Finite geometry and permutation groups: some polynomial links

Peter J. Cameron
School of Mathematical Sciences
Queen Mary, University of London
Mile End Road
London E1 4NS, U.K.

Abstract

Any set of points in a finite projective space PG(n,q) defines a matroid which is representable over GF(q). The Tutte polynomial of the matroid is a two-variable polynomial which includes a lot of numerical information about the configuration of points. For example, it determines the weight enumerator of the code associated with the point set, and hence the cardinalities of hyperplane sections of the set.

Another polynomial used in enumeration is the cycle index of a permutation group, which includes information about the number of orbits of the group on various configurations. This is the subject of a well-developed theory.

The aim (not yet realised) of the research reported here is to combine the Tutte polynomial of a matroid with the cycle index of any group acting on the matroid to obtain a more general polynomial which tells us about the number of orbits of the group on configurations counted by the Tutte polynomial.

The paper includes an introductory exposition of all these topics.

1 Introduction

A set of points in a finite projective space can be regarded as a matroid M (with no dependent set of size 2) together with a vector representation of M over a

finite field. Many geometric properties of the point set, such as the cardinalities of subspace interesections, can be read off from the matroid, or from its Tutte polynomial.

In addition, a (linear) code over a finite field gives rise to a matroid on the set of coordinate positions of the code. According to a theorem of Greene, the weight enumerator of the code is a specialisation of the Tutte polynomial of the matroid.

For example, from this point of view, Segre's problems about arcs in projective spaces have been re-interpreted as problems about representations of uniform matroids, or about linear MDS codes. But the principle applies much more widely.

A linear code also gives rise to a special type of permutation group, a so-called IBIS group. The cycle index of this group is equivalent (under a simple transformation) to the weight enumerator of the code. Every IBIS group acts on a matroid, and in the case of the groups derived from linear codes, the cycle index is a specialisation of the Tutte polynomial. However, there are other IBIS groups for which the cycle index determines the Tutte polynomial of the matroid. These facts suggest that a common generalisation exists.

In this paper, I consider the general situation of a group G of automorphisms of a matroid M. The aim is to find a polynomial which determines both the cycle index of G and the Tutte polynomial of M, and which extends the role of the cycle index in orbit-couting to varius configurations enumerated by the Tutte polynomial. A candidate for such a polynomial is proposed, but its properties have not been determined yet.

2 Codes and weight enumerators

A *linear code* C of length n over $\mathrm{GF}(q)$ is simply a subspace of the vector space $\mathrm{GF}(q)^n$. Each element c of C has weight $\mathrm{wt}(c)$, the number of non-zero coordinates of C. The *weight enumerator* of C is the 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 C of weight i. Although it is really a polynomial in a single variable, it is customary to write it as a homogeneous polynomial in two variables, as done here.

As is well known, codes are used for error correction. The *Hamming distance* between two codewords is the number of places where they differ. If two words v,w have Hamming distance at least $2e+1$, and at most e symbols are received

incorrectly when v is transmitted, then the received word will be closer to v than to w. Thus, if we use a code C with minimum distance at least $2e+1$, then e errors can be corrected. If C is linear, then its minimum distance is equal to the minimal weight of a non-zero codeword, and can be read off from the weight enumerator of C.

We say that C is an $[n,k,d]$ code over $\mathrm{GF}(q)$ if it has length n, dimension k, and minimum distance d.

We call two linear codes *equivalent* if one can be obtained from the other by a monomial transformation (a permutation of the coordinates followed by multiplication of the coordinates by possibly different non-zero scalars). In the case $q=2$, the only non-zero scalar is 1, and equivalence involved merely a coordinate permutation. Note that equivalent codes have the same weight enumerator (but not conversely, as the next example shows).

Example 1 Here are two *binary codes* (that is, codes over the field $\mathrm{GF}(2)$).

000000	000000
110000	110000
001100	101000
000011	011000
+ complements	+ complements

Both codes have length 6 and dimension 3, and it is easy to see that they both have weight enumerator $X^6+3X^4Y^2+3X^2Y^4+Y^6$. In fact they are not equivalent (under permutation of coordinates), as we will see.

