CSG notes, October/November 2004
Tutte polynomial and cycle index

These notes are a composite of three talks I gave on a project whose goal is to use both the Tutte polynomial of a matroid and the cycle index of a permutation group to solve certain counting problems. The first section of the notes provides motivation; the second describes the two polynomials; and the third considers a very interesting special case, involving linear codes.

Four counting problems

To motivate this topic, I start with four counting problems, to which the answers are polynomials. After proving this, I will show that the polynomials in the second and third cases are specialisations of something more general (Tutte polynomial and cycle index respectively). The appropriate generalisation of the last one is not known!

The problems

I have a set X with n elements, and a set C with k 'colours'; I want to colour the elements of X with the colours from C. This is done by means of a function $f : X \to C$.

Case 1 With no restrictions, it is clear that the number of different colourings is precisely k^n.

Case 2 Suppose that X is the vertex set of a graph Γ, and we require the colouring to be *proper*, that is, adjacent vertices should get different colours. Then the number of colourings is a polynomial in k with leading term k^n. This polynomial is the *chromatic polynomial* of the graph Γ. (Proofs will be given after the four problems are stated.)

Case 3 Suppose that G is a group acting faithfully on X (that is, a group of permutations of X). How many colourings are there if we count up to the action of G, that is, we identify functions f and f^g for $g \in G$, where $f^g(x) = f(x^{g^{-1}})$? This asks us to count *orbits* of G on the set of colourings. The number is a polynomial in k with leading term $k^n/|G|$.

Case 4 Now let's combine the two preceding cases. Thus, Γ is a graph on X, and G is a group of automorphisms of Γ. How many proper colourings of Γ up to the action of G? Again the answer is a polynomial in k with leading term $k^n/|G|$.

Example If Γ is the null graph on X, and G is the symmetric group, then we are counting selections of n things from k with repetitions allowed and order unimportant; the answer is $k(k+1)\cdots(k+n-1)/n!$. If Γ is the complete graph and G the symmetric group, then repetitions are forbidden, and the number is $k(k-1)\cdots(k-n+1)/n!$.

Proofs

Case 2: Chromatic Polynomial Let $\chi_\Gamma(k)$ denote the number of proper colourings of the vertices of Γ with k colours. If the graph Γ has no edges, then the answer is the same as in Case 1, v iz. k^n. So we proceed by induction on the number of edges. Let $e = \{v,w\}$ be an edge, and consider the graph $\Gamma\backslash e$ obtained by *deleting* the edge e. We divide the proper colourings of this graph into two classes:

- Those with $f(v) \neq f(w)$ are proper colourings of Γ; there are $\chi_\Gamma(k)$ of them.
- Those with $f(v) = f(w)$ are proper colourings of the graph Γ/e obtained from Γ by *contracting* the edge e; there are $\chi_{\Gamma/e}(k)$ of them.

So

$$\begin{aligned} \chi_{\Gamma\backslash e}(k) &= \chi_\Gamma(k) + \chi_{\Gamma/e}(k), \\ \chi_\Gamma(k) &= \chi_{\Gamma\backslash e}(k) - \chi_{\Gamma/e}(k). \end{aligned}$$

By the induction hypotheses, the terms on the right are polynomials with degrees n and $n-1$ respectively and leading coefficient 1. So the claim is proved for Γ.

The polynomial χ_Γ is the *chromatic polynomial* of Γ.

Case 3: Orbit-Counting Lemma Suppose that the finite group G acts on the set Ω. Two points α, β of Ω lie in the same orbit of G if $\alpha^g = \beta$ for some $g \in G$. This is an equivalence relation, whose equivalence classes are the orbits.

The *Orbit-Counting Lemma* asserts that the number of orbits is equal to

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

where $\mathrm{fix}(g)$ is the number of fixed points of g in Ω: that is, the number of orbits is equal to the expected number of fixed points of a random element selected uniformly from G.

The proof is as follows. Define a bipartite graph with vertex set $\Omega \cup G$, having an edge from α to g if and only if g fixes α. We count edges of this graph in two different ways (the standard combinatorialists' trick).

First, the element $g \in$G lies in $\mathrm{fix}(g)$ edges, so the total number of edges is $\sum_{g\in G} \mathrm{fix}(g)$.

