Orbit-counting polynomials for graphs and codes

Peter J. Cameron [1] Bill Jackson Jason Rudd

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

Abstract

We construct an "orbital Tutte polynomial" associated with a dual pair M and M^* of matrices over a principal ideal domain R and a group G of automorphisms of the row spaces of the matrices. The polynomial has two sequences of variables, each sequence indexed by associate classes of elements of R.

In the case where M is the signed vertex-edge incidence matrix of a graph Γ over the ring of integers, the orbital Tutte polynomial specialises to count orbits of G on proper colourings of Γ or on nowhere-zero flows or tensions on Γ with values in an abelian group A. (In the case of flows, for example, we must substitute for the variable x_i the number of solutions of the equation $ia = 0$ in the group A. In particular, unlike the case of counting nowhere-zero flows, the answer depends on the structure of A, not just on its order.)

In the case where M is the generator matrix of a linear code over $\mathrm{GF}(q)$, the orbital Tutte polynomial specialises to count orbits of G on words of given weight in C or its dual.

Key words: chromatic polynomial, nowhere-zero flows, Tutte polynomial, weight enumerator, group action, orbit-counting

1 Introduction

Two main directions in combinatorial enumeration involve structure and symmetry.

For example, it is trivial that the number of ways of colouring the elements of an n-element set X with k colours is k^n. A structural refinement is to have

[1] Corresponding author.

Preprint submitted to Elsevier Preprint *1 July 2005*

a graph Γ on the vertex set X and count proper colourings of Γ; the answer is a monic polynomial of degree n in k, the *chromatic polynomial* $\chi(\Gamma; k)$ of Γ. A refinement involving symmetry is to have a group G of permutations of X, and to count colourings up to the action of G (that is, orbits of G on colourings); it is a well-known consequence of the orbit-counting lemma that the answer is a polynomial of degree n in k with leading coefficient $1/|G|$.

Our aim is to combine the two approaches; we want to count the number of G-orbits of "structurally restricted" colourings, where G is a group of automorphisms of the structure imposed on X.

As an example, we show in the next section that, if $G \leq \mathrm{Aut}(\Gamma)$, then the number of G-orbits on k-colourings of Γ is a polynomial of degree n in k with leading coefficient $1/|G|$. We call this the *orbital chromatic polynomial* of (Γ, G).

The position is more complicated for flows and tensions, however. In particular, the number G-orbits on nowhere-zero flows (resp. tensions) on Γ with values in an abelian group A of order k depends on the structure of A, not just on its order (as in the case where we count flows or tensions rather than orbits). We show that there are polynomials in countably many variables x_i (for $i \geq 0$, such that the numbers of orbits on nowhere-zero flows (resp. tensions), are obtained by substituting for x_i the number of solutions of the equation $ix = 0$ in A. We also note that a different substitution is required to obtain the orbital chromatic polynomial.

The calculation of these *orbital flow and tension polynomials* involves finding the invariant factors of certain integer matrices. In the following section, we generalise the set-up to pairs of matrices over a principal ideal domain satisfying a duality condition. This allows us to define an *orbital Tutte polynomial* in this general case. In the case of graphs, this polynomial specialises to the orbital flow and tension polynomials, as happens for the usual Tutte polynomial.

A finite field is a principal ideal domain, and so our theory applies to a linear code and its dual, as we explore next.

We conclude with open problems and speculations for further research.

Of course, our main tool in orbit-counting is the *orbit-counting lemma*, asserting that, if the finite group G acts on the finite set X, then the number of G-orbits on X is equal to

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

where $\mathrm{fix}_X(g)$ is the number of points of X fixed by g.

2 Orbital chromatic polynomial

Let G be a group of automorphisms of a graph Γ, and k a positive integer. In order to count the number of G-orbits on proper k-colourings of X, according to the orbit-counting lemma, we must count colourings fixed by each automorphism $g \in G$. Now g fixes a colouring f if and only if f is constant on each cycle of g on vertices of Γ. Hence, if any cycle of g contains an edge, then no proper colouring is fixed. If not, then let Γ_g be obtained from Γ by shrinking each cycle to a single vertex; then g-fixed colourings of Γ are equinumerous with colourings of Γ_g. The number of these is a polynomial $\chi(\Gamma_g; k)$. Since the average of polynomials is a polynomial, we have shown the first part of the following result:

Theorem 1 *Let G be a group of automorphisms of a graph Γ on n vertices. Then the number of orbits of G on proper k-colourings of Γ is $O\chi(\Gamma, G; k)$, where $O\chi(\Gamma, G)$ is a polynomial of degree n with leading coefficient $1/|G|$.*

The assertions about degree and leading coefficient follow from the proof: for the number of colourings fixed by g is either zero or a polynomial in k whose degree is the number of vertices of Γ_g, and this number is largest when no shrinking takes place, that is, when g is the identity.

