Oligomorphic groups and their orbit algebras

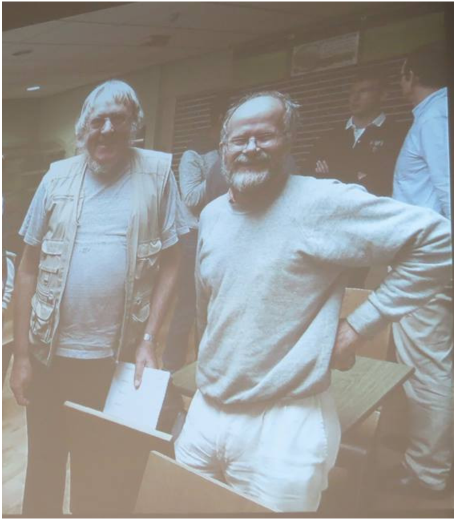
Peter J. Cameron
University of St Andrews

From permutation groups to model theory
Edinburgh, September 2018

Happy birthday Dugald!

$$\mathrm{Age(HDM)} = |A_5|$$

On the big screen



Durham 2015

The early days

After Dugald finished his undergraduate degree in Oxford, and before embarking on his DPhil, he went to the Northern Isles to run a chess workshop for schoolchildren (if my memory is correct).

The early days

After Dugald finished his undergraduate degree in Oxford, and before embarking on his DPhil, he went to the Northern Isles to run a chess workshop for schoolchildren (if my memory is correct).
Before he went, I suggested to him that he might think about the problem of whether, if G is a primitive but not highly homogeneous group, then the number of orbits of G on n-sets grows faster than any polynomial.

The early days

After Dugald finished his undergraduate degree in Oxford, and before embarking on his DPhil, he went to the Northern Isles to run a chess workshop for schoolchildren (if my memory is correct).

Before he went, I suggested to him that he might think about the problem of whether, if G is a primitive but not highly homogeneous group, then the number of orbits of G on n-sets grows faster than any polynomial.

I thought this would be true, but also thought it would be bad news if it were so.

The early days

After Dugald finished his undergraduate degree in Oxford, and before embarking on his DPhil, he went to the Northern Isles to run a chess workshop for schoolchildren (if my memory is correct).

Before he went, I suggested to him that he might think about the problem of whether, if G is a primitive but not highly homogeneous group, then the number of orbits of G on n-sets grows faster than any polynomial.

I thought this would be true, but also thought it would be bad news if it were so.

When Dugald came back, he showed me a proof that the growth rate is at least fractional exponential.

The early days

After Dugald finished his undergraduate degree in Oxford, and before embarking on his DPhil, he went to the Northern Isles to run a chess workshop for schoolchildren (if my memory is correct).

Before he went, I suggested to him that he might think about the problem of whether, if G is a primitive but not highly homogeneous group, then the number of orbits of G on n-sets grows faster than any polynomial.

I thought this would be true, but also thought it would be bad news if it were so.

When Dugald came back, he showed me a proof that the growth rate is at least fractional exponential.

I will explain these things, why I was interested, why I thought it would be bad news, and what has happened since.

Definitions

A permutation group G on the set Ω is oligomorphic if the number of orbits of G on Ω^n, or on the set of n-tuples of distinct elements of Ω, or on the set of n-element subsets of Ω, are finite for all natural numbers n.

Definitions

A permutation group G on the set Ω is oligomorphic if the number of orbits of G on Ω^n, or on the set of n-tuples of distinct elements of Ω, or on the set of n-element subsets of Ω, are finite for all natural numbers n.

The group G may be finite or infinite; thus every finite group is oligomorphic.

Definitions

A permutation group G on the set Ω is oligomorphic if the number of orbits of G on Ω^n, or on the set of n-tuples of distinct elements of Ω, or on the set of n-element subsets of Ω, are finite for all natural numbers n.

The group G may be finite or infinite; thus every finite group is oligomorphic.

The origin of the term "oligomorphic" will be explained when I discuss Fraïssé's Theorem.

Countably categorical structures

By the upward Löwenheim–Skolem theorem, a set of first order sentences cannot specify a unique structure, even up to cardinality: if the set has a model, then it has arbitrarily large models.

Countably categorical structures

By the upward Löwenheim–Skolem theorem, a set of first order sentences cannot specify a unique structure, even up to cardinality: if the set has a model, then it has arbitrarily large models.
So to specify a structure, we have to include at least one non-logical axiom giving the cardinality of the structure.

Countably categorical structures

By the upward Löwenheim–Skolem theorem, a set of first order sentences cannot specify a unique structure, even up to cardinality: if the set has a model, then it has arbitrarily large models.

So to specify a structure, we have to include at least one non-logical axiom giving the cardinality of the structure.

A countable first-order structure M is said to be $\aleph_0$-categorical or countably categorical if any countable first-order structure N satisfying the same first-order sentences as M is actually isomorphic to M.

Countably categorical structures

By the upward Löwenheim–Skolem theorem, a set of first order sentences cannot specify a unique structure, even up to cardinality: if the set has a model, then it has arbitrarily large models.

So to specify a structure, we have to include at least one non-logical axiom giving the cardinality of the structure.

A countable first-order structure M is said to be $\aleph_0$-categorical or countably categorical if any countable first-order structure N satisfying the same first-order sentences as M is actually isomorphic to M.