Second, the number of edges containing $\alpha \in \Omega$ is the order of the *stabiliser* of α, the subgroup

$$G_\alpha = \{g \in G : \alpha^g = \alpha\}$$

of G. So the number of edges is $\sum_{\alpha\in\Omega} |G_\alpha|$. But the size of the orbit containing α is $|G|/|G_\alpha|$. For the set of elements mapping α to a point β of this orbit is a coset of G_α; and the number of cosets is $|G|/|G_\alpha|$, by *Lagrange's Theorem*. So each orbit contributes $|G|$ to the sum, and we see that the number of edges is $|G|$ times the number of orbits. So the lemma is proved.

Now let Ω be the set of colourings of X with k colours. A colouring f is fixed by g if and only if it is constant on the cycles of g; so the number of colourings fixed by g is $k^{c(g)}$, where $c(g)$ is the number of cycles of g on X. So the number of orbits is

$$\frac{1}{|G|} \sum_{g\in G} k^{c(g)}.$$

The leading term $k^n/|G|$ comes from the identity element; any other element has fewer than n cycles.

Case 4 Let G be a group of automorphisms of the graph Γ on X. According to the orbit-counting lemma, the number of orbits is $\sum_{g\in G} \chi_\Gamma^g(k)$, where χ_Γ^g denotes the number of colourings of Γ fixed by g.

Now a colouring is fixed by g if and only if every vertex in a cycle of g has the same colour. So, if any cycle of g contains two adjacent vertices, then the number of fixed colourings is zero. Otherwise, we can count it as follows. Shrink each cycle of g to a single vertex, and join two of these new vertices if and only if there is an edge between some pair of vertices in these cycles in the original graph. Every proper colouring of the resulting graph Γ^g extends uniquely to a proper colouring of Γ fixed by g.

So each term in the sum is either zero or a polynomial in k. The leading term is $\chi_\Gamma(k)$, corresponding to the identity element of G.

Example Let Γ be the graph in Figure 1, and let G be the group whose elements are the identity, $(1,4)$, $(2,3)$, and $(1,4)(2,3)$.

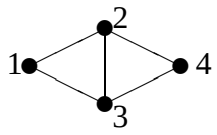

Figure 1: A graph

The chromatic polynomial of Γ is $k(k-1)k-2)^2$. The automorphisms $(2,3)$ and $(1,4)(2,3)$ fix no colourings, whereas $(1,4)$ fixes $(1,4)$ fixes $k(k-1)(k-2)$ colourings, since the graph $\Gamma^{(1,4)}$ is a triangle. So the number of orbits is

$$\tfrac{1}{4}k(k-1)^2(k-2).$$

Matroids and Tutte polynomial

A matroid is an abstract structure designed to capture the features of linear independence in a vector space. Matroids arise in many areas of combinatorics as well as linear algebra: graph theory, transversal theory, coding theory, etc. Associated with a matroid is a two-variable polynomial, and we will see that this specialises to the chromatic polynomial of a graph. It has many other important specialisations: the flow polynomial of a graph, the weight enumerator of a linear code, the Jones polynomial of a knot, etc.

A *matroid* M consists of a pair $(E,\mathscr{I})$, where E is a set, and $\mathscr{I}$ a non-empty set of subsets of E called *independent sets*, satisfying the two properties

- If $I \in \mathscr{I}$ and $J \subseteq I$, then $J \in \mathscr{I}$.
- The *Exchange Axiom*: if $I_1, I_2 \in \mathscr{I}$ with $|I_1| < |I_2|$, then there exists $x \in I_2 \setminus I_1$ with the property that $I_1 \cup \{x\} \in \mathscr{I}$.

It follows from the Exchange Axiom that all maximal independent sets have the same cardinality. This cardinality is called the *rank* of M, and the maximal independent sets are the *bases* of M.

More generally, if A is any subset of E, then all maximal independent subsets of A have the same cardinality, called the *rank* of A and denoted by $\rho(A)$.

Two standard examples will be important to us.

Vector matroids This is the original motivating example. Let $v_1, \ldots, v_n$ be vectors in a vector space V (repetitions are allowed). Take $E = \{1, \ldots, n\}$, and let a subset I of E be independent if and only if the family $(v_i : i \in I)$ of vectors is linearly independent in V. If $\{v_1, \ldots, v_n\}$ spans V, then the rank of the matroid is the dimension of V, and the bases are the vector space bases.