We call the polynomial $O\chi(\Gamma, G)$ the *orbital chromatic polynomial* of Γ and G. If G is the trivial group, then it is the usual chromatic polynomial of Γ. If Γ is a complete graph K_n, then

$$O\chi(\Gamma, G)(k) = \frac{k(k-1)\cdots(k-n+1)}{|G|},$$

while if Γ is a null graph N_n then it is a specialisation of the cycle index of G. In particular,

$$O\chi(K_n, S_n) = \binom{k}{n}, \qquad O\chi(N_n, S_n) = \binom{k+n-1}{n} = (-1)^n \binom{-k}{n}.$$

For example, let Γ be a 4-cycle with one diagonal (Figure 1). The chromatic polynomial is $k(k-1)(k-2)^2$. If $G = \mathrm{Aut}(\Gamma)$, a group of order 4 consisting of the identity and the permutations $(2,3)$, $(1,4)$ and $(2,3)(1,4)$, we see that $(2,3)$ fixes $k(k-1)(k-2)$ colourings, while $(1,4)$ and $(2,3)(1,4)$ do not fix any (since they exchange the ends of the edge $\{1,4\}$). So by the Orbit-counting Lemma,

$$O\chi(\Gamma, G; k) = k(k-1)^2(k-2)/4.$$

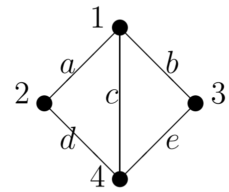

Fig. 1. An example

The positive integer roots of $O\chi(\Gamma, G)$ are obviously the same as those of the chromatic polynomial. However, while the chromatic polynomial has no negative roots, this is not the case for the orbital chromatic polynomial: for example, $O\chi(N_n, S_n)$ has roots $0, -1, \ldots, -(n-1)$.

3 Orbital flow and tension polynomials

In order to define flows and tensions on the graph Γ, we have to choose an arbitrary orientation of the edges of Γ. Our results will not depend on the chosen orientation.

Let A be an abelian group. We consider functions f from the set of oriented edges of Γ to A. Reversing the orientation of an edge is accompanied by negating the value of f on the edge.

The function f is a *flow* if, for any vertex v, the sum of the values of f on edges with terminal vertex v is equal to the sum on edges with initial vertex v (calculated in A). The function f is a *tension* if, for any oriented cycle C, the sum of the values of f on edges of C whose orientation agrees with that of C is equal to the sum on edges whose orientation disagrees with that of C (again calculated in A). It is easy to see that reversing an edge e and negating the value of f on e preserves the property of being a flow, or a tension.

A function f as above is *nowhere-zero* if it does not take the value 0 (the zero element of A).

Given any function f from the vertex set of Γ to a set of k colours, we identify the set of colours with an abelian group A of order k in any manner. Then the *gradient* ∂f of f is the function on oriented edges whose value on the edge

(v,w) is $f(w)-f(v)$. It is easily checked that ∂f is a tension. Any tension arises in this way; indeed, any tension arises from k^c functions on vertices, where c is the number of connected components of Γ. (We may choose arbitarily the value of f on one vertex in each component; the other values are then determined by the gradient.)

Since $f(w)-f(v)=0$ if and only if $f(v)=f(w)$, a tension is nowhere-zero if and only if it is the gradient of a proper colouring. Thus, the number of nowhere-zero tensions on Γ with values in an abelian group A of order k is $\tau(\Gamma;k)=\chi(\Gamma;k)/k^c$, a monic polynomial in k of degree $n-c$. In particular, this number is independent of the structure of the abelian group A.

The number of nowhere-zero flows on Γ with values in A is also a polynomial $\phi(\Gamma;k)$ in $k=|A|$, independent of the structure of A. (This observation is due to Tutte, sometime before 1947 – see [9].)

Now let G be a group of automorphisms of Γ. Then g acts on the functions from oriented edges to A as follows:

$$f^g((v,w))=f((v^{g^{-1}},w^{g^{-1}})),$$

with the convention that if the edge $e^{g^{-1}}=\{v^{g^{-1}},w^{g^{-1}}\}$ has orientation $(w^{g^{-1}},v^{g^{-1}})$, then we also negate the value of f.

Counting orbits on nowhere-zero tensions or flows is less simple. A nowhere-zero tension fixed by an automorphism g is not necessarily the gradient of a proper colouring fixed by g. For example, if Γ is an n-cycle, and $a\in A$ satisfies $na=0$, then the function obtained by orienting edges consistently around C and giving the value a to each edge is a tension, but is the gradient of a fixed vertex function if and only if $a=0$.

