Cycle index, weight enumerator, and Tutte polynomial

Peter J. Cameron
School of Mathematical Sciences
Queen Mary, University of London
Mile End Road
London E1 4NS, U.K.
p.j.cameron@qmul.ac.uk

Submitted: January 9, 2002   Accepted: February 27, 2002

Abstract

With every linear code is associated a permutation group whose cycle index is the weight enumerator of the code (up to a trivial normalisation).

There is a class of permutation groups (the *IBIS groups*) which includes the groups obtained from codes as above. With every IBIS group is associated a matroid; in the case of a group from a code, the matroid differs only trivially from that which arises directly from the code. In this case, the Tutte polynomial of the code specialises to the weight enumerator (by Greene's Theorem), and hence also to the cycle index. However, in another subclass of IBIS groups, the *base-transitive groups*, the Tutte polynomial can be derived from the cycle index but not *vice versa*.

I propose a polynomial for IBIS groups which generalises both Tutte polynomial and cycle index.

1 Cycle index

This note contains some remarks on the relations between the cycle index of a permutation group, the weight enumerator of a linear code, and the Tutte polynomial of a matroid. For more information on permutation groups, codes, and matroids, see [6, 10, 14] respectively.

Let G be a permutation group on a set Ω, where $|\Omega| = n$. For each element $g \in G$, let $c_i(g)$ be the number of i-cycles occurring in the cycle decomposition of g. Now the *cycle index* of G is the polynomial $Z(G)$ in indeterminates $s_1, \ldots, s_n$ given by

$$Z(G) = \frac{1}{|G|} \sum_{g \in G} s_1^{c_1(g)} \cdots s_n^{c_n(g)}.$$

This can be regarded as a multivariate probability generating function for the cycle structure of a random element of G (chosen from the uniform distribution). In particular,

$$P_G(x) = Z(G)(s_1 \leftarrow x, s_i \leftarrow 1 \text{ for } i > 1)$$

is the probability generating function for the number of fixed points of a random element of G, so that substituting $x \leftarrow 0$ gives the proportion of derangements in G. (Here and subsequently, $Z(G)(s_i \leftarrow u_i)$ denotes the result of substituting u_i for s_i in $Z(G)$.)

Many counting problems related to G are solved by specialisations of the cycle index: most notably, the enumeration of G-orbits on functions from Ω to a weighted set is given by the Redfield–Pólya Cycle Index Theorem. Other examples:

- $Z(G)(s_1 \leftarrow x+1, s_i \leftarrow 1 \text{ for } i > 1)$ is the exponential generating function for the number of G-orbits on k-tuples of distinct points (note that this function is $P_G(x+1)$, compare Boston *et al.* [1]);
- $Z(G)(s_i \leftarrow x^i + 1)$ is the ordinary generating function for the number of orbits of G on k-element subsets of Ω;
- $k[(\partial/\partial s_k)Z(G)](s_i \leftarrow 1)$ is the kth component of the *Parker vector* of G, the number of orbits of G on the set of k-cycles occurring in its elements (Gewurz [7]).

2 A group from a linear code

Let C be an $[n,k]$ code over $\mathrm{GF}(q)$ (a k-dimensional subspace of $\mathrm{GF}(q)^n$). The *weight enumerator* of C is the polynomial

$$W_C(X,Y) = \sum_{v \in C} X^{n-\mathrm{wt}(v)} Y^{\mathrm{wt}(v)},$$

where the *weight* $\mathrm{wt}(v)$ of v is the number of non-zero coordinates of v.

