Permutation involvement and groups

M.D. Atkinson
Department of Computer Science
University of Otago
Dunedin, New Zealand
mike@cs.otago.ac.nz
Robert Beals
Department of Mathematics, University of Arizona
617 North Santa Rita, Tucson, Arizona 85721, USA
beals@math.arizona.edu

Abstract

Sets of permutations which are closed under both pattern involvement and multiplication are classified.

Keywords Permutation, forbidden, restricted, group

1 Introduction

Over the last few years there has been much interest in both combinatorics and computer science in the notion of permutation involvement. Although we shall often use cycle notation for permutations, involvement is best described by writing permutations σ in *image* form as a sequence $[1^\sigma, 2^\sigma, \ldots]$. We recall that a permutation π is *involved* in a permutation σ if, when written in image form, σ has a subsequence which is order isomorphic to π. For brevity we generally write $\pi \preceq \sigma$. For example, with $\sigma = [5, 1, 4, 2, 3]$ and $\pi = [1, 3, 2]$, we have $\pi \preceq \sigma$ by virtue of the subsequence $[1, 4, 3]$ of σ. Trivially, involvement is a partial order on the set of all finite permutations. Interest usually centres on *closed* sets of permutations: those sets X for which $\sigma \in X$ and $\pi \preceq \sigma$ imply $\pi \in X$.

In combinatorics closed sets arise in the study of sets defined by forbidden patterns. Often one wants to know how many permutations fail to involve all the permutations of some given set. Examples of this type of investigation are [3, 5, 6, 8]. In computer science closed sets arise in the study of data movement in various environments. Examples of this are [1, 2, 4, 7].

Figure 1: A permuting environment

In this paper we shall study a new question on closed sets. For which closed sets do the permutations of each degree form a group? Our main result is a complete answer to this question. Before giving the details of our methods we pause to motivate the question. Of course, it is about two notions, permutation involvement and permutation composition, which are each studied intensively already; in one sense therefore the question is quite a natural one. But the combination of these two notions has at least one point of independent interest.

Suppose we have an environment through which can pass any finite sequence of items $1, 2, \ldots, n$ and that the effect of the environment is to permute this sequence in one of a number of ways (see Figure 1). Roughly speaking, so long as an environment processes its input by re-ordering it in a way oblivious to the actual item values, and permutes subsequences in the way that they would be permuted if the other items were omitted, then the permutations effected will constitute a closed set. For example, all the network mechanisms described in [2] have this property. Three further examples are

1. a stack, where the numbers $1, 2, \ldots, n$ are subjected to a series of push and pop operations to generate an output,
2. a riffle shuffler, which cuts a deck of cards $1, 2, \ldots, n$ and interleaves the two sections in any way,
3. a card cutter, which simply cuts a deck of cards into two sections and places the bottom section of the cut on top of the top section.

In these cases, and many others, the set of possible permutations (of all lengths) is a closed set. Now suppose we pass the output of the environment on to a copy of the same environment (or feed it back into the original environment) and repeat this as many times as we wish. In the first example this is like having an unlimited number of stacks in series, in the second it is like allowing an unlimited number of riffle shuffles, and in the third it is like allowing an unlimited number of cuts.

When we have an environment that is endowed with feedback it is clear that the set of permutations of each degree which can be generated is a group. It is also quite easy to check that the set of all permutations which can be generated is closed provided that this was true of the original environment. In other words we have an example of the sort of closed set considered in our main result.

In general we use the phrase *group closed set* for a closed set in which the permutations of each degree form a group.

We begin with some notation. If X is any set of permutations we let $X(n) = X \cap S_n$, the subset of X whose permutations have degree n. We let ρ_n be the "reversal" permutation $[n, n-1, \ldots, 2, 1]$ (which, in cycle notation, would be written $(1,n)(2,n-1)\ldots$).

Using this notation we can give some examples of group closed sets X by specifying the groups $X(n)$ for each n.

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

Our results show that in a closed group set the sequence $X(n)$ converges to one of the above types. They also give information about the sort of groups $X(n)$ which can arise before convergence occurs.

Next we have a useful technical construction. If σ is a permutation of $\{1, 2, \ldots, n\}$ and $1 \leq i \leq n$ then, $\sigma - i$ denotes the permutation of $\{1, 2, \ldots, n-1\}$ obtained by removing the image of i from the sequence $[1^\sigma, \ldots, n^\sigma]$ and subtracting 1 from those images greater than i^σ so that the new sequence is indeed a permutation of $\{1, 2, \ldots, n-1\}$. Clearly $\sigma - i \preceq \sigma$.

As an example of the construction $[3, 4, 2, 1, 5] - 3 = [2, 3, 1, 4]$.

