_2C_3 \supseteq \mathrm{INF}$ holds for *any* three classes in S_A moving $|A|$ elements [**D1**, Theorem 2]. It readily follows that $C_1C_2C_3C_4 = S_A$ whenever C_i are classes moving $|A|$ elements [**D1**, Corollary 5.1], which extends (1). See [**D2**] for other extensions of consequences of (2).

A complete proof of T2 is given in §3, where the part $R_iR_jR_k \supseteq \mathrm{INF}$ is derived from a theorem of independent interest: Let $|A| = \aleph_0$. Then $\mathrm{INF} = R_kC$ for $0 \leq k \leq \aleph_0$, where C is the class of permutations having $\aleph_0$ infinite orbits and no finite orbit (Theorem 3.2). In fact, Droste showed [**D1**, Lemma 4.9] that $\mathrm{INF} \subseteq D{\cdot}C$ for any coc $D \subseteq \mathrm{INF}$ (Proposition 3.8). We mention in passing that C was the first class shown to satisfy $C^2 = S_A$ by A. B. Gray in his thesis in 1960 [**G**], and that C is the only class of permutations with infinite orbits only that satisfies $C \subseteq R_iR_j$ for all $0 \leq i, j \leq \aleph_0$ [**M1**, Corollary 2.3(1)]. See [**D3**] for a simple proof of Gray's result and other properties of C.

T3 determines the value of R_0^3, and is restated as (3) in the abstract.[1] As a complete argument for it is a central goal of this paper, we first restate it in more detail. Consider the following four conditions on a permutation θ in S_A:

(3*): θ moves precisely three symbols.

(5*): θ moves precisely five symbols, on which it acts as a 5-cycle.

(2* + 3*): θ moves precisely five symbols, on which it acts as a product of two disjoint cycles, one of length 2 and one of length 3.

(3* + 4*): θ moves precisely seven symbols, on which it acts as a product of two disjoint cycles, one of length 3 and one of length 4.

Call $\theta \in S_A$ *exceptional* if it satisfies one of these conditions, and let $E = E(A)$ denote the set of all exceptional permutations S_A.

[1] In [**MO**, Theorem 3], read "ξ of order 12" instead of "$\xi^{12} = 1$".

T3—or (3) of our abstract—is restated as

THEOREM 0. *Let A be infinite, and let $\theta \in S_A$. The following are equivalent:*
(1) $\theta \notin R_0^3$.
(2) $\theta \in E$; *i.e., θ satisfies one of the conditions* (3^*), (5^*), ($2^* + 3^*$), ($3^* + 4^*$).

§§1 and 2 are devoted to the proof of Theorem 0. (2) $\Rightarrow$ (1) is proved in §1, and (1) $\Rightarrow$ (2) is proved in §2. The condition that A is infinite is essential in Theorem 0, and R_0^3 for finite A will be discussed elsewhere. We mention that while obviously (2) $\Rightarrow$ (1) holds for finite A, (1) $\Rightarrow$ (2) fails there, and there are many examples of finite A's and nonexceptional θ's in S_A which are not a product of three fixed-point-free involutions. However, by Theorem 0 and the discussion preceding Proposition 1.2 in §1, for every such A and θ there is a set $A' \supseteq A$ of cardinality at most $2|A|$ such that the trivial extension θ' of θ to A' ($\theta'(a') = a'$ for $a' \in A' \setminus A$) *is* in fact a product of three fixed-point-free involutions of A'.

In §4 we discuss briefly products of involution classes in S_A other than the R_i's and suggest (as problems) natural sequel to this work. We also provide four tables which complete the proof of (2) $\Rightarrow$ (1), in Theorem 0, given in §1.

1. No exceptional permutation is in R_0^3.

This section is devoted to the proof of the implication (2) $\Rightarrow$ (1) in Theorem 0. We first develop some notation.

Let $\theta \in S_A$, $a \in A$. Then $\theta(a)$ denotes the value of θ at a (so $(\theta\varphi)(a) = \theta(\varphi(a))$; i.e., right acts first on a symbol), and $(a)_\theta$ is the θ-orbit of a; that is $(a)_\theta = \{\theta^m(a)\colon m \in \mathbb{Z}\}$, where $\mathbb{Z} = \{0, +1, -1, +2, -2, \dots\}$ is the set of integers. For $1 \le n \le \aleph_0$ let $\overline{\theta}(n)$ denote the cardinality of the set of θ-orbits of cardinality n. θ is called *nicely even* if $\overline{\theta}(n)$ is an even cardinal for all $1 \le n \le \aleph_0$ (where infinite cardinals are considered even). Let NE=NE(A) denote the set of all nicely even permutations in S_A. The following two propositions hold for A of arbitrary cardinality.

PROPOSITION 1.0 [**M1**]. $R_0^2 = \mathrm{NE}$.

Let $M(\theta) = \{a \in A\colon \theta(a) \ne a\}$ denote the support of θ, and let $m(\theta) = |M(\theta)|$ denote its cardinality.

PROPOSITION 1.1 [**M1**, LEMMA A.3, p. 76]. *Let $\varphi, \psi \in S_A$, $\theta = \varphi\psi$. The smallest subset B of A containing $M(\theta)$ which is both φ- and ψ-invariant is*

$$B = \bigcup_{a \in M(\theta)} (a)_\varphi = \bigcup_{a \in M(\theta)} (a)_\psi .$$

Assume that $\theta \in R_0^3$ and $M(\theta)$ contains m symbols. By Proposition 1.0 $\theta = \varphi\psi$, where $\varphi \in \mathrm{NE}(A)$, $\psi \in R_0(A)$. Let B be the smallest set containing $M(\theta)$ which is both φ- and ψ-invariant. Since $|(a)_\psi| = 2$ for all $a \in A$, we have $|B| \le 2m$, by Proposition 1.1. Let ξ_C denote the restriction of $\xi \in S_A$ to a subset C of A. Since B is both φ- and ψ-invariant, we have $\varphi_B, \psi_B, \theta_B \in S_B$, $\theta_B = \varphi_B\psi_B$; and with $B' = A \setminus B$, $\varphi_{B'}, \psi_{B'}, \theta_{B'} \in S_{B'}$, $\theta_{B'} = \varphi_{B'}\psi_{B'}$. But $\theta_{B'}$ is the identity map of B', so $\varphi_{B'} = \psi_{B'}^{-1}$, $\overline{\varphi}_{B'}(2) = \overline{\psi}_{B'}(2)$, $\overline{\varphi}_{B'}(n) = \overline{\psi}_{B'}(n) = 0$ for $n \ne 2$ by $\psi \in R_0(A)$. Since $\varphi \in \mathrm{NE}$, we conclude that $\overline{\varphi}_B(n) = \overline{\varphi}_B(n) + \overline{\varphi}_{B'}(n) = \overline{\varphi}(n)$ is an even cardinal for $n \ne 2$ (but $\overline{\varphi}_B(2)$ can be odd).

Assume now that $|A| = \aleph_0$, $\theta \in S_A$, and for some coinfinite B, $M(\theta) \subseteq B \subseteq A$, we have $\theta_B = \varphi_B\psi_B$, where $\psi_B \in R_0(B)$ and $\overline{\varphi}_B(n)$ is even for $n \ne 2$. Let

$B' = A \setminus B$ (so $|B'| = \aleph_0$) and let $\varphi_{B'} = \psi_{B'} \in S_{B'}$ be any fixed-point-free involution. Then if $\varphi, \psi \in S_A$ are defined by their restrictions $\varphi_B, \varphi_{B'}$; $\psi_B, \psi_{B'}$ we have $\varphi \in \mathrm{NE}(A)$ (for "$\overline{\varphi}(2)$ is even" we need "$|A \setminus B| = \aleph_0$") and $\psi \in R_0(A)$, so $\theta = \varphi\psi$ implies $\theta \in R_0^3(A)$.

We have proved

PROPOSITION 1.2. *Let A be infinite, $\theta \in S_A$, and let $m(\theta) = |M(\theta)| = m < \aleph_0$. Then the following are equivalent:*

(i) *$\theta \in R_0^3$ (where $R_0 = R_0(A)$).*

(ii) *There is a set B containing $M(\theta)$, $|B| \leq 2m$, and $\varphi, \psi \in S_B$ such that $\theta_B\psi = \varphi$, $\psi \in R_0(B)$, and $\overline{\varphi}(n)$ is an even integer for $n \neq 2$.*

Let now A be infinite, let $\theta \in S_A$ be an exceptional permutation, and let $m = m(\theta)$. Then $m \leq 7$, and by Proposition 1.2 $\theta \notin R_0^3$ follows once we can verify that for no set $B \supseteq A$ of cardinality at most $2m \leq 14$ containing $M(\theta)$, we have $\theta_B = \varphi\psi$ for some $\varphi, \psi \in S_B$, $\psi \in R_0(B)$, and $\overline{\varphi}(n)$ even for $n \neq 2$. Thus, (2) $\Rightarrow$ (1) of Theorem 0 follows from

PROPOSITION 1.3. *Let $|B| \leq 14$, let $\theta \in S_B$ be exceptional, and let $\psi \in S_B$ be a fixed-point-free involution in S_B. Then $\varphi = \theta\psi$ satisfies: $\overline{\varphi}(n)$ is odd for some $n \neq 2$.*

The proof of Proposition 1.3 involves the evaluation of finitely many products of an exceptional permutation by a fixed-point-free involution, and is readily done, e.g., by a graphical method introduced in [**M2**], explained in §2. The outcome of this computation, stated in the notation developed in §2, is given in §4 in Tables 1–4, whose content establishes Proposition 1.3.