We construct a permutation group G from C as follows: the permutation domain Ω is the disjoint union of n copies of $\mathrm{GF}(q)$, and a codeword acts by translating the ith copy by its ith coordinate. More formally, $\Omega = \mathrm{GF}(q) \times \{1, \ldots, n\}$, and the codeword $v = (v_1, \ldots, v_n)$ acts as the permutation

$$(x,i) \mapsto (x+v_i, i).$$

Now G is isomorphic to the additive group of C (so $|G| = |C|$), and all the cycles of G have length 1 or p, where p is the characteristic of $\mathrm{GF}(q)$, so $Z(G)$ involves s_1 and s_p only. Furthermore, we have:

$$\frac{1}{|C|} W_C(X,Y) = Z(G; s_1 \leftarrow X^{1/q}, s_p \leftarrow Y^{p/q}),$$

For a zero coordinate in v gives rise to q fixed points, and a non-zero coordinate to q/p cycles of length p.

3 Symmetrised weight enumerator

There has been a lot of interest recently (arising from [9]) in codes over Z_4 (the integers mod 4); that is, additive subgroups of Z_4^n. In place of the weight enumerator, one usually considers the *symmetrised weight enumerator* $S_C(X,Y,Z)$ defined by

$$S_C(X,Y,Z) = \sum_{v\in C} X^{n_0(v)}Y^{n_2(v)}Z^{n_{13}(v)},$$

where $n_0(v)$, $n_2(v)$ and $n_{13}(v)$ are respectively the numbers of coordinates of v which are 0, 2, or (1 or 3) mod 4.

We can construct a group from a Z_4-code just as in the linear case, replacing $\mathrm{GF}(q)$ by Z_4. Arguing as above we see that

$$\frac{1}{|C|}S_C(X,Y,Z) = Z(G; s_1 \leftarrow X^{1/4}, s_2 \leftarrow Y^{1/2}, s_4 \leftarrow Z).$$

More generally, let $A_1,\ldots,A_n$ be groups of the same order. We can regard a group code over the alphabets $A_1,\ldots,A_n$ as a subgroup G of $A_1\times\cdots\times A_n$. Then the cycle index of G, suitably normalised, is a kind of symmetrised weight enumerator of the form

$$\sum_{g\in G}\prod_m X_m^{o_m(g)},$$

where $o_m(g)$ is the number of coordinates of g which have order m (in the appropriate group).

4 Tutte polynomial

With a linear $[n,k]$ code C we may associate in a canonical way a matroid M_C on the set $\{1,\ldots,n\}$ whose independent sets are the sets I for which the columns $(c_i : i \in I)$ of a generator matrix for C are linearly independent. Any matroid M on the ground set E has a *Tutte polynomial*, a two-variable polynomial of the form

$$T(M;x,y) = \sum_{A\subseteq E}(x-1)^{\rho(E)-\rho(A)}(y-1)^{|A|-\rho(A)},$$

where ρ is the rank function of M.

Greene [8] showed the following theorem:

Theorem 4.1 *Let M be the matroid associated with a linear $[n,k]$ code C over* $\mathrm{GF}(q)$. *Then the weight enumerator of C is a specialisation of the Tutte polynomial of M:*

$$W_C(X,Y) = Y^{n-k}(X-Y)^kT\left(M_C; x \leftarrow \frac{X+(q-1)Y}{X-Y}, y \leftarrow \frac{X}{Y}\right).$$

We might ask whether it is possible to associate an analogue of the Tutte polynomial with any permutation group, and if so, what is its relation to the cycle index. Recent results of Rutherford [13] show that in general this will be very difficult.

Rutherford associated a three-variable analogue of the Tutte polynomial with any Z_4-code C. This polynomial behaves in the expected way with respect to the analogues of restriction and contraction, and it specialises to the weight enumerators of each of the "elementary divisors" of C (the two binary codes $C \bmod 2$ and $(C \cap 2Z_4^n)/2$). However, it does not specialise to the symmetrised weight enumerator of C; indeed, Rutherford showed that, under reasonable assumptions, there is no analogue of the Tutte polynomial which does so specialise.

In the next section we describe a class of permutation groups which give rise to matroids (and hence Tutte polynomials) in a natural way.

5 IBIS groups

Let G be a permutation group on Ω. A *base* for G is a sequence of points of Ω whose stabiliser is the identity. It is *irredundant* if no point in the sequence is fixed by the stabiliser of its predecessors.