If, by a slight abuse of notation, we identify $\sigma - i$ with the permutation of degree n that fixes n and otherwise acts as $\sigma - i$, we have

$$\sigma - i = C(i, n)\sigma C(i^\sigma, n)^{-1}$$

where $C(i, n)$ denotes the cycle $(i, i+1, \ldots, n)$.

Lemma 1 *Suppose that X is a group closed set, $\sigma \in X(n)$, and $1 \leq i \leq n-1$. Let $j = i^\sigma$, $k = (i+1)^\sigma$ and let $\tau = (\sigma - i)^{-1}(\sigma - (i+1)) \in X(n-1)$. Then τ is the cycle $(j, j+1, \ldots, k-1)$ if $j < k$ and the cycle $(k, k+1, \ldots, j-1)^{-1}$ if $j > k$. In addition, if j and k are not consecutive modulo n, then $X(n-2)$ contains a transposition of the form $(t, t+1)$.*

PROOF: For the first statement we have:

$$\begin{aligned}(\sigma - i)^{-1}(\sigma - (i+1)) &= C(i^\sigma, n)\sigma^{-1}C(i,n)^{-1}C(i+1,n)\sigma C((i+1)^\sigma, n)^{-1} \\ &= C(j,n)\sigma^{-1}(i, i+1)\sigma C(k,n)^{-1} \\ &= (j, \ldots, n)(j,k)(k, \ldots, n)^{-1}\end{aligned}$$

and the result follows.

For the second part, note that both τ and τ^{-1} lie in $X(n-1)$ since $X(n-1)$ is a group. Without loss in generality assume that $\tau = (j, j+1, \ldots, k-1)$. Since j and k are not consecutive modulo n, τ is not the identity nor the permutation $(1, 2, \ldots, n-1)$. If $j \neq 1$ then $(j-1)^\tau = j-1$ and $j^\tau = j+1$ so, by part 1, $X(n-2)$ contains $(\tau - (j-1))^{-1}(\tau - j) = (j-1, j)$. On the other hand, if $k \neq n$ then $k^{\tau^{-1}} = k$ and $(k-1)^{\tau^{-1}} = k-2$ so that, again by part 1, $X(n-2)$ contains $(k-2, k-1)$. ■

Our analysis of group closed sets X divides naturally into two cases according to whether $X(n)$ is transitive for all n (the transitive case) or intransitive for some n (the intransitive case).

2 Intransitive groups

Throughout this section X will denote a group closed set for which not every $X(n)$ is transitive. Notice that if $X(n)$ is transitive then so also is $X(n-1)$. For suppose that $1 \leq i \leq n-1$. Then $i \in 1^{X(n)}$ so there is a permutation $\sigma \in X(n)$ with $1^\sigma = i$. But then, putting $k = n^{\sigma^{-1}}$, we have $1^{\sigma - k} = i$ and $\sigma - k \in X(n-1)$. We can deduce that, as there is at least one intransitive $X(L)$, the groups $X(n)$ are intransitive for all $n \geq L$.

For each $n \geq L$ we define an integer 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 $1 \leq j \leq k_n$, then $1^\sigma = j$ for some $\sigma \in X(n)$. Then, as $(k_n+1)^\sigma > k_n$, $1^{\sigma - (k_n+1)} = j$. This shows that $k_{n-1} \geq k_n$. 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 2 *There exist constants k, ℓ, M such that, for all $n \geq M$, $\{1, 2, \ldots, k\} \subseteq 1^{X(n)}$, $k+1 \notin 1^{X(n)}$ and $\{n - \ell + 1, \ldots, n\} \subseteq n^{X(n)}$, $n - \ell \notin n^{X(n)}$*

Lemma 3 *Let $t-1, t$ be in different orbits of $X(n-1)$ and let $\sigma \in X(n)$. Then either*

1. $t^\sigma = t$ *and* σ *preserves both* $\{1, \ldots, t-1\}$ *and* $\{t+1, \ldots, n\}$ *or*

2. $t^\sigma = n - t + 1$, $(n-t+1)^\sigma = t$ *and* σ *interchanges* $\{1, \ldots, t-1\}$ *and* $\{n-t+2, \ldots, n\}$

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

Lemma 4 *There exists a constant* N *such that either*

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

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

PROOF: Let $n \geq \max\{M+1, 2k, 2\ell\}$, where M is the constant defined in Lemma 2, and let $\sigma \in X(n)$. Since k and $k+1$ are in different orbits of $X(n-1)$ we know from Lemma 3 that we have one of

A1. σ preserves $\{1, \ldots, k\}$ or

A2. σ interchanges $\{1, \ldots, k\}$ and $\{n-k+1, \ldots, n\}$

Also $n-\ell$ and $n-\ell+1$ are in different orbits of $X(n-1)$ and another application of Lemma 3 yields