The classic example is Cantor's theorem, asserting that the ordered set $\mathbb{Q}$ is the unique countable dense totally ordered set without endpoints. (All hypotheses except "countable" are first-order.)

Connections with model theory

The following theorem is due to Engeler, Ryll-Nardzewski, and Svenonius, independently, in 1959. The three authors stated the result in different ways; I will give just the version which forms a bridge between model theory and permutation groups.

Connections with model theory

The following theorem is due to Engeler, Ryll-Nardzewski, and Svenonius, independently, in 1959. The three authors stated the result in different ways; I will give just the version which forms a bridge between model theory and permutation groups.

Theorem

For a countable first-order structure M, the following are equivalent:

- *M is countably categorical;*

Connections with model theory

The following theorem is due to Engeler, Ryll-Nardzewski, and Svenonius, independently, in 1959. The three authors stated the result in different ways; I will give just the version which forms a bridge between model theory and permutation groups.

Theorem

For a countable first-order structure M, the following are equivalent:

- *M is countably categorical;*
- *the automorphism group of M is oligomorphic (as a permutation group on the domain of M.*

Connections with model theory

The following theorem is due to Engeler, Ryll-Nardzewski, and Svenonius, independently, in 1959. The three authors stated the result in different ways; I will give just the version which forms a bridge between model theory and permutation groups.

Theorem

For a countable first-order structure M, the following are equivalent:

- *M is countably categorical;*
- *the automorphism group of M is oligomorphic (as a permutation group on the domain of M.*

So, in this case, first-order axiomatisability is equivalent to a large amount of symmetry.

Homogeneity and ages

The best (in some sense only) source of examples is the following. A relational first-order structure is homogeneous if every isomorphism between finite substructures can be extended to an automorphism of the structure.

Homogeneity and ages

The best (in some sense only) source of examples is the following. A relational first-order structure is homogeneous if every isomorphism between finite substructures can be extended to an automorphism of the structure.

Thus, if G is the automorphism group of a homogeneous structure M, then the orbits of G on n-sets correspond to the isomorphism types or "shapes" of the n-element substructures of M. So G is oligomorphic if and only if M has only "few shapes" of finite substructures (finitely many of each cardinality).

Homogeneity and ages

The best (in some sense only) source of examples is the following. A relational first-order structure is homogeneous if every isomorphism between finite substructures can be extended to an automorphism of the structure.

Thus, if G is the automorphism group of a homogeneous structure M, then the orbits of G on n-sets correspond to the isomorphism types or "shapes" of the n-element substructures of M. So G is oligomorphic if and only if M has only "few shapes" of finite substructures (finitely many of each cardinality).

This is the origin of the term "oligomorphic". I understand that it is used also in computer science for computer viruses which can exist in only a few different forms, as opposed to polymorphic viruses which occur in many forms.

Ages

The age of a relational structure M is the class $\mathrm{Age}(M)$ of all finite structures embeddable into M. Clearly, if M is homogeneous and $\mathrm{Age}(M)$ contains only finitely many n-element structures for all natural numbers n, then $\mathrm{Aut}(M)$ is oligomorphic.

Ages

The age of a relational structure M is the class $\mathrm{Age}(M)$ of all finite structures embeddable into M. Clearly, if M is homogeneous and $\mathrm{Age}(M)$ contains only finitely many n-element structures for all natural numbers n, then $\mathrm{Aut}(M)$ is oligomorphic.

Fraïssé's Theorem tells us exactly when this happens …

Fraïssé's Theorem

Theorem

The class $\mathcal{C}$ of finite structures is the age of a countable homogeneous relational structure M if and only if it satisfies the following:

Fraïssé's Theorem

Theorem

The class $\mathcal{C}$ of finite structures is the age of a countable homogeneous relational structure M if and only if it satisfies the following:

- *$\mathcal{C}$ is closed under isomorphism;*

Fraïssé's Theorem

Theorem

The class $\mathcal{C}$ of finite structures is the age of a countable homogeneous relational structure M if and only if it satisfies the following:

- *$\mathcal{C}$ is closed under isomorphism;*
- *$\mathcal{C}$ is closed under taking induced substructures;*

Fraïssé's Theorem

Theorem

The class $\mathcal{C}$ of finite structures is the age of a countable homogeneous relational structure M if and only if it satisfies the following:

- *$\mathcal{C}$ is closed under isomorphism;*
- *$\mathcal{C}$ is closed under taking induced substructures;*
- *$\mathcal{C}$ contains only countably many members up to isomorphism;*

Fraïssé's Theorem

Theorem

The class $\mathcal{C}$ of finite structures is the age of a countable homogeneous relational structure M if and only if it satisfies the following:

- *$\mathcal{C}$ is closed under isomorphism;*
- *$\mathcal{C}$ is closed under taking induced substructures;*
- *$\mathcal{C}$ contains only countably many members up to isomorphism;*
- *$\mathcal{C}$ has the amalgamation property: that is, if two structures B_1 and B_2 have a common substructure A, they can be "glued together" along A (and possibly more) to form a structure in $\mathcal{C}$.*

Fraïssé's Theorem

Theorem

The class $\mathcal{C}$ of finite structures is the age of a countable homogeneous relational structure M if and only if it satisfies the following:

- *$\mathcal{C}$ is closed under isomorphism;*
- *$\mathcal{C}$ is closed under taking induced substructures;*
- *$\mathcal{C}$ contains only countably many members up to isomorphism;*
- *$\mathcal{C}$ has the amalgamation property: that is, if two structures B_1 and B_2 have a common substructure A, they can be "glued together" along A (and possibly more) to form a structure in $\mathcal{C}$.*

If these conditions hold, then M is unique (it is called the Fraïssé limit of $\mathcal{C}$).