Cameron and Fon-Der-Flaass [3] showed:

Theorem 5.1 *The following three conditions on a permutation group are equivalent:*

(a) all irredundant bases have the same number of points;

(b) re-ordering any irredundant base gives an irredundant base;

(c) the irredundant bases are the bases of a matroid.

A permutation group satisfying these conditions is called an *IBIS group* (short for Irredundant Bases of Invariant Size).

For example, any Frobenius group is an IBIS group of rank 2, associated with the uniform matroid; the general linear and symplectic groups, acting on their natural vector spaces, are IBIS groups, associated with the vector matroid (defined by all vectors in the space); the Mathieu group M_{24} in its natural action is an IBIS group of rank 7.

The permutation group constructed from an $[n,k]$ linear code over $\mathrm{GF}(q)$ in Section 2 is an IBIS group of degree nq and rank k; a base is a set of size k containing one point from each copy of $\mathrm{GF}(q)$ corresponding to a set of k linearly independent columns of a generator matrix. The associated matroid is obtained from the matroid of the code simply by replacing each element by a set of q parallel elements. It is straightforward to obtain the Tutte polynomial of the group matroid from that of the code matroid and *vice versa*, using the following elementary result:

Proposition 5.2 *If M_q is obtained from M by replacing each element by q parallel elements, then*

$$T(M_q;x,y) = \left(\frac{y^q-1}{y-1}\right)^{\rho(E)} T\left(M; x \leftarrow \frac{xy-x-y+y^q}{y^q-1}, y \leftarrow y^q\right).$$

Any semiregular permutation group of degree n is an IBIS group. The corresponding matroid consists simply of n parallel elements. The cycle index conveys much more information, for example, the number of orbits of G and the number of elements of each order in G. (This case is a "generalised repetition code" of length n over G.)

The authors of [3] asked for a classification of the matroids associated with IBIS groups. In view of the observation that the group associated with any linear code is an IBIS group, this seems hopelessly optimistic. Note, however, that the IBIS groups associated with uniform matroids of rank greater than 2 are explicitly known.

In the rest of the paper, I will use "base" (of a permutation group) to mean "irredundant base".

6 Perfect matroid designs

A *perfect matroid design*, or PMD, is a matroid having the property that the cardinality of a flat depends only on its rank. Not very many PMDs are known: among the geometric matroids, only uniform matroids, truncations of projective and affine spaces, Steiner systems, and Hall triple systems. See Deza [5] for a survey.

The following theorem is due to Mphako [12]: I outline the proof.

Theorem 6.1 *Let M be a PMD of rank k whose i-flats have cardinality n_i for $i \leq k$. The Tutte polynomial of M is determined by the numbers $n_0, \ldots, n_k$.*

Proof It is enough to determine the number $a(m,i)$ of subsets of the domain which have cardinality m and rank i for all m and i: for

$$T(M;x,y) = \sum_{i=0}^{k} \sum_{m=i}^{n} a(m,i)(x-1)^{k-i}(y-1)^{m-i}.$$

Let $s(i,j)$ be the number of i-flats containing a given j-flat for $j \leq i$. Then

$$\begin{aligned} s(i,j) &= \prod_{h=j}^{i-1} \frac{n-n_h}{n_i-n_h}, \\ s(i,0)\binom{n_i}{m} &= \sum_{j=0}^{i} a(m,j)s(i,j). \end{aligned}$$

The first equation determines the numbers $s(i,j)$. The second is a a triangular system of equations for $a(m,j)$ with diagonal coefficients $s(i,i) = 1$. We see that the $a(m,j)$ are indeed determined.

The next result is not immmediately related to the topic of this paper, but we will see an application in the next section. We say that the action of a group G on a matroid M is *flat* if the fixed points of any element of G form a flat of the matroid. Any group has a flat action on the free matroid; and any linear group has a flat action on the vector matroid of its vector space.