The *dual code* $C^\perp$ of a code C is defined by

$$C^\perp = \{v \in \mathrm{GF}(q)^n : v\cdot c = 0 \text{ for all } c \in C\}.$$

If C has length n and dimension k, then $C^\perp$ has dimension $n-k$. More surprisingly, *MacWilliams' Theorem* shows that the weight enumerator of $C^\perp$ is determined by that of C:

Theorem 2.1 *Let C be a linear code. Then*

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

In coding theory, there is a tension between the minimum distance and cardinality of a code; they cannot both be too large. One result along these lines is the *Singleton bound*, stated here just for linear codes:

Theorem 2.2 *If C is an $[n,k,d]$ code, then $k \leq n-d+1$.*

A code attaining this bound is called *maximum distance separable*, or an *MDS code*.

3 Matroids and Tutte polynomials

Matroids were introduced by Whitney to model the notion of linear independence in a vector space. A matroid consists of a pair $(E, \mathscr{I})$, where $\mathscr{I}$ is a non-empty set of subsets (called *independent sets*) of the ground set E satisfying the two conditions

(M1) $\mathscr{I}$ is closed downwards, that is, if $J \subseteq I \in \mathscr{I}$, then $J \in \mathscr{I}$.

(M2) The *exchange axiom*: if $I_1, I_2 \in \mathscr{I}$ and $|I_2| > |I_1|$, then there exists $x \in I_2 \setminus I_1$ such that $I_1 \cup \{x\} \in \mathscr{I}$.

It follows that any two *bases* (maximal independent sets) have the same cardinality, called the *rank* of the matroid. More generally, the *rank* rank $\rho(A)$ of a subset A of E is the size of a maximal independent subset of A. Matroids can be axiomatised in terms of the bases or their rank function (or indeed in various other ways).

A family of vectors in a vector space V forms a matroid, where independence is linear independence. Such a matroid is called a *vector matroid*. If all sets of size at most 2 in such a matroid are independent, then each 1-dimensional subspace contains at most one vector in E. In this case, the matroid represents a subset of the projective space based on V. We call such a matroid a *projective matroid*.

Matroids arise in many other situations too. For example:

- E is a subset of an algebraically closed field, and independence is algebraic independence over the prime subfield (this is an *algebraic matroid*);
- E indexes a family of sets, and a subset of E is independent if it indexes a subfamily possessing a transversal (this is a *transversal matroid*);

- E is the edge set of an undirected graph, and a subset is independent if it contains no cycle (this is a *graphic matroid*).

An important though easy example of a matroid is the *uniform matroid* $U_{k,n}$, whose independent sets are all subsets of cardinality at most k of the ground set of size n.

The *dual* M^* of a matroid M is the matroid whose bases are the complements of the bases of M.

Associated with a matroid M on E, with rank function ρ, is a two-variable polynomial called the Tutte polynomial of the matroid, defined as follows:

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

(This is not Tutte's original definition, but is essentially due to Whitney; it is not at all trivial to prove the equivalence of the two definitions.) It is easy to see that $T(M^*,x,y) = T(M;y,x)$.

In the case of a matroid representing a subset E of a projective space, the Tutte polynomial encodes a lot of geometric information about E, such as cardinalities of its intersections with subspaces of the projective space.

4 Matroids and codes

Let A be a $k \times n$ matrix over $\mathrm{GF}(q)$ with linearly independent rows. There are two natural objects we can obtain from A:

- The row space of A is a linear code C with length n and dimension k.
- The columns of A are vectors in $\mathrm{GF}(q)^k$, and so define a vector matroid M of rank k and cardinality n.

Row operations on A don't change C, and merely change the basis of the vector space in which M is represented. Monomial transformations on the columns replace C by an equivalent code and merely re-label the points of M. Thus either of these combinatorial objects is a natural invariant for matrices under the equivalence relation generated by these operations.

The code C and the matroid M which correspond in this way have closely related properties. Here are a couple of examples.

- The dual matroid M^* correspondsto the dual code $C^\perp$.

- M is projective if and only if $C^\perp$ has minimum weight at least 3.
- M is represented by an n-arc in $\mathrm{PG}(k-1,q)$ (a set of n points, no $k+1$ contained in a hyperplane) if and only if C is an MDS code of length n and dimension k. Thus Segre's fundamental problems [6] on arcs in projective space are equivalent to problems about the existence of linear MDS codes, or about vector representations of uniform matroids. I refer to [1] or to Hirschfeld's article in these Proceedings for further details.