B1. σ preserves $\{n-\ell+1, \ldots, n\}$ or

B2. σ interchanges $\{1, \ldots, \ell\}$ and $\{n-\ell+1, \ldots, n\}$

Since $n \geq \max\{2k, 2\ell\}$, A1 and B2 are incompatible as are A2 and B1. We therefore have, for all $\sigma \in X(n)$,

C1. σ preserves $\{1, \ldots, k\}$ and $\{n-\ell+1, \ldots, n\}$ or

C2. $k = \ell$ and σ interchanges $\{1, \ldots, k\}$ and $\{n-k+1, \ldots, n\}$

Therefore according to whether C1 holds for all σ or not we have

1. $1^{X(n)} = \{1, \ldots, k\}$ and $n^{X(n)} = \{n-\ell+1, \ldots, n\}$ or

2. $k = \ell$ and $1^{X(n)} = \{1, \ldots, k, n-k+1, \ldots, n\}$

Finally we notice that if the first of these holds for a particular n then it must hold for $n+1$ also since, if $1^\sigma = n+1$ for some $\sigma \in X(n+1)$, then $1^{\sigma-(n+1)} = n$ in $X(n)$. Thus one of the two alternatives holds uniformly from some point on. ■

Lemma 5 *If the first case of Lemma 4 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 $\sigma \in X(n)$ either σ fixes every point in $k+1, \ldots, n-k$ or σ maps every such point s to $n-s+1$.*

PROOF: Suppose that the first alternative of Lemma 4 holds. Suppose that $n \geq N$, the constant defined in Lemma 4. Then k and $k+1$ are in different orbits of $X(n)$ as are $n-\ell$ and $n-\ell+1$. Hence, by Lemma 3, 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 $n > 2N$, all of the points in $k+1, \ldots, n-\ell$ are fixed in $X(n)$.

If the second alternative of Lemma 4 holds the same argument shows that if $\sigma \in X(n)$ and $k+1 \leq s \leq n-k$ then, provided $n > 2N$, $s^\sigma = s$ or $s^\sigma = n-s+1$. However, Lemma 3 proves that $s^\sigma = s$ precisely when $\{1, 2, \ldots, k\}$ is preserved by σ. Thus in this case $s^\sigma = s$ for all s in the range $k+1, \ldots, n-k$ or $s^\sigma = n-s+1$ for all s in this range. ■

Theorem 1 *Let X be a group closed set in which not every $X(n)$ is a transitive group. 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. *$X(n) = S_k \wr Z_2 = (S_k \times S_k).\langle \rho_n \rangle$ where the group $S_k \times S_k$ acts 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 Lemmas 4 and 5 hold. Suppose first that $X(n)$ fixes every point from $k+1$ to $n-\ell$. Then $\{1, \ldots, k\}$ is an orbit of $X(n)$ but rather more than this is true: if $Y(n)$ denotes the point stabiliser of $n-\ell+1, \ldots, n$ then $Y(n)$ is also transitive on $\{1, \ldots, k\}$. To see this notice that in $X(n+\ell)$ we can find a permutation mapping the point 1 to an arbitrarily chosen point i of $\{1, \ldots, k\}$ and this permutation involves a permutation of $X(n)$ that also maps 1 to i and fixes $n-\ell+1, \ldots, n$.

In $X(n+1)$ there are permutations σ_i that map the symbol k to each of $1, 2, \ldots, k$ in turn (and fix $k+1$ and also $n-\ell+2, \ldots, n+1$). But then the permutations $\sigma_i - 1$ lie in $Y(n)$, fix k, and map $k-1$ to each of $1, \ldots, k-1$.

Thus $Y(n)$ is 2-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 $Y(n)$ on $\{1,\ldots,k\}$ so it acts on this orbit as the full symmetric group. In the same way the pointwise stabiliser in $X(n)$ of $\{1,\ldots,k\}$ acts on the orbit $\{n-\ell+1,\ldots,n\}$ as the full symmetric group. This proves that $X(n) = S_k \times S_\ell$.