2. Every nonexceptional permutation is in R_0^3. This section is devoted to the proof of the implication (1) $\Rightarrow$ (2) in Theorem 0. We shall actually prove that (1) $\Rightarrow$ (2) when θ moves only finitely many symbols. If θ moves infinitely many symbols, i.e., $\theta \in \mathrm{INF}$, then $\theta \in R_0^3$ follows from (2)(a) in the abstract, which is proved in §3. Our goal then is to prove

THEOREM 2.0. *Let A be an infinite set, and let $\theta \in S_A$ move finitely many symbols. If $\theta \notin R_0^3$ then $\theta \in E$.*

Our proof makes use of [**M2**] and requires some more notation. Let $\mathbb{N} = \{1, 2, \dots\}$ denote the set of positive integers, $\mathbb{N}^+ = \mathbb{N} \cup \{\aleph_0\}$ and $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. A *type* is a cardinal valued function defined on $\mathbb{N}^+$. We shall use small letters $r, s, t, \dots$ to denote types, and boldface small letters $\mathbf{r}, \mathbf{s}, \mathbf{t}, \dots$ to denote sets of types. The *zero type* o is defined by $o(n) = 0$, $n \in \mathbb{N}^+$, and for each $n \in \mathbb{N}^+$, n^* is the type defined by $n^*(m) = \delta_{nm}$, $m \in \mathbb{N}^+$. The sum $\sum_{i \in I} t_i$ of a set of types $\{t_i : i \in I\}$ and the product $k \cdot t$ (or briefly, kt) of a type t by a cardinal number k are defined naturally by

$$\left(\sum_{i \in I} t_i\right)(n) = \sum_{i \in I}(t_i(n)), \quad (kt)(n) = k(t(n)) \qquad (n \in \mathbb{N}^+).$$

Thus, for any type t we have

$$t = \sum_{n \in \mathbb{N}^+} t(n) \cdot n^*.$$

We note that the types with the addition as a binary operation and multiplication by a cardinal number form a semimodule over the semiring of cardinal numbers in a natural way.

For $\theta \in S_A$, the type $\overline{\theta}$ defined on $\mathbb{N}^+$ in §1 by $\overline{\theta}(n) =$ cardinality of the set of θ-orbits of cardinality n is called the *type* of θ, and θ is called *a t-permutation* if $\overline{\theta} = t$. Since $\theta, \theta' \in S_A$ are conjugate if and only if $\overline{\theta} = \overline{\theta}'$, types serve as convenient "names" for classes in the symmetric groups, and we proceed to use them to produce convenient notation for class invariants. For a type t let

$$|t| = \sum_{n \in \mathbb{N}^+} nt(n) \quad \text{(cardinality of the domain)},$$

$$m(t) = \sum_{1 < n \in \mathbb{N}^+} nt(n) \quad \text{(cardinality of the support)}.$$

$|t|$ is also called the *cardinality* of t, and t is called *finite* if $|t| < \aleph_0$. t is called *finitary* if $m(t) < \aleph_0$.

Define a three-place relation $P(r,s,t)$ on types as follows [**M5**]:

$P(r,s,t)$ iff there is a set A and $\xi, \eta, \varsigma \in S_A$ such that $\overline{\xi} = r$, $\overline{\eta} = s$, $\overline{\varsigma} = t$ and $\xi = \eta\varsigma$ (equivalently, $\xi\eta\varsigma = 1_A$).

Thus, $P(r,s,t)$ implies $|r| = |s| = |t|$. The most useful properties of P are [**M5**, Lemma 1]:

SYMMETRY: $P(t_1, t_2, t_3)$ if and only if $P(t_i, t_j, t_k)$ whenever $\{i,j,k\} = \{1,2,3\}$,

SUPERADDITIVITY: $P(r_i, s_i, t_i)$ for all $i \in I$ implies

$$P\left(\sum_{i \in I} r_i, \sum_{i \in I} s_i, \sum_{i \in I} t_i\right).$$

HOMOGENEITY: $P(r,s,t)$ implies $P(kr, ks, kt)$ for every cardinal number k.

We now use P to model the product of conjugacy classes in symmetric groups and, more generally, the products of conjugacy sets (subsets of S_A closed under conjugacy in S_A) in the realm of types.

DEFINITION 2.0. Let $\mathbf{s}, \mathbf{t}$ be sets of types. Define a set of types $\mathbf{s} \odot \mathbf{t}$ called *the composition of* $\mathbf{s}$ *and* $\mathbf{t}$ by

$$r \in \mathbf{s} \odot \mathbf{t} \quad \text{iff} \quad P(r,s,t) \text{ holds for some } s \in \mathbf{s},\ t \in \mathbf{t}.$$

When no confusion may arise, it will be convenient to use the same symbol for a type and the singleton containing it. Thus, if s, t are types we have

$$s \odot t = \{s\} \odot \{t\}.$$

The nth power $\mathbf{t}^n$ of a set of types $\mathbf{t}$ is defined inductively by $\mathbf{t}^1 = \mathbf{t}$, $\mathbf{t}^{n+1} = \mathbf{t}^n \odot \mathbf{t}$.

If t is a type, we let $t^n = \{t\}^n$.

The class of sets of types forms a commutative semigroup with the composition operator $\odot$.

The addition of types extends naturally to sets of types by

$$\mathbf{u} + \mathbf{v} = \{u + v \colon u \in \mathbf{u}, v \in \mathbf{v}\}.$$

Similarly, the product of a type by a cardinal number (scalar multiplication) extends naturally to sets of types by

$$k \cdot \mathbf{u} = \{ku\colon u \in \mathbf{u}\}.$$

The class of sets of types with addition $+$ and scalar multiplication again forms a semimodule over the semiring of cardinal numbers, which carry also the semigroup operation of composition $\odot$. We shall use the following convention in forming expressions (terms) in this structure:

1. A type t may always stand for the singleton $\{t\}$.

2. Priorities of operations in expressions involving $\cdot, \odot, +$ is in this order, unless indicated otherwise by bracketing.

Thus, for example,

$$2 \cdot \aleph_0^* \odot \aleph_0 \cdot \{3^*, 1^* + 2^*\} + 7^* = ((2 \cdot \aleph_0^*) \odot \{\aleph_0 \cdot 3^*, \aleph_0 \cdot 1^* + \aleph_0 \cdot 2^*\}) + 7^*.$$

A most useful observation is

$$u \odot v + u' \odot v' \subseteq (u + u') \odot (v + v'),$$

and, more generally,

$$\sum_{i\in I} u_i \odot v_i \subseteq \left(\sum_{i\in I} u_i\right) \odot \left(\sum_{i\in I} v_i\right).$$

For $n \in \mathbb{N}^+$ let $n^\oplus = \aleph_0 \cdot n^*$. For a set of permutations X, let $\overline{X} = \{\overline{\xi}\colon \xi \in X\}$.

Thus, if $|A| = \aleph_0$, then $\overline{R}_0 = \{2^\oplus\} = 2^\oplus$ (by our convention that allows a type to stand for its singleton). We now define for $0 \leq i \leq \aleph_0$ a type r_i, so that $r_i = \overline{R}_i$, by

$$r_i = i \cdot 1^* + \aleph_0 \cdot 2^* = i \cdot 1^* + 2^\oplus.$$

By Proposition 1.0 we have

$$r_0^2 = \{t\colon |t| = \aleph_0, t(n) \text{ is even for all } n \in \mathbb{N}^+\}$$

and

$$r_0^3 = r_0^2 \odot r_0 = \overline{R_0^3} = \{\overline{\theta}\colon \theta \in R_0^3\}.$$

We note that by $r_0 \in r_0^2$, $1^\oplus \in r_0^3$ (i.e., the identity permutation 1_A of a countable set A is a product of three fixed-point-free involutions), and so in Theorem 2.0 we may, with no loss of generality, assume that A is countable. Thus, Theorem 2.0 is equivalent to

THEOREM 2.1. *Let $|t| = \aleph_0$, $m(t) < \aleph_0$, $t \notin r_0^3$. Then $t \in 1^\oplus + \{3^*, 5^*, 2^* + 3^*, 3^* + 4^*\}$.*

Our next goal is to formulate a theorem on *finite* types, implying Theorem 2.1. First define some sets of finite types as follows.