An IBIS group has a flat action on its associated matroid. (This is easily proved by induction, on noting that the loops of the matroid are the global fixed points of the group, since any non-fixed point is the first point in some irredundant base.) The converse is far from true: as we noted, every permutation group has a flat action on the free matroid.

Theorem 6.2 *Let M be a PMD of rank k on n elements, in which an i-flat has cardinality n_i for $i = 0\dots,k$ (with $n_k = n$). Then there are numbers $b(m,i)$, for $0 \le m \le n$ and $0 \le i \le k$, depending only on $n_0,\dots,n_k$, such that the following is true: If a group G has a flat action on M and has x_i orbits on independent i-tuples and y_m orbits on m-tuples of distinct elements, then*

$$y_m = \sum_{i=0}^{k} b(m,i)x_i$$

for $m = 0,\dots,n$.

Remarks: 1. In the case of the free matroid, the matrix $(b(m,i))$ is the identity. For the vector matroid, it is the composition of the matrix of Gaussian coefficients with the matrix of Stirling numbers of the second kind (Cameron and Taylor [4]).

2. The exponential generating function for the numbers $y_0,\dots,y_n$ is $P_G(x+1)$ (Boston *et al.* [1]); so the numbers $x_0,\dots,x_k$ determine $P_G(x)$.

Proof By the Orbit-Counting Lemma, it suffices to show that such a linear relation holds between the number of linearly independent i-tuples fixed by an arbitrary element $g \in G$ and the total number of m-tuples of distinct elements fixed by g. Since the fixed points of G form a flat, it suffices to establish such a relation between the numbers of tuples in any flat of M.

So let F be an r-flat. Then

$$\begin{aligned} x_i &= \prod_{j=0}^{i-1}(n_r - n_j) = X_i(n_r), \\ y_m &= \prod_{s=0}^{m-1}(n_r - s) = Y_m(n_r), \end{aligned}$$

where X_i and Y_i are polynomials of degree i. It follows immediately that the theorem holds for $m \le k$, with $(b(m,i))$ the transition matrix between the two sequences of polynomials.

For $m > k$, let $F_m(x)$ be the unique monic polynomial of degree m having roots $n_0,\dots,n_k$ and no term in x^l for $k+1 \le l \le m-1$. Using F_m, we can express n_i^m (and hence $Y_m(n_i)$) as a linear combination of $1,n_i,\dots,n_i^k$ (and hence of $X_0(n_i),\dots,X_k(n_i)$). This concludes the proof.

7 Base-transitive groups

If G is a permutation group which permutes its (irredundant) bases transitively, then G is clearly an IBIS group, and the associated matroid is a PMD. Such groups have been given the somewhat unfortunate name of "geometric groups"; I will simply call them *base-transitive groups*.

The base-transitive groups of rank greater than 1 were determined by Maund [11], using the Classification of Finite Simple Groups; those of sufficiently large rank by Zil'ber [15] by geometric methods not requiring the Classification. Base-transitive groups of rank 1 are just regular permutation groups (possibly with some global fixed points).

Theorem 7.1 *For a base-transitive group G, the p.g.f. $P_G(x)$ and the Tutte polynomial of the associated matroid determine each other, and each is determined by knowledge of the numbers of fixed points of elements of G.*

Proof A permutation group G is base-transitive if and only if the stabiliser of any sequence of points acts transitively on the points that it doesn't fix (if any). Thus the fixed points of every element form a flat. Also, by Jordan's theorem (asserting that a transitive permutation group of degree greater than 1 contains a fixed-point-free element), every flat is the fixed point set of some element. So the numbers of fixed points of the elements of G determine the cardinalities of flats, and hence the Tutte polynomial of the matroid, by Theorem 6.1.

Theorem 6.2 shows that the numbers $n_0,\ldots,n_k$ of fixed points of elements in a base-transitive group determine the function $P_G(x)$, since the numbers $x_0,\ldots,x_k$ are all equal to 1.

