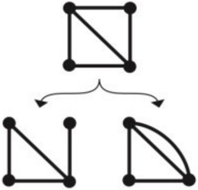
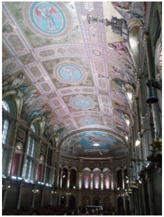
Tutte polynomial and orbit-counting

Peter J. Cameron
University of St Andrews

New directions for the Tutte Polynomial
Royal Holloway, University of London
July 2015





Much of this is joint work with
Dima Fon-Der-Flaass, Bill Jackson, Koko Kayibi, Jason Rudd

Sampling

In how many ways can we sample n objects from a set of q?

Sampling

In how many ways can we sample n objects from a set of q?

	Order significant	Order not significant
With replacement	q^n	$\binom{q+n-1}{n}$
Without replacement	$(q)_n$	$\binom{q}{n}$

Sampling

In how many ways can we sample n objects from a set of q?

	Order significant	Order not significant
With replacement	q^n	$\binom{q+n-1}{n}$
Without replacement	$(q)_n$	$\binom{q}{n}$

Here q^n is the number of colourings of a set of size n with q colours.

Sampling

In how many ways can we sample n objects from a set of q?

	Order significant	Order not significant
With replacement	q^n	$\binom{q+n-1}{n}$
Without replacement	$(q)_n$	$\binom{q}{n}$

Here q^n is the number of colourings of a set of size n with q colours.
In the second row we put on a structural restriction: we want proper colourings of the complete graph. So this is the chromatic polynomial of K_n.

Sampling

In how many ways can we sample n objects from a set of q?

	Order significant	Order not significant
With replacement	q^n	$\binom{q+n-1}{n}$
Without replacement	$(q)_n$	$\binom{q}{n}$

Here q^n is the number of colourings of a set of size n with q colours.
In the second row we put on a structural restriction: we want proper colourings of the complete graph. So this is the chromatic polynomial of K_n.
In the second column, we count up to symmetry, specifically the symmetric group S_n, the automorphism group of the complete graph.

Orbit counting

My aim is to generalise this simple observation. The chromatic polynomial of a graph counts colourings with a structural restriction; it is a specialisation of the Tutte polynomial. If we have a group G of automorphisms, we want to count G orbits on such objects.

Orbit counting

My aim is to generalise this simple observation. The chromatic polynomial of a graph counts colourings with a structural restriction; it is a specialisation of the Tutte polynomial. If we have a group G of automorphisms, we want to count G orbits on such objects.

The basic tool is the orbit-counting lemma:

Orbit counting

My aim is to generalise this simple observation. The chromatic polynomial of a graph counts colourings with a structural restriction; it is a specialisation of the Tutte polynomial. If we have a group G of automorphisms, we want to count G orbits on such objects.

The basic tool is the orbit-counting lemma:

Theorem

Let the finite group G act on the finite set X. Then the number of orbits of G on X is equal to the average number of fixed points of its elements:

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

The Tutte polynomial

As you know, the Tutte polynomial counts many things; for example,

The Tutte polynomial

As you know, the Tutte polynomial counts many things; for example,

- bases, independent sets and spanning sets in a matroid (in particular, spanning trees, forests, and connected subgraphs in a connected graph);

The Tutte polynomial

As you know, the Tutte polynomial counts many things; for example,

- bases, independent sets and spanning sets in a matroid (in particular, spanning trees, forests, and connected subgraphs in a connected graph);
- colourings, nowhere-zero flows, and acyclic orientations in a graph;

The Tutte polynomial

As you know, the Tutte polynomial counts many things; for example,

- bases, independent sets and spanning sets in a matroid (in particular, spanning trees, forests, and connected subgraphs in a connected graph);
- colourings, nowhere-zero flows, and acyclic orientations in a graph;
- for matroids representable over a finite field, words of each weight in the code spanned by the rows of a representing matrix.

The Tutte polynomial

As you know, the Tutte polynomial counts many things; for example,

- bases, independent sets and spanning sets in a matroid (in particular, spanning trees, forests, and connected subgraphs in a connected graph);
- colourings, nowhere-zero flows, and acyclic orientations in a graph;
- for matroids representable over a finite field, words of each weight in the code spanned by the rows of a representing matrix.

We would like to find polynomials for which suitable coefficients or evaluations give us the number of orbits of a group of automorphisms of the graph or matroid on the objects mentioned above (and others if possible).

Orbital chromatic polynomial

Theorem

Let G be a group of automorphisms of the graph X. Then there is a polynomial $\mathrm{OP}_{X,G}$ whose value at a positive integer q is equal to the number of orbits of G on proper q-colourings of X.