Curtis Greene greene proved that the weight enumerator of C is a specialisation of the Tutte polynomial of M:

Theorem 4.1 *If the code C and matroid M are associated as above, then*

$$W_C(X,Y) = (X-Y)^{n-k}Y^k T\left(M; \frac{X+(q-1)Y}{X-Y}, \frac{X}{Y}\right).$$

Note that Greene's Theorem, together with the above observation abbout duality, can be used to give a purely combinatorial proof of MacWilliams' Theorem. (The original proof involved character sums.)

The Tutte polynomial is not a complete invariant of matroids; there exist non-isomorphic matroids with the same Tutte polynomial. Nevertheless, it is more discriminating than the weight enumerator. For example, the two codes in Example 1 have different Tutte polynomials, and so are not equivalent. Indeed, we find that the first has eight bases while the second has ten.

5 Permutation groups and cycle index

The *cycle index* of a permutation group is the multivariate probability generating function for cycle lengths of a random element of the group. That is, the cycle index $Z(G)$ is a polynomial in the indeterminates $s_1,\ldots,s_n$ (where n is the degree) given by

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

where $c_i(g)$ is the number of i-cycles of the permutation g.

As an indication of its use, I state the Cycle Index Theorem. Suppose that we are given a set F of *figures* with non-negative integer weights, where a_i is the number of figures of weight i. Let $A(x) = \sum a_i x^i$ be the generating function for these numbers.

Now let G be a permutation group on E. We wish to count orbits of G on the set of functions from E to F by weight, where the weight of a function ϕ is the sum of the weights of its values, and the G-action is given by $(\phi^g)(x) = \phi(xg^{-1})$. Let b_i be the number of orbits on functions of weight i, and $B(x) = \sum b_i x^i$ its generating function. The *Cycle Index Theorem* asserts that

$$B(x) = Z(G; s_i \leftarrow A(x^i)),$$

where $F(s_i \leftarrow t_i)$ denotes the result of substituting t_i for s_i in F, for all i.

For example, $Z(G; s_i \leftarrow 1 + x^i)$ is the generating function for the numbers of orbits of G on k-sets, for all k. (Take two figures, with weights 1 and 0; now functions from E to F are characteristic functions of subsets of E, and the weight of a function is the cardinality of the set.)

Example 2 below shows that a permutation group is not determined up to permutation ismorphism by its cycle index. (Indeed, it is not even determined up to group isomorphism.)

One result we require later is the *Shift Theorem*. In this theorem, $\mathscr{P}E/G$ denotes a set of representatives of the orbits of G on the power set of E, and $G(A)$ denotes the permutation group induced on the set A by its setwise stabiliser in G.

Theorem 5.1 *For any permutation group G on a set E, we have*

$$\sum_{A \in \mathscr{P}E/G} Z(G(A)) = Z(G; s_i \leftarrow s_i + 1).$$

This theorem is the basis for extending the cycle index to infinite permutation groups. The definition of cycle index fails for infinite groups. But the expression on the left-hand side of the equation in the theorem (where the summation is over orbit representatives of finite sets) is well-defined if and only if the permutation group is *oligomorphic*, that is, has only finitely many orbits on n-sets for all n. But that is another story!

6 Comparisons

In this section, we meet two special situations where a permutation group and a matroid are associated with each other. In the first case, the Tutte polynomial determines the cycle index but not the other way round; in the second case, the reverse is true.

6.1 Groups from codes

Let C be a linear code of length n and dimension k over GF(q). We represent the additive group of C as a permutation group on the set $E = \{1,\ldots,n\} \times \mathrm{GF}(q)$ as follows: the codeword $c = c_1 \ldots c_n$ induces the permutation

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

There is a matroid defined onthe set E, by *blowing up* the matroid on $\{1,\ldots,n\}$ associated with C (replacing each point i by q pairwise dependent points (i,x) for $x \in \mathrm{GF}(q)$). We will see later a procedure for obtaining the matroid directly from the permutation group.

It is easy to see that the weight enumerator of the code and the cycle index of the group are related by

$$Z(G) = \frac{1}{|C|} W_C(s_1^q, s_0^{q/p}),$$

where p is the characteristic of GF(q).

Example 2 The binary *repetition code* $\{000, 011, 101, 110\}$ of length 3 corresponds to the permutation group of degree 6 consisting of the identity and the three permutations $(3,4)(5,6)$, $(1,2)(5,6)$, and $(1,2)(3,4)$. We have $W_C(X,Y) = X^3 + 3XY^2$ and $Z(G) = \frac{1}{4}(s_1^6 + 3s_1^2 s_2^2)$.

