Permuting mechanisms and closed classes of permutations

M.D. Atkinson
Robert Beals

December 16, 1998

1 Introduction

A *permuting mechanism* M is a device that accepts any finite input sequence of objects (normally denoted by $1, 2, \ldots$) and produces a permutation of these objects. We let $\text{perm}(M)$ denote the set of possible permutations that M might produce.

Examples

1. A *riffle shuffler* divides the input sequence into two segments $1, 2, \ldots, m$ and $m+1, \ldots, n$ and then interleaves them in any way. Thus $\text{perm}(M) = \{1, 12, 21, 123, 132, 213, 231, 312, 1234, 1243, 1342, \ldots \text{etc.}\}$
2. A *stack* receives members of the input sequence and outputs them under a last-in-first-out discipline
3. A *transportation network* [2] is any finite directed graph with a node to represent the input queue and a node to represent the output queue. The other nodes can each hold one of the input objects and the objects are moved around the graph until they emerge at the output node

All of these examples are *hereditary* in that a permutation effected on any subsequence of the input is a permutation that could be produced if the subsequence was the entire input sequence. For example, in any riffle shuffle of $1, 2, \ldots, n$ every subsequence of the input is permuted as though by a riffle shuffle.

We say that two sequences $[\alpha_1, \ldots, \alpha_n]$ and $[\beta_1, \ldots, \beta_n]$ are *order isomorphic* if $\alpha_i < \alpha_j$ precisely when $\beta_i < \beta_j$. Then, for two permutations π, σ, we define $\pi \preceq \sigma$, and say that π is *involved* in σ if σ has a subsequence which is order isomorphic to π. A *closed* class X of permutations is a class with the property

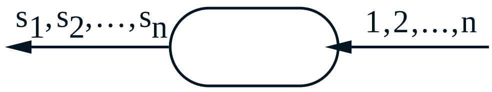

Figure 1: A permuting mechanism

$\tau \in X$ and $\sigma \preceq \tau$ implies $\sigma \in X$. Clearly, if M is an hereditary permuting mechanism then perm(M) is closed. On the other hand, given a closed class X, we can simply define a black box permuting mechanism M for which perm(M) = X and then M will be hereditary.

The permuting mechanisms which arise in practice generally process inputs of all lengths and so give rise to infinite closed classes. The two simplest infinite closed classes are I, the set of all identity permutations $[1, 2, \ldots, n]$, and R, the set of all reversed identities $[n, n-1, \ldots, 1]$.

Lemma 1 *Every infinite closed class contains I or R.*

Proof: If the closed class X contains neither I nor R then, for some fixed r, s, X contains neither $[1, 2, \ldots, r]$ nor $[s, s-1, \ldots, 1]$. By the closure property the permutations of X will have neither an increasing subsequence of length r nor a decreasing subsequence of length s. A theorem of Erdös and Szekeres [4] then implies that all permutations in X have length at most $(r-1)(s-1)$. ■

Very important in the study of closed classes is the idea of a basis. The *basis* of a closed class X is the set of permutations σ minimal with respect to the property $\sigma \notin X$. The basis of a closed class is important because of the following lemma, a direct consequence of the definition, which shows that a closed class is determined by its basis.

Lemma 2 *If X is a closed class with basis B then $\sigma \in X$ if and only if $\beta \not\preceq \sigma$ for all $\beta \in B$.*

Notice that the basis of a closed class necessarily consists of permutations incomparable with respect to $\preceq$. Also, in view of the lemma, every set of incomparable permutations is the basis of some closed class. In [6, 7] examples of infinite sets of incomparable permutations were given. It follows immediately that there are uncountably many closed classes of which but countably many have a finite basis. It is therefore a significant question to distinguish the finitely based closed classes from those which are not finitely based.

This paper is concerned with three constructions which correspond to combining permuting mechanisms in series and in parallel, and endowing them with feedback. In particular we study how they respect the finite basis property.

