Reducibility of the cycle index

Abstract

We discuss the question: when is the cycle index polynomial of a finite permutation group irreducible over $\mathbb{Z}$? We conjecture that this is the case if G is primitive, and give a number of examples and related results.

1 Introduction

There are several examples of polynomials attached to combinatorial or algebraic structures. A famous example is the *Tutte polynomial* $T(M;x,y)$ of a matroid M (see [20]). It is known that, if a matroid M is not connected, then its Tutte polynomial is the product of the Tutte polynomials of its connected components. Merino, de Mier and Noy [17] proved the converse, which provided the inspiration for this paper.

Theorem 1.1 *If M is a connected matroid, then $T(M;x,y)$ is irreducible in $\mathbb{Z}[x,y]$ (and even in $\mathbb{C}[x,y]$).*

We ask whether a similar result holds for the cycle index of a permutation group. Recall that, if G is a permutation group on a set of n elements, then its *cycle index* is the polynomial in indeterminates $s_1,\ldots,s_n$ given by

$$Z(G;s_1,\ldots,s_n)=\frac{1}{|G|}\sum_{g\in G}\prod_{i=1}^{n}s_i^{c_i(g)},$$

where $c_i(g)$ is the number of cycles of length i in the cycle decomposition of g. The factor $1/|G|$ is crucial for the use of the cycle index in enumeration, but has no effect on reducibility, so we ignore it where convenient.

We will see that, if $G = G_1 \times G_2$ in its intransitive action, then $Z(G) = Z(G_1)Z(G_2)$. (It does not follow that the cycle index of any intransitive group is reducible!) So one might be tempted to conjecture that the cycle index of a transitive group is irreducible. This is not so; we construct two infinite families of counterexamples, and show that the wreath product produces many more counterexamples. All known counterexamples are imprimitive; we make the following conjecture:

Conjecture If G is a primitive permutation group of degree n, then $Z(G)$ is irreducible in $\mathbb{Z}[s_1, \ldots, s_n]$.

The notion of cycle index can be extended to infinite, *oligomorphic* permutation groups (those having only finitely many orbits on the set of n-tuples of points of the domain, for all $n \in \mathbb{N}$). We will see that the conjecture fails spectacularly for these.

There is another product on cycle indices, the *circle product* $\circ$, which has the property that $Z(G_1 \times G_2) = Z(G_1) \circ Z(G_2)$ (where $G_1 \times G_2$ is given its *product action*), see [7]. In the final section we review the little that is known about reducibility with respect to this product.

For background on permutation groups we refer to [3] or [8], while for the use of cycle index in enumeration see [14] or [12].

2 General considerations

For a permutation g having n_i cycles of length i, we put

$$z(g) = \prod_{i=1}^{n} s_i^{n_i},$$

so that

$$Z(G) = \frac{1}{|G|} \sum_{g \in G} z(g).$$

The weight of a monomial $\prod s_i^{a_i}$ is defined to be $\sum i a_i$ (in other words, we give the indeterminate s_i weight i). If g is a permutation on n points, then $z(g)$ has weight n; so, if G is a permutation group on n points, then $Z(G)$ is *weight-homogeneous* (every term has the same weight) of weight n.

Proposition 2.1 *The factors of a weight-homogeneous polynomial are weight-homogeneous.*

Proof Suppose that $F = PQ$ is weight-homogeneous of weight n. Let P_1 and Q_1 be the sums of terms of P and Q with smallest weight. Then the terms in P_1Q_1 are not cancelled by any other terms in the product PQ; so the sum of their degrees is n. The same holds for the terms of largest weight in P and Q. So P and Q are weight-homogeneous.

Corollary 2.2 *Let G be a permutation group of degree n*

(a) If G contains an n-cycle, then $Z(G)$ is irreducible.

(b) If G contains an $(n-1)$-cycle, then either it has a global fixed point, or $Z(G)$ is irreducible.

Proof (a) $Z(G)$ contains a term s_n, and is clearly irreducible.

(b) $Z(G)$ contains a term s_1s_{n-1}. So, if it is reducible, then it has a factor s_1, so that every element of G fixes a point. Such a group must be intransitive, by Jordan's Theorem [19], and so has a fixed point.