$$\mathbf{r}_0 = \{k \cdot 2^*\colon k \in \mathbb{N}_0\} \quad \text{(set of finite fixed-point-free involution types)},$$

$$\mathbf{ne} = r_0^2 \quad \text{(set of finite NE types)},$$

$$\mathbf{r}_{00} = \mathbf{ne} \cup (\mathbf{ne} + 2^*) \quad \text{(set of finite types } t \text{satisfying:} t(n) \text{ is even for } n \neq 2),$$

$$\mathbf{r}_{000} = \mathbf{r}_{00} \odot \mathbf{r}_0.$$

We have [**M2**, Lemma 1, p. 5]
(i) $\mathbf{r}_0 \subseteq \mathbf{r}_{00} \subseteq \mathbf{r}_{000}$.
(ii) each of $\mathbf{r}_0$, $\mathbf{r}_{00}$, $\mathbf{r}_{000}$ is additively closed.
We now restate Proposition 1.2 as

PROPOSITION 2.2. *Let $t = 1^\oplus + t_0$, where $|t_0| = m(t) = m < \aleph_0$. Then $t \in r_0^3$ if and only if $t_0 + k \cdot 1^* \in \mathbf{r}_{000}$ for some $k \leq m$.*

Thus, Theorem 2.1 (hence Theorem 2.0) follows from

THEOREM 2.3. *Let $|t| < \aleph_0$, $t(1) = 0$. The following are equivalent:*
(a) *For all $k \in \mathbb{N}_0$, $k \cdot 1^* + t \notin \mathbf{r}_{000}$,*
(b) *$t \in \{3^*, 5^*, 2^* + 3^*, 3^* + 4^*\}$.*

PROOF OF THEOREM 2.3. (b) $\Rightarrow$ (a). Indeed, otherwise we have some $t \in \{3^*, 5^*, 2^* + 3^*, 3^* + 4^*\}$ and some $k \in \mathbb{N}_0$ satisfying $k \cdot 1^* + t \in \mathbf{r}_{000}$, and so by Proposition 2.2, $m \cdot 1^* + t \in \mathbf{r}_{000}$, for some $m \leq 7$, contradicting Proposition 1.3.

The rest of this section is devoted to the proof of (a) $\Rightarrow$ (b). The argument for (a) $\Rightarrow$ (b) splits into five steps, the first three of which are essentially reproduced from [**M2**]. We first give

OUTLINE OF PROOF OF (a) $\Rightarrow$ (b).

First. Define a large additively closed subset $\mathbf{p}$ of $\mathbf{r}_{000}$ and a set of finite types called *residua*.

Second. Recall that every finite type t admits a representation $t = t_0 + t_1$ where $t_0 \in \mathbf{p}$ and t_1 is a residuum.

Third. Describe a graphical method of establishing $t \in \mathbf{r}_{000}$.

Assume now that $|t| < \aleph_0$, $t(1) = 0$ and for all $k \in \mathbb{N}_0$ $t + k \cdot 1^* \notin \mathbf{r}_{000}$.

Fourth. Let $t = t_0 + t_1$, where $t_0 \in \mathbf{p}$ and t_1 is a residuum. Then $t_1 = 3^*$ or $t_1 = 5^*$.

Fifth. If $t_1 = 3^*$ then $t_0 \in \{o, 2^*, 4^*\}$. If $t_1 = 5^*$ then $t_0 = o$.
Obviously, this establishes (a) $\Rightarrow$ (b).

Let us turn to the details.

Define three families of finite types $\mathbf{f}_i$, $i = 1, 2, 3$, as follows:

$$t \in \mathbf{f}_1 \quad \text{iff} \quad t = 2 \cdot n^* \text{ for some } n \in \mathbb{N}.$$
$$t \in \mathbf{f}_2 \quad \text{iff} \quad t = (2n)^* \text{ for some } n \in \mathbb{N}_0.$$
$$t \in \mathbf{f}_3 \quad \text{iff} \quad t = (1+2k)^* + (7+2l)^* \text{ for some } k, l \in \mathbb{N}_0.$$

Let $\mathbf{p}$ denote the additive closure of $\mathbf{f} = \mathbf{f}_1 \cup \mathbf{f}_2 \cup \mathbf{f}_3$; that is,

$$t \in \mathbf{p} \quad \text{iff} \quad t \text{ is a finite sum of members of } \mathbf{f}.$$

($\mathbf{p}$ is the class of types of the "proper permutations" in the terminology of [**M2**]; see [**M2**, Definition 4.5, p. 15].)

Notice that $o \in \mathbf{p}$ and that $|t|$ is even for every $t \in \mathbf{p}$, as this holds for any $t \in \mathbf{f}$. This follows also from

PROPOSITION 2.4 [**M2**, PROPOSITION 4.6]. $\mathbf{p} \subseteq \mathbf{r}_{000}$.

We call a finite type t a *residuum* iff $t = t_0 + t_1$, $t_0 \in \mathbf{p} \Rightarrow t_0 = o$. This definition immediately gives the following.

PROPOSITION 2.5. *Let t be any finite type. Then $t = t_0 + t_1$, where $t_0 \in \mathbf{p}$ and t_1 is a residuum.*

Notice that this representation is not unique. Indeed, if $t = 1^* + 3^* + 5^* + 7^*$, then $t = t_0 + t_1 = t'_0 + t'_1$ are two distinct such representations, with $t_0 = 5^* + 7^*$, $t_1 = 1^* + 3^*$, $t'_0 = 3^* + 7^*$, $t'_1 = 1^* + 5^*$.

By inspecting the family $\mathbf{f}$ one easily sees

PROPOSITION 2.6. *Let t be a residuum. Then t satisfies one of the following three conditions:*

(0) $t = o$.

(1) $t = (2n+1)^*$ *for some* $n \in \mathbb{N}_0$.

(2) $t \in \{1^* + 3^*, 1^* + 5^*, 3^* + 5^*, 1^* + 3^* + 5^*\}$.

(See [**M2**, Definition 4.7 and Lemma 4.8, p. 16].)

Our argument in the sequel requires the verification of claims "$t \in \mathbf{r}_{000}$" for various types. We will use the graphical method introduced in the appendix of [**M2**] which we reproduce here for the reader's convenience.

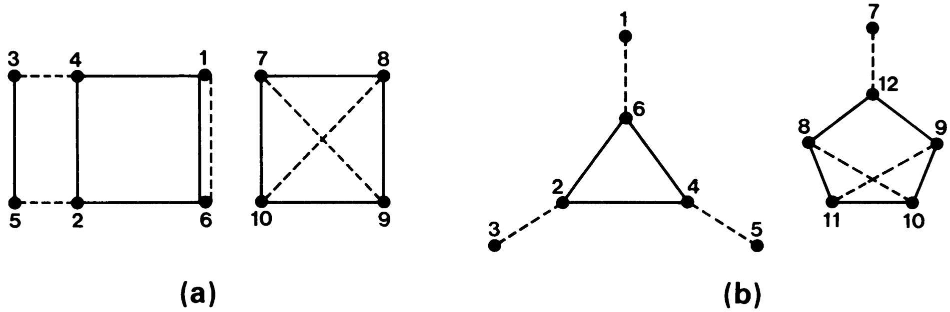

FIGURE 0

(a) Displays $\theta = \varphi\psi$, where

$$\theta = (1)(2,3)(4,5,6)(7,8,9,10)$$
$$\varphi = (3,5)(1,4,2,6)(7,10,9,8)$$
$$\psi = (1,6)(2,5)(3,4)(7,9)(8,10).$$

Hence, $P(1^* + 2^* + 3^* + 4^*, 2^* + 2\cdot 4^*, 5\cdot 2^*)$, and so $1^* + 2^* + 3^* + 4^* \in (2^* + 2\cdot 4^*) \odot 5\cdot 2^* \subseteq \mathbf{r}_{00} \odot \mathbf{r}_0 = \mathbf{r}_{000}$.

(b) Displays $\varphi = \theta\psi$, where

$$\varphi = (1,2,3,4,5,6)(7,8,9,10,11,12)$$
$$\theta = (1)(3)(5)(7)(2,4,6)(8,11,10,9,12)$$
$$\psi = (1,6)(2,3)(4,5)(7,12)(8,10)(9,11).$$

Hence, $P(2\cdot 6^*, 4\cdot 1^* + 3^* + 5^*, 6\cdot 2^*)$, and so (by symmetry of P), $4\cdot 1^* + 3^* + 5^* \in 2\cdot 6^* \odot 6\cdot 2^* \subseteq \mathbf{r}_{00} \odot \mathbf{r}_0 = \mathbf{r}_{000}$.