Let D, E be hereditary permuting mechanisms with associated closed classes X, Y. The serial composition of D with E is shown in Figure 2 and it is clear

Figure 2: Serial composition of permuting mechanisms

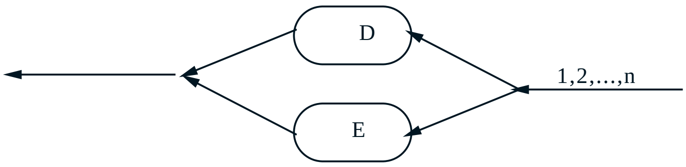

Figure 3: Parallel composition of permuting mechanisms

that the corresponding class of permutations is the serial composition of X and Y defined as $XY = \{\theta | \theta = \sigma\tau, \sigma \in X, \tau \in Y\}$

The parallel composition of two hereditary permuting mechanisms D, E with associated closed classes X, Y is shown in Figure 3. This mechanism begins by partitioning the input into two subsequences which are then fed into D and E whose outputs are then merged. We denote the set of permutations so obtained by $X \sqcup Y$, the parallel composition.

Intuitively it is clear that the serial and parallel compositions of hereditary permuting mechanisms is also hereditary. A formal proof of this is given in [1].

One might hope that the serial composition of two finitely based closed classes was also finitely based but this is false in general [1]. Indeed, very little is known about when a serial composition is finitely based; for example it is not even known whether the class corresponding to two stacks in series is finitely based. In section 2 we give some special cases of finitely based serial compositions. We do not know whether the parallel composition of finitely based classes is always finitely based but it seems unlikely. In section 3 we give some finitely based parallel compositions.

Suppose that M is a permuting mechanism and we 'enhance' it by allowing the output sequence to be channelled back into the input as many times as we like (see Figure 4) and call the new permuting mechanism M^*. Let $X = \mathrm{perm}(M)$. Then M^* can produce all the permutations in X (by disregarding the feedback option), all the permutations of X^2 by feeding the output of M once more through M, and all other powers X^k by $k-1$ feedbacks. Therefore $X^* = \mathrm{perm}(M^*) = X \cup X^2 \cup X^3 \ldots$ and this is closed. Clearly $X^* \cap S_n$ is a group for all n. In section 4 we give a complete characterisation of those closed classes Z with the property that $Z \cap S_n$ is a group for all n. We shall see that the condition is very restrictive.

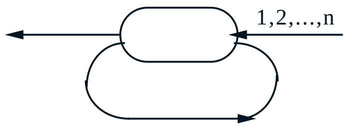

Figure 4: A permuting mechanism with feedback

We end this section with some notation that will be useful elsewhere in the paper.

If σ is a permutation of $\{1, 2, \ldots, n\}$ and $1 \le i \le n$ then we let $\sigma - i$ denote the permutation obtained from σ by deleting the ith symbol (image of i) and relabelling to obtain a permutation. Let $C(i, n)$ be the cycle $(i, i+1, \ldots, n)$. Then, by a slight abuse of notation in which we identify $\sigma - i$ with the permutation of degree n that fixes n and otherwise acts as $\sigma - i$, it is easy to see that $\sigma - i = C(i, n)\sigma C(i^\sigma, n)^{-1}$. Direct calculation then confirms that

Lemma 3 $(\sigma - i)(\tau - i^\sigma) = \sigma\tau - i$

2 Serial composition

Our first example of a finitely based serial composition class features the closed class C whose permutations of length n are $[1, 2, \ldots, n]$ and $[n, 1, 2, \ldots, n-1]$ (the identity permutation together with an n-cycle). C is a finitely based class with basis $\{[3, 2, 1], [2, 3, 1], [1, 3, 2], [2, 1, 3]\}$.