Graphic matroids Let Γ be a graph (in the general sense: loops and multiple edges are allowed). Let E be the set of edges of Γ. A subset I of E is independent if I contains no circuit of the graph. (Here we regard a loop, or two edges joining the same pair of vertices, as forming a circuit.) This is the *cycle matroid* of the graph Γ. If Γ is connected, then the bases are the (edge sets of) spanning trees of Γ. In general, the rank of M is the number of vertices of Γ minus the number of connected components.

The *Tutte polynomial* of a matroid $M = (E, \mathscr{I})$ is defined to be the polynomial

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

Note that this was not Tutte's original definition, and a non-trivial argument is required to show that the two definitions are the same.

The formula we have given for the Tutte polynomial contains $2^{|E|}$ terms, and in general it is hard to compute. We now give another method of computation which is theoretically important but is also hard to compute. It may be worth mentioning two important results here:

- Jaeger, Vertigan and Welsh showed that computing the value $T(M; x, y)$ at a specific point (x, y) in the plane is #P-complete, except for some special points and curves.

- Freedman, Kitaev, Larsen and Wang showed that any efficient quantum computation is equivalent to a classical computation together with one evaluation of the Jones polynomial of a braid at a fifth root of unity. This evaluation can be regarded as an evaluation of the Tutte polynomial at a 'difficult' point. In fact, Bordewich, Freedman, Lovász and Welsh showed that we don't need the exact value; it's enough to be able to answer questions like "in which quartile of its possible range does it lie?" Even this seems hard!

Operations on matroids Let $M = (E, \mathscr{I})$ be a matroid. We call a point $e \in E$ a *loop* if it lies in no basis of M, and a *coloop* if it lies in every basis. In a graphic matroid, loops have precisely their graph-theoretic meaning, while a coloop is a *bridge* or *isthmus* of the graph.

We define three operations on M, as follows.

- If $e \in E$ is not a coloop, we define the *deletion* of E to be the matroid $M\backslash e$ on $E \setminus \{e\}$ whose independent sets are precisely the independent sets of M not containing e.
- If $e \in E$ is not a loop, we define the *contraction* of E to be the matroid M/e on $E \setminus \{e\}$ whose independent sets are all those of the form $I \setminus \{e\}$, where I is an independent set of M containing e.
- The *dual* M^* of M is the matroid whose bases are the complements of the bases of M.

If M is a graphic matroid, then deletion and contraction of an edge have their usual graph-theoretic meanings. The dual of M is less clear in this case, except that if the graph happens to be planar, then the dual of M is associated with the planar dual graph (obtained by putting one vertex in each face of the original, and one edge crossing each edge of the original). The skeletons of the Platonic solids thus satisfy just the duality relations we would expect.

Now it is easy to see that, if e is not a coloop of M, then it is not a loop of M^*, and

$$(M\backslash e)^* = M^*/e.$$

The relation between the Tutte polynomials of a matroid and its dual is very simple:

$$T(M^*; x, y) = T(M; y, x).$$

Careful analysis of the definition of the Tutte polynomial shows that the following four assertions hold. These allow a recursive method of calculating the Tutte polynomial, rather like that for the chromatic polynomial of a graph. The *empty matroid* $(\emptyset, \{\emptyset\})$ is just a convenient place to start the induction.

Let $M = (E, \mathscr{I})$ be a matroid.

- If M is the empty matroid then $T(M; x, y) = 1$.
- If e is a loop, then $T(M; x, y) = yT(M\backslash e; x, y)$.
- If e is a coloop, then $T(M; x, y) = xT(M/e; x, y)$.

- If e is neither a loop nor a coloop, then $T(M;x,y) = T(M\backslash e;x,y) + T(M/e;x,y)$.

Using these formulae in connection with the deletion-contraction formulae for the chromatic polynomial χ_Γ of a graph Γ, we come up with the following: for any graph Γ, with graphic matroid $M(\Gamma)$,

$$\chi_\Gamma(k) = (-1)^{\rho(\Gamma)} k^{\kappa(\Gamma)} T(M; 1-k, 0),$$

where $\kappa(\Gamma)$ is the number of connected components of Γ and $\rho(\Gamma) + \kappa(\Gamma)$ the number of vertices (so that $\rho(\Gamma)$ is the rank of M).

