Journal of Algebraic Combinatorics, 5, (1996), 315–322
© 1996 Kluwer Academic Publishers, Boston. Manufactured in The Netherlands.

Cycle-Closed Permutation Groups

PETER J CAMERON p.j.cameron@qmw.ac.uk

School of Mathematical Sciences, Queen Mary and Westfield College, Mile End Road, London E1 4NS, U.K.

Received December 1, 1994; Revised June 13, 1995

Abstract. A finite permutation group is cycle-closed if it contains all the cycles of all of its elements. It is shown by elementary means that the cycle-closed groups are precisely the direct products of symmetric groups and cyclic groups of prime order. Moreover, from any group, a cycle-closed group is reached in at most three steps, a step consisting of adding all cycles of all group elements. For infinite groups, there are several possible generalisations. Some analogues of the finite result are proved.

Keywords: Permutation group, cycle, Hopf algebra, Fourier series

1. Introduction

For any finite permutation group G, let $C(G)$ be the group generated by all the cycles of the elements of G. We say that G is *cycle-closed* if $C(G) = G$. This concept arises in the work of Lenart and Ray [1] on a Hopf algebra translation of set systems with given automorphism groups. (I am grateful to Christian Lenart for communicating this to me.) I show in Theorem 1 below that the only cycle-closed finite permutation groups are direct products of cyclic groups of prime order and symmetric groups. Moreover, starting from any finite permutation group, we obtain a cycle-closed group after at most three applications of the function C (and this is best possible).

Less is known about infinite groups, and indeed there are several possible generalisations of cycle closure. With the strongest concept, we again reach a cycle-closed group in at most three steps, such a group being a cartesian product of symmetric groups and cyclic groups of prime order as in the finite case. Even with the weakest concept, starting with an infinite transitive group, after at most three steps we reach a group containing all the finitary permutations. I conjecture that this group is in fact cycle-closed. The conjecture is proved in some cases.

If G is transitive, then $C(G)$ is a very special kind of Jordan group. A lot is known about Jordan groups. All finite primitive Jordan groups were determined, using the classification of finite simple groups, by Kantor and Neumann; and there is a structure theorem for infinite Jordan groups by Adeleke and Macpherson (which, however, gives no information in the highly transitive case). See Macpherson [2] for an up-to-date survey of this material. However, none of this is required here; the methods used are completely elementary.

A general reference on permutation groups is Wielandt [4].

2. The finite case

Given a permutation group G on a finite set Ω, we define $C_0(G) = G$ and $C_{n+1}(G) = C(C_n(G))$ for $n \geq 0$.

Theorem 1 *(a) A finite permutation group is cycle-closed if and only if it is a direct product of symmetric groups and cyclic groups of prime order.*

(b) For any finite permutation group G, $C_3(G)$ is cycle-closed.

(c) There exist finite permutation groups G such that $C_2(G)$ is not cycle-closed; such a group, if transitive, is a p-group, for some odd prime p.

In the proof, we need the following simple result. (Of course, much stronger assertions have been proved; what we need is much less than even Jordan knew.)

Lemma 1 *Let g and h be permutations of Ω, each of which is a cycle of prime order. Let $S(g)$ and $S(h)$ be the supports of g and h; suppose that neither of $S(g)$ and $S(h)$ contains the other, and that their intersection is non-empty. Then the group generated by g and h has even order.*

Proof: We may suppose that $S(g) \cup S(h) = \Omega$, so that $G = \langle g, h \rangle$ is transitive. Let g and h have orders p and q, and suppose that $p \geq q$. It is straightforward to show that the conjugates of g by powers of h whose supports do not contain a particular point $\alpha \notin S(g)$ generate a transitive group on $\Omega \setminus \{\alpha\}$. So G is doubly transitive, and has even order. □

We also use the facts that a primitive group containing a transposition is the symmetric group, while a primitive group containing a 3-cycle is symmetric or alternating.

Proof of Theorem 1: First, suppose that G is intransitive. If its transitive constituents are $G_1, \ldots, G_k$, then $C(G) = C(G_1) \times \ldots \times C(G_k)$, since any permutation in G is a product of elements $g_i \in G_i$ $(i = 1, \ldots, k)$, and all these elements are in $C(G)$. So it suffices to prove all parts of the Theorem for transitive groups.