Theorem 1 *If D is any finitely based closed class then CD is finitely based*

PROOF: Let $\pi = p_1, p_2 \ldots, p_n$ be a permutation of degree n. Then $\pi \notin CD$ if and only if $p_1, p_2, \ldots, p_n \notin D$ and $p_2, p_3, \ldots, p_n, p_1 \notin D$. We choose a smallest such π (a basis element of CD). Then there exists a subsequence σ of $p_1, p_2, \ldots, p_n$ order isomorphic to a basis element of D and a subsequence τ of $p_2, p_3, \ldots, p_n, p_1$ also order isomorphic to a basis element of D.

If σ were contained in $p_2, \ldots, p_n$ then it would be contained in both $p_1\sigma$ and σp_1 and $p_1\sigma$ (a subsequence of π) would also not belong to CD. Then, by the minimality of π, we would have $\pi = p_1\sigma$. Since D is finitely based there are only a finite number of permutations π of this type. A similar argument applies if τ is contained in $p_2, \ldots, p_n$.

We may now assume that $\sigma = p_1\lambda$ and $\tau = \mu p_1$ for subsequences λ and μ of $p_2, \ldots, p_n$. Now let ω be the union of λ and μ. It follows that σ is a subsequence of $p_1\omega$ and that τ is a subsequence of ωp_1. Thus neither of $p_1\omega$ and ωp_1 are in D and, by the minimality of π again, $\pi = p_1\omega$ and so is of bounded length. ■

The class C has only two permutation of each length; it is a *bounded* class. One of the simplest unbounded closed classes is the *Coxeter* class in which the permutations of degree n are the identity permutation and the $n-1$ transpositions $\xi_i = (i, i+1)$. This is a finitely based class and the basis is the set $\{[3,2,1],[3,1,2],[2,3,1],[2,1,4,3]\}$.

Theorem 2 *Let X be the Coxeter class and Y any finitely based closed class. Then XY is finitely based.*

Proof: Let $\pi = p_1, p_2, \ldots, p_n$ be a permutation of degree n. Then $\pi \notin XY$ if and only if $\xi_i \pi \notin Y$ for all $i = 1, \ldots, n-1$. We choose π to be minimal with respect to this property, that is, π is a basis element of XY. Certainly $\pi \notin Y$ and so it has some subsequence $\beta = b_1 b_2 \ldots b_k$ which is order isomorphic to a basis element of Y; and, as Y is finitely based, k is bounded independently of n. Since β is a subsequence of π, π has a segment of the form $\beta_1\gamma_1\beta_2\ldots\beta_{r-1}\gamma_{r-1}\beta_r$ where each β_i, γ_i is a non-empty segment of π, $\beta_1\beta_2\ldots\beta_r = \beta$, and $r \le k$. For each $i = 1, 2, \ldots, r-1$ let g_i be an element of γ_i.

Consider any $b_j b_{j+1}$ contained in some β_i. The interchange of b_j and b_{j+1} in π results in a permutation that is not in Y and so there must be subsequences λ_j, μ_j of π such that $\lambda_j b_j b_{j+1} \mu_j$ is a subsequence of π and $\lambda_j b_{j+1} b_j \mu_j$ is order isomorphic to a basis element of Y (and so of length bounded independently of n).

Now define θ to be the union of all β_i, g_i and all λ_j, μ_j. This subsequence of π is not order isomorphic to any permutation of XY. To see this we consider the effect of interchanging any two adjacent symbols of θ. If the adjacent symbols are not adjacent in some β_i the result will have β as a subsequence. On the other hand, if the adjacent symbols are of the form b_j, b_{j+1} within some β_i, the result will have $\lambda_j b_{j+1} b_j \mu_j$ as a subsequence. In each case, the result has a subsequence order isomorphic to a basis element of Y. Thus θ is order isomorphic to a permutation which does not lie in XY and, by the minimality of π, we have $\pi = \theta$. However, θ has been defined as a union of a bounded number of sequences of bounded length; therefore there are only a finite number of possibilities for π. ■

3 Parallel Composition

Parallel composition appears to be a slightly easier notion than serial composition. For example, it is commutative while serial composition is not. Moreover, while we have not been able to find a method for producing explicit elements not in XY from bases of X and Y we have the following argument for $X \sqcup Y$.