(For the experts: I assume there is only one kind of empty set; so the amalgamation property implies the joint embedding property.)

A note

Any permutation group G on a countable set Ω is contained in the automorphism group of a countable homogeneous structure: simply take all the G-orbits on Ω^n for all n as relations.

A note

Any permutation group G on a countable set Ω is contained in the automorphism group of a countable homogeneous structure: simply take all the G-orbits on Ω^n for all n as relations.
So Fraïssé's Theorem, in a sense, constructs all examples.

A note

Any permutation group G on a countable set Ω is contained in the automorphism group of a countable homogeneous structure: simply take all the G-orbits on Ω^n for all n as relations.
So Fraïssé's Theorem, in a sense, constructs all examples.
Moreover, the following are equivalent:

A note

Any permutation group G on a countable set Ω is contained in the automorphism group of a countable homogeneous structure: simply take all the G-orbits on Ω^n for all n as relations.
So Fraïssé's Theorem, in a sense, constructs all examples.
Moreover, the following are equivalent:

- G is the full automorphism group of some first-order structure;

A note

Any permutation group G on a countable set Ω is contained in the automorphism group of a countable homogeneous structure: simply take all the G-orbits on Ω^n for all n as relations.

So Fraïssé's Theorem, in a sense, constructs all examples.

Moreover, the following are equivalent:

- G is the full automorphism group of some first-order structure;
- G is the full automorphism group of the homogeneous structure just constructed;

A note

Any permutation group G on a countable set Ω is contained in the automorphism group of a countable homogeneous structure: simply take all the G-orbits on Ω^n for all n as relations.

So Fraïssé's Theorem, in a sense, constructs all examples.

Moreover, the following are equivalent:

- G is the full automorphism group of some first-order structure;
- G is the full automorphism group of the homogeneous structure just constructed;
- G is closed in the symmetric group $\mathrm{Sym}(\Omega)$ (in the topology of pointwise convergence).

Counting the orbits

Let G be an oligomorphic permutation group on Ω. I will consider three counting functions for orbits:

Counting the orbits

Let G be an oligomorphic permutation group on Ω. I will consider three counting functions for orbits:

- f_n is the number of G-orbits on n-element subsets;

Counting the orbits

Let G be an oligomorphic permutation group on Ω. I will consider three counting functions for orbits:

- f_n is the number of G-orbits on n-element subsets;
- F_n is the number of G-orbits on n-tuples of distinct elements;

Counting the orbits

Let G be an oligomorphic permutation group on Ω. I will consider three counting functions for orbits:

- f_n is the number of G-orbits on n-element subsets;
- F_n is the number of G-orbits on n-tuples of distinct elements;
- F_n^* is the number of G-orbits on all n-tuples.

Counting the orbits

Let G be an oligomorphic permutation group on Ω. I will consider three counting functions for orbits:

- f_n is the number of G-orbits on n-element subsets;
- F_n is the number of G-orbits on n-tuples of distinct elements;
- F_n^* is the number of G-orbits on all n-tuples.

We have $F_n^* = \sum_{k=1}^{n} S(n,k)F_k$, so (F_n) and (F_n^*) determine each other by Stirling inversion.

Counting the orbits

Let G be an oligomorphic permutation group on Ω. I will consider three counting functions for orbits:

- f_n is the number of G-orbits on n-element subsets;
- F_n is the number of G-orbits on n-tuples of distinct elements;
- F_n^* is the number of G-orbits on all n-tuples.

We have $F_n^* = \sum_{k=1}^{n} S(n,k)F_k$, so (F_n) and (F_n^*) determine each other by Stirling inversion.
Also $f_n \leq F_n \leq n! f_n$, so (at least for rapid growth) (f_n) and (F_n) are not too far apart.

Counting the orbits, 2

To a logician, we are counting n-types over an $\aleph_0$-categorial theory.

Counting the orbits, 2

To a logician, we are counting n-types over an $\aleph_0$-categorial theory.

To a combinatorial enumerator, we are counting labelled structures (for (F_n) or unlabelled structures (for (f_n))) in classes satisfying the hypotheses of Fraïïssé's theorem. There are many interesting such classes.

Counting the orbits, 2

To a logician, we are counting n-types over an $\aleph_0$-categorial theory.

To a combinatorial enumerator, we are counting labelled structures (for (F_n) or unlabelled structures (for (f_n)) in classes satisfying the hypotheses of Fraïssé's theorem. There are many interesting such classes.

Note that the orbit counts for G and its closure in the symmetric group are the same; so we can assume without loss that G is closed, that is, G is the full automorphism group of a first-order structure (or a homogeneous relational structure).

Counting the orbits, 2

To a logician, we are counting n-types over an $\aleph_0$-categorial theory.

To a combinatorial enumerator, we are counting labelled structures (for (F_n) or unlabelled structures (for (f_n))) in classes satisfying the hypotheses of Fraïïssé's theorem. There are many interesting such classes.