Next, suppose that G is transitive but imprimitive. Take any system of blocks of imprimitivity. Suppose that $g \in G$ induces a cycle of length m on the blocks. Then g^m fixes all the blocks in the cycle and induces similar permutations on them. If h is a cycle of g^m on the block Δ, then $h \in C(G)$, and $gh^{-1} \in C(G)$ has a cycle $g' \in C_2(G)$ of length m meeting every block in at most one point. We draw two conclusions:

- $C_2(G)$ does not preserve the block system. Since this holds for any block system, $C_2(G)$ is primitive.

- $C(G)$ contains an element h' whose support is contained in Δ and meets the support of g' in one point. The commutator of g' and h' is a 3-cycle in $C_2(G)$.

We conclude that $C_2(G)$ contains the alternating group A_n, where $n = |\Omega|$, and $C_3(G)$ is the symmetric group S_n.

Now suppose that G is primitive. If $C(G)$ has even order, then $C_2(G)$ contains a transposition, and is the symmetric group. So suppose that the order of $C(G)$ is odd. If G is cyclic of prime order, then it is cycle-closed; so assume not. Take an element g_0 of prime order in G which is not a single cycle on all the points, and let g be a cycle of g_0 (in $C(G)$). Now the support of g is not a block of imprimitivity; so there is a conjugate h of g whose support meets that of g. By Lemma 1, g and h generate a group of even order. So $C_2(G)$ contains a transposition, and is symmetric.

We have shown that $C_3(G)$ is cycle-closed for any transitive group G (and hence for any group G), and also that the only transitive cycle-closed groups are symmetric groups and cyclic groups of prime order. So parts (a) and (b) of the Theorem are proved.

The above analysis shows that, if $C_2(G)$ is not cycle-closed, then G is imprimitive, and $C(G)$ has odd order. Let g_0 be an element of prime order p in G, and g a cycle of g_0. By Lemma 1, the support of g is a block of imprimitivity for $C(G)$. If $|G|$ is divisible by another prime q, there would also be a q-cycle $h \in C(G)$ whose support is a block of imprimitivity. Now we could find two such blocks with non-empty intersection, and again the Lemma would imply that $C(G)$ has even order. So G must be a p-group.

The cyclic group G of order p^2, where p is an odd prime, is an example. For let g be the generator. The only elements of G with non-trivial cycles are the powers of g^p. Their orbits are blocks in the unique system of imprimitivity for G, which is thus preserved by $C(G)$; so $C(G) = C_p \operatorname{Wr} C_p$.This group has odd order, so all its cycles are even permutations, and $C_2(G)$ is contained in the alternating group, and is not cycle-closed. (In fact, $C_2(G) = A_{p^2}$ and $C_3(G) = S_{p^2}$.) □

The following lemma will be needed in the next section. It follows from the proof of Theorem 1.

Lemma 2 *Suppose that n is even and not a power of 2, and let G be the cyclic group of order n acting regularly. Then $C(G) = S_n$.*

3. The infinite case

In what follows, a *restriction* of a permutation g always refers to the restriction to a fixed set Δ of g, and is the permutation which agrees with g on Δ and fixes every point outside Δ.

We have to modify the definition of cycle closure in the infinite case, since (for example) a permutation with infinitely many cycles does not lie in the group generated by its cycles. Accordingly, we set $C^-(G)$ to be the group generated the cycles of the elements of G, and $C(G) = \langle G, C^-(G)\rangle$; we call G *cycle-closed* if $G = C(G)$. Note that G normalises $C^-(G)$, so $C(G)$ is the product $C^-(G)\cdot G$. Also, if G is transitive, primitive, or k-transitive, then so is $C^-(G)$.