Let t be a finite type. To show $t \in \mathbf{r}_{000}$, one has to produce permutations φ, ψ of a set of cardinality $|t|$ with $\overline{\varphi} \in \mathbf{r}_{00}$ and $\overline{\psi} \in \mathbf{r}_0$ such that $\theta = \varphi\psi$ satisfies $\overline{\theta} = t$. We denote a φ-orbit of length k greater than 2 as the set of vertices of a k-gon in the plane, whose sides, oriented positively (counterclockwise), describe the action of φ on the vertices. φ-orbits of cardinality 2 are described as the endpoints of a line segment, and fixed points of φ as isolated points. We describe the action of ψ (who has only orbits of cardinality 2) by disjointed dashed segments, connecting pairs of points. The action of θ is obtained by following ψ-action first, then φ-action. To verify that indeed $t \in \mathbf{r}_{000}$, mark in order points as the θ-action dictates. The disjoint-cycle decomposition obtained for θ should indicate that $\overline{\theta} = t$. (See Figure 0(a).) Equivalently, one can start with a description of the θ-action by solid polygonal lines on the points, and the ψ-action by dashed line segment, and verify that $\varphi = \theta\psi$ satisfies $\overline{\varphi} \in \mathbf{r}_{00}$ (see Figure 0(b)).

We are now ready to proceed with the proof of (a) $\Rightarrow$ (b).

Let t be a fixed type satisfying $|t| < \aleph_0$, $t(1) = 0$ and for all $k \in \mathbb{N}_0$ $t+k\cdot 1^* \notin \mathbf{r}_{000}$. Let further $t = t_0+t_1$, where $t_0 \in \mathbf{p}$ and t_1 is a residuum, as provided by Proposition 2.5.

PROPOSITION 2.7. *$t_1 = 3^*$ or $t_1 = 5^*$.*

PROOF. We have to deny all other options for t_1 listed in Proposition 2.6.

$t_1 = o$ is ruled out, as then $t \in \mathbf{p} \subseteq \mathbf{r}_{000}$.

$t_1 = 3^* + 5^*$ is ruled out, as $4 \cdot 1^* + t_1 = 4 \cdot 1^* + 3^* + 5^* \in \mathbf{r}_{000}$ by Figure 0(b), and so $4 \cdot 1^* + t = t_0 + (4 \cdot 1^* + t_1) \in \mathbf{r}_{000}$ as $t_0 \in \mathbf{p} \subseteq \mathbf{r}_{000}$, $4 \cdot 1^* + t_1 \in \mathbf{r}_{000}$, and $\mathbf{r}_{000}$ is additively closed. $t_1 \in \{1^* + 3^*, 1^* + 5^*, 1^* + 3^* + 5^*\}$ is ruled out by $t(1) = t_1(1) = 0$.

Thus, $t_1 = (2n + 1)^*$ for some $n \in \mathbb{N}_0$. We need to show that $n = 1$ or $n = 2$. Indeed, $n = 0$ is ruled out, as then $t_1 = 1^*$ and so $1^* + t = t_0 + 2 \cdot 1^* \in \mathbf{r}_{000}$. If $n \geq 3$, then $1^* + t_1 = 1^* + (7 + 2k)^*$, where $k = n - 3 \geq 0$, and so $1^* + t_1 \in \mathbf{f}_3 \subseteq \mathbf{p}$, and $1^* + t = t_0 + (1^* + t_1) \in \mathbf{p} + \mathbf{p} \subseteq \mathbf{p} \subseteq \mathbf{r}_{000}$, i.e., $1^* + t \in \mathbf{r}_{000}$.

Thus $n = 1$ or $n = 2$ and $t_1 = 3^*$ or $t_1 = 5^*$. □

PROPOSITION 2.8. *If $t_1 = 3^*$ then $t_0 \in \{o, 2^*, 4^*\}$. If $t_1 = 5^*$ then $t_0 = o$.*

PROOF. We start with seven observations (1)–(7) of the form $s \in \mathbf{r}_{000}$, proved graphically by Figures 1–7.

(1) $1^* + (3 + 2k)^* + (6 + 2l)^* \in \mathbf{r}_{000}$ for $k, l \in \mathbb{N}_0$. Indeed, by Figure 1,

$$1^* + (3 + 2k)^* + (6 + 2l)^* \in (2 \cdot 1^* + (k + l) \cdot 2^* + 2 \cdot 4^*) \odot (5 + k + l) \cdot 2^* \subset \mathbf{r}_{000}.$$

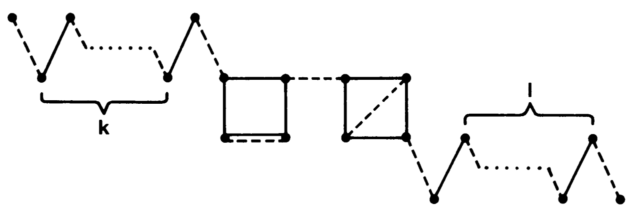

FIGURE 1

(2) $5 \cdot 1^* + 3 \cdot 3^* \in \mathbf{r}_{000}$.
Indeed, by Figure 2,

$$5 \cdot 1^* + 3 \cdot 3^* \in (2^* + 2 \cdot 6^*) \odot 7 \cdot 2^* \subseteq \mathbf{r}_{000}.$$

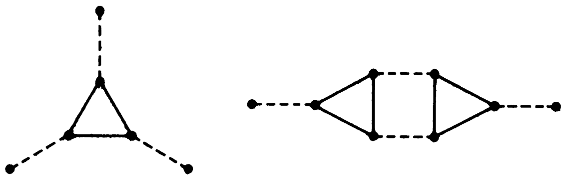

FIGURE 2

(3) $1^* + (3+2k)^* + (3+2l)^* + (5+2m)^* \in \mathbf{r}_{000}$ for $k, l, m \in \mathbb{N}_0$.
Indeed, by Figure 3

$$\begin{aligned} &1^* + (3+2k)^* + (3+2l)^* + (5+2m)^* \\ &\qquad \in (4 \cdot 1^* + (k+l+m) \cdot 2^* + 2 \cdot 4^*) \odot (6+k+l+m) \cdot 2^* \subseteq \mathbf{r}_{000}. \end{aligned}$$

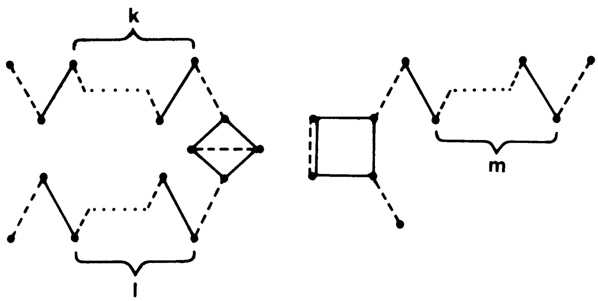

FIGURE 3

(4) $5 \cdot 1^* + 2 \cdot 2^* + 3^* \in \mathbf{r}_{000}$.
Indeed, by Figure 4,

$$5 \cdot 1^* + 2 \cdot 2^* + 3^* \in 2 \cdot 6^* \odot 6 \cdot 2^* \subseteq \mathbf{r}_{000}.$$

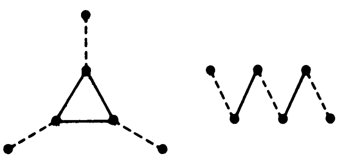

FIGURE 4

(5) $1^* + 2^* + 3^* + 4^* \in \mathbf{r}_{000}$.
Indeed, see Figure 1(a).
(6) $7 \cdot 1^* + 3^* + 2 \cdot 4^* \in \mathbf{r}_{000}$.
Indeed, by Figure 5,

$$7 \cdot 1^* + 3^* + 2 \cdot 4^* \in (2^* + 2 \cdot 8^*) \odot 9 \cdot 2^* \subseteq \mathbf{r}_{000}.$$

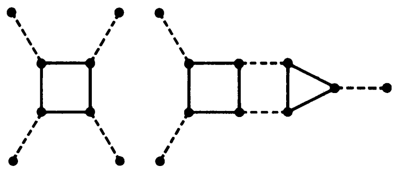

FIGURE 5

(7) $1^* + 5^* + (2n)^* \in \mathbf{r}_{000}$ for all $n \in \mathbb{N}$.

Indeed, for $n = 1$ we have, by Figure 6,

$$1^* + 2^* + 5^* \in (2^* + 2 \cdot 3^*) \odot 4 \cdot 2^* \subseteq \mathbf{r}_{000};$$

for $n = 2$ we have, by Figure 7,

$$1^* + 4^* + 5^* \in (2 \cdot 1^* + 2 \cdot 4^*) \odot 5 \cdot 2^* \subseteq \mathbf{r}_{000};$$

and for $n > 2$, (7) follows from (1).

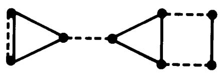

FIGURE 6

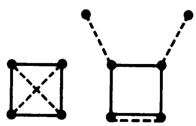

FIGURE 7

We proceed to prove Proposition 2.8. Thus, t is a finite type satisfying $t(1) = 0$, $t = t_0 + t_1$, where $t_0 \in \mathbf{p}$ and by Proposition 2.7 $t_1 = 3^*$ or $t_1 = 5^*$, and in addition, for all $k \in \mathbb{N}_0$, $k \cdot 1^* + t \notin \mathbf{r}_{000}$.