From $Z(G)$, one obtains univariate polynomials by specialising all the variables except s_i to constant values. If $Z(G)$ is reducible, then either the resulting univariate polynomial is reducible, or one of the factors of $Z(G)$ does not contain the variable s_i. In the case $i = 1$, the second alternative cannot happen, since $Z(G)$ contains the term s_1^n. In this case, there is one particularly important specialisation.

The *probability generating function for fixed points* is the polynomial

$$P_G(x) = \frac{1}{|G|}\sum_{g\in G} x^{\mathrm{fix}(g)},$$

where $\mathrm{fix}(g)$ is the number of fixed points of g (see [2]). The coefficient of x^k is the probability that a random element of G has exactly k fixed points. Clearly $P_G(x)$ is obtained from $Z(G)$ by substituting x for s_1 and 1 for s_i $(i > 1)$. Hence:

Corollary 2.3 *If $P_G(x)$ is irreducible, then so is $Z(G)$.*

Note that

$$P_G(x+1) = \sum_{i=0}^{n} \frac{F_i x^i}{i!},$$

where F_i is the number of orbits of G on i-tuples of distinct points (see [2]).

Another general result (depending on the Classification of Finite Simple Groups) is the following.

Proposition 2.4 *Let G be a finite transitive permutation group. If $Z(G)$ is reducible, then the degrees of its factors are not coprime.*

Proof By a theorem of Fein, Kantor and Schacher [9], G contains a fixed-point-free element whose order is a power of a prime number p. So $Z(G)$ contains a term involving only the variables s_{p^i} for $i > 0$. Any factor of $Z(G)$ contains a factor of this term, and so has weight divisible by p.

Stronger results are known for primitive groups (Giudici [11]), and it might be hoped that these can be applied to our main conjecture.

3 Intransitive groups

Let G_1 and G_2 be permutation groups on disjoint sets Ω_1 and Ω_2. The *intransitive action* of $G_1 \times G_2$ is the action on $\Omega_1 \cup \Omega_2$ given by

$$\alpha(g_1, g_2) = \alpha g_i \text{ if } \alpha \in \Omega_i,$$

while the *product action* is the action on $\Omega_1 \times \Omega_2$ given by

$$(\alpha_1, \alpha_2)(g_1, g_2) = (\alpha_1 g_1, \alpha_2 g_2).$$

In the case of the intransitive action, $z((g_i, g_j)) = z(g_i)z(g_j)$. Hence,

Proposition 3.1 *The cycle index of $G_1 \times G_2$ in its intransitive action is given by*

$$Z(G_1 \times G_2) = Z(G_1)Z(G_2).$$

In particular, if G has a global fixed point, then s_1 is a divisor of $Z(G)$.

It does not follow that the cycle index of any intransitive group is reducible. For example, the cycle index of C_2, acting on four points with two orbits of length 2, is $s_1^4 + s_2^2$. Indeed, sometimes a factorisation appears to be accidental. For example, the cycle index of C_5, acting with four orbits of length 5, is

$$s_1^{20} + 4s_5^4 = (s_1^{10} + 2s_1^5 s_5 + 2s_5^2)(s_1^{10} - 2s_1^5 s_5 + 2s_5^2).$$

Further examples can be constructed as follows. The *permutation character* of a permutation group G is the function mapping a group element to its number of fixed points. Two actions of a group with the same permutation character have the same cycle index [5, p. 50]. Also, by Block's Lemma, the actions of a group of automorphisms of a symmetric design on the sets of points and blocks have the same permutation character [1]. It follows that, for example, if G is a group of automorphisms of a symmetric design which fixes a block, then $Z(G)$ has a factor s_1, even if G has no global fixed point.

4 Imprimitive groups

The *wreath product* of two permutation groups G_1 (on Ω_1) and G_2 (on Ω_2) is the permutation group on $\Omega_1 \times \Omega_2$ generated by

- the *base group*, the direct product of $|\Omega_2|$ copies of G_1, where (for $\omega \in \Omega_2$) the copy indexed by ω acts on the pairs (α, ω) for $\alpha \in \Omega_1$ and fixes all others; and
- the *top group*, a copy of G_2 permuting the second coordinates of the ordered pairs.