Permutation groups and cycle index

Let X be a set of n elements. Any permutation g of X has a decomposition into disjoint cycles: let $c_i(g)$ be the number of cycles of length i, for $1 \le i \le n$ (so that $c_1(g) + 2c_2(g) + \cdots = n$). Take indeterminates $s_1, \ldots, s_n$, and define the *cycle index* of g to be the monomial

$$z(g) = s_1^{c_1(g)} s_2^{c_2(g)} \cdots s_n^{c_n(g)}.$$

Now let G be a group of permutations of X. We define the *cycle index* of G to be the average of the cycle indices of its elements:

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

It is a polynomial in $s_1, \ldots, s_n$; every term has "degree" n, if we count the degree of the indeterminate s_i as being i, for all i.

The cycle index can be used to solve in a systematic way many orbit-counting problems related to G. I will state the Cycle Index Theorem, which is not the most general result about this but probably enough for our needs.

We have a set A of *figures*, each of which has a non-negative integer *weight*. There may be infinitely many figures, but we assume that there are only finitely many of given weight, say a_i of weight i. We define the *figure-counting series* to be

$$A(x) = \sum_{i \ge 0} a_i x^i.$$

Now a function $f : X \to A$ has a weight given by

$$w(f) = \sum_{x \in X} w(f(x)).$$

If G is a permutation group om X, then G acts on the set of functions from X to A preserving the weights. So we can ask for the number of orbits of G on functions of weight i; call this number b_i. Then the *function-counting series* is given by

$$B(x) = \sum_{i \geq 0} b_i x^i.$$

The *Cycle Index Theorem* asserts that the relation between these two series is given by

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

where $F(s_i \leftarrow t_i)$ means the result of substituting t_i for s_i in the polynomial F for $i = 1, \ldots, n$.

This can be applied to the second of our four motivating problems. If we are colouring X with k colours, take each figure to be a colour, having weight zero; then the number of orbits on colourings is $Z(G; s_i \leftarrow k)$. But the extra freedom allows us to do much more. Suppose for example, that one of the colours is black, and we want to count the colourings in which black is used exactly j times. Now we take black to have weight 1 and all the others to have weight 0, so that the figure-counting series is $x + k - 1$; then the required number of orbits is the coefficient of x^j in the polynomial $Z(G; s_i \leftarrow x^i + k - 1)$.

One result about the cycle index which we need is the *Shift Theorem*. Let G be a permutation group on Ω. Let $\mathscr{P}\Omega/G$ denote a set of representatives for the G-orbits on the set of subsets of Ω. For any subset A of Ω, let $G[A]$ denote the permutation group on A induced by its setwise stabiliser in G. (By convention, the cycle index of a permutation group on the empty set is taken to be 1.) Then we have

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

Example Let G be the symmetric group of degree 3. As orbit representatives we can take one set of each cardinality 0, 1, 2, 3; the group induced on each set is the symmetric group. The equation above says

$$1 + s_1 + \tfrac{1}{2}(s_1^2 + s_2) + \tfrac{1}{6}(s_1^3 + 3s_1 s_2 + 2s_3) = \tfrac{1}{6}((s_1+1)^3 + 3(s_1+1)(s_2+1) + 2(s_3+1)).$$

The main problem

The main problem that I would like solved is the following.

Is there a polynomial (somehow 'including' both the Tutte polynomial of M and the cycle index of G) associated with the action of a group G of automorphisms of a matroid M, with the property that, given any nice specialisation of $T(M)$ solving a counting problem associated with M (such as the chromatic polynomial of a graph), there is a corresponding specialisation of the new polynomial to count the orbits of G on the objects being counted?

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, over G, the terms in the summation for the Tutte polynomial fixed by the element $g \in G$. That is,

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

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

It is clear 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 sets in M.

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

So it is clear that the equivariant Tutte polynomial defined above is not particularly useful. However, we will see that it is also a specialisation of the polynomial

defined below.

Example Let M be the uniform matroid $U(2,3)$ (the cycle matroid of the 3-cycle), 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,

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

Tutte cycle index

Our polynomial 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 $Z(G;s_i \leftarrow s_i+1)$, 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, $Z(G(A);s_i \leftarrow t) = t^{|A|}$. So we obtain

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

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

Codes and matroids

In what follows, *monomial column operations* on a matrix mean column permutations and multiplying columns by non-zero scalars. We say two matrices are *rmc-equivalent* if one can be transformed into the other by a combination of row operations and monomial column operations.