If σ and τ are permutations of m and n elements respectively define $\sigma \otimes \tau$ as a permutation $\rho = r_1, \ldots, r_{mn}$ of degree mn where each of the n segments

$[r_{mi+1}, \ldots, r_{mi+m}], 0 \leq i < n$ is a rearrangement of $\{mi+1, mi+2, \ldots, mi+m\}$ order isomorphic to σ and one (and so every) sequence formed by choosing a representative from among each $[r_{mi+1}, \ldots, r_{mi+m}]$ is order isomorphic to τ. It is then straightforward to confirm

Proposition 1 *Suppose that $\sigma \notin X$ and $\tau \notin Y$ then $\sigma \otimes \tau \notin X \sqcup Y$*

Simple examples of the parallel composition are $I \sqcup I$ which is the set of all permutations with no decreasing subsequence of length 3, and $I \sqcup R$ which is the set of permutations which are the merge of an increasing sequence and a decreasing sequence; the latter class has recently been studied in [3, 5].

Lemma 4 *Let F_k denote the (finite) closed class of all permutations of length at most k and let X be any closed class. Then*

1. *$X \sqcup F_{m+n} = X \sqcup F_m \sqcup F_n$*
2. *If X is finitely based so is $X \sqcup F_n$ for all n.*

PROOF: The first part follows directly from the definitions. For the second part it is enough to prove that $X \sqcup F_1$ is finitely based since $X \sqcup F_n = (X \sqcup F_{n-1}) \sqcup F_1$. Let π be a basis element of $X \sqcup F_1$ and let $\mathcal{B}$ denote the set of all subsequences of π that are order isomorphic to basis elements of X. Since X is finitely based, all subsequences in $\mathcal{B}$ have length at most t for some fixed t.

Since $\pi \notin X \sqcup F_1$, $\pi - i \notin X$ for all $i = 1, \ldots, \text{length}(\pi)$, and so each $\pi - i$ contains some subsequence in $\mathcal{B}$. In particular, it follows that the intersection of all the sequences in $\mathcal{B}$ is empty since, if π_j were in this intersection, $\pi - j$ could not have a subsequence in $\mathcal{B}$.

It follows that we may choose subsequences $\beta_1, \beta_2, \ldots, \beta_t \in \mathcal{B}$ such that, for each s, $\cap_{i=1}^{s+1} \beta_i$ is properly contained in $\cap_{i=1}^{s} \beta_i$ and therefore $\cap_{i=1}^{t} \beta_i$ is empty. Put $\beta = \cup_{i=1}^{t} \beta_i$.

Then β clearly has the property that every $\beta - i$ has at least one of $\beta_1, \beta_2, \ldots, \beta_t$ as a subsequence. Therefore, if $\beta^\star$ denotes the permutation order isomorphic to β then $\beta^\star - i \notin X$ for all i and so $\beta^\star \notin X \sqcup F_1$. But $\beta^\star \preceq \pi$ and, as π is a basis element of $X \sqcup F_1$, $\beta^\star = \pi$ and so π has length at most t^2. Since there are only a finite number of such permutations π the result is proved. ■

4 Feedback

In this section we investigate when a closed class X can have the property that $X(n) = X \cap S_n$ is a group for all n. We call such a class a *group class*. Group classes arise out of permuting mechanisms with feedback. We shall see that the sequence of groups $X(n)$ eventually settles down to one of the following families of groups:

1. For some fixed k and ℓ, $X(n) = S_k \times S_\ell$, acting as S_k on $\{1, \dots, k\}$, fixing each point in $\{k+1, \dots, n-\ell\}$, and acting as S_ℓ on $\{n-\ell+1, \dots, n\}$.
2. The cyclic groups: $X(n) = \langle [2, 3, 4, \dots, n, 1] \rangle$.
3. The full symmetric group: $X(n) = S_n$.
4. The group generated by any of the above (with $k = \ell$ in example 1) together with the reversals R.