To obtain $P_G(x)$ directly from the Tutte polynomial, we show the following:

$$P_G(x+1)=\sum_{m=0}^{n}\left(\sum_{i=0}^{k}\frac{a(m,i)}{r(i)}\right)x^m,$$

where $n=n_k$ is the number of points, and $r(i)$ is the number of independent i-tuples in the matroid; as in Theorem 6.1, $a(m,i)$ is the number of m-sets of rank i.

To prove this, we note that each m-set can be ordered in $m!$ different ways. If the rank of the m-set is i, the resulting sequence has stabiliser of order $\prod_{j=i}^{k-1}(n-n_j)$, and so lies in an orbit of size $\prod_{j=0}^{i-1}(n-n_j)=r(i)$. Thus, the number of orbits on such tuples is $a(m,i)m!/r(i)$. We obtain the total number of orbits on m-tuples by summing over i, and so we find that the exponential generating function is the right-hand side of the displayed equation. But this e.g.f. is $P_G(x+1)$, by the result of Boston *et al.* [1].

As noted, even for a regular permutation group, knowledge of the fixed point numbers does not determine the cycle index. A regular permutation group is base-transitive; we have seen that the cycle index contains more information than the Tutte polynomial in this case.

8 An example

Unfortunately, the cycle index does not in general tell us whether a permutation group is base-transitive. The simplest counterexample consists of the two permutation groups of degree 6,

$$G_1=\langle(1,2)(3,4),(1,3)(2,4)\rangle,\quad G_2=\langle(1,2)(3,4),(1,2)(5,6)\rangle.$$

The first is base-transitive; the second is an IBIS group of rank 2 (indeed, it is the group arising from the binary even-weight code of length 3), but not base-transitive. A simple modification of this example shows that the cycle index does not determine whether the IBIS property holds.

Suppose we are given the cycle index of one of these groups, namely $Z(G) = \frac{1}{4}(s_1^6 + 3s_1^2 s_2^2)$, or simply the p.g.f. for fixed points, namely $P_G(x) = \frac{1}{4}(x^6 + 3x^2)$.

- If we are told that the group is base-transitive, then we know that its matroid is a PMD with $n_0 = 2$, $n_1 = 6$, and so we can compute that its Tutte polynomial is $y^2(y^3 + y^2 + y + x)$.
- If we are told that the group arises from a linear code C, then we can deduce that $W_C(X,Y) = X^3 + 3XY^2$. In general the Tutte polynomial is not computable from the weight enumerator, but in this case the code must be the even-weight code and so the Tutte polynomial of the code matroid is $x^2 + x + y$. Now Proposition 5.2 shows that the Tutte polynomial of the group matroid is $y^4 + 2y^3 + 3y^2 + y + 3xy + x^2 + x$.
- This matroid on 6 elements arises from two different base-transitive groups of order 24. Using any of several methods we've seen, it follows that, for any such group G, we have $P_G(x) = \frac{1}{24}(x^6 + 9x^2 + 14)$. However, the stabiliser of a point is cyclic of order 4 in one case and is a Klein group in the other, so the two groups have different cycle index.

9 Ingredient X?

In some IBIS groups, the Tutte polynomial of the matroid determines the cycle index, while in others, it is the other way about. Is there a more general gadget including both polynomials?

Following the definition of the Tutte polynomial, we try for a sum, over subsets, of "local" terms. First, some terminology and observations. Let G be a permutation group on Ω. For any subset A of Ω, G_A and $G_{(A)}$ are the setwise and pointwise stabilisers of A, and G_A^A the permutation group induced on A by its setwise stabiliser (so that $G_A^A \cong G_A/G_{(A)}$). Let $b(G)$ denote the minimum size of a base for G. (This is the rank of the associated matroid if G is an IBIS group.)