Note that the orbit counts for G and its closure in the symmetric group are the same; so we can assume without loss that G is closed, that is, G is the full automorphism group of a first-order structure (or a homogeneous relational structure).

I will speak mainly about the sequence (f_n).

Examples: constant

Theorem

Suppose that Ω *is countable and* G *is closed, and that* $f_n(G) = 1$ *for all* n*. Then one of the following holds:*

Examples: constant

Theorem

Suppose that Ω is countable and G is closed, and that $f_n(G) = 1$ for all n. Then one of the following holds:

- *Ω is bijective with $\mathbb{Q}$, and G is the group of order preserving, or order preserving/reversing, permutations;*

Examples: constant

Theorem

Suppose that Ω is countable and G is closed, and that $f_n(G) = 1$ for all n. Then one of the following holds:

- *Ω is bijective with $\mathbb{Q}$, and G is the group of order preserving, or order preserving/reversing, permutations;*
- *Ω is bijective with the set of complex roots of unity, and G is the group of circular order preserving, or circular order preserving/reversing, permutations;*

Examples: constant

Theorem

Suppose that Ω is countable and G is closed, and that $f_n(G) = 1$ for all n. Then one of the following holds:

- *Ω is bijective with $\mathbb{Q}$, and G is the group of order preserving, or order preserving/reversing, permutations;*
- *Ω is bijective with the set of complex roots of unity, and G is the group of circular order preserving, or circular order preserving/reversing, permutations;*
- $G = \mathrm{Sym}(\Omega)$.

Examples: constant

Theorem

Suppose that Ω is countable and G is closed, and that $f_n(G) = 1$ for all n. Then one of the following holds:

- *Ω is bijective with $\mathbb{Q}$, and G is the group of order preserving, or order preserving/reversing, permutations;*
- *Ω is bijective with the set of complex roots of unity, and G is the group of circular order preserving, or circular order preserving/reversing, permutations;*
- $G = \mathrm{Sym}(\Omega)$.

The first two types have $F_n = n!$ or $n!/2$ for $n \geq 2$; the third and fourth have $F_n = (n-1)!$ or $(n-1)!/2$, for $n \geq 3$. The last has $F_n = 1$ for all n.

Examples: constant

Theorem

Suppose that Ω is countable and G is closed, and that $f_n(G) = 1$ for all n. Then one of the following holds:

- *Ω is bijective with $\mathbb{Q}$, and G is the group of order preserving, or order preserving/reversing, permutations;*
- *Ω is bijective with the set of complex roots of unity, and G is the group of circular order preserving, or circular order preserving/reversing, permutations;*
- $G = \mathrm{Sym}(\Omega)$.

The first two types have $F_n = n!$ or $n!/2$ for $n \geq 2$; the third and fourth have $F_n = (n-1)!$ or $(n-1)!/2$, for $n \geq 3$. The last has $F_n = 1$ for all n.
Further examples with f_n ultimately constant can be obtained from these by adding a finite set fixed by G.

Examples: polynomial

For the remaining examples, I will be very selective. Let S be the symmetric group of countable degree, S_k the symmetric group of finite degree k.

Examples: polynomial

For the remaining examples, I will be very selective. Let S be the symmetric group of countable degree, S_k the symmetric group of finite degree k.

The group $G = S \times \cdots \times S$ (preserving all parts of a partition into k infinite parts) has $f_n = \binom{n+k-1}{k-1}$. If we allow the parts to be permuted, then $G = S \operatorname{Wr} S_k$ and f_n is the number of partitions of n into at most k parts. The same value is obtained for $G = S_k \operatorname{Wr} S$ (fixing a partition into infinitely many parts of size k).

Examples: polynomial

For the remaining examples, I will be very selective. Let S be the symmetric group of countable degree, S_k the symmetric group of finite degree k.

The group $G = S \times \cdots \times S$ (preserving all parts of a partition into k infinite parts) has $f_n = \binom{n+k-1}{k-1}$. If we allow the parts to be permuted, then $G = S \operatorname{Wr} S_k$ and f_n is the number of partitions of n into at most k parts. The same value is obtained for $G = S_k \operatorname{Wr} S$ (fixing a partition into infinitely many parts of size k).

In all these examples, (f_n) grows as a polynomial of degree $k - 1$ in n.

Examples: polynomial

For the remaining examples, I will be very selective. Let S be the symmetric group of countable degree, S_k the symmetric group of finite degree k.
The group $G = S \times \cdots \times S$ (preserving all parts of a partition into k infinite parts) has $f_n = \binom{n+k-1}{k-1}$. If we allow the parts to be permuted, then $G = S \operatorname{Wr} S_k$ and f_n is the number of partitions of n into at most k parts. The same value is obtained for $G = S_k \operatorname{Wr} S$ (fixing a partition into infinitely many parts of size k).
In all these examples, (f_n) grows as a polynomial of degree $k-1$ in n.
So all integral degrees of polynomial growth occur.

Examples: fractional exponential

For $G = S \operatorname{Wr} S$ (fixing a partition into infinitely many parts), f_n is the number of partitions of n. The asymptotics of this sequence are known very precisely; the growth is roughly $\exp(n^{1/2})$.