Our results also give information about the sort of groups $X(n)$ which can arise before convergence to one of the above types.

4.1 Intransitive groups

For each n we define k_n in terms of the orbit $1^{X(n)}$ of $X(n)$: $k_n + 1$ is the smallest point not in this orbit. In a similar way we define ℓ_n using the orbit of $X(n)$ containing n: $n - \ell_n$ is the largest point not in this orbit.

We first note that (k_n) is a non-increasing sequence. For, if $1 \le j \le k_n$, then $1^g = j$ for some $g \in X(n)$. Then, as $(k_n+1)^g > k_n$, $1^{g-k_n} = j$. This shows that $k_{n-1} \ge k_n$. A similar argument shows that (ℓ_n) is non-increasing. Since the two sequences $(k_n), (\ell_n)$ are non-increasing and bounded below they have limits k, ℓ. Therefore we have

Lemma 5 *There exist constants k, ℓ, N such that, for all $n \ge N$, $\{1, 2, \dots, k\} \subseteq 1^{X(n)}$, $k+1 \notin 1^{X(n)}$ and $\{n-\ell+1, \dots, n\} \subseteq n^{X(n)}$, $n - \ell \notin n^{X(n)}$*

Lemma 6 *Let $t-1, t$ be in different orbits of $X(n-1)$ and let $g \in X(n)$. Then either*

1. *$t^g = t$ and g preserves $\{1, \dots, t-1\}$ and $\{t+1, \dots, n\}$ or*
2. *$t^g = n-t+1$, $(n-t+1)^g = t$ and g interchanges $\{1, \dots, t-1\}$ and $\{n-t+2, \dots, n\}$*

Proof: Let $i, j \in \{1, \dots, n\}$ be such that $i < t < j$. Then, for any $g \in X(n)$, $(t-1)^{g-i} \ne t^{g-j}$. This can only occur if $i^g < t^g < j^g$ or $j^g < t^g < i^g$. In other words, the triple i, t, j is monotonically mapped by any $g \in X(n)$. Since the choices of i and j were independent, it follows that any $g \in X(n)$ either preserves the sets $\{1, \dots, t-1\}$ and $\{t+1, \dots, n\}$ or maps $\{1, \dots, t-1\}$ onto $\{t^g+1, \dots, n\}$. In the first case, $t^g = t$ and in the second case $t^g = n-t+1$. However, in the second case we can consider $h = g^2$ and conclude that $t^h = t$ and $\{1, \dots, t-1\}^h = \{1, \dots, t-1\}$ which completes the proof. ■

Lemma 7 *There exists a constant $M > N$ such that either*

1. *For all $n \geq M$, $1^{X(n)} = \{1, \ldots, k\}$ and $n^{X(n)} = \{n - \ell + 1, \ldots, n\}$ or*
2. *$k = \ell$ and for all $n \geq M$ $1^{X(n)} = \{1, \ldots, k, n - k + 1, \ldots, n\}$*

Proof: Let $n \geq N$ and let $g \in X(n)$. By Lemma 5 and Lemma 6 we have either

(i) $(k+1)^g = k+1$ and $\{1, \ldots, k\}^g = \{1, \ldots, k\}$ or

(ii) $(k+1)^g = n-k$ and $\{1, \ldots, k\}^g = \{n-k+1, \ldots, n\}$

Suppose that (i) holds for all $g \in X(n)$ (so that $1^{X(n)} = \{1, \ldots, k\}$). Then k and $k+1$ are in different orbits of $X(n)$ and by Lemma 6 again we have, for all $h \in X(n+1)$, either $(k+1)^h = k+1$ or $(k+1)^h = n+1-(k+1)+1$ and $(n+1)^h < n+1-k$. But the last alternative is impossible for it would imply that the element $h - (n+1) \in X(n)$ maps $k+1$ to $n-k$, a contradiction.