Orbital chromatic polynomial

Theorem

Let G be a group of automorphisms of the graph X. Then there is a polynomial $\mathrm{OP}_{X,G}$ whose value at a positive integer q is equal to the number of orbits of G on proper q-colourings of X.

Specifically,

$$\mathrm{OP}_{X,G}(q) = \frac{1}{|G|} \sum_{g \in G} P_{X/g}(q),$$

where P_X denotes the chromatic polynomial of X, and X/g denotes the graph obtained from X by shrinking each cycle of the permutation g to a single vertex (with a loop at that vertex if the cycle contains an edge of the graph – in this case $P_{X/g} = 0$).

Acyclic orientations

Theorem (Stanley)

The number of acyclic orientations of the graph X is $(-1)^{|VX|}P_X(-1)$.

Acyclic orientations

Theorem (Stanley)

The number of acyclic orientations of the graph X is $(-1)^{|VX|}P_X(-1)$.

It is natural, then, to wonder whether the number of G-orbits on acyclic orientations of X would be $(-1)^{|VX|}\,\mathrm{OP}_{X,G}(-1)$.

Acyclic orientations

Theorem (Stanley)

The number of acyclic orientations of the graph X is $(-1)^{|VX|}P_X(-1)$.

It is natural, then, to wonder whether the number of G-orbits on acyclic orientations of X would be $(-1)^{|VX|}\,\mathrm{OP}_{X,G}(-1)$. This is not quite true. We have to modify the polynomial by multiplying the term corresponding to the element $g \in G$ by the sign of g (as permutation on the vertices).

Acyclic orientations

Theorem (Stanley)

The number of acyclic orientations of the graph X is $(-1)^{|VX|}P_X(-1)$.

It is natural, then, to wonder whether the number of G-orbits on acyclic orientations of X would be $(-1)^{|VX|}\,\mathrm{OP}_{X,G}(-1)$. This is not quite true. We have to modify the polynomial by multiplying the term corresponding to the element $g \in G$ by the sign of g (as permutation on the vertices).
If the resulting polynomial is $\mathrm{OP}^*_{X,G}$, then the number of orbits on acyclic orientations is $(-1)^{|VX|}\,\mathrm{OP}^*_{X,G}(-1)$.

Flows and tensions

It is often said that flows are dual to colourings. Actually they are dual to tensions, and the orbital perspective makes this clear.

Let A be a finite abelian group. Take a fixed but arbitrary orientation of the edges of the graph X. An A-flow on X is a function from oriented edges to A such that the algebraic sum of the flows into any vertex is 0 (where flows out have a $-$ sign).

Flows and tensions

It is often said that flows are dual to colourings. Actually they are dual to tensions, and the orbital perspective makes this clear.

Let A be a finite abelian group. Take a fixed but arbitrary orientation of the edges of the graph X. An A-flow on X is a function from oriented edges to A such that the algebraic sum of the flows into any vertex is 0 (where flows out have a $-$ sign).

An A-tension is a function from the oriented edges to A such that the algebraic sum of the flows around any directed cycle is 0 (where flows on edges directed against the cycle have a $-$ sign.)

Flows and tensions

It is often said that flows are dual to colourings. Actually they are dual to tensions, and the orbital perspective makes this clear.

Let A be a finite abelian group. Take a fixed but arbitrary orientation of the edges of the graph X. An A-flow on X is a function from oriented edges to A such that the algebraic sum of the flows into any vertex is 0 (where flows out have a $-$ sign).

An A-tension is a function from the oriented edges to A such that the algebraic sum of the flows around any directed cycle is 0 (where flows on edges directed against the cycle have a $-$ sign.)

A flow or tension is nowhere-zero if it does not take the value 0.

Flows and tensions

It is often said that flows are dual to colourings. Actually they are dual to tensions, and the orbital perspective makes this clear.

Let A be a finite abelian group. Take a fixed but arbitrary orientation of the edges of the graph X. An A-flow on X is a function from oriented edges to A such that the algebraic sum of the flows into any vertex is 0 (where flows out have a $-$ sign).

An A-tension is a function from the oriented edges to A such that the algebraic sum of the flows around any directed cycle is 0 (where flows on edges directed against the cycle have a $-$ sign.)

A flow or tension is nowhere-zero if it does not take the value 0.

It is easy to see that the number of nowhere-zero tensions is $P_X(q)/q^\kappa$, where $q = |A|$, and P_X and κ are the chromatic polynomial and the number of connected components of X.