Examples: fractional exponential

For $G = S \operatorname{Wr} S$ (fixing a partition into infinitely many parts), f_n is the number of partitions of n. The asymptotics of this sequence are known very precisely; the growth is roughly $\exp(n^{1/2})$.
More generally, the wreath product of a group with polynomial growth of degree $k - 1$ with S has growth roughly $\exp(n^{k/(k+1)})$.

Examples: fractional exponential

For $G = S \operatorname{Wr} S$ (fixing a partition into infinitely many parts), f_n is the number of partitions of n. The asymptotics of this sequence are known very precisely; the growth is roughly $\exp(n^{1/2})$.

More generally, the wreath product of a group with polynomial growth of degree $k-1$ with S has growth roughly $\exp(n^{k/(k+1)})$.

It is not known whether other fractional exponential growth is possible. But we can have growth faster than any $\exp n^c$ for $c < 1$ but slower than exponential: $S \operatorname{Wr} S \operatorname{Wr} S$ is an example.

Primitive groups

Dugald's great theorem says:

Theorem

There is an absolute constant c such that, if G is primitive and oligomorphic, but $f_n(G) \neq 1$ for some n, then $f_n(G) \geq c^n/p(n)$ for some polynomial p.

Primitive groups

Dugald's great theorem says:

Theorem

There is an absolute constant c such that, if G is primitive and oligomorphic, but $f_n(G) \neq 1$ for some n, then $f_n(G) \geq c^n/p(n)$ for some polynomial p.

So, for primitive groups, there is a huge gap, between constant and exponential. Dugald gave $c = 2^{1/5}$; Francesca Merola improved this to $c = 1.324\ldots$. The best known examples have $c = 2$.

Primitive groups

Dugald's great theorem says:

Theorem

There is an absolute constant c such that, if G is primitive and oligomorphic, but $f_n(G) \neq 1$ for some n, then $f_n(G) \geq c^n / p(n)$ for some polynomial p.

So, for primitive groups, there is a huge gap, between constant and exponential. Dugald gave $c = 2^{1/5}$; Francesca Merola improved this to $c = 1.324\ldots$. The best known examples have $c = 2$.

Problem

Show that $c = 2$ is the correct value.

Exponential growth

All known examples of primitive groups with exponential growth are built from circles and trees. Some of these are associated with Jordan groups arising in the work of Adeleke, Macpherson and Neumann.

Exponential growth

All known examples of primitive groups with exponential growth are built from circles and trees. Some of these are associated with Jordan groups arising in the work of Adeleke, Macpherson and Neumann.
I do not know how to make this statement precise, and I certainly cannot prove that all examples have this form.

Exponential growth

All known examples of primitive groups with exponential growth are built from circles and trees. Some of these are associated with Jordan groups arising in the work of Adeleke, Macpherson and Neumann.
I do not know how to make this statement precise, and I certainly cannot prove that all examples have this form.

Problem

Make sense of the above; and find all the possible exponential growth constants $\lim_{n\to\infty} (f_n)^{1/n}$ *for primitive groups.*

Exponential growth

All known examples of primitive groups with exponential growth are built from circles and trees. Some of these are associated with Jordan groups arising in the work of Adeleke, Macpherson and Neumann.

I do not know how to make this statement precise, and I certainly cannot prove that all examples have this form.

Problem

Make sense of the above; and find all the possible exponential growth constants $\lim_{n\to\infty} (f_n)^{1/n}$ *for primitive groups.*

See Pierre Simon's talk on Thursday for more about this.

Examples: faster growth

For k “random” linear orders on Ω (the Fraïssé limit of the class of finite sets carrying k linear orders), we have $f_n = (n!)^{k-1}$.

Examples: faster growth

For k "random" linear orders on Ω (the Fraïssé limit of the class of finite sets carrying k linear orders), we have $f_n = (n!)^{k-1}$.

The Fraïssé limit of the class of finite graphs is the Erdős–Rényi random graph, also known as the Rado graph. Here f_n is the number of n-vertex graphs up to isomorphism, which is about $2^{n(n-1)/2}/n!$.

Examples: faster growth

For k "random" linear orders on Ω (the Fraïssé limit of the class of finite sets carrying k linear orders), we have $f_n = (n!)^{k-1}$.

The Fraïssé limit of the class of finite graphs is the Erdős–Rényi random graph, also known as the Rado graph. Here f_n is the number of n-vertex graphs up to isomorphism, which is about $2^{n(n-1)/2}/n!$.

There is no upper bound to the growth: just take the Fraïssé limit of the class of structures containing a_n n-ary relations which hold only if all arguments are distinct, for all n, to get a sequence growing faster than (a_n). (However, for homogeneous structures over finite relational languages, f_n is bounded by the exponential of a polynomial in n.)

So what should be true?

The upshot of all this is that, at least for primitive groups, the sequence (f_n) should grow rapidly and smoothly.

So what should be true?

The upshot of all this is that, at least for primitive groups, the sequence (f_n) should grow rapidly and smoothly.
Dugald's theorem shows that the first is true, but questions remain, such as the possible exponential constants, and the existence of gaps above exponential growth. (We have seen factorial growth; but S acting on the set of 2-subsets of its domain grows a little slower than factorial.)

So what should be true?

The upshot of all this is that, at least for primitive groups, the sequence (f_n) should grow rapidly and smoothly.
Dugald's theorem shows that the first is true, but questions remain, such as the possible exponential constants, and the existence of gaps above exponential growth. (We have seen factorial growth; but S acting on the set of 2-subsets of its domain grows a little slower than factorial.)
For smoothness, we have

Theorem

The sequence (f_n) is non-decreasing.