Step 1. $t_0(2n) = 0$ for $n \geq 3$.

Otherwise, let t_0' satisfying $t_0 = t_0' + (2n)^*$, $n \geq 3$. Then $t_0' \in \mathbf{p}$, and we have by (1)

$$1^* + t = 1^* + (3 + 2k)^* + (2n)^* + t_0' \in \mathbf{r}_{000}$$

where $k = 0$ if $t_1 = 3^*$, and $k = 1$ if $t_1 = 5^*$.

Step 2. $t_0(2n + 1) = 0$ for $n \geq 2$.

Otherwise, let $t_0 = (5+2m)^* + t_0''$, where $5+2m = 2n+1$, $m \in \mathbb{N}_0$. Since $t_0 \in \mathbf{p}$, t_0 is a finite sum of members of $\mathbf{f}$ and so $t_0 = (5+2m)^* + t_0'' = (5+2m)^* + (1+2k')^* + t_0'$, where $t_0' \in \mathbf{p}$ and $(1 + 2k')^* + (5 + 2m)^* \in \mathbf{f}$. Since $t(1) = 0$ we have $k' > 0$, and so $k' = k + 1$ for some $k \in \mathbb{N}_0$, and we have $t_0 = (3 + 2k)^* + (5 + 2m)^* + t_0'$ with $t_0' \in \mathbf{p}$. Thus,

$$t = t_0 + t_1 = (3 + 2k)^* + (3 + 2l)^* + (5 + 2m)^* + t_0',$$

where $l = 0$ if $t_1 = 3^*$ and $l = 1$ if $t_1 = 5^*$. But then, by (3)

$$1^* + t = 1^* + (3 + 2k)^* + (3 + 2l)^* + (5 + 2m)^* + t_0' \in \mathbf{r}_{000}.$$

Step 3. $t_0(n) = 0$ for $n \neq 2, 3, 4$.

This follows from Steps 1,2 and $t(1) = 0$.

Step 4. $t_0(2) \leq 1$ if $t_1 = 3^*$, $t_0(2) = 0$ if $t_1 = 5^*$. Indeed:

1. If $t_1 = 3^*$ and $t_0(2) \geq 2$, let $t_0 = 2 \cdot 2^* + t_0'$. Then $t_0' \in \mathbf{p}$ and we have, by (4)

$$5 \cdot 1^* + t = 5 \cdot 1^* + 2 \cdot 2^* + 3^* + t_0' \in \mathbf{r}_{000}.$$

2. If $t_1 = 5^*$ and $t_0(2) \geq 1$, let $t_0 = 2^* + t_0'$.

Then $t_0' \in \mathbf{p}$ and we have by (7)

$$1^* + t = 1^* + 2^* + 5^* + t_0' \in \mathbf{r}_{000}.$$

Step 5. $t_0(3) = 0$.

Indeed, if $t_0(3) > 0$ then $t_0(3) \geq 2$, as $t_0 \in \mathbf{p}$ and by Step 3, $t_0(2n+1) = 0$ for $n \neq 1$. Let $t_0 = 2 \cdot 3^* + t_0'$. Then $t_0' \in \mathbf{p}$, and we have:

If $t_1 = 3^*$, then by (2)

$$5 \cdot 1^* + t = 5 \cdot 1^* + 3 \cdot 3^* + t_0' \in \mathbf{r}_{000}.$$

If $t_1 = 5^*$, then by (3) (with $k = l = m = 0$)

$$1^* + t = 1^* + 2 \cdot 3^* + 5^* + t_0' \in \mathbf{r}_{000}.$$

Step 6. $t_0(4) \leq 1$ if $t_1 = 3^*$, $t_0(4) = 0$ if $t_1 = 5^*$.

Indeed, if $t_1 = 3^*$ and $t_0(4) \geq 2$, then $t_0 = 2 \cdot 4^* + t_0'$, where $t_0' \in \mathbf{p}$, and we have, by (6)

$$7 \cdot 1^* + t = 7 \cdot 1^* + 3^* + 2 \cdot 4^* + t_0' \in \mathbf{r}_{000},$$

while if $t_1 = 5^*$ and $t_0(4) > 0$, then $t_0 = 4^* + t_0'$, where $t_0' \in \mathbf{p}$, and we have by (7)

$$1^* + t = 1^* + 4^* + 5^* + t_0' \in \mathbf{r}_{000}.$$

Step 7. If $t_1 = 5^*$ then $t_0 = o$.

This corollary of Steps 3–6 establishes Proposition 2.8 if $t_1 = 5^*$.

Step 8. If $t_1 = 3^*$ then $t_0(2) + t_0(4) \leq 1$.

By Steps 4 and 6 $t_0(2), t_0(4) \leq 1$, so we have only to show that $t_0(2) = t_0(4) = 1$ is impossible. Indeed, assume $t_0(2) = t_0(4) = 1$. Then $t_0' \in \mathbf{p}$, where t_0' is defined by $t_0 = 2^* + 4^* + t_0'$, and we have by (5)

$$1^* + t = 1^* + 2^* + 3^* + 4^* + t_0' \in \mathbf{r}_{000}.$$

Step 9. If $t_1 = 3^*$ then $t_0 \in \{o, 2^*, 4^*\}$.

This corollary of Steps 3, 5 and 8 establishes Proposition 2.8 if $t_1 = 3^*$. $\square$

The proof of Proposition 2.8 is complete, and Theorems 2.3, 2.1, 2.0 are proved.

3. The products $R_iR_jR_k$, $i + j + k > 0$. This section is devoted to the proof of the statements (2)(a) and (2)(b) of the abstract. We first reduce the argument to two theorems that deal with countable A (Theorems 3.2, 3.3).

Let $|A| = \aleph_\nu, \nu \geq 0$, and recall that

$$R_i = R_i(A) = \{\varphi \in S_A : \varphi^2 = 1_A, \varphi \text{ fixes } i \text{ symbols and moves } \aleph_\nu \text{ symbols}\},$$
$$C = C(A) = \{\theta \in S_A : \theta \text{ has } \aleph_\nu \text{ infinite orbits and no finite orbits}\},$$
$$\mathrm{INF} = \mathrm{INF}(A) = \{\psi \in S_A : \psi \text{ moves infinitely many symbols}\}.$$

By [**M1**, Theorem 2.1] (or by simple direct argument, using Proposition 1.0 and [**M1**, Theorem 3.2(3)]) we have the following.

PROPOSITION 3.0. *$C \subseteq R_iR_j$ for all $0 \leq i,j \leq \aleph_\nu$.*

By [**M1**, Corollary 2.3(3); (3) on p. 77] we have

PROPOSITION 3.1. *If $\{i,j,k\}$ has two integers of different parity, then $R_iR_jR_k \subseteq \mathrm{INF}$.*

We shall prove

THEOREM 3.2. *Let $|A| = \aleph_0$. Then $\mathrm{INF} = C \cdot R_k$ for $0 \leq k \leq \aleph_0$.*

THEOREM 3.3. *Let $|A| = \aleph_0$. If $0 \leq i,j,k \leq \aleph_0$, $i+j+k > 0$ and all integers in $\{i,j,k\}$ have the same parity, then $S_A = R_iR_jR_k$.*

We now derive (2)(a) and (2)(b) using the terminology developed in §2.
For any ordinal ν let

$$\mathbf{tp}_\nu = \{t\colon |t| = \aleph_\nu\}.$$

Thus $\mathbf{tp}_\nu = \overline{S}_A$ whenever $|A| = \aleph_\nu$.

$$\mathbf{inf}_\nu = \{t\colon |t| = \aleph_\nu,\ m(t) \geq \aleph_0\}.$$

Thus, $\mathbf{inf}_\nu = \overline{\mathrm{INF}(A)}$ whenever $|A| = \aleph_\nu$.

$$r_{i,\nu} = i \cdot 1^* + \aleph_\nu \cdot 2^*.$$

Thus $r_{i,0} = r_i$, and $r_{i,\nu} = \overline{\psi}$ for any $\psi \in R_i(A)$ if $|A| = \aleph_\nu$.
We have

(i) $\mathbf{tp}_\nu = r_{k,\nu} \odot r_{k,\nu}$ for $\aleph_0 \leq k \leq \aleph_\nu$ if $\nu > 0$ [**M2**, Corollary 2.5].

(ii) $\mathbf{inf_0} \subseteq r_{i,0} \odot r_{j,0} \odot r_{k,0}$ for $0 \leq i,j,k \leq \aleph_0$, by Proposition 3.0 and Theorem 3.2.

(iii) $\mathbf{inf_0} \subseteq \aleph_0^\oplus \odot r_{k,0}$ for $0 \leq k \leq \aleph_0$, by Theorem 3.2.

(iv) $\aleph_0^\oplus \in r_{i,0} \odot r_{j,0}$ for $0 \leq i,j \leq \aleph_0$, by Proposition 3.0.