Tutte showed that the number of nowhere-zero flows also depends only on $q = |A|$ and not on the structure of A.

Tutte showed that the number of nowhere-zero flows also depends only on $q = |A|$ and not on the structure of A. However, if G is a group of automorphisms of X, then the number of G-orbits on nowhere-zero flows and tensions does depend on the structure of X:

Tutte showed that the number of nowhere-zero flows also depends only on $q = |A|$ and not on the structure of A. However, if G is a group of automorphisms of X, then the number of G-orbits on nowhere-zero flows and tensions does depend on the structure of X:

Theorem

There are polynomials $\mathrm{OT}_{X,G}$ *and* $\mathrm{OF}_{X,G}$ *in indeterminates* $x_0, x_1, x_2, \ldots$ *such that the number of* G*-orbits on nowhere-zero* A*-tensions (resp.* A*-flows) are obtained from* $\mathrm{OT}_{X,G}$ *(resp.* $\mathrm{OF}_{X,G}$ *by substituting for* x_i *the number of solutions of* $ia = 0$ *in* A*.*

Tutte showed that the number of nowhere-zero flows also depends only on $q = |A|$ and not on the structure of A. However, if G is a group of automorphisms of X, then the number of G-orbits on nowhere-zero flows and tensions does depend on the structure of X:

Theorem

There are polynomials $\mathrm{OT}_{X,G}$ *and* $\mathrm{OF}_{X,G}$ *in indeterminates* $x_0, x_1, x_2, \ldots$ *such that the number of G-orbits on nowhere-zero A-tensions (resp. A-flows) are obtained from* $\mathrm{OT}_{X,G}$ *(resp.* $\mathrm{OF}_{X,G}$ *by substituting for x_i the number of solutions of $ia = 0$ in A.*

Note that $x_0 = |A|$ and $x_1 = 1$. Moreover, x_i occurs in one of these polynomials only if G contains an element of order i. So we recover Tutte's observation when G is the trivial group.

Matrices over PIDs

The proof of the theorem involves finding a generalised Tutte polynomial associated with a matrix M over a principal ideal domain. The polynomial has two sequences of variables $x_0, x_1, x_2, \ldots$ and $y_0, y_1, y_2, \ldots$; the x variables give the orbital tension polynomial and the y variables the orbital flow polynomial.

Matrices over PIDs

The proof of the theorem involves finding a generalised Tutte polynomial associated with a matrix M over a principal ideal domain. The polynomial has two sequences of variables $x_0, x_1, x_2, \ldots$ and $y_0, y_1, y_2, \ldots$; the x variables give the orbital tension polynomial and the y variables the orbital flow polynomial.

Now tensions are elements of the kernel of the vertex-edge incidence matrix of the graph, and flows are elements of the kernel of the cycle-edge incidence matrix. Both matrices are unimodular. To count fixed points of a permutation g with permutation matrix P_g, we append $I - P_g$ to the appropriate incidence matrix; this is no longer unimodular, so we need variables for all the possible invariant factors of the matrix (indexed by the associate classes in the ring $\mathbb{Z}$).

Matrices over PIDs

The proof of the theorem involves finding a generalised Tutte polynomial associated with a matrix M over a principal ideal domain. The polynomial has two sequences of variables $x_0, x_1, x_2, \ldots$ and $y_0, y_1, y_2, \ldots$; the x variables give the orbital tension polynomial and the y variables the orbital flow polynomial.

Now tensions are elements of the kernel of the vertex-edge incidence matrix of the graph, and flows are elements of the kernel of the cycle-edge incidence matrix. Both matrices are unimodular. To count fixed points of a permutation g with permutation matrix P_g, we append $I - P_g$ to the appropriate incidence matrix; this is no longer unimodular, so we need variables for all the possible invariant factors of the matrix (indexed by the associate classes in the ring $\mathbb{Z}$).

All this can be done for matrices over any principal ideal domain.

Finite fields and codes

If we use the finite field $\mathrm{GF}(q)$ instead of the integers as our principal ideal domain, then the kernel of a matrix is a *linear code* over $\mathrm{GF}(q)$.

Finite fields and codes

If we use the finite field $\mathrm{GF}(q)$ instead of the integers as our principal ideal domain, then the kernel of a matrix is a *linear code* over $\mathrm{GF}(q)$.
So the general machinery gives us an *orbital weight enumerator* associated with a linear code and a group of automorphisms.