Note that there is another permutation group which has the same cycle index, namely the group consisting of the identity and the three permutations $(1,2)(3,4)$, $(1,3)(2,4)$, and $(1,4)(2,3)$ (all fixing 5 and 6). This group does not arise from a code.

6.2 Base-transitive groups

A *base* for a permutation group is a sequence of points of the domain whose pointwise stabiliser is the identity. A base is *irredundant* if no point is fixed by the pointwise stabiliser of its predecessors. A permutation group is called *base-transitive* if it permutes its irredundant bases transitively.

Examples of base-transitive groups include the symmetric and alternating groups, and the general linear and affine groups. For example, in the general linear group GL(d,q), the bases are precisely the vector space bases of GF$(q)^d$.

The bases of a base-transitive group are the bases of a matroid. (This is not the case for arbiitrary permutation groups; later we will examine the class of groups

for which it holds.) This matroid is a *perfect matroid design*: that is, the cardinality of a flat of rank k (a maximal subset of rank k) depends only on k. Mphako [5] showed that the Tutte polynomial of a perfect matroid design is determined by the cardinalities of the flats.

A base-transitive group of rank 1 is simply a regular permutation group (possibly with some global fixed points). Using the Classification of Finite Simple Groups, Maund [4] determined all the finite base-transitive groups.

Example 3 There are two permutation groups which are base-transitive and whose associated matroid is $U_{2,3}$ with each point blown up to a pair of points:

- the symmetric group S_4, acting on the set of unordered pairs from $\{1,2,3,4\}$;
- the rotation group of the cube, acting on the set of faces of the cube.

Both are abstractly isomorphic to S_4, but the actions are non-isomorphic and the cycle indices are unequal. In the first group, an element of order 4 has a 2-cycle and a 4-cycle; in the second, such an element has two fixed points and a 4-cycle.

7 IBIS groups

Recall the definition of an irredundant base for a permutation group. The following was shown by Cameron and Fon-Der-Flaass [3]:

Theorem 7.1 *For a permutation group G, the following are equivalent:*

- *all irredundant bases have the same size;*
- *the irredundant bases are preserved by re-ordering;*
- *the irredundant bases are the bases of a matroid.*

A group satisfying these conditions is called an *IBIS group* (an acronym for "Irredundaant Bases of Invariant Size").

The IBIS groups form a special class of permutation groups connected with matroids which includes both classes (groups derived from codes and base-transitive groups) described earlier.

In the case of a permutation group G from a code C, the matroid associated with G as IBIS group coincides with the one obtained by blowing up the matroid of C. Thus, in this case, the cycle index is a specialisation of the Tutte polynomial.

By contrast, in the base-transitive groups of Example 3, the Tutte polynomial is determined by the cardinalities of the fixed-point sets, and so is determined by the cycle index (but not conversely).

The two permutation groups with the same cycle index in Example 2 are both IBIS groups, but with different rank, and corresponding to very different matroids: in the first case, a blow-up of $U_{2,3}$, and in the second case, $U_{1,4}$ with two added loops (elements of rank 0).

Thus, in all three cases, the Tutte cycle index suffices to distinguish the groups concerned.

There are many other IBIS groups: for example, all Frobenius or Zassenhaus groups, symplectic and unitary groups (acting on their natural vector spaces). The classification problem for these groups, or even for the associated matroids, is open.

8 A generalisation

In this section, there are some speculations about constructing a polynomial associated with a group G acting on a matrooid M. We want a polynomial with the following properties:

- it specialises to both the Tutte polynomial of M and the cycle index of G;
- for each "standard" enumeration problem solved by a specialisation of the Tutte polynomial, the problem of counting G-orbits should be solved by a specialisation of the new polynomial.

This aim has not yet been realised!

8.1 Equivariant Tutte polynomial

Let G be a group of automorphisms of the matroid M. The *equivariant Tutte polynomial* $T(M,G)$ is obtained in the manner suggested by the Orbit-counting Lemma: we average, for $g \in G$, the terms in the summation for the Tutte polynomial corresponding to sets fixed by g. That is,

$$T(M,G;x,y) = \frac{1}{|G|}\sum_{g\in G}\sum_{\substack{A\subseteq E\\ Ag=A}}(x-1)^{\rho(E)-\rho(A)}(y-1)^{|A|-\rho(A)}$$

$$
\begin{aligned}
&= \frac{1}{|G|}\sum_{A\subseteq E}\sum_{g\in G_A}(x-1)^{\rho(E)-\rho(A)}(y-1)^{|A|-\rho(A)}\\
&= \frac{1}{|G|}\sum_{A\in\mathscr{P}E/G}\frac{|G|}{|G_A|}|G_A|(x-1)^{\rho(E)-\rho(A)}(y-1)^{|A|-\rho(A)}\\
&= \sum_{A\in\mathscr{P}E/G}(x-1)^{\rho(E)-\rho(A)}(y-1)^{|A|-\rho(A)}.
\end{aligned}
$$

Thus, an alternative description of the equivariant Tutte polynomial is that it contains the terms in the usual Tutte polynomial but summed over orit representatives only.