This proves that either $\{1, \ldots, k\}$ is the entire orbit of 1 under $X(n)$ for all n from some point on, or that this set is never the entire orbit for $n \geq N$. In the former case we can consider $n-\ell$ and $n-\ell+1$, which are not in the same orbit of $X(n)$, and apply Lemma 6. This gives the first alternative of the lemma. In the latter case, the element g satisfying (ii) above always exists and the second alternative must hold. ■

Lemma 8 *If the first case of Lemma 7 holds then there exists K such that, for all $n > K$, $X(n)$ fixes all points in $k+1, \ldots, n-\ell$. If the second case holds then there exists K such that for all $n > K$ and all $g \in X(n)$ either g fixes every point in $k+1, \ldots, n-k$ or g maps every such point s to $n-s+1$.*

Proof: Suppose that the first alternative of Lemma 7 holds. Suppose that $n \geq M$. Then k and $k+1$ are in different orbits of $X(n)$ as are $n-\ell$ and $n-\ell+1$. Hence, by Lemma 6, both $k+1$ and $n-\ell+1$ are fixed in $X(n+1)$. But then $k, k+1, k+2$ are in different orbits of $X(n+1)$ and so $k+1$ and $k+2$ are fixed in $X(n+2)$; similarly, $n-\ell+1$ and $n-\ell+2$ are fixed in $X(n+2)$. Continuing this argument we see that, whenever $n > 2M$, all of the points in $k+1, \ldots, n-\ell$ are fixed in $X(n)$.

If the second alternative of Lemma 7 holds the same argument shows that if $g \in X(n)$ and $k+1 \leq s \leq n-k$ then, provided $n > 2M$, $s^g = s$ or $s^g = n-s+1$. However, Lemma 6 proves that $s^g = s$ precisely when $\{1, 2, \ldots, k\}$ is preserved by g. Thus $s^g = s$ for all $k+1 \leq s \leq n-k$ or $s^g = n-s+1$ for all such s. ■

Theorem 3 *Let X be a group class in which not every $X(n)$ is transitive. Then one of the following holds:*

1. *$X(n) = S_k \times S_\ell$, acting as S_k on $\{1, 2, \ldots, k\}$ and as S_ℓ on $\{n-\ell+1, n-\ell+2, \ldots, n\}$, and fixing the remaining points, for all $n \geq n_0$.*

2. *$X(n)$ is generated by $R(n)$ and the group $S_k \times S_k$ acting as in the previous case (with $k = \ell$) for all $n \geq n_0$.*

Proof: Consider values of n large enough that the conclusions of Lemma 8 hold. Suppose first that $X(n)$ fixes every point from $k+1$ to $n-\ell$. In $X(n+1)$ there are permutations g_i that map the symbol k to each of $1, 2, \ldots, k$ in turn (and fix $k+1$). But then the permutations $g_i - 1 \in X(n)$ fix k and map $k-1$ to each of $1, \ldots, k-1$. Thus $X(n)$ is doubly transitive on its orbit $\{1, \ldots, k\}$. A similar argument with the groups $X(n+2), \ldots, X(n+k-1)$ establishes the $k-$transitivity of $X(n)$ on $\{1, \ldots, k\}$ so it acts on this orbit as the full symmetric group. In the same way $X(n)$ also acts on the orbit $\{n-\ell+1, \ldots, n\}$ as the full symmetric group. Moreover, as $X(n+\ell) - \{n+1, \ldots, n+\ell\} \subseteq X(n)$ fixes $n-\ell+1, \ldots, n$ and acts as S_k on $\{1, \ldots, k\}$ we have $X(n) = S_k \times S_\ell$.

Now suppose that the second case of Lemma 8 holds. Then $X(n)$ has a subgroup $Y(n)$ of index 2 fixing all of $k+1, \ldots, n-k+1$ and the above arguments prove that $Y(n) = S_k \times S_k$ acting in the natural way on $\{1, \ldots, k, n-k+1, \ldots, n\}$. By Lemma 8 the single permutation of $R(n)$ lies in $X(n) \setminus Y(n)$ and the proof is complete. ■

4.2 Transitive groups

We denote by Z_n (D_n respectively) the permutation group of degree n generated by the n-cycles $(1, 2, \ldots, n)$ ($(1, 2, \ldots, n)$ and $(n, n-1, \ldots, 2, 1)$ respectively). We call these groups the *natural* cyclic and dihedral groups of degree n.

