Slide 1

Finite geometry and permutation groups: some polynomial links

Peter J Cameron

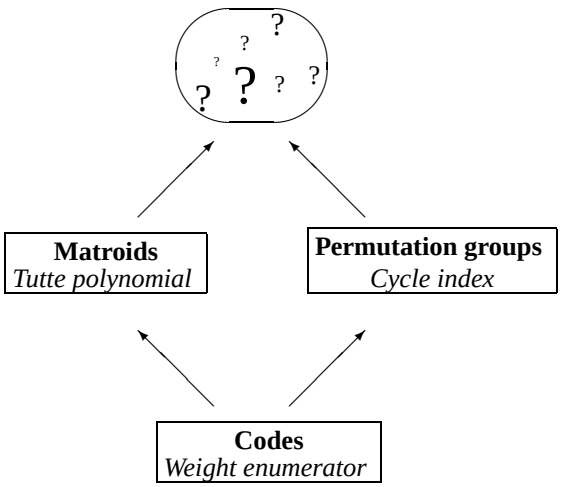
Queen Mary University of London

p.j.cameron@qmul.ac.uk

Trends in Geometry
Roma, June 2004

Slide 2

A map



Slide 3

Codes

An $[n,k]$ *code* over GF(q) is a k-dimensional subspace of GF$(q)^n$. Its elements are called *codewords*. The *weight* wt(v) of v is the number of non-zero coordinates of v. The *weight enumerator* of C is the polynomial

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

The weight enumerator of a code carries a lot of information about it; but different codes can have the same weight enumerator.

Slide 4

Matroids

A *matroid* on a set E is a family I of subsets of E (called *independent sets*) with the properties
• a subset of an independent set is independent;
• if A and B are independent with $|A| < |B|$, then there exists $x \in B \setminus A$ such that $A \cup \{x\}$ is independent.
The *rank* $\rho(A)$ of a subset A of E is the common size of maximal independent subsets of A.
Examples of matroids:
• E is a family of vectors in a vector space, independence is linear independence;
• E is a family of vectors in a vector space, independence is affine independence;
• E is a family of elements in a field K, independence is algebraic independence over a subfield F;
• E is the set of edges of a graph, a set is independent if it is acyclic;
• E is the index set of a family $(A_i : i \in E)$ of subsets of X, a set I is independent if $(A_i : i \in I)$ has a system of distinct representatives.

Slide 5

Matroids and finite geometry

Specialising the first example above, we see that any set of points in a finite projective space gives rise to a matroid, which captures a lot of the geometric properties of the set.

In particular, Segre's fundamental problem about the size and classification of arcs in $\mathrm{PG}(k,q)$ is equivalent to the problem of classifying representations of the *uniform matroid* $U_{k+1,n}$ (whose bases are all $(k+1)$-subsets of an n-set) over $\mathrm{GF}(q)$. The coding theory version of this problem is the classification of the *maximum distance separable* codes over $\mathrm{GF}(q)$.

Slide 6

Tutte polynomial

The *Tutte polynomial* of a matroid M is given by

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

where ρ is the rank function of M.

The Tutte polynomial carries a lot of information about the matroid; e.g. $T(M;2,1)$ is the number of independent sets, and $T(M;1,1)$ is the number of bases (maximal independent sets). But there exist different matroids with the same Tutte polynomial.

The Tutte polynomial of a matroid generalises the Jones polynomial of a knot, percolation polynomials, etc.; and also the weight enumerator of a code, as we will see.

Slide 7

Matroids and codes

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.

Curtis Greene showed that the weight enumerator of the code is a specialisation of the Tutte polynomial of the matroid:

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

I use the notation $F(x \leftarrow t)$ to denote the result of substituting the term t for x in the polynomial F.

Slide 8

Permutation groups

Let G be a permutation group on E, that is, a subgroup of the symmetric group on E, where $|E| = n$. The *cycle index* of G is the polynomial $Z(G)$ in indeterminates $s_1,\ldots,s_n$ given by

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

In particular,

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

is the p.g.f. for the number of fixed points of a random element of G.

The cycle index is very important in enumeration theory. Two simple 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 $P_G(x+1)$);
- $Z(G)(s_i \leftarrow x^i + 1)$ is the ordinary generating function for the number of orbits of G on k-subsets of E.

Slide 9

The Shift Theorem

We require the *Shift Theorem*:

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

where $E = \{1, \ldots, n\}$, $\mathcal{P}E/G$ denotes a set of orbit representatives for G acting on the power set $\mathcal{P}E$ of E, and $G(A)$ is the permutation group induced on A by its setwise stabiliser G_A in G.
For example, if we sum the cycle indices of the symmetric groups of degree k for $k = 0, 1, \ldots, n$, then we obtain $Z(S_n)$ with the substitution $s_i \leftarrow s_i + 1$.

