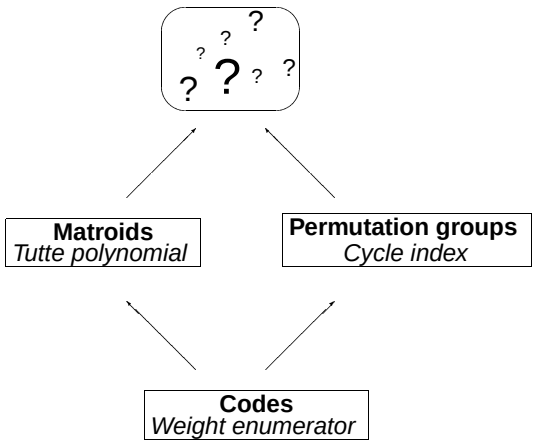
Polynomials associated with permutation groups, matroids and codes

Peter J Cameron

School of Mathematical Sciences
Queen Mary, University of London
London E1 4NS, U.K.
p.j.cameron@qmul.ac.uk

A map



Codes

An $[n,k]$ *code* over $\mathrm{GF}(q)$ is a k-dimensional subspace of $\mathrm{GF}(q)^n$. Its elements are called *codewords*.

The *weight* $\mathrm{wt}(v)$ 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.

Matroids

A *matroid* on a set E is a family $\mathcal{I}$ 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 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.

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.

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.

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.

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.

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 showed that the following three conditions on a permutation group are equivalent:

- all irredundant bases have the same number of points;
- re-ordering any irredundant base gives an irredundant base;
- 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).

Examples of IBIS groups

- 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 $\mathrm{GF}(q)$ is an IBIS group of degree nq and rank k. 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*.

Base-transitive groups

A permutation group is *base-transitive* if it permutes its irredundant bases transitively. A base-transitive group is clearly an IBIS group.

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.

The matroid associated with a base-transitive group is 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.

Mphako showed that the Tutte polynomial of a PMD is determined by the cardinalities $n_1,\ldots,n_r$ of its flats. If the matroid arises from a base-transitive group, these are the numbers of fixed points of group elements. Thus, for a base-transitive group, the cycle index determines the Tutte polynomial of the matroid, but not conversely.

An example

The cycle index does not in general tell us whether a permutation group is base-transitive. The groups

$$\begin{aligned} G_1 &= \{1,(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\},\\ G_2 &= \{1,(1,2)(3,4),(1,2)(5,6),(3,4)(5,6)\} \end{aligned}$$

of degree 6 have the same cycle index, namely $Z(G)=\frac{1}{4}(s_1^6+3s_1^2s_2^2)$. The first is base-transitive with rank 1; the second is an IBIS group of rank 2 (arising from the binary even-weight code of length 3).

If a group with this cycle index is base-transitive then Mphako's result gives the Tutte polynomial as $y^2(y^3+y^2+y+x)$.

If a group with this cycle index comes from a code, we can calculate the Tutte polynomial to be $y^4+2y^3+3y^2+y+3xy+x^2+x$.

In the second case, the matroid admits two different base-transitive groups with different cycle indices (both isomorphic to S_4 as abstract groups).

A polynomial for IBIS groups

There is a polynomial associated with an IBIS group which includes both to the cycle index and to the Tutte polynomial of the matroid. This is the *Tutte cycle index*, given by

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

where G_A and $G_{(A)}$ are the setwise and pointwise stabilisers of A, G_A^A the permutation group induced on A by G_A, and $b(G)$ is the base size of G.

We have:

$$\left(\frac{\partial}{\partial u} ZT(G)\right)(u \leftarrow 1, v \leftarrow 1) = Z(G; s_i \leftarrow s_i + 1);$$

$$|G| ZT(G; u \leftarrow 1, s_i \leftarrow t^i) = t^{b(G)} T\left(M; x \leftarrow \frac{v}{t} + 1, y \leftarrow t + 1\right),$$

where M is the matroid associated with the IBIS group G.

More generally?

For an arbitrary permutation group, the irredundant bases are not the bases of a matroid. Is there a more general combinatorial structure defined by these bases? Can we associate an analogue of the Tutte polynomial (or the Tutte cycle index) with it?

Note that the first specialisation on the preceding slide works for an arbitrary permutation group; we could simply put $v \leftarrow 1$ and omit all mention of matroid rank.

References

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.

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

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

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

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

References

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

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

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

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