Now we have

(a) $\displaystyle\sum_{A \in \mathcal{P}\Omega/G} Z(G_A^A) = Z(G; s_i \leftarrow s_i + 1 \text{ for } i = 1, \ldots, n)$,
where $\mathcal{P}\Omega/G$ denotes a set of orbit representatives for G on the power set of Ω. This is proved in [2], where it is exploited to extend the definition of cycle index to certain infinite permutation groups.

(b) If G is an IBIS group, then the fixed point set of $G_{(A)}$ is the flat spanned by A; so $G_{(A)}$ is an IBIS group, and $\rho(A) = b(G) - b(G_{(A)})$. In fact, G_A^A is also an IBIS group, but its base size may be smaller than $\rho(A)$.

Now we define the *Tutte cycle index* of G to be the polynomial in $u, v, s_1, \ldots, s_n$ given by

$$ZT(G) = \frac{1}{|G|} \sum_{A \subseteq \Omega} u^{|G_A|} v^{b(G_{(A)})} Z(G_A^A).$$

One obvious flaw in this definition is that the factors $u^{|G_A|}$ and $v^{b(G_{(A)})}$ are not really "local". Nevertheless, we have the properties we are looking for:

Proposition 9.1 *Let G be an IBIS permutation group, with associated matroid M.*

(a) $\left(\dfrac{\partial}{\partial u}ZT(G)\right)(u \leftarrow 1, v \leftarrow 1) = Z(G; s_i \leftarrow s_i + 1 \textit{ for } i = 1, \ldots, n).$

(b) $|G|ZT(G; u \leftarrow 1, s_i \leftarrow t^i \textit{ for } i = 1, \ldots, n) = t^{b(G)}T(M; x \leftarrow vt^{-1} + 1, y \leftarrow t + 1).$

Proof (a) The G-orbit of the subset A has cardinality $|G|/|G_A|$. Dividing by this number has the same effect as choosing one representative set from each orbit. Now apply point (a) before the Proposition.

(b) Point (b) before the Proposition shows that $\rho(A) = b(G) - b(G_{(A)})$. Also, substituting t^i for s_i in $Z(H)$ gives t^n, where n is the degree of the permutation group H. The rest is just manipulation.

Part (a) does not require that G is an IBIS group. The indeterminate v is irrelevant for this part; we could substitute $v \leftarrow 1$ and delete all reference to matroid rank.

As a final speculation, the (irredundant) bases in an arbitrary permutation group form a combinatorial structure more general than a matroid; perhaps there is an analogue of Tutte polynomial or some generalisation for such structures, which would be related to the cycle index in the group case.

References

[1] 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.

[2] P. J. Cameron, *Oligomorphic Permutation Groups*, London Math. Soc Lecture Notes **152**, Cambridge University Press, Cambridge, 1990.

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

[4] P. J. Cameron and D. E. Taylor, Stirling numbers and affine equivalence, *Ars Combinatoria* **20B** (1985), 3–14.

[5] M. Deza, Perfect matroid designs, *Encycl. Math. Appl.* **40** (1992), 54–72.

[6] J. D. Dixon and B. Mortimer, *Permutation Groups*, Springer, New York, 1996.

[7] D. Gewurz, *Sui vettori di Parker e concetti correlati*, Ph.D. thesis, Università di Roma “La Sapienza”, 1999.

[8] C. Greene, Weight enumeration and the geometry of linear codes, *Studia Appl. Math.* **55** (1976), 119–128.

[9] A. R. Hammons Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane and P. Solé, The Z_4-linearity of Kerdock, Preparata, Goethals and related codes, *IEEE Trans. Inform. Theory* **40** (1994), 301–319.

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

[11] T. C. Maund, D.Phil. thesis, University of Oxford, 1989.

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

[13] C. G. Rutherford, *Matroids, codes and their polynomial links*, Ph.D. thesis, University of London, 2001.

[14] D. J. A. Welsh, *Matroid Theory*, Academic Press, London, 1976.

[15] B. I. Zil'ber, The structure of models of uncountably categorical theories, pp. 359–368 in *Proc. Internat. Congr. Math.* Vol. 1 (Warsaw 1983).