The cycle index of $G_1 \operatorname{Wr} G_2$ is obtained from $Z(G_2)$ as follows: for $i \in \mathbb{N}$, let $Z_i(G_1)$ be obtained from $Z(G_1)$ by substituting s_{ij} for s_j for all $j \in \mathbb{N}$; then $Z(G_1 \operatorname{Wr} G_2)$ is obtained from $Z(G_2)$ by substituting $Z_i(G_1)$ for s_i for all $i \in \mathbb{N}$. Since it is a specialisation of $Z(G_2)$, we see:

Proposition 4.1 *If $Z(G_2)$ is reducible, then so is $Z(G_1 \operatorname{Wr} G_2)$.*

In order to use this result to construct imprimitive groups with reducible cycle index, we need some starting examples. Our main conjecture says that we can't start with primitive groups! However, imprimitive examples are provided by the next result.

The proof uses some concepts concerning linear codes. We begin with a brief summary. We refer to [15] for further background.

The *weight* $\mathrm{wt}(v)$ of a vector $v = (v_1, \ldots, v_n) \in \mathbb{F}_p^n$ is the number of non-zero coordinates of v.

A *(linear) code* C of length n over $\mathbb{F}_p$ is a vector subspace of $\mathbb{F}_p^n$. Its *dual* $C^\perp$ is the linear code

$$C^\perp = \{v \in \mathbb{F}_p^n : v \cdot c = 0 \text{ for all } c \in C\},$$

where $v \cdot c$ is the standard inner product $\sum v_i c_i$.

The *weight enumerator* of a linear code C is the homogeneous polynomial

$$W_C(X,Y) = \sum_{c \in C} X^{n-\mathrm{wt}(c)} Y^{\mathrm{wt}(c)} = \sum_{i=0}^{n} a_i X^{n-i} Y^i,$$

where a_i is the number of words of weight i in C. According to MacWilliams' Theorem, the weight enumerators of a code and its dual are related by

$$W_{C^\perp}(X,Y) = \frac{1}{|C|} W_C(X + (p-1)Y, X - Y).$$

A code $C \leq \mathbb{F}_p^n$ is *cyclic* if $(c_1, \ldots, c_n) \in C$ implies $(c_n, c_1, \ldots, c_{n-1}) \in C$; in other words, the permutation $(1, 2, \ldots, n)$ is an automorphism of C.

From a code C we can construct a permutation group $G(C)$ as in [4], as follows. Let $\Omega = \{1, \ldots, np\}$. For $i = 1, \ldots, n$, let e_i be the p-cycle $((i-1)p+1, (i-1)p+2, \ldots, ip)$ for $i = 1, \ldots, n$. Then

$$G(C) = \{e_1^{c_1} e_2^{c_2} \cdots e_n^{c_n} : c = (c_1, c_2, \ldots, c_n \in C\}.$$

Its cycle index is given by

$$Z(G(C)) = \frac{1}{|C|} W_C(s_1^p, s_p).$$

This shows that the weight enumerators of codes are specialisations of cycle indices. Note that they are also specialisations of Tutte polynomials [13].

Proposition 4.2 *Let p be an odd prime. Then there are two imprimitive groups of degree p^2 (with orders p^{p-1} and p^p) whose cycle index is divisible by $Z(C_p)$.*

Proof Our proof is based on the following construction. Let C be a linear code of length p over the alphabet $\mathbb{F}_p$. Suppose that the following three conditions hold:

(a) C is cyclic;

(b) C contains the all-1 vector;

(c) C has exactly $p-1$ words of weight p (namely the non-zero scalar multiples of the all-1 vector).

Now we build a permutation group G as follows.

Take $\Omega = \{1, \ldots, p^2\}$, and let g be the permutation

$$(1, p+1, \ldots, p^2-p+1)(2, p+2, \ldots, p^2-p+2)\cdots(p, 2p, \ldots, p^2).$$

Let $H = G(C^\perp)$ and $G = \langle H, g\rangle$. Note that, since C is cyclic, so is $C^\perp$, so that g normalises H, and $|G| = p|H|$.

Claim: Any element belonging to $G\backslash H$ is a product of p cycles of length p.