Finite fields and codes

If we use the finite field $\mathrm{GF}(q)$ instead of the integers as our principal ideal domain, then the kernel of a matrix is a *linear code* over $\mathrm{GF}(q)$.
So the general machinery gives us an *orbital weight enumerator* associated with a linear code and a group of automorphisms.
In the case of the trivial group, we get the weight enumerator of the code as a specialisation of our (four-variable) Tutte polynomial. Curiously, the connection we get is slightly different from the one in Curtis Greene's famous theorem!

More generally . . .

Even if you are not at all interested in automorphisms and orbit-counting, the above technique might be useful.

More generally ...

Even if you are not at all interested in automorphisms and orbit-counting, the above technique might be useful.

Let C be a linear code over $\mathbb{Z}_4$, the integers modulo 4. (These codes have been of some interest since the paper of Hammons *et al.* showed that certain famous non-linear binary codes such as the Nordstrom–Robinson, Preparata and Kerdock codes are images, under the non-linear Gray map, of linear $\mathbb{Z}_4$ codes.)

More generally . . .

Even if you are not at all interested in automorphisms and orbit-counting, the above technique might be useful.

Let C be a linear code over $\mathbb{Z}_4$, the integers modulo 4. (These codes have been of some interest since the paper of Hammons *et al.* showed that certain famous non-linear binary codes such as the Nordstrom–Robinson, Preparata and Kerdock codes are images, under the non-linear Gray map, of linear $\mathbb{Z}_4$ codes.)

The symmetrised weight enumerator of such a code has three indeterminates X_0, X_2, and X_{13}: each codeword w contributes a term $X_0^a X_2^b X_{13}^c$, where a, b and c are respectively the numbers of entries equal to 0, 2, and (1 or 3) respectively – in other words, the associate classes!

More generally . . .

Even if you are not at all interested in automorphisms and orbit-counting, the above technique might be useful.

Let C be a linear code over $\mathbb{Z}_4$, the integers modulo 4. (These codes have been of some interest since the paper of Hammons *et al.* showed that certain famous non-linear binary codes such as the Nordstrom–Robinson, Preparata and Kerdock codes are images, under the non-linear Gray map, of linear $\mathbb{Z}_4$ codes.)

The symmetrised weight enumerator of such a code has three indeterminates X_0, X_2, and X_{13}: each codeword w contributes a term $X_0^a X_2^b X_{13}^c$, where a, b and c are respectively the numbers of entries equal to 0, 2, and (1 or 3) respectively – in other words, the associate classes!

Carrie Rutherford gave an analogue of the deletion–contraction formula for such codes, which involves a third operation which she called "detraction".

More generally . . .

Even if you are not at all interested in automorphisms and orbit-counting, the above technique might be useful.

Let C be a linear code over $\mathbb{Z}_4$, the integers modulo 4. (These codes have been of some interest since the paper of Hammons *et al.* showed that certain famous non-linear binary codes such as the Nordstrom–Robinson, Preparata and Kerdock codes are images, under the non-linear Gray map, of linear $\mathbb{Z}_4$ codes.)

The symmetrised weight enumerator of such a code has three indeterminates X_0, X_2, and X_{13}: each codeword w contributes a term $X_0^a X_2^b X_{13}^c$, where a, b and c are respectively the numbers of entries equal to 0, 2, and (1 or 3) respectively – in other words, the associate classes!

Carrie Rutherford gave an analogue of the deletion–contraction formula for such codes, which involves a third operation which she called "detraction".

So our approach gives a generalisation to codes over $\mathbb{Z}_q$, or more general finite rings.

Cycle index

Let G be a permutation group on a set X. The cycle index of G is the polynomial in indeterminates $s_1, s_2, \ldots$ given by

$$Z(G) = \frac{1}{|G|} \sum_{g \in G} s_1^{c_1(g)} s_2^{c_2(g)} \cdots ,$$

where $c_i(g)$ is the number of i-cycles in the cycle decomposition of G.

Cycle index

Let G be a permutation group on a set X. The cycle index of G is the polynomial in indeterminates $s_1, s_2, \ldots$ given by

$$Z(G) = \frac{1}{|G|} \sum_{g \in G} s_1^{c_1(g)} s_2^{c_2(g)} \cdots ,$$

where $c_i(g)$ is the number of i-cycles in the cycle decomposition of G.

This gadget automates many orbit counting problems. If we have a set of "figures" with non-negative integer "weights", with $A(x)$ the generating function of figures by weight, then any orbit of G on "functions" (from X to the set of figures) has an associated weight, and the generating function for functions by weight is given by the cycle index, with s_i substituted by $A(x^i)$ for all i: this is the cycle index theorem.