(v) $r_{k,\nu} \in r_{i,\nu} \odot r_{j,\nu}$ iff all integers in $\{i,j,k\}$ have the same parity.

(v) follows from [**M1**, Theorem 2.1], but we sketch a direct proof here:

1. If, say, $i+j < \aleph_0$ and $i+j \equiv 1 \pmod 2$, then any $t \in r_{i,\nu} \odot r_{j,\nu}$ satisfies $t(\aleph_0) > 0$ by [**M1**, Corollary 2.3(3)], so for all k, $r_{k,\nu} \notin r_{i,\nu} \odot r_{j,\nu}$.

2. If all integers in $\{i,j,k\}$ have the same parity, then $r_{k,\nu} \in r_{i,\nu} \odot r_{j,\nu}$. Indeed, w.l.o.g. $i \leq j,k$ and so, by assumption, $j = i+2u$, $k = i+2v$ for some $0 \leq u,v \leq \aleph_\nu$. Let $A = A_0 \cup A_1$, where $|A_0| = i$, $|A_1| = \aleph_\nu$ and let $A_1 = B \,\dot\cup\, C \,\dot\cup\, D$ where $|B| = 2u$, $|C| = 2v$, $|D| = \aleph_\nu$. Then one easily defines $\varphi, \psi \in S_A$ such that A_0, B, C, D are φ- and ψ-invariant, $\varphi_{A_0} = \psi_{A_0} = 1_{A_0}$, φ_{A_1} is a fixed-point-free involution, $\psi_B = 1_B$, $\psi_C = \varphi_C$, and ψ_D is a fixed-point-free involution, as is $\varphi_D\psi_D$. Then $\overline{\varphi} = r_{i,\nu}$, $\overline{\psi} = r_{j,\nu}$ and $\overline{\varphi\psi} = r_{k,\nu}$.

With no loss of generality, assume $0 \leq i \leq j \leq k \leq \aleph_\nu$ in the sequel.

PROPOSITION 3.4. *If $\nu > 0$, $k \geq \aleph_0$, and $j \geq \aleph_0$ or $j < \aleph_0$ and $i \equiv j \pmod 2$, then $R_iR_jR_k = S_A$.*

PROOF. We have to show $\mathbf{tp}_\nu = r_{i,\nu} \odot r_{j,\nu} \odot r_{k,\nu}$. But under these assumptions, we have $r_{k,\nu} \in r_{i,\nu} \cdot r_{j,\nu}$ by (v), and $r_{k,\nu} \cdot r_{k,\nu} = \mathbf{tp}_\nu$ by (i). Thus,

$$\mathbf{tp}_\nu = r_{k,\nu} \cdot r_{k,\nu} \subseteq r_{i,\nu} \cdot r_{j,\nu} \cdot r_{k,\nu} \subseteq \mathbf{tp}_\nu. \quad \square$$

PROPOSITION 3.5. *INF $\subseteq R_iR_jR_k$ for all $0 \leq i,j,k \leq |A|$.*

PROOF. For $\nu = 0$ this holds by Theorem 3.2 and Proposition 3.0, so assume $\nu > 0$. We have to show $\mathbf{inf} \subseteq r_{i,\nu} \odot r_{j,\nu} \odot r_{k,\nu}$.

Case 1. $k \geq \aleph_0$. By Proposition 3.4, INF $\subseteq R_iR_jR_k$ if $j \geq \aleph_0$, so assume $j < \aleph_0$. Thus, we have $r_{i,\nu} = r_{i,0} + r_{0,\nu}$, $r_{j,\nu} = r_{j,0} + r_{0,\nu}$. Hence, by (iv)

$$\begin{aligned}\aleph_0^{\oplus} + r_{k,\nu} &\in r_{i,0} \odot r_{j,0} + r_{0,\nu} \odot r_{0,\nu} \subseteq (r_{i,0} + r_{0,\nu}) \odot (r_{j,0} + r_{0,\nu}) \\ &= r_{i,\nu} \odot r_{j,\nu}.\end{aligned}$$

Also, by (i), (iii) and $r_{k,\nu} = r_{0,0} + r_{k,\nu}$,

$$\mathbf{inf}_{\nu} = \mathbf{inf_0} + \mathbf{tp}_{\nu} \subseteq \aleph_0^{\oplus} \odot r_{0,0} + r_{k,\nu} \odot r_{k,\nu} \subseteq (\aleph_0^{\oplus} + r_{k,\nu}) \odot r_{k,\nu}.$$

Thus

$$\mathbf{inf}_{\nu} \subseteq (\aleph_0^{\oplus} + r_{k,\nu}) \odot r_{k,\nu} \subseteq r_{i,\nu} \odot r_{j,\nu} \odot r_{k,\nu}.$$

Case 2. $k < \aleph_0$. First note that by (ii), $\mathbf{inf_0} \subseteq r_{0,0}^3$. Since $1^{\oplus} \in r_{0,0}^3$ as well, and $r_{0,\nu} = \aleph_{\nu} \cdot r_{0,0}$, we conclude that $\mathbf{inf}_{\nu} \subseteq r_{0,\nu}^3$. Indeed, any $t \in \mathrm{inf}_{\nu}$ is representable as $t = \sum_{i \in I} t_i$, where $|I| = \aleph_{\nu}$ and $t_i \in \mathbf{inf_0} \cup \{1^{\oplus}\}$; so $t_i \in r_{0,0}^3$ for all $i \in I$ and we have

$$t = \sum_{i \in I} t_i \in \aleph_{\nu} \cdot (r_{0,0}^3) \subseteq (\aleph_{\nu} \cdot r_{0,0})^3 = r_{0,\nu}^3.$$

By $r_{i,\nu} = r_{i,0} + r_{0,\nu}, r_{j,\nu} = r_{j,0} + r_{0,\nu}$ and (iv) we obtain

$$\begin{aligned}\aleph_0^{\oplus} + r_{0,\nu}^2 &\subseteq r_{i,0} \odot r_{j,0} + r_{0,\nu} \odot r_{0,\nu} \subseteq (r_{i,0} + r_{0,\nu}) \odot (r_{j,0} + r_{0,\nu}) \\ &= r_{i,\nu} \odot r_{j,\nu}.\end{aligned}$$

Hence, by $r_{k,\nu} = r_{k,0} + r_{0,\nu}$ and (ii)

$$\begin{aligned}\mathbf{inf_0} + \mathbf{inf}_{\nu} &\subseteq \aleph_0^{\oplus} \odot r_{k,0} + r_{0,\nu}^2 \odot r_{0,\nu} \\ &\subseteq (\aleph_0^{\oplus} + r_{0,\nu}^2) \odot (r_{k,0} + r_{0,\nu}) = (\aleph_0^{\oplus} + r_{0,\nu}^2) \odot r_{k,\nu}.\end{aligned}$$

Similarly,

$$\mathbf{inf_0} + \aleph_{\nu} \cdot 1^* \subseteq (\aleph_0^{\oplus} + \nu_{0,\nu}^2) \odot \nu_{k,\nu}$$

Also,

$$\mathbf{inf}_{\nu} = (\mathbf{inf_0} + \mathbf{inf}_{\nu}) \cup (\mathbf{inf_0} + \aleph_{\nu} \cdot 1^*)$$

so

$$\mathbf{inf}_{\nu} \subseteq (\aleph_0^{\oplus} + r_{0,\nu}^2) \odot \nu_{k,\nu}.$$

Thus, again

$$\mathbf{inf}_{\nu} \subseteq (\aleph_0^{\oplus} + r_{0,\nu}^2) \odot r_{k,\nu} \subseteq r_{i,\nu} \odot r_{j,\nu} \odot r_{k,\nu}. \quad \square$$

PROPOSITION 3.6. *$R_iR_jR_k =$ INF if $\{i,j,k\}$ contains two integers of different parity.*

PROOF. By Proposition 3.5 $R_iR_jR_k \supseteq$ INF, and by Proposition 3.1 $R_iR_jR_k \subseteq$ INF. $\square$

PROPOSITION 3.7. *$R_iR_jR_k = S_A$ if $i+j+k>0$ and all integers in $\{i,j,k\}$ have the same parity.*

PROOF. For $\nu = 0$ this identity holds by Theorem 3.3, so assume $\nu > 0$. We have to show $\mathbf{tp}_\nu \subseteq r_{i,\nu} \odot r_{j,\nu} \odot r_{k,\nu}$. By Proposition 3.4 we may further assume $k < \aleph_0$. Hence

$$r_{i,\nu} = r_{i,0} + r_{0,\nu}, \quad r_{j,\nu} = r_{j,0} + r_{0,\nu}, \quad r_{k,\nu} = r_{k,0} + r_{0,\nu}.$$