Consider the example in the last section. Direct all the edges downwards. Let a,b,c,d,e be values in the abelian group A. They form a flow if and only if $a=d$, $b=e$, and $a+b+c=0$ (in A). So there are $(k-1)(k-2)$ nowhere-zero flows: choose $a\neq 0$ and $b\notin\{0,-a\}$, then the remaining values are determined. Now a flow is fixed by $(2,3)$ if and only if $a=b$; this requires $2a\neq 0$, so there are $k-\alpha$ solutions, where α is the number of elements $a\in A$ satisfying $2a=0$. A flow is fixed by $(1,4)$ if and only if each of a,b,c is equal to its negative; there are $(\alpha-1)(\alpha-2)$ solutions. Finally, a flow is fixed by $(1,4)(2,3)$ if and only if $a=-e$ and $b=-d$; but then $c=-(a+b)=0$, so there are no such nowhere-zero flows. So the number of orbits on nowhere-zero flows is

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

This example also shows that the number of orbits may depend on the structure of A.

Our main theorem is the following.

Theorem 2 *There are polynomials* $O\phi(\Gamma, G)$ *and* $O\tau(\Gamma, G)$ *in indeterminates* $(x_n : n = 0, 1, 2, \ldots)$*, such that the numbers of orbits of* G *on nowhere-zero flows and tensions with values in the finite abelian group* A *are respectively* $O\phi(\Gamma, G; x_i \leftarrow \alpha_i)$ *and* $O\tau(\Gamma, G; x_i \leftarrow \alpha_i)$*, where* α_i *is the number of solutions of* $ia = 0$ *in the abelian group* A*.*

The polynomials $O\phi$ and $O\tau$ are called the *orbital flow polynomial* and the *orbital tension polynomial* respectively.

Note that $\alpha_0 = |A|$ and $\alpha_1 = 1$. So,if no indeterminates other than x_0 and x_1 appear, then the number of orbits depends only on $|A|$ and not on the structure of A. A consequence of Theorem 8 is that this is the case if G is the trivial group.

The proof will be given later. The flow and tension polynomials of a graph (with trivial automorphism group) are known to be specialisations of the Tutte polynomial of the graph. We define an "orbital Tutte polynomial" which similarly specialises to the orbital flow and tension polynomials.

4 Invariant factors and duality

Let R be a principal ideal domain. Given an $m \times n$ matrix M over R, we define the *row space* of $\rho(M)$ and the *null space* $\nu(M)$ as usual:

$$\begin{aligned}\rho(M) &= \{yM : y \in R^m\},\\ \nu(M) &= \{x \in R^n : Mx^\top = 0\}.\end{aligned}$$

M can be put into *Smith normal form* by elementary row and column operations: this is a matrix with r non-zero diagonal elements $d_1, \ldots, d_r$ and all other entries zero, where d_i divides d_{i+1} for $i = 1, \ldots, r-1$. The elements $d_1, \ldots, d_r$ are uniquely determined up to multiplication by units of R. They are the *invariant factors* of M. By convention, we also take 0 to be an invariant factor with multiplicity $n - r$, so that there are n invariant factors in all. The R-module $R^n/\rho(M)$ is the direct sum of cyclic modules R/d_iR for $i = 1, \ldots, n$.

Using the freedom to multiply by units, we will assume:

- if $R = \mathbb{Z}$, then the invariant factors are non-negative;

- if R is a field, then the invariant factors are zero or one.

Two matrices M and M^* over the PID R are *dual* if the row space of M is equal to the null space of M^* and *vice versa*.

A matrix is *totally unimodular* if every subdeterminant is zero or a unit. (This property is *not* preserved by elementary operations.)

Let M be any matrix, and $\rho(M)$ its row space. Then the null space of M is $\rho(M)^\perp$ (the space orthogonal to $\rho(M)$ with respect to the standard inner product), and we can choose a matrix M^* having this as its row space. However, $\rho(M)^{\perp\perp} \geq \rho(M)$ in general, so not every matrix has a dual. The following result holds:

Theorem 3 *Let M be a matrix over R. Then the following are equivalent:*

(a) M has a dual;
(b) all invariant factors of M are zero or units;
(c) M is equivalent to a totally unimodular matrix.

PROOF. (a) implies (b): suppose that M and M^* are duals. This fact remains true under the following operations:

- row operations on M;
- row operations on M^*;
- column operations on M and simultaneously their inverse duals on M^*.

(This means, for example, that if we add α times the ith column of M to the jth, then we should subtract α times the jth column of M^* from the ith.)

This is clear for row operations since these don't change the row space or null space. The third type don't change the orthogonality of the rows of M and M^*; but duality is defined in terms of this relation, as we have seen.

Now use these operations to put M into Smith normal form. Suppose that there are r non-zero invariant factors. Then the null space of M consists of all vectors with zero in the first r coordinates, so we can take $M^* = [O\,I]$. But then the null space of M^* is spanned by $[I\,O]$; this is strictly bigger than the row space of M if any invariant factor is not zero or a unit.