Cycle index

Let G be a permutation group on a set X. The cycle index of G is the polynomial in indeterminates $s_1, s_2, \ldots$ given by

$$Z(G) = \frac{1}{|G|} \sum_{g \in G} s_1^{c_1(g)} s_2^{c_2(g)} \cdots ,$$

where $c_i(g)$ is the number of i-cycles in the cycle decomposition of G.

This gadget automates many orbit counting problems. If we have a set of "figures" with non-negative integer "weights", with $A(x)$ the generating function of figures by weight, then any orbit of G on "functions" (from X to the set of figures) has an associated weight, and the generating function for functions by weight is given by the cycle index, with s_i substituted by $A(x^i)$ for all i: this is the cycle index theorem.

This is fine for counting unrestricted colourings, but for e.g. proper colourings of graphs something more is required.

Cycle index

Let G be a permutation group on a set X. The cycle index of G is the polynomial in indeterminates $s_1, s_2, \ldots$ given by

$$Z(G) = \frac{1}{|G|} \sum_{g \in G} s_1^{c_1(g)} s_2^{c_2(g)} \cdots,$$

where $c_i(g)$ is the number of i-cycles in the cycle decomposition of G.

This gadget automates many orbit counting problems. If we have a set of "figures" with non-negative integer "weights", with $A(x)$ the generating function of figures by weight, then any orbit of G on "functions" (from X to the set of figures) has an associated weight, and the generating function for functions by weight is given by the cycle index, with s_i substituted by $A(x^i)$ for all i: this is the cycle index theorem.

This is fine for counting unrestricted colourings, but for e.g. proper colourings of graphs something more is required.

If G is a group of automorphisms of a matroid M on X, can one combine the cycle index of G with the Tutte polynomial of M?

IBIS groups

A base for a permutation group is a sequence of points whose stabiliser is the identity. It is irredundant if no point is fixed by the stabiliser of its predecessors.

A base for a permutation group is a sequence of points whose stabiliser is the identity. It is irredundant if no point is fixed by the stabiliser of its predecessors.

Theorem

For a finite permutation group, the following are equivalent:

A base for a permutation group is a sequence of points whose stabiliser is the identity. It is irredundant if no point is fixed by the stabiliser of its predecessors.

Theorem

For a finite permutation group, the following are equivalent:

- *all irredundant bases have the same size;*

A base for a permutation group is a sequence of points whose stabiliser is the identity. It is irredundant if no point is fixed by the stabiliser of its predecessors.

Theorem

For a finite permutation group, the following are equivalent:

- *all irredundant bases have the same size;*
- *irredundant bases are preserved by reordering;*

A base for a permutation group is a sequence of points whose stabiliser is the identity. It is irredundant if no point is fixed by the stabiliser of its predecessors.

Theorem

For a finite permutation group, the following are equivalent:

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

A base for a permutation group is a sequence of points whose stabiliser is the identity. It is irredundant if no point is fixed by the stabiliser of its predecessors.

Theorem

For a finite permutation group, the following are equivalent:

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

A permutation group having these equivalent properties is called an IBIS group (for Irredundant Bases of Invariant Size). There are many examples.

A base for a permutation group is a sequence of points whose stabiliser is the identity. It is irredundant if no point is fixed by the stabiliser of its predecessors.

Theorem

For a finite permutation group, the following are equivalent:

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

A permutation group having these equivalent properties is called an IBIS group (for Irredundant Bases of Invariant Size). There are many examples.

For IBIS groups, the connection between cycle index and Tutte polynomial should be closer.

Tutte cycle index

My first attempt went like this. Let G be an IBIS group, and M the associated matroid.

The Tutte cycle index of G is given by

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

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.

Tutte cycle index

My first attempt went like this. Let G be an IBIS group, and M the associated matroid.
The Tutte cycle index of G is given by

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

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 recover the cycle index by the rule that $\left(\frac{\partial}{\partial u} ZT(G)\right)(u = 1, v = 1)$ is equal to $Z(G)$ with $s_i + 1$ substituted for s_i.

Tutte cycle index

My first attempt went like this. Let G be an IBIS group, and M the associated matroid.
The Tutte cycle index of G is given by

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

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 recover the cycle index by the rule that $\left(\frac{\partial}{\partial u} ZT(G)\right)(u = 1, v = 1)$ is equal to $Z(G)$ with $s_i + 1$ substituted for s_i.
We recover the Tutte polynomial of M by the rule that $|G| ZT(G; u = 1, s_i = t^i)$ is equal to $t^{b(G)} T(M; v/t + 1, t + 1)$.

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?

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 $v = 1$ and omit all mention of matroid rank.