Slide 10

Permutation groups and codes

Let C be an $[n,k]$ code over $\mathrm{GF}(q)$. The additive group G of C acts as a permutation group on the set $E = \mathrm{GF}(q) \times \{1, \ldots, n\}$ by the rule that the codeword $v = (v_1, \ldots, v_n)$ acts as the permutation

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

Now each permutation has cycles of length 1 and p only, where p is the characteristic of $\mathrm{GF}(q)$; and 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. So the cycle index of G carries the same information as the weight enumerator of C, and is determined by the Tutte polynomial.

Slide 11

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 is fixed bu the pointwise stabiliser of its predecessors.
A permutation group is *base-transitive* if it permutes its irredundant bases transitively. In this case, the irredundant bases are the bases of a matroid, indeed a *perfect matroid design*; this is a matroid of rank r for which the cardinality n_i of an i-flat (a maximal set of rank i) depends only on i. In this case the Tutte polynomial is determined by the numbers $n_0, \ldots, n_r$.
All base-transitive groups of rank at least 2 have been determined by Maund, using CFSG; those of large rank (at least 7) by Zil'ber, by a geometric argument not using CFSG.
For base-transitive groups, the cycle index determines the cardinalities of the flats, and hence the Tutte polynomial, but not conversely.

Slide 12

The main problem

As we have seen, there are cases when the Tutte polynomial determines the cycle index (groups from codes), and cases where the cycle index determines the Tutte polynomial (base-transitive groups).
Is there a more general polynomial which determines both?
The situation we will take is a matroid M and a group G of automorphisms of M.
We would like this polynomial to specialise to allow us to count orbits of G on configurations enumerated by the Tutte polynomial of M (such as bases or independent sets, or coefficients of the weight enumerator of a code).

Slide 13

Equivariant Tutte polynomial

A first attempt is the *equivariant Tutte polynomial*, obtained by averaging the Tutte polynomial as in the Orbit-Counting Lemma:

$$\begin{aligned} & T(M,G;x,y) \\ = & \frac{1}{|G|}\sum_{g\in G}\sum_{\substack{A\subseteq E\\ Ag=A}}(x-1)^{\rho E-\rho A}(y-1)^{|A|-\rho A} \\ = & \frac{1}{|G|}\sum_{A\subseteq E}\sum_{g\in G_A}(x-1)^{\rho E-\rho A}(y-1)^{|A|-\rho A} \\ = & \frac{1}{|G|}\sum_{A\in\mathcal{P}E/G}\frac{|G|}{|G_A|}|G_A|(x-1)^{\rho E-\rho A}(y-1)^{|A|-\rho A} \\ = & \sum_{A\in\mathcal{P}E/G}(x-1)^{\rho E-\rho A}(y-1)^{|A|-\rho A}. \end{aligned}$$

Here, $\mathcal{P}E/G$ denotes a set of G-orbit representatives on the power set of E. Thus, an alternative description of the equivariant Tutte polynomial is that it contains the terms in the usual Tutte polynomial but summed over orbit representatives only.

Slide 14

Equivariant Tutte polynomial

This polynomial specialises to the number of G-orbits on bases, independent sets, spanning sets, and arbitrary sets, by substituting $(1,1)$, $(1,2)$, $(2,1)$ or $(2,2)$ for (x,y).

However, it does not solve our problem: the uniform matroid $U_{2,3}$ is the cycle matroid of the complete graph K_3, with Tutte polynomial x^2+x+y; taking $G=S_3$, the equivariant Tutte polynomial is x^2-x+y. Now the number of k-colourings of K_3 is $k(k-1)(k-2)$ (this is $kT(M;1-k,0)$), and so the number of G-orbits on k-colourings is one-sixth of this number, but the same substitution in the equivariant Tutte polynomial is $k^2(k-1)$.

Slide 15

Tutte cycle index

Our second attempt is the *Tutte cycle index*, defined as follows:

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

It has the following specialisations:

- Put $u\leftarrow 1$, $v\leftarrow 1$: we obtain $Z(G;s_i\leftarrow s_i+1)$, by the Shift Theorem.
- Differentiate with respect to v and put $v\leftarrow 1$, $s_i\leftarrow t^i$ (for all i): we obtain

$$t^{\rho E}T(M;x\leftarrow u/t+1,y\leftarrow t+1).$$

- Put $v\leftarrow 1$, $s_i\leftarrow t^i$ for all i: we obtain the equivariant Tutte polynomial (with the same substitution as in the previous case).

I do not know whether this polynomial gives a solution to our main problem!

Slide 16

IBIS groups

The permutation group G is an IBIS group if all irredundant bases have the same size. (The name is an acronym for "**I**rredundant **B**ases of **I**nvariant **S**ize".) Cameron and Fon-Der-Flaass showed that, in an IBIS group G, the irredundant bases are the bases of a matroid (which clearly admits G as a group of automorphisms).

In this case, the Tutte cycle index can be defined directly from the group, since if $b(H)$ denotes the minimum base size of a subgroup H of G, then $\rho(A)=b(G)-b(G_{(A)})$, where $G_{(A)}$ denotes the pointwise stabiliser of A.

Obviously, the IBIS groups include the base-transitive groups as a special case.