So what should be true?

The upshot of all this is that, at least for primitive groups, the sequence (f_n) should grow rapidly and smoothly.

Dugald's theorem shows that the first is true, but questions remain, such as the possible exponential constants, and the existence of gaps above exponential growth. (We have seen factorial growth; but S acting on the set of 2-subsets of its domain grows a little slower than factorial.)

For smoothness, we have

Theorem

The sequence (f_n) is non-decreasing.

The Fraïssé trick shows that the sequence can suddenly "jump up". But it seems that the growth cannot then slow right down. There should be a lower bound for f_{n+2} in terms of f_n and f_{n+1}.

So what should be true?

The upshot of all this is that, at least for primitive groups, the sequence (f_n) should grow rapidly and smoothly.
Dugald's theorem shows that the first is true, but questions remain, such as the possible exponential constants, and the existence of gaps above exponential growth. (We have seen factorial growth; but S acting on the set of 2-subsets of its domain grows a little slower than factorial.)
For smoothness, we have

Theorem

The sequence (f_n) is non-decreasing.

The Fraïssé trick shows that the sequence can suddenly "jump up". But it seems that the growth cannot then slow right down. There should be a lower bound for f_{n+2} in terms of f_n and f_{n+1}.
I now turn to some more algebraic tools which allow us to prove some results of this form. But the final story is not yet told ...

Generating functions

We can express the counting sequences as formal power series,

$$f(x) = \sum f_n x^n, \quad F(x) = \sum F_n x^n / n!, F^*(x) = \sum F_n^* x^n / n!.$$

(The exponential generating functions for the second and third are related to the fact that they count labelled structures in the age.)

Generating functions

We can express the counting sequences as formal power series,

$$f(x) = \sum f_n x^n, \quad F(x) = \sum F_n x^n / n!, F^*(x) = \sum F_n^* x^n / n!.$$

(The exponential generating functions for the second and third are related to the fact that they count labelled structures in the age.)
The Stirling relationship gives us $F^*(x) = F(\exp(x) - 1)$.

Generating functions

We can express the counting sequences as formal power series,

$$f(x) = \sum f_n x^n, \quad F(x) = \sum F_n x^n/n!, F^*(x) = \sum F_n^* x^n/n!.$$

(The exponential generating functions for the second and third are related to the fact that they count labelled structures in the age.)

The Stirling relationship gives us $F^*(x) = F(\exp(x) - 1)$.

The series have non-zero radius of convergence only in the slow growth cases. The most interesting is the case where (f_n) grows polynomially.

Generating functions

We can express the counting sequences as formal power series,

$$f(x) = \sum f_n x^n, \quad F(x) = \sum F_n x^n / n!, F^*(x) = \sum F_n^* x^n / n!.$$

(The exponential generating functions for the second and third are related to the fact that they count labelled structures in the age.)

The Stirling relationship gives us $F^*(x) = F(\exp(x) - 1)$.

The series have non-zero radius of convergence only in the slow growth cases. The most interesting is the case where (f_n) grows polynomially.

There are formulae for direct products. Suppose that $G = H \times K$, where H and K act on Γ and Δ.

Generating functions

We can express the counting sequences as formal power series,

$$f(x) = \sum f_n x^n, \quad F(x) = \sum F_n x^n/n!, F^*(x) = \sum F_n^* x^n/n!.$$

(The exponential generating functions for the second and third are related to the fact that they count labelled structures in the age.)
The Stirling relationship gives us $F^*(x) = F(\exp(x) - 1)$.
The series have non-zero radius of convergence only in the slow growth cases. The most interesting is the case where (f_n) grows polynomially.
There are formulae for direct products. Suppose that $G = H \times K$, where H and K act on Γ and Δ.

- If G has its intransitive action on $\Gamma \cup \Delta$, then $F_G(x) = F_H(x) F_K(x)$ and $f_G(x) = f_H(x) f_K(x)$.

Generating functions

We can express the counting sequences as formal power series,

$$f(x) = \sum f_n x^n, \quad F(x) = \sum F_n x^n/n!, F^*(x) = \sum F_n^* x^n/n!.$$

(The exponential generating functions for the second and third are related to the fact that they count labelled structures in the age.)

The Stirling relationship gives us $F^*(x) = F(\exp(x) - 1)$.

The series have non-zero radius of convergence only in the slow growth cases. The most interesting is the case where (f_n) grows polynomially.

There are formulae for direct products. Suppose that $G = H \times K$, where H and K act on Γ and Δ.

- If G has its intransitive action on $\Gamma \cup \Delta$, then $F_G(x) = F_H(x)F_K(x)$ and $f_G(x) = f_H(x)f_K(x)$.
- If G has its product action on $\Gamma \times \Delta$, then $F_G^*(x)$ is the Hadamard product of $F_H^*(x)$ and $F_K^*(x)$.

The orbit algebra

We can bring in more structure. First we define the "reduced incidence algebra" of finite subsets of Ω. Let $\mathbb{F}$ be a field of characteristic zero. Let V_n denote the vector space of functions from the set of n-element subsets of Ω to $\mathbb{F}$, with pointwise operations. We take A to be the direct sum of these spaces for all $n \geq 0$, with multiplication defined as follows: for $f \in V_n$, $g \in V_m$, let fg be the function in V_{n+m} defined by

$$(fg)(K) = \sum_{L \subseteq K, |L|=n} f(L)g(K \setminus L).$$

Then A is a commutative and associative graded algebra.