More strongly, we let $R(G)$ be the group generated by all restrictions of elements of G, and call G *restriction-closed* if $R(G) = G$. Finally, we let $C^+(G)$ be the group generated by all permutations g with the property that every cycle of g is a cycle of an element of G, and call G *strongly cycle-closed* if $C^+(G) = G$. We have $G \leq C(G) \leq R(G) \leq C^+(G)$ for any G, so the various closures do indeed get stronger. For example, consider the group G generated by an infinite set of permutations g_i, where g_i has infinitely many cycles T_{ij} each of length 2 (all these cycles disjoint). Then

- G consists of all permutations which interchange the points in T_{ij} for only finitely many i, and act non-trivially on T_{ij} for all or no values of j for each i.
- $C^-(G)$ consists of all permutations which interchange the points in T_{ij} for only finitely many i, j.
- $C(G)$ consists of all permutations which interchange the points in T_{ij} for only finitely many i, and act non-trivially on T_{ij} for finitely many or all but finitely many j for each i (and $C(G)$ is cycle-closed).
- $R(G)$ consists of all permutations which interchange the points in T_{ij} for only finitely many i, but without further restrictions (and $R(G)$ is restriction-closed).
- $C^+(G)$ consists of permutations which interchange the points in T_{ij} without restriction (and $C^+(G)$ is strongly cycle-closed).

We define $C_n(G)$ as before and $C_n^-(G)$, $R_n(G)$ and $C_n^+(G)$ analogously.

Below, I consider the two extreme cases C^- and C^+. I begin with the reduction to the transitive case. Given a family $(G_i : i \in I)$ of groups let $\prod_{i\in I} G_i$ denote the Cartesian product of the family, and $\prod_{i\in I}^D G_i$ the direct product (consisting of elements of the cartesian product which are the identity in all but finitely many coordinates). Just as in the finite case, we have:

Theorem 2 *Let G be a permutation group with transitive constituents G_i for $i \in I$. Then $C^-(G) = \prod_{i\in I}^D C^-(G_i)$, and $C^+(G) = \prod_{i\in I} C^+(G_i)$.*

For transitive groups, we have the following result. Let $FS(\Omega)$ denote the *finitary symmetric group* on Ω (the group of permutations of finite support).

Theorem 3 *Let G be an infinite transitive permutation group on Ω. Then $C_3^-(G)$ contains $FS(\Omega)$; and $C_3^+(G)$ is the full symmetric group on Ω.*

Proof: If G is imprimitive, argue exactly as in the finite case, with the extra observation that an infinite cycle on blocks cannot revisit a block, to show that $C_3^-(G)$ contains $FS(\Omega)$.

Suppose that G is primitive. If an element of G has a cycle of finite length, then $C^-(G)$ contains an element g which is a finite prime cycle. As before, the support of g is not a block of imprimitivity, so $C^-(G)$ contains a finite subgroup of even order. Then $C_2^-(G)$ contains a transposition, and hence contains the finitary symmetric group. The same conclusion holds for infinite cycles, in view of the next result.

Lemma 3 *If G is the infinite cyclic group, then $C(G) = C^-(G)$ is 2-transitive.*

Proof: It is clearly transitive. Identify the points permuted with the integers, so that the generator g of G is $x \mapsto x + 1$. Suppose we want to fix 0 and map l to m. Choose two coprime integers x, y both greater than the larger of $|l|$ and $|m|$; then use the Chinese Remainder Theorem to find n such that $n \equiv l \pmod{x}$ and $n \equiv m \pmod{y}$. Now g^x has a cycle consisting of all integers congruent to l mod x, and adds x to each of these integers. Some power of this cycle fixes 0 and carries l to n. Similarly, we can find a power of a cycle of g^y which fixes 0 and maps n to m. (In fact, a similar argument shows that $C(G)$ is *highly transitive*, that is, k-transitive for all k.) □

Now $C_2^+(G)$ contains $C_2^-(G)$, which contains the alternating group in all cases. It follows that $C_3^+(G)$ contains all permutations all of whose cycles are finite. But every permutation is a product of two permutations with finite cycles. (It suffices to prove this for a cyclic permutation, which we can take to be the permutation $x \mapsto x + 1$ of the integers. This is the product of the two involutions $x \mapsto -x$ and $x \mapsto -x + 1$.) □

Conjecture *For any permutation group G, $C_3(G)$ is cycle-closed.*

The obvious strategy is to prove this conjecture first for transitive groups. If this could be done, then at least the fact that $C_4(G)$ is cycle-closed for any G would follow. For suppose that $C_4(G_i) = C_3(G_i)$ for any transitive constituent G_i of G. Then $C_5^-(G_i) = C_4^-(G_i)$; so

$$C_5^-(G) = \prod^D C_5^-(G_i) = \prod^D C_4^-(G_i) = C_4^-(G)$$

by Theorem 2, whence

$$C_5(G) = C_5^-(G)C_4(G) = C_4(G).$$

I conclude this section with a proof of the conjecture in a couple of special cases.