It is cleaar that, if we substitute $(1,1)$, $(1,2)$, $(2,1)$ or $(2,2)$ into the equivariant Tutte polynomial, we obtain the number of orbits of G on bases, independent sets, spanning sets, and arbitrary subsets of E.

Unfortunately, not all specialisations work so nicely. It is not true that the substitution which gives the chromatic polynomial of a graph from its Tutte polynomial, when applied to the equivariant Tutte polynomial, gives the generating function for the number of orbits on colourings. A similar remark applies to the weight enumerator of a code.

So the equivariant Tutte polynomial is not the one we are looking for. We will see, however, that it does arise as a specialisation of the Tutte cycle index introduced below.

Example Let M be the uniform matroid $U_{2,3}$ (the cycle matroid of the triangle graph K_3), and G the symmetric group S_3. Then

$$
\begin{aligned}
T(M) &= (x-1)^2+3(x-1)+3+(y-1)=x^2+x+y,\\
T(M,G) &= (x-1)^2+(x-1)+1+(y-1)=x^2-x+y.
\end{aligned}
$$

The chromatic polynomial of K_3 is

$$P(k) = kT(M;1-k,0) = k(k-1)(k-2),$$

and no colouring is invariant under any permutation, so the number of orbits on k-colourings is obtained by dividing by 6. However,

$$kT(M,G;1-k,0) = k^2(k-1).$$

8.2 The Tutte cycle index

The *Tutte cycle index* is defined as follows:

$$ZT(M,G) = \sum_{A \in \mathscr{P}E/G} u^{\rho(E)-\rho(A)} v^{|G:G_A|} Z(G(A)).$$

It has the following specialisations:

- Put $u \leftarrow 1$, $v \leftarrow 1$: we obtain $Z(G; s_i \leftarrow s_i + 1 \text{ for all } i)$, by the Shift Theorem.
- Differentiate with respect to v and put $v \leftarrow 1$, $s_i \leftarrow t^i$ for all i. Since $|G : G_A|$ is the size of the orbit of A, we obtain the sum over all of $\mathscr{P}E$; moreover, $Z(G(A); s_i \leftarrow t^i) = t^{|A|}$. So we obtain

$$t^{\rho(E)} \sum_{A \subseteq E} t^{|A|-\rho(A)} (u/t)^{\rho(E)-\rho(A)} = t^{\rho(E)} T(M; x \leftarrow u/t+1, y \leftarrow t+1).$$

- Put $v \leftarrow 1$, $s_i \leftarrow t^i$ (without differentiating): as in the preceding item, we obtain the equivariant Tutte polynomial (with the same substitution).

I do not know whether the Tutte cycle index has the other desirable properties listed earlier.

Remark The Tutte cycle index given here is essentially the same as the one given in [2], but in a more general situation. Note that, if G is an IBIS group and M the corresponding matroid, then the rank function of M is given by $\rho(A) = b(G) - b(G_{(A)})$, where $G_{(A)}$ is the pointwise stabiliser of A, and $b(G)$ denotes the minimum base size of the permutation group G. So in this case the entire definition can be written in terms of the permutation group, without mentioning the matroid.

References

[1] A. A. Bruen, J. A. Thas and A. Blokhuis, On MDS codes, arcs in PG(n,q) with q even, and a solution of three fundamental problems of B. Segre, *Invent. Math.* **92** (1988), 441–459.

[2] Peter J. Cameron, Cycle index, weight enumerator, and Tutte polynomial. *Electronic J. Combinatorics* **9(1)** (2002), #N2 (9pp.)

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

[4] T. C. Maund, *Bases for Permutation Groups*, D.Phil. thesis, University of Oxford, 1988.

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

[6] B. Segre, Curve razionali normali e *k*-archi negli spazi finiti, *Ann. Mat. pura appl.* (IV) **39** (1955), 357–379.