(b) implies (a): Suppose (b) holds, and reduce M to Smith normal form $[I\,O]$ by elementary operations. The reduced form has a dual $[O\,I]$; hence so does M (arguing as in the preceding paragraph).

(b) implies (c): if (b) holds, the Smith normal form of A is totally unimodular.

(c) implies (b): the product of the first k invariant factors is the g.c.d. of the order-k subdeterminants.

Corollary 4 *For any matrix M, the matrices M^* and M^{**} form a dual pair.*

Now if Γ is a graph with oriented edges, and M and M^* are the signed vertex-edge and cycle-edge incidence matrices, then M and M^* are dual in the above sense. For it is clear that any vector in the row space of one of these matrices does lie in the null space of the other. Now to show that the null space of M^* is spanned by the rows of M, observe:

- An element x of the null space of M^* is determined by its values on a spanning forest F of Γ. For, if e is an edge not in F, then $e \cup F$ contains a cycle, and the sum of the values of x on this cycle is zero; so $x(e)$ is determined.
- Any function on the edge set of a forest F can be obtained as a linear combination of rows of M. For such a function is a tension on F (since there are no cycles), and so is the gradient of a function y on the vertices. Then the linear combination of rows of M, where the row indexed by v has coefficient $y(v)$, takes the prescribed values on the edges of F.

The argument to show that the null space of M is spanned by the rows of M^* is similar.

As is well-known, the matrix M is totally unimodular, but M^* is not in general.

5 Orbital Tutte polynomial

Throughout this section, we assume that (M, M^*) is a dual pair over a principal ideal domain R. The linearly independent sets of columns of M are the independent sets of a matroid (representable over the field of fractions of R), and the linearly independent sets of columns of M^* form the dual matroid.

We define an *automorphism* of M to be an automorphism of the free module R^n (where n is the number of columns of M) which preserves the row space and null space of M. Note that M and M^* have the same automorphisms. If g is an automorphism of M (represented as an $n \times n$ matrix), and 1 is the identity matrix, set

$$M_g = \begin{pmatrix} M \\ g-1 \end{pmatrix}, \qquad M_g^* = \begin{pmatrix} M^* \\ g-1 \end{pmatrix}.$$

For any subset S of $E = \{1, \ldots, n\}$, and any matrix N with n columns, we let $N[S]$ be the submatrix of N consisting of the columns with indices in S.

Take two sets $(x_i : i \in I)$ and $(x_i^* : i \in I)$ of indeterminates, where the index set I is the set of associate classes in R. For any matrix N, let $x(N)$ be the monomial defined as follows: take the invariant factors of N (completed with zeros so that the number of them is equal to the number of columns of N), and multiply the corresponding indeterminates. Define $x^*(N)$ similarly, using the other set of indeterminates.

Now let G be a finite group of automorphisms of M, and define the *orbital Tutte polynomial* $OT(M,G)$ in the indeterminates $(x_i, x_i^* : i \in I)$ as follows:

$$OT(M,G) = \frac{1}{|G|}\sum_{g\in G}\sum_{S\subseteq E} x(M_g[S])x^*(M_g^*[E\setminus S]).$$

Theorem 5 *If G is the trivial group, then $OT(M,G)$ involves only x_0, x_1, x_0^* and x_1^*; the substitution $x_1 = x_1^* = 1$, $x_0 = y-1$, $x_0^* = x-1$ gives the Tutte polynomial of M.*

PROOF. The Tutte polynomial is defined as

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

where $\mathrm{rk}(S)$ denotes the rank of the matrix $M[S]$.

Now if $G=1$, the matrices M and M^* have invariant factors 0 and 1 only; and $\mathrm{rk}(S)$ is the multiplicity of the invariant factor 1. Thus the power of $y-1$ in the formula for $T(M)$ is equal to the power of x_0 in the formula for $OT(M,1)$. It is easily verified directly, or follows from the definition of matroid dual, that

$$\mathrm{rk}^*(E) - \mathrm{rk}^*(E\setminus S) = |S| - \mathrm{rk}(S),$$

where $\mathrm{rk}^*(S)$ denotes the rank of the matrix $M^*[S]$.

For a graph Γ with n edges, we let $OT(\Gamma,G)$ denote $OT(M,G)$, where M is the signed vertex-edge incidence matrix of Γ. (The rows of M are indexed by vertices, the columns by edges, and the (v,e) entry is $+1$ if v is the terminal vertex of $\vec{e}$, -1 if v is the initial vertex of $\vec{e}$, and 0 otherwise.) An automorphism g of Γ is represented by a signed permutatation matrix, with (e,e') entry 1 if g maps e to e' preserving the orientation, -1 if g maps e to e' reversing the orientation, and 0 otherwise. Recall that $\alpha_i(A)$ is the number of solutions of $ix = 0$ in A.