Let A be a $k \times n$ matrix with rank k over a field F. There are two constructions we can perform on A:

1. Let C be the row space of A. Then C is an $[n,k]$ code over F (a subspace of F^n of dimension k). Row operations simply change the basis for C while leaving it unaltered. Monomial column operations replace C by an "equivalent" code (in the usual sense in coding theory – this is sometimes called "monomial equivalent"). So matrices up to rmc-equivalence correspond to linear codes up to equivalence.

2. Let $E = \{1, \ldots, n\}$, and

$$\mathscr{I} = \{I \subseteq E : (c_i : i \in I) \text{ is linearly independent}\}.$$

   Then $(E, \mathscr{I})$ is a matroid, indeed a vector matroid over F (we are given an explicit representation). Now row operations on M correspond to changing the representation to an equivalent one (two representations being equivalent if they differ by an invertible linear transformation of the underlying space), while monomial column operations relabel the elements of the matroid and the choice of representing vectors. So matrices up to rmc-equivalence correspond to representations of matroids up to equivalence.

So there is a natural correspondence between linear codes and representable matroids, up to the natural notion of equivalence for each.

Note that, if the matrix A has no zero columns (equivalently, if the matroid has no loops), then another way of viewing the matroid is as a family of points in the projective space $\mathrm{PG}(k-1,F)$, since multiplying a point by a non-zero scalar doesn't change the projective point it spans. Moreover, if any two columns are linearly independent (equivalently, if the matroid has no parallel elements), then the points of projective space are all distinct. This occurs if and only if the dual code $C^\perp$ of C has minimum weight at least 3.

Matroid and code operations

We now consider some matroid operations and the corresponding operations on codes.

1. *Deletion* of the element e of the matroid $M = (E, \mathscr{I})$ gives $M\backslash e = (E \setminus \{e\}, \mathscr{I}')$, where
$$\mathscr{I}' = \{I \in \mathscr{I} : e \notin I\}.$$
The corresponding operation on codes is *puncturing*, that is, deleting the coordinate e from all codewords.

2. *Contraction* of the element e of the matroid $M = (E, \mathscr{I})$ gives $M/e = (E \setminus \{e\}, \mathscr{I}'')$, where
$$\mathscr{I}' = \{I \setminus \{e\} : e \in I \in \mathscr{I}\}.$$
The corresponding operation on codes is *shortening*: take all codewords which have entry 0 in the eth coordinate, and then delete this coordinate.

3. *Dual* M^* of M is the matroid whose bases are the complements of the bases of M. The corresponding operation on codes is the usual dual
$$C^\perp = \{v \in F^n : v.w = 0 \text{ for all } w \in C\}.$$

Polynomials

The *weight* of $v \in F^n$, denoted $\mathrm{wt}(v)$, is the number of non-zero coordinates of v. The *weight enumerator* of C is the polynomial

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

where a_i is the number of words of C of weight i. It is a homogeneous polynomial of degree n.

Recall that the *Tutte polynomial* of a matroid M is

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

where ρ is the rank function of M.

Greene's Theorem shows that the weight enumerator of C is a specialisation of the Tutte polynomial of the corresponding matroid M:

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

where $q = |F|$ and k is the dimension of C.

Let us illustrate this by deducing *MacWilliams' Theorem*:

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

Since $C^\perp$ corresponds to M^*, and $T(M^*;x,y) = T(M;y,x)$, we have

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

On the other hand, if $U = X+(q-1)Y$ and $V = X-Y$, then $U+(q-1)V = qX$ and $U-V = qY$, so

$$\frac{1}{|C|} W_C(U,V) = \frac{1}{q^k} V^{n-k}(U-V)^k T\left(M; \frac{qX}{qY}, \frac{X+(q-1)Y}{X-Y}\right),$$

which reduces to the same as the other expression.

Singleton bound and MDS codes

The *Singleton bound* asserts that, if C is a code of length n over an alphabet with q symbols (not necessarily linear) and C has minimum distance d, then $|C| \leq q^{n-d+1}$.