For any ordinal ν, let

$$\mathbf{e}_\nu = \aleph_\nu \cdot 1^* + \{3^*, 5^*, 2^* + 3^*, 3^* + 4^*\}.$$

By Proposition 3.5 and Theorem 2.0 $r^3_{0,\nu} = \mathbf{tp}_\nu \setminus \mathbf{e}_\nu$. Hence, by $\mathbf{e}_\nu = \mathbf{e}_0 + \aleph_\nu \cdot 1^* \subseteq \mathbf{tp}_0 + r^3_{0,\nu}$ and $r^3_{0,\nu} \subseteq \mathbf{tp}_0 + r^3_{0,\nu}$, we have $\mathbf{tp}_0 + r^3_{0,\nu} = \mathbf{tp}_\nu$. Since by Theorem 3.3 $r_{i,0} \odot r_{j,0} \odot r_{k,0} = \mathbf{tp}_0$, we have

$$\begin{aligned}\mathbf{tp}_\nu &= \mathbf{tp}_0 + r^3_{0,\nu} = r_{i,0} \odot r_{j,0} \odot r_{k,0} + r_{0,\nu} \odot r_{0,\nu} \odot r_{0,\nu} \\ &\subseteq (r_{i,0} + r_{0,\nu}) \odot (r_{j,0} + r_{0,\nu}) \odot (r_{k,0} + r_{0,\nu}) \\ &= r_{i,\nu} \odot r_{j,\nu} \odot r_{k,\nu}. \quad \square\end{aligned}$$

(2)(a) and (2)(b) are Propositions 3.6 and 3.7, respectively.

We now prove Theorems 3.2 and 3.3. Recall that for $0 \le i \le \aleph_0$, $r_i = i \cdot 1^* + \aleph_0 \cdot 2^* = i \cdot 1^* + 2^\oplus$.

PROOF OF THEOREM 3.2. Obviously $C \cdot R_k \subseteq \mathrm{INF}$ for all $0 \le k \le \aleph_0$. Indeed, if $\varphi \in S_A$ is finitary, i.e., moves finitely many symbols, $\theta \in C$, then $\psi = \theta\varphi$ must have infinite orbits, and so $\psi \notin R_k$ for all $0 \le k \le \aleph_0$. Thus, $C \cdot R_k$ contains no finitary permutations; i.e., $C \cdot R_k \subseteq \mathrm{INF}$.

$\mathrm{INF} \subseteq C \cdot R_k$ for all $0 \le k \le \aleph_0$ is a consequence of Droste's result:

PROPOSITION 3.8 [**D1**, LEMMA 4.9]. *$\mathrm{INF} \subseteq C \cdot D$ for any class $D \subseteq \mathrm{INF}$.*

PROOF OF THEOREM 3.3. By Proposition 3.5 it is enough to establish:

PROPOSITION 3.9. *Let $\mathbf{fin} = \{t \colon m(t) < |t| = \aleph_0\}$, and let $0 \le i \le j \le k \le \aleph_0$. If*

(*) $\{i,j,k\}$ has no two integers of different parity,

(**) $0 < k$,

then $\mathbf{fin} \subseteq r_i \odot r_j \odot r_k$.

Proposition 3.9 is established via a sequence of reductions.

3.9.1. $r_l \in r_i \odot r_j$ iff $\{i,j,l\}$ does not contain an even integer and an odd integer.

3.9.1 is a restatement of (v).

3.9.2. $\mathbf{fin} \subseteq r_{\aleph_0} \odot r_{\aleph_0}$. Indeed,

$$\mathbf{fin} \subseteq \left\{ t \colon |t| = \sum_{n \in N^+} t(n) = \aleph_0 \right\} = r_{\aleph_0} \odot r_{\aleph_0},$$

where the last equality is a restatement of [**M1**, Corollary 2.4].

3.9.3. We may assume $k < \aleph_0$. Indeed, by (*) and 3.9.1, $r_k \in r_i \odot r_j$, so $r_k^2 = r_k \odot r_k \subseteq r_i \odot r_j \odot r_k$. If $k = \aleph_0$ then, by 3.9.2, $\mathbf{fin} \subseteq r_i \odot r_j \odot r_k$.

3.9.4. $r_0^3 \cap \mathbf{fin} \subseteq r_i \odot r_j \odot r_k$. Indeed, $r_i = r_i + r_0$, $r_j = r_j + r_0$, $r_k = r_k + r_0$; hence

$$r_i \odot r_j \odot r_k = (r_i + r_0) \odot (r_j + r_0) \odot (r_k + r_0) \supseteq r_i \odot r_j \odot r_k + r_0^3.$$

But by $(*)$ and 3.9.1 $r_k \in r_i \odot r_j$, so $1^\oplus \in r_k \odot r_k \subseteq r_i \odot r_j \odot r_k$. Hence $1^\oplus + r_0^3 \subseteq r_i \odot r_j \odot r_k$. But by $\mathbf{fin} \cap r_0^3 \subseteq 1^\oplus + r_0^3$ we have $r_0^3 \cap \mathbf{fin} \subseteq r_i \odot r_j \odot r_k$.

3.9.5. Let $n^+ = n^* + 1^\oplus$ $(n \in \mathbb{N}^+)$. Let $\mathbf{e} = \mathbf{e}_0$ denote the set of four types $\{3^+, 5^+, 2^+ + 3^+, 3^+ + 4^+\}$. If $\mathbf{e} \subseteq r_i \odot r_j \odot r_k$ then $\mathbf{fin} \subseteq r_i \odot r_j \odot r_k$.

Indeed, by Theorem 2.0, $\mathbf{fin} \setminus \mathbf{e} \subseteq r_0^3$ so by 3.9.4, $\mathbf{fin} \setminus \mathbf{e} \subseteq r_i \odot r_j \odot r_k$.

3.9.6. For any $k \in \mathbb{N}$ we have $3^+, 5^+ \in r_k \odot r_k$, $2^+ + 3^+$, $3^+ + 4^+ \in r_{k+2} \odot r_k$. Indeed, $3^* \in (1^* + 2^*)^2$, $5^* \in (1^* + 2 \cdot 2^*)^2$ by

$$(1,2,3) = [(1,2)(3)][(1),(2,3)],$$
$$(1,2,3,4,5) = [(1,2)(3,5)(4)][(1),(2,5)(3,4)].$$

Also, $1^\oplus \in t^2$ whenever $|t| = \aleph_0$, so, since $k - 1 \geq 0$,

$$3^+ = 3^* + 1^\oplus \in (1^* + 2^*) \odot (1^* + 2^*) + r_{k-1} \odot r_{k-1} \subseteq (1^* + 2^* + r_{k-1})^2 = r_k^2,$$
$$5^+ = 5^* + 1^\oplus \in (1^* + 2 \cdot 2^*) \odot (1^* + 2 \cdot 2^*)$$
$$+ r_{k-1} \odot r_{k-1} \subset (1^* + 2 \cdot 2^* + r_{k-1})^2 = r_k^2.$$

Similarly,

$$2^* + 3^* \in (3 \cdot 1^* + 2^*) \odot (1^* + 2 \cdot 2^*),$$
$$(3^* + 4^*) \in (3 \cdot 1^* + 2 \cdot 2^*) \odot (1^* + 3 \cdot 2^*)$$

by

$$(1,2,3)(4,5) = [(1,2)(3)(4)(5)][(1)(2,3)(4,5)],$$
$$(1,2,3)(4,5,6,7) = [(1,2)(3)(4,6)(5)(7)][(1)(2,3)(4,5)(6,7)].$$

Thus

$$2^+ + 3^+ = (2^* + 3^*) + 1^\oplus \in (3 \cdot 1^* + 2^*) \odot (1^* + 2 \cdot 2^*) + r_{k-1} \odot r_{k-1}$$
$$\subseteq (3 \cdot 1^* + 2^* + r_{k-1}) \odot (1^* + 2 \cdot 2^* + r_{k-1}) = r_{k+2} \odot r_k$$

and

$$3^+ + 4^+ = 3^* + 4^* + 1^\oplus \in (3 \cdot 1^* + 2 \cdot 2^* + r_{k-1}) \odot (1^* + 2 \cdot 2^* + r_{k-1}) = r_{k+2} \odot r.$$

3.9.7. $\mathbf{e} \subseteq r_i \odot r_j \odot r_k$ whenever $k \in \mathbb{N}$. Indeed, by 3.9.6 $\mathbf{e} \subseteq r_k^2 \cup (r_{k+2} \odot r_k)$, and by $(*)$ and 3.9.1 $r_k, r_{k+2} \in r_i \odot r_j$, so $\mathbf{e} \subseteq r_i \odot r_j \odot r_k$.

PROOF OF PROPOSITION 3.9. If $k = \aleph_0$, $\mathbf{fin} \subseteq r_i \odot r_j \odot r_k$ by 3.9.2. If $0 < k < \aleph_0$, $\mathbf{fin} \subseteq r_i \odot r_j \odot r_k$ by 3.9.5 and 3.9.7.

The proof of Theorem 3.3 is complete.