Also, we say that the integers y, z are *consecutive modulo n* if $\{y, z\}$ is a consecutive pair of elements in the list $1, 2, \ldots, n, 1$. Then we observe

Lemma 9 *Let G be a transitive group of degree n. Then G is the natural cyclic or dihedral group if and only if for all $g \in G$ and all $1 \leq x < n$, x^g and $(x+1)^g$ are consecutive modulo n.*

Lemma 10 *A permutation group G of degree n that contains cycles $g = (1, 2, \ldots, n)$ and $h = (1, 2, \ldots, m)$ with $m < n$ contains the alternating group of degree n.*

Proof: The group is obviously transitive. Indeed, since it contains all cycles of the form $(i, i+1, \ldots, i+m-1)$ (conjugates of h under powers of g) it is easy to see that the stabilizer of the point n is transitive on the remaining points:– that is, G is doubly transitive. The commutator $[g, h]$ is the $3-$cycle $(1, 2, m+1)$. But a doubly transitive group containing a $3-$ cycle necessarily contains A_n. ■

Lemma 11 *Suppose that $g \in X(n)$ and that $1 \leq x \leq n-1$. Let $u = x^g$, v=$(x+1)^g$ and let $h = (g-x)^{-1}(g-(x+1)) \in X(n-1)$. Then h is the cycle $(y, y+1, \ldots, z-1)$ if $y < z$ and the cycle $(z, z+1, \ldots, y-1)$ if $y > z$. In addition, if y and z are not consecutive modulo n then $X(n-2)$ contains a transposition of the form $(t, t+1)$.*

PROOF: The first statement follows directly from the definitions. For the second part, note that both h and h^{-1} lie in $X(n-1)$ since $X(n-1)$ is a group. Without loss in generality assume that $h = (y, y+1, \ldots, z-1)$. Since y and z are not consecutive modulo n, h is not the identity nor the permutation $(1, 2, \ldots, n-1)$. If $y \neq 1$ then $(y-1)^h = y-1$ and $y^h = y+1$ so, by part 1, $X(n-2)$ contains $(h-(y-1))^{-1}(h-y) = (y-1, y)$. On the other hand, if $z \neq n$ then $z^{h^{-1}} = z$ and $(z-1)^{h^{-1}} = z-2$ so that, again by part 1, $X(n-2)$ contains $(z-2, z-1)$. ■

Lemma 12 *If $X(n)$ is transitive for all n then each $X(n)$ contains the cycle $(1, 2, \ldots, n)$.*

PROOF: Suppose, for a contradiction, that there is some integer n_1 for which $X(n_1)$ does not contain $(1, 2, \ldots, n_1)$. Let p be any prime larger than n_1 and put $q = p+2$. Then $X(q)$ also does not contain a cycle $(1, 2, \ldots, q)$ and so it is not the natural cyclic or dihedral group of degree q. Hence, by Lemma 9 $X(q)$ has a permutation g for which there are two points $x, x+1$ with $u = x^g$ and $v = (x+1)^g$ not consecutive modulo q.

However, Lemma 11, now shows that $X(p) = X(q-2)$ contains a transposition of the form $(t, t+1)$. But a transitive group of prime degree containing a transposition is necessarily the full symmetric group; therefore it contains $(1, 2, \ldots, p)$. Therefore, $X(n_1)$ must contain $(1, 2, \ldots, n_1)$, a contradiction. ■

A permutation group G of degree n with an $n-$cycle $(1, 2, \ldots, n)$ is said to be *peculiar* if

$$H = \langle g - x | g \in G, 1 \leq x \leq n \rangle \neq S_{n-1}$$

The natural cyclic and dihedral groups of degree n are both peculiar (the group H being cyclic or dihedral of degree $n-1$).