The orbit algebra

We can bring in more structure. First we define the "reduced incidence algebra" of finite subsets of Ω. Let $\mathbb{F}$ be a field of characteristic zero. Let V_n denote the vector space of functions from the set of n-element subsets of Ω to $\mathbb{F}$, with pointwise operations. We take A to be the direct sum of these spaces for all $n \geq 0$, with multiplication defined as follows: for $f \in V_n$, $g \in V_m$, let fg be the function in V_{n+m} defined by

$$(fg)(K) = \sum_{L \subseteq K, |L|=n} f(L)g(K \setminus L).$$

Then A is a commutative and associative graded algebra.

If G is a permutation group on Ω, we let $A(G)$ be the subalgebra of A consisting of elements whose homogeneous components are fixed by G (that is, functions constant on the G-orbits). Then $A(G)$ is also a graded algebra. If G is oligomorphic, then the dimension of the nth homogeneous component $V_n(G)$ is $f_n(G)$.

The orbit algebra

We can bring in more structure. First we define the "reduced incidence algebra" of finite subsets of Ω. Let $\mathbb{F}$ be a field of characteristic zero. Let V_n denote the vector space of functions from the set of n-element subsets of Ω to $\mathbb{F}$, with pointwise operations. We take A to be the direct sum of these spaces for all $n \geq 0$, with multiplication defined as follows: for $f \in V_n$, $g \in V_m$, let fg be the function in V_{n+m} defined by

$$(fg)(K) = \sum_{L \subseteq K, |L|=n} f(L)g(K \setminus L).$$

Then A is a commutative and associative graded algebra.

If G is a permutation group on Ω, we let $A(G)$ be the subalgebra of A consisting of elements whose homogeneous components are fixed by G (that is, functions constant on the G-orbits). Then $A(G)$ is also a graded algebra. If G is oligomorphic, then the dimension of the nth homogeneous component $V_n(G)$ is $f_n(G)$. Thus, the Hilbert series of $A(G)$ is the generating function $f(x)$ of the sequence $(f_n(G))$.

The element e

Since there is only one empty set, $V_0(G)$ is 1-dimensional, and is a copy of $\mathbb{F}$; the element corresponding to 1 is the identity of $A(G)$.

The element e

Since there is only one empty set, $V_0(G)$ is 1-dimensional, and is a copy of $\mathbb{F}$; the element corresponding to 1 is the identity of $A(G)$.

An interesting element is $e \in V_1(G)$, the function on Ω with constant value 1.

The element e

Since there is only one empty set, $V_0(G)$ is 1-dimensional, and is a copy of $\mathbb{F}$; the element corresponding to 1 is the identity of $A(G)$.
An interesting element is $e \in V_1(G)$, the function on Ω with constant value 1.

Theorem
e is a non-zero divisor; that is, $ef = 0$ implies $f = 0$.

The element e

Since there is only one empty set, $V_0(G)$ is 1-dimensional, and is a copy of $\mathbb{F}$; the element corresponding to 1 is the identity of $A(G)$.
An interesting element is $e \in V_1(G)$, the function on Ω with constant value 1.

Theorem

e is a non-zero divisor; that is, $ef = 0$ implies $f = 0$.

Thus, multiplication by e is a monomorphism from V_n to V_{n+1}; this shows that $f_{n+1} \geq f_n$.

The element e

Since there is only one empty set, $V_0(G)$ is 1-dimensional, and is a copy of $\mathbb{F}$; the element corresponding to 1 is the identity of $A(G)$.

An interesting element is $e \in V_1(G)$, the function on Ω with constant value 1.

Theorem

e is a non-zero divisor; that is, $ef = 0$ implies $f = 0$.

Thus, multiplication by e is a monomorphism from V_n to V_{n+1}; this shows that $f_{n+1} \geq f_n$.

We also see that, if $G = S$, then $A(G)$ is the polynomial algebra in one variable generated by e.

Examples

More generally, if G is the direct product of r copies of S, acting on disjoint sets, then $A(G)$ is a polynomial algebra in r variables.

Examples

More generally, if G is the direct product of r copies of S, acting on disjoint sets, then $A(G)$ is a polynomial algebra in r variables.

Now let H be a finite permutation group of degree r. The extension of S^r by H (the wreath product $S \operatorname{Wr} H$), then $A(G)$ is the ring of invariants of H (regarded as a linear group acting by permutation matrices). In particular, if $H = S_r$, then $A(S \operatorname{Wr} H)$ is the ring of symmetric polynomials in r variables, which is a polynomial algebra in the elementary symmetric polynomials.

Examples

More generally, if G is the direct product of r copies of S, acting on disjoint sets, then $A(G)$ is a polynomial algebra in r variables.

Now let H be a finite permutation group of degree r. The extension of S^r by H (the wreath product $S \operatorname{Wr} H$), then $A(G)$ is the ring of invariants of H (regarded as a linear group acting by permutation matrices). In particular, if $H = S_r$, then $A(S \operatorname{Wr} H)$ is the ring of symmetric polynomials in r variables, which is a polynomial algebra in the elementary symmetric polynomials.