Theorem 6 *Let M be the incidence matrix of a graph Γ over $\mathbb{Z}$, and let G be a group of automorphisms of Γ. Let A be a finite Abelian group. Then the substitution $x_i \leftarrow \alpha_i(A)$, $x_i^* \leftarrow -1$ (for all i) in $OT(\Gamma, G)$ gives the number of G-orbits on nowhere-zero A-flows on Γ, while the substitution $x_i \leftarrow -1$, $x_i^* \leftarrow \alpha_i(A)$ gives the number of G-orbits on nowhere-zero A-tensions on Γ.*

PROOF. First we show that $x(M_g)$, with the given substitution, is equal to the number of flows fixed by g. For a vector $x \in A^n$ is a flow if and only if $Mx^\top = 0$, and is fixed by g if and only if $gx^\top = x^\top$; so x is a flow fixed by g if and only if $M_g x^\top = 0$.

Applying elementary row and column operations to M_g does not change the number of solutions of these equations: row operations leave the solution set unaltered, while column operations apply an invertible transformation to it. So we may assume that M_g has been brought to Smith normal form. If the invariant factors are $d_1, d_2, \ldots, d_r$, and 0 with multiplicity $n-r$, then the equations are $d_1x_1 = 0, \ldots, d_rx_r = 0$, with $x_{r+1}, \ldots, x_n$ arbitrary; so the number of solutions is $\alpha_{d_1} \cdots \alpha_{d_r} \alpha_0^{n-r}$, as required.

Now let $\theta(S)$ be the number of g-fixed flows which vanish on the edges in $E \setminus S$ (and possibly more), and $\phi(S)$ the number of g-fixed flows vanishing precisely on $E \setminus S$. The flows counted by $\theta(S)$ are flows on the subgraph with edge set S, and so are the solutions of $M_g[S]x^\top = 0$, extended with zeros on the remaining edges. So the number of such flows is obtained from $x(M_g[S])$ by the substitution of the theorem. Now the Inclusion-Exclusion Principle shows that

$$\phi(E) = \sum_{S \subseteq E} (-1)^{n-|S|} \theta(S),$$

and $(-1)^{n-|S|}$ is precisely what arises from $x^*(M_g^*[E \setminus S])$ by setting all the variables equal to -1.

Finally, an application of the Orbit-Counting Lemma gives the result for orbits on nowhere-zero flows.

The result for orbits on nowhere-zero tensions is obtained in dual fashion using the matrix M^*.

This theorem can be generalised: we can specialise the polynomial OT to get a generating function for the number of G-orbits on flows or tensions with given support size. (We are grateful to Alan Sokal for this observation.)

Theorem 7 *(a) Let f_m be the number of G-orbits on A-flows supported on precisely $n-m$ edges of Γ. Then*

$$\sum f_m x^m = OT(\Gamma, G; x_i \leftarrow \alpha_i(A), x_i^* \leftarrow x-1).$$

(b) Let t_m be the number of G-orbits on A-tensions supported on precisely $n-m$ edges of Γ. Then

$$\sum t_m x^m = OT(\Gamma, G; x_i \leftarrow x-1, x_i^* \leftarrow \alpha_i(A)).$$

PROOF. (a) With the notation of the above proof, Inclusion-Exclusion gives

$$\phi(T) = \sum_{S \subseteq T} (-1)^{|T|-|S|} \theta(S),$$

and so

$$\begin{aligned} \sum_{T \subseteq E} \phi(T) x^{n-|T|} &= \sum_{S \subseteq E} \theta(S) \sum_{T \supseteq S} (-1)^{|T|-|S|} x^{n-|T|} \\ &= \sum_{S \subseteq E} \theta(S)(x-1)^{n-|S|}. \end{aligned}$$

The proof concludes as before.

(b) The proof is similar.

6 Which variables occur?

In this section we show that the indices of the variables which occur in the orbital Tutte polynomial are restricted.

Theorem 8 *If the indeterminate x_i actually appears in the orbital Tutte polynomial of (Γ, G), then either $i = 0$, or i is the order of an element of G.*

PROOF. It suffices to prove that only zero and divisors of the order i of the automorphism g can appear as invariant factors of the modules $\mathbb{Z}^E/\rho(M_g)$ and $\mathbb{Z}^E/\rho(M_g^*)$. In other words, each of these modules is the direct sum of a free module and a module annihilated by i. This is a consequence of the following lemma.

Lemma 9 *Let W be a free $\mathbb{Z}$-module, and g an automorphism of W of order i. Then any invariant factor of $W/(g-1)W$ is either zero or a divisor of i.*

PROOF. We can write $W/(g-1)W$ as the direct sum of a torsion-free module U_0 and a torsion module U_1. The invariant factors of U_0 are all zero, so it suffices to consider U_1. Let W_1 be its preimage in W.