For such an element has the form hg^i for $h \in H$ and $1 \leq i \leq p-1$. We have

$$(hg^i)^p = h \cdot g^i h g^{-i} \cdot g^{2i} h g^{-2i} \cdots g^{(p-1)i} h g^{-(p-1)i}.$$

Each conjugate belongs to H, and indeed we have $g^i e_j g^{-i} = e_{j-i}$, where the subscript is taken mod p. So, if $h = e_1^{c_1} e_2^{c_2} \cdots e_p^{c_p}$, then

$$g^i h g^{-i} = e_1^{c_{i+1}} e_2^{c_{i+2}} \cdots e_p^{c_{i+p}}.$$

Thus the exponent of e_j in $(hg^i)^p$ is

$$c_j + c_{j+i} + c_{j+2i} + \cdots + c_{j+(p-1)i},$$

since the subscripts run through all of $0, 1, \ldots, p-1$. But since the all-1 vector is in C, every word of $C^\perp$ has coordinate sum zero. Thus

$$(hg^i)^p = 1.$$

Now hg^i permutes the blocks of imprimitivity in a cycle, so it cannot have any fixed points. Thus it is a product of p cycles of length p, as claimed.

Now let $\dim(C) = k$, so that $\dim(C^\perp) = p-k$. Thus, $|H| = p^{p-k}$, and $|G| = p^{p-k+1}$. We compute the cycle index of G as follows.

By the preceding claim, each of the $p^{p-k}(p-1)$ elements of $G \setminus H$ contributes a term s_p^p to the cycle index. Moreover, the cycle index of H is $W_C^\perp(s_1^p, s_p)$.

By assumption, the weight enumerator of C is $XF(X,Y) + (p-1)Y^p$ for some homogeneous polynomial F of degree $p-1$.

By MacWilliams' Theorem, the weight enumerator of $C^\perp$ is

$$\frac{1}{|C|}W_C(X+(p-1)Y,X-Y) = \frac{1}{p^k}\Big((X+(p-1)Y)F^*(X,Y)+(p-1)(X-Y)^p\Big),$$

where $F^*(X,Y) = F(X+(p-1)Y, X-Y)$. So, with $X = s_1^p$ and $Y = s_p$, the cycle index of G (ignoring the factor $1/|G|$) is

$$\begin{aligned} & \frac{1}{p^k}\Big((X+(p-1)Y)F^*(X,Y)+(p-1)(X-Y)^p\Big) + p^{p-k}(p-1)Y^p \\ = \quad & \frac{1}{p^k}\Big((X+(p-1)Y)F^*(X,Y)+(p-1)\Big((X-Y)^p+(pY)^p\Big)\Big) \end{aligned}$$

The first term is divisible by $X+(p-1)Y$. Since p is odd, the second term is divisible by $(X-Y)+pY = X+(p-1)Y$. So the result is proved.

Which codes satisfy the three assumptions? Clearly we can take C to be the repetition code spanned by $(1,1,\ldots,1)$, to obtain a group of order p^p. In this case, $F(X,Y) = X^{p-1}$.

We can also take the code spanned by $(1,1,\ldots,1)$ and $(0,1,\ldots,p-1)$: note that a cyclic shift of the second vector can be obtained by adding to it a multiple of the first vector, so that the code is cyclic, and only the subcode consisting of multiples of the first vector contains words of weight p. This gives a group of order p^{p-1}. Here $F(X,Y) = X^{p-1} + p(p-1)Y^{p-1}$.

There can be no larger code. For, if there are three basis vectors in echelon form, then one of them has two components equal to zero, so that some scalar does not occur as a component; subtracting this multiple of the all-1 vector we obtain another word of weight p, and the last condition fails.

Remark All transitive groups with reducible cycle index that we know are covered by the propositions above. The groups of smallest degree covered by the above proposition are two groups of degree 9. A search with GAP [10] showed that these are the only transitive groups up to degree 15 with reducible cycle index.

5 Primitive groups

We conjecture that, if G is a primitive permutation group, then $Z(G)$ is irreducible. The conjecture is true for many classes of primitive groups. Here are a few. The first result is immediate from Corollary 2.2.