More generally still, if the age of a homogeneous structure contains a subclass of "connected" structures satisfying some simple axioms, and G is the automorphism group of the Fraïssé limit, then $A(G)$ is a polynomial algebra generated by the characteristic functions of the connected structures.

Examples

More generally, if G is the direct product of r copies of S, acting on disjoint sets, then $A(G)$ is a polynomial algebra in r variables.

Now let H be a finite permutation group of degree r. The extension of S^r by H (the wreath product $S \operatorname{Wr} H$), then $A(G)$ is the ring of invariants of H (regarded as a linear group acting by permutation matrices). In particular, if $H = S_r$, then $A(S \operatorname{Wr} H)$ is the ring of symmetric polynomials in r variables, which is a polynomial algebra in the elementary symmetric polynomials.

More generally still, if the age of a homogeneous structure contains a subclass of "connected" structures satisfying some simple axioms, and G is the automorphism group of the Fraïssé limit, then $A(G)$ is a polynomial algebra generated by the characteristic functions of the connected structures.

In particular this holds for the automorphism group of the random graph, where the generators correspond to the finite connected graphs.

Integral domain?

If G has a finite orbit, then $A(G)$ has nilpotent elements (the characteristic function of the orbit squares to zero).

Integral domain?

If G has a finite orbit, then $A(G)$ has nilpotent elements (the characteristic function of the orbit squares to zero).
On the other hand, I conjectured:

Integral domain?

If G has a finite orbit, then $A(G)$ has nilpotent elements (the characteristic function of the orbit squares to zero).
On the other hand, I conjectured:

Conjecture

Suppose that G has no finite orbits. Then

- *$A(G)$ is an integral domain;*

Integral domain?

If G has a finite orbit, then $A(G)$ has nilpotent elements (the characteristic function of the orbit squares to zero).
On the other hand, I conjectured:

Conjecture

Suppose that G has no finite orbits. Then

- *$A(G)$ is an integral domain;*
- *e is prime in $A(G)$, that is, $e \mid fg$ implies $e \mid f$ or $e \mid g$.*

Integral domain?

If G has a finite orbit, then $A(G)$ has nilpotent elements (the characteristic function of the orbit squares to zero).
On the other hand, I conjectured:

Conjecture

Suppose that G has no finite orbits. Then

- *$A(G)$ is an integral domain;*
- *e is prime in $A(G)$, that is, $e \mid fg$ implies $e \mid f$ or $e \mid g$.*

These conjectures have implications for smoothness of growth.
The first, for example, implies

$$f_{m+n}(G) \geq f_m(G) + f_n(G) - 1.$$

A proof

The first conjecture, that $A(G)$ is an integral domain, has been proved by Maurice Pouzet.

A proof

The first conjecture, that $A(G)$ is an integral domain, has been proved by Maurice Pouzet.

Pouzet's ingenious proof (which I cannot give here) works over the complex numbers, encoding orbits by sequences and using ideas from language theory. The crucial result (which works in the algebra A without any group) asserts that, if $f \in V_m$, $g \in V_n$, and $fg = 0$, then the union of the supports of f and g is bounded by a function of m and n.

A proof

The first conjecture, that $A(G)$ is an integral domain, has been proved by Maurice Pouzet.

Pouzet's ingenious proof (which I cannot give here) works over the complex numbers, encoding orbits by sequences and using ideas from language theory. The crucial result (which works in the algebra A without any group) asserts that, if $f \in V_m$, $g \in V_n$, and $fg = 0$, then the union of the supports of f and g is bounded by a function of m and n.

The second conjecture remains open.

Polynomial growth

The most important recent development is a result of Justine Falque and Nicolas Thiéry.

Theorem

Suppose that (f_n) grows no faster than polynomial. Then

Polynomial growth

The most important recent development is a result of Justine Falque and Nicolas Thiéry.

Theorem

Suppose that (f_n) grows no faster than polynomial. Then

- *$A(G)$ is a Cohen–Macauley algebra;*

Polynomial growth

The most important recent development is a result of Justine Falque and Nicolas Thiéry.

Theorem

Suppose that (f_n) grows no faster than polynomial. Then

- *$A(G)$ is a Cohen–Macauley algebra;*
- *the generating function $f(x)$ of $(f_n(G))$ is a rational function of the form*

$$f(x) = \frac{P(x)}{\prod_{i \in I}(1 - x^i)},$$

where the multiset I is determined by the blocks of imprimitivity of G.

Polynomial growth

The most important recent development is a result of Justine Falque and Nicolas Thiéry.

Theorem

Suppose that (f_n) grows no faster than polynomial. Then

- *$A(G)$ is a Cohen–Macauley algebra;*
- *the generating function $f(x)$ of $(f_n(G))$ is a rational function of the form*
$$f(x) = \frac{P(x)}{\prod_{i \in I}(1 - x^i)},$$
where the multiset I is determined by the blocks of imprimitivity of G.

This implies that $f_n(G) \sim an^k$ for some $a > 0$ and $k \in \mathbb{N}$: indeed, $f_n(G)$ is quasi-polynomial in n.

A special case

Note that the algebra of invariants of a finite permutation group is of this form; the result on $f(x)$ in that case follows from Molien's Theorem, of which the Falque–Thiéry result is a wide generalisation.