Now suppose that the second case of Lemma 5 holds. Then $X(n)$ has a subgroup $Z(n)$ of index 2 fixing all of $k+1,\ldots,n-k+1$ and the above arguments prove that $Z(n) = S_k \times S_k$ acting in the natural way on $\{1,\ldots,k,n-k+1,\ldots,n\}$. Using Lemma 5 it is easily seen that the permutation ρ_n lies in $X(n)\setminus Z(n)$ and the proof is complete. ■

3 Transitive groups

We denote by Z_n the permutation group of degree n generated by the n-cycle $(1,2,\ldots,n)$, and we denote by D_n the permutation group generated by $(1,2,\ldots,n)$ and $(1,n)(2,n-1)\cdots$. We call these groups the *natural* cyclic and dihedral groups of degree n. It is clear that

Lemma 6 *Let G be a transitive group of degree n. Then G is the natural cyclic or dihedral group if and only if for all $\sigma \in G$ and all $i = 1,2,\ldots,n$, i^σ and $(i+1)^\sigma$ are consecutive modulo n.*

Also, from elementary facts about permutation groups, we have

Lemma 7 *A permutation group G of degree n that contains cycles $\gamma = (1,2,\ldots,n)$ and $\delta = (1,2,\ldots,m)$ with $1 < m < n$ contains the alternating group of degree n.*

Lemma 8 *If X is a group closed set and $X(n)$ 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 6, $X(q)$ has a permutation σ for which there are two points $i, i+1$ with i^σ and $(i+1)^\sigma$ not consecutive modulo q.

However, Lemma 1, now shows that $X(q-2)$ contains a transposition of the form $(t,t+1)$. But $X(q-2)$ is primitive since $q-2$ is prime and so is necessarily the full symmetric group; therefore it contains $(1,2,\ldots,q-2)$. It follows that $X(n_1)$ 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 *anomalous* if

$$H = \langle \sigma - i \mid \sigma \in G, 1 \leq i \leq n \rangle \neq S_{n-1}$$

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

Lemma 9 *If G is an anomalous group of degree n and not cyclic or dihedral then n is even, and G has a block system with two blocks, one consisting of the odd points the other the even points. Conversely, any group with a cycle $(1, 2, \ldots, n)$ and satisfying these conditions is anomalous. For anomalous groups which are not cyclic or dihedral the group H is the alternating group A_{n-1}.*

PROOF: As G contains $\gamma = (1, 2, \ldots, n)$ it follows that H must contain $\gamma - n = (1, 2, \ldots, n-1)$. For any $\sigma \in G$ and $1 \leq i < n$ let $\delta(\sigma, i) = (\sigma - i)^{-1}(\sigma - (i+1))$. By Lemma 1 $\delta(\sigma, i)$ is a cycle of length $m(\sigma, i) = |i^\sigma - (i+1)^\sigma|$. 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 7, H contains A_{n-1}. By hypothesis, however, H is not the full symmetric group and therefore both $n-1$ and all $m(\sigma, i)$ must be odd. The latter condition implies that the elements of $1^\sigma, 2^\sigma, \ldots, n^\sigma$ are alternately even and odd. Hence each element σ maps odd points to odd points or maps odd points to even points, giving the required block system.

The converse follows by reversing the arguments. ■

Theorem 2 *Let X be a closed set in which every $X(n)$ is a transitive group. Then, with the exception of at most two groups, one of the following occurs.*

1. *Every $X(n)$ is a symmetric group.*
2. *For some integer M, $X(n)$ is a symmetric group for $n = 1, 2, \ldots, M$, and the remaining groups are natural dihedral.*
3. *For some integers $M \leq N$, $X(n)$ is a symmetric group for $n = 1, 2, \ldots, M$, $X(n)$ is natural dihedral for $n = M+1, \ldots, N$, and the remaining groups are natural cyclic.*

The exceptions, if they arise at all, are in the second and third cases and are of two types:

(i) *$X(M+1)$ is the alternating group and $X(M+2)$ is an imprimitive group of the type described in Lemma 9, or*

(ii) *$X(M+1)$ contains a full cycle but is not dihedral.*

PROOF: Since X is closed

$$\langle \sigma - i \mid \sigma \in X(n), 1 \leq i \leq n \rangle \subseteq X(n-1) \text{ for all } n.$$

Suppose that not every $X(n)$ is the symmetric group S_n and let $X(M+1)$ be the first that is not. Then $X(M+2)$ is anomalous and either

1. $X(M+2)$ is an imprimitive group of the type appearing in Lemma 9 and $X(M+1)$ is the alternating group, or
2. $X(M+2)$ is the natural cyclic or dihedral group

In either case, by Lemma 9 again, $X(n)$ is the natural cyclic or natural dihedral group for all $n \geq M+3$. 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: Generalized stack permutations, Combinatorics, Probability and Computing 7 (1998), 239-246.

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

[5] L. Shapiro, A.B. Stephens, Bootstrap percolation, the Schröder number, and the N-kings problem, SIAM J. Discrete Math. 2 (1991), 275–280.

[6] R. Simion, F.W. Schmidt: Restricted permutations, Europ. J. Combinatorics 6 (1985), 383-406.

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

[8] J. West: Generating trees and the Catalan and Schröder numbers, Discrete Math. 146 (1995), 247-262.