Proposition 5.1 *If G is the symmetric or alternating group of degree $n \geq 3$, then $Z(G)$ is irreducible.*

Proposition 5.2 *If G is the symmetric or alternating group of degree $m \geq 5$, acting on the set of 2-element subsets of $\{1, \ldots, n\}$, then $Z(G)$ is irreducible.*

Proof Consider first $G = S_m$, Let g and h be elements of G which are cycles of lengths m and $m-1$ in the natural action. If m is odd, then g acts on 2-sets as a product of m-cycles, and h as a product of $(m-1)$-cycles with one $(m-1)/2$-cycle. So the degree of a factor of $Z(G)$ is divisible by both m and $(m-1)/2$, and so is equal to $m(m-1)/2$. The argument for even m is similar.

If $G = A_m$, then one of g and h belongs to G, as does the square of the other. We find that $Z(G)$ is irreducible if m is congruent to 2 or 3 mod 4, but we have to deal with a possible factor of weight $m(m-1)/4$ in the case where m is congruent to 0 or 1 mod 4. This can be excluded by considering elements consisting of either an $(m-2)$ cycle, or its product with a transposition. We omit details.

Of course, the groups $\mathrm{PSL}(2, p)$ and $\mathrm{PGL}(2, p)$ of degree $p + 1$ (for p prime) contain p-cycles, and are handled by Corollary 2.2.

6 Base-transitive groups

A *base* for a permutation group is a sequence of points whose pointwise stabiliser is the identity. A base is *irredundant* if no point in the base is fixed by the pointwise stabiliser of its predecessors.

A permutation group is an *IBIS group* if all irredundant bases have the same number of elements; it is *base-transitive* if it permutes its irredundant bases transitively. Clearly a base-transitive group is an IBIS group.

Cameron and Fon-Der-Flaass [6] showed that the bases of an IBIS group are the bases of a matroid admitting the group as an automorphism group. In the case of a base-transitive group, the matroid is a *perfect matroid design* (PMD); that is, the cardinality of a flat depends only on its rank. The Tutte polynomial of a PMD is determined by these cardinalities (Mphako [18]). Hence in the base-transitive case, the Tutte polynomial is determined by the cycle index ([4, Theorem 7.1]). By the theorem of Merino *et al.* [17], the

Tutte polynomial is irreducible. It does not follow that the cycle index is irreducible, however.

For example, if G is the elementary abelian group of order 9 acting regularly, the cycle index is

$$s_1^9 + 8s_3^3 = (s_1^3 + 2s_3)(s_1^6 - 2s_1^3 s_3 + 4s_3^2),$$

while the corresponding matroid consists of nine parallel elements of rank 1, so that the Tutte polynomial is irreducible.

The base-transitive groups of rank 1 are the regular permutation groups; those of rank greater than 1 have been determined (using the classification of finite simple groups) by Maund [16].

7 Oligomorphic groups

The notion of cycle index can be extended to certain infinite permutation groups, namely those which are *oligomorphic* (that is, have only finitely many orbits on Ω^n for all $n \in \mathbb{N}$). The *modified cycle index* $\tilde{Z}(G)$ of such a group is obtained by summing the cycle index of $G[\Delta]$ as Δ runs over a set of G-orbit representatives for the finite subsets of Ω, where $G[\Delta]$ is the group induced on Δ by its setwise stabiliser.

For finite groups G, $\tilde{Z}(G)$ is obtained from $Z(G)$ by substituting $s_i + 1$ for s_i for all $i \in \mathbb{N}$; so $\tilde{Z}(G)$ is irreducible if and only if $Z(G)$ is. However, for infinite groups, where $\tilde{Z}(G)$ is a formal power series, we cannot expect irreducibility. For example, if S is the infinite symmetric group, then

$$\tilde{Z}(S) = \sum_{n \geq 0} Z(S_n) = \prod_{i \geq 1} \exp\left(\frac{s_i}{i}\right).$$

8 The circle product

The circle product is defined as follows. For two indeterminates s_i and s_j, we put

$$s_i \circ s_j = \left(s_{\mathrm{lcm}(i,j)}\right)^{\gcd(i,j)};$$

then extend multiplicatively to the circle product of two monomials and additively to the circle product of any element of $\mathbb{Z}[s_1, s_2, \ldots]$.