To prove this, write out all the codewords in a $|C| \times n$ array. Choose any $n-d+1$ columns of the array, and make a window which shows only those columns. As we slide the window down the array, all the views through the window are distinct; for, if two of them agreed, the corresponding codewords would agree in at least $n-d+1$ positions, and would have distance at most $d-1$, contrary to assumption. Since there are at most q^{n-d+1} different views, the result is proved.

A code is called *MDS* (for *maximum distance separable*) if it attains this bound.

Suppose that C is a linear code which is MDS. Then C has dimension $k = n-d+1$. The argument shows that, given any k columns, all possible k-tuples occur

in those positions in the code; so the corresponding k coordinates are independent in the matroid. The converse is clear. Thus, a linear code is MDS if and only if the corresponding matroid is a *uniform matroid* $U_{k,n}$ (that is, the independent sets are all subsets of cardinality at most k).

This result makes obvious a fact which is rather difficult to see directly: if C is a linear MDS code, then $C^\perp$ is also MDS. For the dual of the uniform matroid $U_{k,n}$ is just $U_{n-k,n}$.

Clearly the Tutte polynomial of the uniform matroid is

$$T(U_{k,n};x,y) = \sum_{i=0}^{k} \binom{n}{i} (x-1)^{k-i} + \sum_{i=k+1}^{n} \binom{n}{i} (y-1)^{i-k}.$$

By Greene's Theorem, we can calculate explicitly the weight enumerator of a linear MDS code.

If C is a linear $[n,k]$ MDS code over $\mathrm{GF}(q)$, then the corresponding points of $\mathrm{PG}(k-1,q)$ form an *arc*: that is, no k of them are contained in a hyperplane of the projective space. Thus, the study of arcs in projective space, linear MDS codes, and representations of uniform matroids are all the same subject.

Example Let C be a linear $[n,3]$ MDS code over $\mathrm{GF}(q)$. Then

$$n \le \begin{cases} q+1 & \text{if } q \text{ is odd,} \\ q+2 & \text{if } q \text{ is even.} \end{cases}$$

For C corresponds to a set S of n points in the projective plane $\mathrm{PG}(2,q)$, no three collinear. The upper bound $q+2$ arises because, if $p \in S$, then the lines joining it to the other $n-1$ points in the set are all distinct, and there are exactly $q+1$ lines through a point in the projective plane. If equality holds, then every line meets S in either 0 or 2 points. Take a point p' outside S; the lines through p' which meet S partition it into sets of size 2, so $|S| = q+2$ must be even.

Hamming bound and perfect codes

There are other bounds for codes. One of the best-known is the *sphere-packing bound* or *Hamming bound*: if C has length n and minimum distance at least $2e+1$ over an alphabet of size q, then

$$|C| \le \frac{q^n}{\sum_{i=0}^{e} \binom{n}{i} (q-1)^i}.$$

This holds because, given $d \geq 2e+1$, the triangle inequality shows that the balls of radius e centred at the codewords are pairwise disjoint. Each ball contains $\sum_{i=0}^{e} \binom{n}{i}(q-1)^i$ words, and there are q^n words altogether.

Equality holds if and only if every word is distant e or less from a unique codeword. A code with these properties is called *perfect*. Tietäväinen showed that, if q is a prime power, then perfect codes have parameters from the following list:

- $e = 1$ (Hamming codes are examples);
- $q = 2$, $e = (n-1)/2$ (binary repetition codes);
- $q = 2$, $e = 3$, $n = 23$ (the binary Golay code);
- $q = 3$, $e = 2$, $n = 11$ (the ternary Golay code).

It is known that, for a perfect code containing the all-zero word, the weight enumerator is determined by the parameters. So we conclude with two questions:

- What properties distinguish matroids corresponding to linear perfect codes?
- Is the Tutte polynomial determined by the parameters (as for MDS codes)?

Finally, in connection with the general project, the following problem arises: Given a group G of automorphisms of a code C, construct a polynomial which can be used to count orbits of G on words of given weight in C.

End note

Following the Study Group sessions, Bill Jackson has shown that, if A is the abelian group C_2^m, then for any graph Γ and group G of automorphisms of Γ, the number of orbits of G on nowhere-zero A-flows in Γ is given by a polynomial in $k = |A|$, and has calculated the degree and leading term of this polynomial. However, if we use other abelian groups A, then the answer is not determined by A alone, but depends on the structure of A. We hope to report more news about this later.