We claim that $g^{i-1} + \cdots + 1$ annihilates W_1. For let $V_1 = W_1 \otimes \mathbb{Q}$. The eigenvalues of g on V_1 are ith roots of unity. If 1 is an eigenvalue with eigenvector v, then some integer multiple w of v lies in W_1, and generates a torsion-free submodule of $W_1/(g-1)W_1$, contrary to assumption. (For suppose that $kw \in (g-1)W$, say $kw = (g-1)x$, with $gw = w$. Then $kw = (g^2 - g)x, \ldots, kw = (1 - g^{i-1})x$; and so $ikw = 0$, contradicting the fact that w lies in a free $\mathbb{Z}$-module.)

So the minimum polynomial of g on V_1 divides $(x^i - 1)/(x-1) = x^{i-1} + \cdots + 1$, and $g^{i-1} + \cdots + 1$ annihilates V_1 and hence W_1.

There exists an integer polynomial $f(x)$ such that

$$(x^{i-1} + \cdots + 1) - f(x)(x-1) = i.$$

(This is easily seen by substituting $x = y + 1$.) Now both $g^{i-1} + \cdots + 1$ and $g - 1$ annihilate the $\mathbb{Z}$-module $W_1/(g-1)W_1$, and hence i annihilates this module. So its invariant factors divide i, as required.

There are further restrictions on the orbital Tutte polynomial. Each monomial has the form $x(A)x^*(B)$ for some matrices A and B. Hence, if it has the form $x_{d_1}x_{d_2}\cdots x_{d_r}x_0^{k-r}$ (ignoring the starred variables), then necessarily d_i divides d_{i+1} for $1 \le i \le r-1$. A similar comment holds for the starred variables.

7 Chromatic polynomial revisited

For connected graphs, the orbital chromatic polynomial is also a specialisation of the orbital Tutte polynomial.

Theorem 10 *Let Γ be a connected graph. Then the orbital chromatic polynomial of (Γ, G) is obtained from the orbital tension polynomial by substituting $x_0^* = k$, $x_i^* = 1$ for $i > 0$, and multiplying by k.*

PROOF. We show first that, for any automorphism g, the number of g-fixed colourings (not necessarily proper) is obtained from the monomial $x^*(M_g^*)$ by making the above substitution and multiplying by k. Now the multiplicity of 0 as an invariant factor of M_g^* is the nullity of M_g^*, so the result of the substitution is $(x^*)^{1+n(M_g^*)}$. On the other hand, the number of colourings fixed by g is $k^{c(g)}$, where $c(g)$ is the number of vertex cycles of g. So we are required to prove that

$$1 + n(M_g) = c(g).$$

In this section, we denote the signed permutation matrix corresponding to the action of g on edges by g^E, and the permutation matrix on vertices by g^V. Using the fact that g is an automorphism of Γ, it is not difficult to show that $g^V M = M g^E$; hence $(g^V - 1)M = M(g^E - 1)$.

Now each vertex cycle of g corresponds to a square block matrix in g^V with corank 1; so $c(g) = n(g^V - 1)$. Indeed, this shows that the (row) null space of $g^V - 1$ consists of vectors constant on the vertex cycles of g. Since Γ is connected, the row null space of M is spanned by the constant vector $\underline{1}$, and so is contained in the row null space of $g^V - 1$. Thus, if $\underline{x}(g^V - 1)M = 0$, then $\underline{x}(g^V - 1) = c\underline{1}$ for some constant c. But this implies that $c = 0$, since the sums of the entries in $\underline{x}$ and $\underline{x}g^V$ are equal. Hence the null space of $(g^V - 1)M$ (call it W) is equal to that of $g^V - 1$, and so $\dim(W) = c(g)$.

By our earlier observation, W is also the row null space of $M(g^E - 1)$.

Now clearly $\nu(M_g^*) = \nu(M^*) \cap \nu(g^E - 1)$ (where, here as earlier, $\nu(N)$ denotes the column null space of N, the set of vectors $\underline{x}$ such that $N\underline{x}^\top = 0$). Since M and M^* are dual,

$$\begin{aligned}
\nu(M_g^*) &= \rho(M) \cap \nu(g^E - 1) \\
&= \{\underline{x}M : \underline{x}M(g^E - 1) = 0\} \\
&= \{\underline{x}M : x \in W\}.
\end{aligned}$$

Since the kernel of M restricted to W has dimension 1, we have

$$n(M_g^*) = \dim(W) - 1 = c(g) - 1,$$

as required.

This argument shows that the tensions which are the gradients of fixed colourings are counted by $x^*(M_g^*)$ with the substitution of the theorem applied. Now consider the inclusion-exclusion argument which counts non-zero fixed tensions within the class of all fixed tensions. This involves an alternating sum over subsets B of the edge-set, the term corresponding to B counting tensions which vanish outside B. These tensions are obtained by imposing $n - |B|$ equations each asserting that some variable is zero. Clearly the same equations select those tensions which are gradients of fixed colourings vanishing outside B. As above, the nullity of the appropriate matrix is equal to the number of invariant factors which are zero. For each such term, the number of fixed colourings of which these tensions are the gradients is obtained by multiplying the number of such tensions by k. The final outcome is that the number of fixed tensions which are gradients of fixed proper colourings is given by the substitution of the theorem into the term corresponding to g in the orbital tension polynomial, and the number of fixed proper colourings is k times the result.