Lemma 13 *If G is a peculiar group of degree n and not cyclic or dihedral then n is even, G has a block system $\{$even points$\}$, $\{$odd points$\}$ and the stabilizer of a block is the set of even permutations of G. Conversely, any group with a cycle $(1, 2, \ldots, n)$ and satisfying these conditions is peculiar. For peculiar groups which are not cyclic or dihedral the group H is the alternating group A_{n-1}.*

PROOF: As G contains $c = (1, 2, \ldots, n)$ H must contain $c-n = (1, 2, \ldots, n-1)$. Now let $g \in G$ and $1 \leq x < n$ and put $u = x^g, v = (x+1)^g$. Let $h(g, x) =$

$(g-x)^{-1}(g-(x+1))$ be a cycle of length $m(g,x) = |u-v|$ (see Lemma 11). Since G is neither cyclic nor dihedral, at least one of these cycle lengths must lie strictly between 1 and $n-1$; therefore, by Lemma 10, H contains A_{n-1}. By hypothesis, however, H is not the full symmetric group and therefore both $n-1$ and all $m(g,x)$ must be odd. The latter condition implies that the elements of $1^g, 2^g, \ldots, n^g$ are alternately even and odd. Hence each element g maps odd points to odd points or maps odd points to even points, giving the required block system.

Since $h(g,x)$ is even, $g-x$ and $g-(x+1)$ have the same parity. This parity is also the parity of $g-n$ and is easily seen to be the parity of g minus the parity of n^g. But this means that g has even parity if and only if it fixes the set of even points. ■

Theorem 4 *Let X be a group class in which every $X(n)$ is transitive. Then, the sequence of groups $X(n)$ begins with a number of symmetric groups (possibly none or an infinite number), then has at most one alternating group which must then be followed by a peculiar group or has at most one group that properly contains Z_n but is not dihedral, then has a number of natural dihedral groups (possibly none or an infinite number), and finally has a number of natural cyclic groups (none or an infinite number).*

PROOF: Since X is closed

$$\langle g-x | g \in X(n), 1 \leq x \leq n \rangle \subseteq X(n-1) \text{ for all } n$$

Suppose that not every $X(n)$ is the symmetric group S_n and let $X(m-1)$ be the first that is not. Then $X(m)$ is peculiar and either

1. $X(m)$ is an imprimitive group of the type appearing in Lemma 13 and $X(m-1)$ is the alternating group, or
2. $X(m)$ is the natural cyclic or dihedral group

In either case, by Lemma 13 again, $X(n)$ is the natural cyclic or natural dihedral group for all $n \geq m+1$. Finally we note that, if $X(n)$ is the natural cyclic group then $X(n+1)$ is also the natural cyclic group. ■

References

[1] M.D. Atkinson, R. Beals: Finiteness conditions on closed classes of permutations, in preparation.

[2] M.D. Atkinson, M.J. Livesey, D. Tulley: Permutations generated by token passing in graphs, Theoretical Computer Science 178 (1997), 103-118.

[3] M. D. Atkinson: Permutations which are the union of an increasing and a decreasing subsequence, Electronic J. Combinatorics 5 (1998), Paper R6 (13 pp.).

[4] D. I. A. Cohen: *Basic Techniques of Combinatorial Theory*, John Wiley & Sons, New York, 1978.

[5] A.E. Kézdy, H.S. Snevily, C. Wang: Partitioning permutations into increasing and decreasing subsequences, J. Combinatorial Theory A 74 (1996), 353-359.

[6] V.R. Pratt: Computing permutations with double-ended queues, parallel stacks and parallel queues, Proc. ACM Symp. Theory of Computing 5 (1973), 268-277

[7] R.E. Tarjan: Sorting using networks of queues and stacks, Journal of the ACM 19 (1972), 341-346.