4. Odds and ends. 1. We mention some problems suggested by the results of this paper.

We did not evaluate products of involution classes in S_A involving classes moving less than $|A|$ elements. Some such products are, however, readily available. For instance, if $|A| = \aleph_\nu$ and R is an involution class moving $\aleph_\tau$ symbols where $0 \leq \tau < \nu$, then R^2 is the group $S_A^{\tau+1}$ of permutations of A moving at most $\aleph_\tau$ symbols (this follows from [**M1**, Corollary 2.5] and mentioned in [**MO**]); it follows that if

R' is another class moving $\aleph_\sigma$ symbols, $\tau \leq \sigma \leq \nu$, then $RR' = S_A^{\tau+1} \cdot R'$. Thus, products of arbitrary number of involution classes moving infinitely many symbols, can be evaluated easily (compare [**M1**, Theorem A.1, p. 75]). Thus, the following seems to be interesting (and, we believe, tractable):

Problem 1. Let $|A| = \aleph_0$. Determine the products $I_{n_1} \cdots I_{n_k}$, where I_n is an involution class in S_A whose members move $2n$ symbols.

For $k = 2$ this problem is solved in [**M1**]. The powers I_n^k can be recovered from [**M2**, **M3**].

Theorem 3.2 and Proposition 3.8 suggest

Problem 2. Determine the set K all cocs $E \subseteq \mathrm{INF}$ satisfying $E \subseteq D_1 \cdot D_2$ for all cocs D_1, $D_2 \subseteq \mathrm{INF}$.

$C \in K$ by Droste's result [**D1**, Lemma 4.9 (Proposition 3.8)].

2. We complete the proof of the implication of (2) $\Rightarrow$ (1) in §1 by displaying the products of the exceptional classes in S_A by the class of fixed-point-free involutions of A, where $m \leq |A| \leq 2m$, $|A|$ even, and m is the number of symbols moved by a member of the exceptional class under discussion. The proof is completed in verifying that each permutation in each such product has an odd number of orbits of length n for some $n \neq 2$.

This can be checked in the following listing of the twelve relevant sets of types (see §2). The set is denoted on top of a column, under which its members are listed.

TABLE 1

$(1^* + 3^*) \odot 2 \cdot 2^*$	$(3 \cdot 1^* + 3^*) \odot 3 \cdot 2^*$
$1^* + 3^*$	$1^* + 2^* + 3^*$
	6^*

TABLE 2

$(1^* + 5^*) \odot 3 \cdot 2^*$	$(3 \cdot 1^* + 5^*) \odot 4 \cdot 2^*$	$(5 \cdot 1^* + 5^*) \odot 5 \cdot 2^*$
$1^* + 2^* + 3^*$	$1^* + 2 \cdot 2^* + 3^*$	$1^* + 3 \cdot 2^* + 3^*$
$2 \cdot 1^* + 4^*$	$2 \cdot 1^* + 2^* + 4^*$	$2 \cdot 1^* + 2 \cdot 2^* + 4^*$
6^*	$2^* + 6^*$	$2 \cdot 2^* + 6^*$
	$1^* + 7^*$	$1^* + 2^* + 7^*$
	$3^* + 5^*$	$2^* + 3^* + 5^*$
		10^*

TABLE 3

$(1^* + 2^* + 3^*) \odot 3 \cdot 2^*$	$(3 \cdot 1^* + 2^* + 3^*) \odot 4 \cdot 2^*$	$(5 \cdot 1^* + 2^* + 3^*) \odot 5 \cdot 2^*$
$3 \cdot 1^* + 3^*$	$3 \cdot 1^* + 2^* + 3^*$	$3 \cdot 1^* + 2 \cdot 2^* + 3^*$
$1^* + 5^*$	$1^* + 2^* + 5^*$	$1^* + 2 \cdot 2^* + 5^*$
$2^* + 4^*$	$2 \cdot 2^* + 4^*$	$3 \cdot 2^* + 4^*$
	$1^* + 3^* + 4^*$	$1^* + 2^* + 3^* + 4^*$
	8^*	$2^* + 8^*$
		$4^* + 6^*$

TABLE 4

$(1^* + 3^* + 4^*) \odot 4 \cdot 2^*$	$(3 \cdot 1^* + 3^* + 4^*) \odot 5 \cdot 2^*$	$(5 \cdot 1^* + 3^* + 4^*) \odot 6 \cdot 2^*$	$(7 \cdot 1^* + 3^* + 4^*) \odot 7 \cdot 2^*$
$3 \cdot 1^* + 2^* + 3^*$	$3 \cdot 1^* + 2 \cdot 2^* + 3^*$	$3 \cdot 1^* + 3 \cdot 2^* + 3^*$	$3 \cdot 1^* + 4 \cdot 2^* + 3^*$
$1^* + 3^* + 4^*$	$1^* + 2^* + 3^* + 4^*$	$1^* + 2 \cdot 2^* + 3^* + 4^*$	$1^* + 3 \cdot 2^* + 3^* + 4^*$
$1^* + 2^* + 5^*$	$1^* + 2 \cdot 2^* + 5^*$	$1^* + 3 \cdot 2^* + 5^*$	$1^* + 4 \cdot 2^* + 5^*$
$2 \cdot 2^* + 4^*$	$3 \cdot 2^* + 4^*$	$4 \cdot 2^* + 4^*$	$5 \cdot 2^* + 4^*$
$2 \cdot 1^* + 6^*$	$2 \cdot 1^* + 2^* + 6^*$	$2 \cdot 1^* + 2 \cdot 2^* + 6^*$	$2 \cdot 1^* + 3 \cdot 2^* + 6^*$
8^*	$2^* + 8^*$	$2 \cdot 2^* + 8^*$	$3 \cdot 2^* + 8$
	$1^* + 3 \cdot 3^*$	$1^* + 2^* + 3 \cdot 3^*$	$1^* + 2 \cdot 2^* + 3 \cdot 3^*$
	$2 \cdot 1^* + 3^* + 5^*$	$2 \cdot 1^* + 2^* + 3^* + 5^*$	$2 \cdot 1^* + 2 \cdot 2^* + 3^* + 5^*$
	$2 \cdot 1^* + 2^* + 6^*$	$2 \cdot 1^* + 2 \cdot 2^* + 6^*$	$2 \cdot 1^* + 3 \cdot 2^* + 6^*$
	$4^* + 6^*$	$2^* + 4^* + 6^*$	$2 \cdot 2^* + 4^* + 6^*$
	$3^* + 7^*$	$2^* + 3^* + 7^*$	$2 \cdot 2^* + 3^* + 7^*$
	$1^* + 9^*$	$1^* + 2^* + 9^*$	$1^* + 2 \cdot 2^* + 9^*$
		$1^* + 5^* + 6^*$	$1^* + 2^* + 5^* + 6^*$
		$2 \cdot 3^* + 6^*$	$2^* + 2 \cdot 3^* + 6^*$
		$1^* + 3^* + 8^*$	$1^* + 2^* + 3^* + 8^*$
		12^*	$2^* + 12^*$
			$6^* + 8^*$

REFERENCES

[**B**] E. Bertram, *On a theorem of Schreier and Ulam for countable permutations*, J. Algebra **24** (1973), 316–322.

[**Bo**] G. Boccara, *Cycles comme produit de deux permutations de classes donnees*, Discrete Math. **38** (1982), 129–142.

[**D1**] M. Droste, *Products of conjugacy classes of the infinite symmetric groups*, Discrete Math. **47** (1983), 35–48.

[**D2**] ——, *Cubes of conjugacy classes covering the infinite symmetric groups*, Trans. Amer. Math. Soc. **288** (1985), 381–393.

[**D3**] ——, *Classes of universal words for the infinite symmetric groups*, Algebra Universalis **20** (1985), 205–216.

[**DG**] M. Droste and R. Göbel, *On a theorem of Baer, Schreier and Ulam for permutations*, J. Algebra **58** (1979), 282–290.

[**Dv**] 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-Verlag, 1985.

[**G**] A. B. Gray, *Infinite symmetric and monomial groups*, Ph.D. Thesis, New Mexico State Univ., Las Cruces, N.M., 1960.

[**MO**] G. Moran, *The algebra of reflections of an infinite set*, Notices Amer. Math. Soc. **73T** (1973), A193.

[**M1**] ——, *The product of two reflection classes of the symmetric group*, Discrete Math. **15** (1976), 63–77.

[**M2**] ——, *Reflection classes whose cubes cover the alternating group*, J. Combin. Theory Ser. A **21** (1976), 1–19.

[**M3**] ——, *Permutations as products of k conjugate involutions*, J. Combin. Theory Ser. A **19** (1975), 240–242.

[**M4**] ——, *Trees and the bireflection property*, Israel J. Math. **41** (1982), 244–260.

[**M5**] ——, *Of planar Eulerian graphs and permutations*, Trans. Amer. Math. Soc. **287** (1985), 323–341.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF HAIFA, MOUNT CARMEL, HAIFA 31999, ISRAEL