So the theorem is proved.

If Γ is disconnected, the orbital chromatic polynomial cannot be obtained as a specialisation of the orbital Tutte polynomial as defined here. Arguing as above, we can show that the number of proper colourings fixed by an automorphism g is

$$k^{c'(g)} \sum_{S \subseteq E} x(M_g[S]; x_i \leftarrow -1) x^*(M^*[E \setminus S]; x_0^* \leftarrow k, x_i^* \leftarrow 1 \text{ for } i > 0),$$

where $c'(g)$ is the number of cycles of g on the set of connected components of Γ. The factor $k^{c'(g)}$ will vary from one automorphism to another, so cannot be taken out as a prefactor of the sum over G. A solution would be to modify our definition of the orbital Tutte polynomial by putting a factor $u^{c'(g)}$, where u is a new indeterminate. Further comments on this appear in the last section.

8 An example

Let Γ be a 4-cycle with a diagonal, and G the full group of automorphisms of Γ (see Figure 1). The orbital Tutte polynomial of Γ and G is

$$\begin{aligned}
&\tfrac{1}{4}(x_0^2x_1^3 + 2x_0x_1^4 + 6x_0x_1^3x_1^* + 2x_0x_1^2x_0^*x_1^* + 8x_1^4x_1^* + x_1^3x_2^2 \\
&\quad + 6x_1^3x_2x_1^* + 36x_1^3x_1^{*2} + 2x_1^2x_2x_0^*x_1^* + 18x_1^2x_0^*x_1^{*2} + 20x_1^2x_1^{*3} \\
&\quad + 2x_1^2x_1^{*2}x_2^* + 6x_1x_0^{*2}x_1^{*2} + 10x_1x_0^*x_1^{*3} + 4x_1x_1^{*3}x_2^* + x_0^{*3}x_1^{*2} \\
&\quad + 2x_0^{*2}x_1^{*3} + x_0^*x_1^{*3}x_2^*).
\end{aligned}$$

Substituting $x_i = -1$ for all i, $x_0^* = k$, $x_1^* = 1$, $x_2^* = \alpha$, we find that the number of orbits of G on nowhere-zero tensions on Γ with values in an abelian group A of order k containing α elements a satisfying $2a = 0$:

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

Putting $\alpha = 1$ and multiplying by k gives the orbital chromatic polynomial, counting orbits of G on proper k-colourings of Γ (as calculated earlier):

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

Dually, substituting $x_i^* = -1$ for all i, $x_0 = k$, $x_1 = 1$ and $x_2 = \alpha$, we count orbits of G on nowhere-zero flows with values in an abelian group A as above:

$$\tfrac{1}{4}((k-1)^2 + (\alpha-1)(\alpha-3)).$$

All these are easily checked directly.

9 Codes

A linear code over $\mathrm{GF}(q)$ is the row space of a *generator matrix* M over $\mathrm{GF}(q)$, and is the null space of a *parity check matrix* M^* (the generator matrix of the dual code). These matrices are duals in our previous sense, so if G is a group of automorpisms of C, the orbital Tutte polynomial P is defined as before. Since $\mathrm{GF}(q)$ is a field, P involves only the variables x_0, x_1, x_0^*, x_1^*.

The *orbital weight enumerator* is the homogeneous polynomial

$$W_{C,G}(X,Y) = \sum_{i=0}^{n} a_i X^{n-i} Y^i,$$

where a_i is the number of G-orbits on words of weight i in C.

Theorem 11 *Let G be the automorphism group of a linear code over* $\mathrm{GF}(q)$*. Then the orbital weight enumerator C is obtained from the orbital Tutte polynomial by the substitution*

$$x_0 = x_1 = X - Y, \quad x_0^* = qY, \quad x_1^* = Y.$$

PROOF. Let $a(S)$ be the number of codewords with support S fixed by the automorphism g, and $b(S)$ the number with support contained in S. Then

$b(S) = q^t$, where t is the nullity of $M_g^*[S]$. So $b(S)Y^{|S|}$ is obtained from $x^*[S]$ by the substitution $x_0^* = qY$, $x_1^* = Y$.