Proposition 1 *Let G be a transitive permutation group in which all the cycles of all elements of G are finite. Then $C(G) \leq FS(\Omega) \cdot G$. Hence $C_3(G) = FS(\Omega) \cdot G$ is cycle-closed.*

Proof: The first assertion is clear since $C^-(G) \leq FS(\Omega)$. Then $C(G)$ also satisfies the hypothesis of the Proposition, and by induction $C_n(G) \leq FS(\Omega) \cdot G$ for all n. Now the result follows from Theorem 3. □

The hypothesis holds for any torsion group, and for many other groups as well.

The next result concerns the simplest group failing the hypothesis of Proposition 1, the infinite cyclic group $\mathbb{Z}$ acting regularly. This was briefly considered in Lemma 3; a more detailed analysis follows.

Proposition 2 *Let G be the infinite cyclic group $\mathbb{Z}$ acting regularly.*

(a) $C_1(G)$ is the set of all permutations g of $\mathbb{Z}$ for which there exist $n > 0$ and $b_0, \ldots, b_{n-1}$ such that $(kn + i)g = kn + b_i$ for $0 \leq i \leq n - 1$.

(b) $C_2(G)$ is the semidirect product $FS(\mathbb{Z}) \cdot C_1(G)$.

(c) $C_3(G)$ is the set of all permutations g of $\mathbb{Z}$ for which there exist $r > 0$ and $h_+, h_- \in C_1(G)$ such that $xg = xh_+$ for $x > r$ and $xg = xh_-$ for $x < -r$.

(d) $C_4(G) = C_3(G)$, that is, $C_3(G)$ is cycle-closed.

Proof: (a) Let $z : x \mapsto x + 1$ generate G. Any cycle of z^m has the form $km + i \mapsto km + (m + i)$ for fixed i, all other points fixed. Such an element can be written in the form (a) of the Proposition for any n which is a multiple of m.

Consider now the composition of finitely many such cycles. Replacing the individual values of n by their least common multiple, we may assume that the same value of n occurs for each element. Now it is clear that the composition is also of the form (a).

Finally, we must show that every permutation g of the form (a) is in $C_1(G)$. Replacing n by a multiple, we may assume that n is even and not a power of 2. By Lemma 2, $C(Z_n) = S_n$, and so $C(G)$ contains an element g' agreeing with g modulo n. Now g is obtained from g' by multiplying by a word in the cycles of z^n.

(b) $C(G)$ contains elements inducing the symmetric group on $\{0, \ldots, n-1\}$ for any n, so $C_2(G)$ contains the finitary symmetric group. We show that any infinite cycle of an element of $C(G)$ belongs to $C(G)$, from which the result follows. So let g be an infinite cycle of an element of the form (a). Some power g^r acts trivially modulo n, so $xg^r = x + dn$ (where d may depend on x). Of course, $d = 0$ if g fixes x. Suppose that g moves x. Since $xg^r \equiv x \pmod{n}$, we have $xg^{r+1} - xg^r = xg - x$, so $(xg)g^r - xg = xg^r - x$. So the value of d is constant on the cycle of elements moved by g. Replacing n by dn, the support of g is a union of congruence classes modulo n, so that g is indeed of the form (a).

The product is semidirect because $C(G)$ contains no elements of finite support.

(c) We show first that any cycle of an element of $C_2(G)$ satisfies the specifications of (c). This is clear for a finite cycle, so let g be an infinite cycle. The two 'ends' of g agree with those of two cycles (possibly equal) of an element of $C(G)$. Since $C(G)$ contains all infinite cycles of all its elements, the result is true. (Note that the 'ends' of g may be contained in the same or different ends of $\mathbb{Z}$.)

It follows easily that any element of $C_3(G)$ has the form (c).

To conclude, we must show that every permutation of the form (c) belongs to $C_3(G)$. So let g be such a permutation. By multiplying g by h_-^{-1}, we may assume that $h_- = 1$. Now any cycle of h_+ is either ascending, descending, or finite. (We call an infinite cycle *ascending* if some power of it translates points in its support by a positive number; see the argument in (b). *Descending* cycles are defined analogously.) If the numbers of ascending and descending cycles are unequal, then no permutation g satisfies the specification of (c): for any such permutation has two 'ends', one ascending and the other descending. So we may assume that these numbers are equal. Thus we may pair the ascending and descending cycles of h_+. We can find an element of $C_2(G)$ with a cycle which agrees with the product of a paired pair of cycles of h_+ on the positive end of $\mathbb{Z}$, and fixes the negative end pointwise. (This element is the product of the two paired cycles and a transposition interchanging points in the two cycles.)