Proposition 8.1 *Let G_1 and G_2 be permutation groups on Ω_1 and Ω_2. Then the cycle index of $G_1 \times G_2$ in its product action is given by*

$$Z(G_1 \times G_2) = Z(G_1) \circ Z(G_2).$$

Proof It is enough to show that if $g_i \in G_i$ for $i = 1, 2$, then (in product action)

$$z(g_1 g_2) = z(g_1) \circ z(g_2).$$

Now, if C and C' are cycles of g_1 and g_2, with lengths i and j respectively, then $C \times C'$ is the disjoint union of $\gcd(i, j)$ cycles of length $\mathrm{lcm}(i, j)$ of $g_1 g_2$.

Note that, for the group $G = C_3 \times C_3$ acting regularly, $Z(G)$ is reducible both for the usual product and the circle product; from Propositions 4.2 and 8.1, we have

$$\begin{aligned}
Z(G) &= \frac{1}{9}(s_1^9 + 8s_3^3) \\
&= \left(\frac{1}{3}(s_1^3 + 2s_3)\right)\left(\frac{1}{3}(s_1^6 - 2s_1^3 s_3 + 4s_3^2\right) \\
&= \left(\frac{1}{3}(s_1^3 + 2s_3)\right) \circ \left(\frac{1}{3}(s_1^3 + 2s_3)\right).
\end{aligned}$$

References

[1] R. E. Block, On the orbits of collineation groups, *Math. Z.* **96** (1967), 33–49.

[2] N. Boston, W. Dabrowski, T. Foguel, P. J. Gies, J. Leavitt, D. T. Ose and D. A. Jackson, The proportion of fixed-point-free elements of a transitive permutation group, *Commun. Algebra* **21** (1993), 3259–3275.

[3] P. J. Cameron, *Permutation Groups*, London Math. Soc. Lecture Notes **45**, Cambridge University Press, Cambridge, 1999.

[4] P. J. Cameron, Cycle index, weight enumerator and Tutte polynomial, *Electronic J. Combinatorics* **9** (2002), #N2 (10pp), available from `http://www.combinatorics.org`

[5] P. J. Cameron, Partitions and permutations, *Discrete Math.* **291** (2005), 45–54.

[6] P. J. Cameron and D. G. Fon-Der-Flaass, Bases for permutation groups and matroids, *Europ. J. Combinatorics* **16** (1995), 537–544.

[7] P. J. Cameron, D. Gewurz and F. Merola, Product action, preprint.

[8] J. D. Dixon and B. Mortimer, *Permutation Groups*, Graduate Texts in Mathematics, **163**, Springer-Verlag, New York, 1996.

[9] B. Fein, W. M. Kantor and M. Schacher, Relative Brauer groups, II, *J. Reine Angew. Math.* **328** (1981), 39–57.

[10] The GAP Group, GAP — Groups, Algorithms, and Programming, Version 4.4.9 (2006); `http://www.gap-system.org`

[11] M. Giudici, Quasiprimitive permutation groups no fixed point free element of prime order, *J. London Math. Soc.* **67** (2003), 73–84.

[12] I. P. Goulden and D. M. Jackson, *Combinatorial Enumeration*, Wiley-Interscience Series in Discrete Mathematics, John Wiley & Sons, Inc., New York, 1983.

[13] C. Greene, Weight enumeration and the geometry of linear codes, *Studies in Applied Math.* **55** (1976), 119–128.

[14] F. Harary and E. M. Palmer, *Graphical Enumeration* Academic Press, New York, 1973.

[15] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.

[16] T. Maund, *Bases for Permutation Groups*, D. Phil. thesis, Oxford University, 1989.

[17] C. Merino, A. de Mier and M. Noy, Irreducibility of the Tutte polynomial of a connected matroid, *J. Combinatorial Theory* Ser B **83** (2001), 298–304.

[18] E. G. Mphako, Tutte polynomials of perfect matroid designs, *Combinatorics, Probability and Computing* **9** (2000), 363–367.

[19] J.-P. Serre, On a theorem of Jordan, *Bull. Amer. Math. Soc.* **40** (2003), 429–440.

[20] D. J. A. Welsh, *Complexity: Knots, Colourings and Counting*, London Math. Soc. Lecture Notes **186**, Cambridge University Press, Cambridge, 1993.