Also, by the Inclusion-Exclusion Principle,

$$a(S) = \sum_{T \subseteq S} (-1)^{|S|-|T|} b(T).$$

So

$$\begin{aligned}\sum_S a(S) X^{n-|S|} Y^{|S|} &= \sum_S \sum_{T \subseteq S} b(T)(-1)^{|S|-|T|} X^{n-|S|} Y^{|S|} \\ &= \sum_T b(T) Y^{|T|} \sum_{S \supseteq T} X^{n-|S|} (-Y)^{|S|-|T|} \\ &= \sum_T b(T) Y^{|T|} (X-Y)^{n-|T|},\end{aligned}$$

and the last expression is exactly what is obtained by substituting $x_0 = x_1 = X - Y$, $x_0^* = qY$, $x_1^* = Y$ into the summand indexed by g in the orbital Tutte polynomial. Now averaging over G gives the result.

Greene[4] showed that the weight enumerator of a linear code is a specialisation of the Tutte polynomial of the corresponding matroid. In terms of our orbital polynomial, if G is the trivial group, then the weight enumerator of C is obtained from the orbital Tutte polynomial by the substitution

$$x_0 = \frac{X-Y}{Y}, x_0^* = \frac{qY}{X-Y}, x_1 = x_1^* = 1,$$

and then multiplying by $Y^{n-k}(X-Y)^k$ to clear denominators. Curiously, this is a different substitution from the one in the above theorem, and does not generalise to the orbital Tutte polynomial.

Indeed, Greene observed that his theorem together with the facts that $T(M^*; x, y) = T(M; y, x)$ and that dual codes correspond to dual matroids, implies the MacWilliams relation between the weight enumerators of a code and its dual. No such relation holds between the orbital weight enumerators of a code and its dual.

Example Let C be the repetition code of length 3 over GF(3) For any subgroup G of the symmetric group S_3, the orbital weight enumerator is $W_{C,G}(X,Y) = X^3 + 2Y^3$; however, $W_{C^\perp,G}(X,Y) = X^3 + aXY^2 + 2Y^3$, where $a = 6/|G|$.

10 Related results and further directions

Several multi-variable Tutte polynomials have appeared in the literature. These include Tutte's universal V-function [9], the U-polynomial of Noble and Welsh [5], Stanley's chromatic symmetric polynomial [8], Brylawski's polychromate [2], and Sokal's multivariate Tutte polynomial [6] (essentially the Potts model partition function of a graph). It is not clear what relationship, if any, these polynomials have to our orbital Tutte polynomial. Cameron's "Tutte cycle index" [3] specialises to both the Tutte polynomial of a matroid M and the cycle index of a group of automorphisms of M, but again its relationship with our polynomial is unknown.

We note that other authors, for example Sokal [6], Beck and Zaslavsky [1], have used invariant factors of matrices in constructing graph or matroid polynomials.

We are not convinced that our orbital Tutte polynomial is the last word on the subject. We already saw that, in order to count orbits of colourings in disconnected graphs, we require a new indeterminate, whose exponent in the term corresponding to an automorphism g is the number of cycles of g on connected components. Similarly, in order to extend Stanley's result [7] that the number of acyclic orientations is $\chi(-1)$, we appear to need an indicator variable for the number of cycles of g on vertices. It would appear natural to do the same thing for edges as well. We hope to investigate this in further research.

We would also like to find a way to combine our orbital Tutte polynomial with the cycle index of the permutation group G in order to perform more elaborate counting.

Another direction would be to allow symmetry or structure on the set of colours. For example we could have the group acting on the set of colours as well as on the graph; or we could count orbits of G on homomorphisms from Γ to a fixed target graph Δ (proper colourings correspond to the case where Δ is the complete graph K_k).

References

[1] M. Beck and T. Zaslavski, The number of nowhere-zero flows in graphs and signed graphs, preprint.

[2] T. H. Brylawski, Hyperplane reconstruction of the Tutte polynomial of a geometric lattice, *Discrete Math.* **35** (1981), 25–38.

[3] P. J. Cameron, Cycle index, weight enumerator and Tutte polynomial, *Electronic J. Combinatorics* **9(1)** (2002), #N2 (10pp).

[4] C. Greene, Weight enumeration and the geometry of linear codes, *Studies in Applied Math.* **55** (1976), 119–128.

[5] S. D. Noble and D. J. A. Welsh, A weighted graph polynomial from chromatic invariants of knots, Symposium à la Mémoire de François Jaeger (Grenoble, 1998). *Ann. Inst. Fourier* (Grenoble) **49** (1999), 1057–1087.

[6] A. D. Sokal, The multivariate Tutte polynomial (alias Potts model) for graphs and matroids, *Surveys in Combinatorics 2005* (ed. B. S. Webb), London Math. Soc. Lecture Notes, to appear.

[7] R. P. Stanley, Acyclic orientations of graphs, *Discrete Math.* **5** (1973), 171–178.

[8] R. P. Stanley, A symmetric function generalization of the chromatic polynomial of a graph, *Advances Math.* **111** (1995), 166–194.

[9] W. T. Tutte, A ring in graph theory, *Proc. Cambridge Philos. Soc.* **43** (1947), 26–40.