It remains to deal with finite cycles. Now the finite cycles of h_+ fall into congruence classes modulo n, for some n. We express the product of the positive cycles in each class as an element of $C_3(G)$. Take one congruence class of cycles, defining a permutation

g. Suppose first that some congruence class (say $x \bmod n$) is fixed. Let $y \bmod n$ be a congruence class moved by g. There is a permutation $g_1' \in C_2(G)$ having a cycle g' satisfying $(kn+x)g' = k(n-1)+x$ and $(kn+y)g' = k(n+1)+y$ for sufficiently large k, all negative points being fixed. (Take g_1' to be the product of two infinite cycles and a transposition interchanging points in the two cycles.) Then gg' has a single infinite cycle g'' on the positive end of $\mathbb{Z}$, and $g'' \in C_3(G)$. We conclude that $g''(g')^{-1}$ belongs to $C_3(G)$ and agrees with g on the positive end of $\mathbb{Z}$, fixing the negative end pointwise. On the other hand, if g has no fixed points, we can write it as a product of two permutations in $C_3(G)$ with finite cycles, each of which has fixed points; then the positive end of each factor belongs to $C_3(G)$, and hence so does the positive end of g.

(d) Finally we show that $C_3(G)$ is cycle-closed. Clearly it contains all the finite cycles. Any infinite cycle of a permutation satisfying (c) itself satisfies (c), and so also belongs to $C_3(G)$. □

Remark An interesting example resembling the groups $C(\mathbb{Z})$ and $C_2(\mathbb{Z})$ of the previous result was considered by Rudin [3]. (I am grateful to Chris Woodcock for bringing this to my attention.) This paper characterised the permutations of $\mathbb{Z}$ which map Fourier series (of integrable periodic functions) to Fourier series. (A permutation of $\mathbb{Z}$ acts on the indices of the Fourier coefficients.) Rudin showed that the group of such permutations is the semidirect product $FS(\mathbb{Z}) \cdot G$, where G consists of those permutations g of $\mathbb{Z}$ for which there exist $n > 0$ and a_i, b_i $(0 \le i \le n-1)$ such that $(kn+i)g = ka_i + b_i$ for $0 \le i \le n-1$. This group G contains $C(\mathbb{Z})$ and a lot more besides. Rudin gave as an example the permutation g defined by

$$(3k)g = 2k, \qquad (3k+1)g = 4k+1, \qquad (3k-1)g = 4k-1.$$

Clearly $C(G) \ge FS(\mathbb{Z}) \cdot G$; does equality hold? And can the cycle-closure of G be described?

4. Applications and open problems

The original application by Lenart and Ray to the combinatorics of "objects with group action" is somewhat technical; interested readers are referred to their paper [1]. Another application is the construction and analysis of interesting infinite groups.

I list a few open problems.

(a) Which finite transitive permutation groups G satisfy $C_2(G) \ne C_3(G)$? (These are all p-groups, for odd primes p.)

(b) Is it true that $C_3(G) = C_4(G)$ for all permutation groups G?

(c) The group $C(\mathbb{Z})$ has an obvious homomorphism onto $\mathbb{Z}$. Is the kernel simple? What are the normal subgroups of $C_3(\mathbb{Z})$, or of Rudin's group?

(d) What can be said about the "restriction" operator R?

References

1. C. Lenart and N. Ray, "A Hopf algebraic framework for set system colourings with a group action," preprint.
2. H. D. Macpherson, "A survey of Jordan groups", *Automorphisms of First-Order Structures* (ed. R. Kaye and H. D. Macpherson), pp. 73–110, Oxford University Press, Oxford, 1994.
3. W. Rudin, "The automorphisms and the endomorphisms of the group algebra of the unit circle", *Acta Math.* **95** (1956), 39–56.
4. H. Wielandt, *Finite Permutation Groups*, Academic Press, New York, 1964.