On an algebra related to orbit-counting

Peter J. Cameron

School of Mathematical Sciences
Queen Mary and Westfield College
London E1 4NS
U.K.

Abstract

With any permutation group G on an infinite set Ω is associated a graded algebra $\mathcal{A}^G$ (the algebra of G-invariants in the reduced incidence algebra of finite subsets of Ω). The dimension of the nth homogeneous component of $\mathcal{A}^G$ is equal to the number of orbits of G on n-subsets of Ω. If it happens that G is the automorphism group of a homogeneous structure M, then this is the number of unlabelled n-element substructures of M. Many combinatorial enumeration problems fit into this framework.

I conjectured 20 years ago that, if G has no finite orbits on Ω, then $\mathcal{A}^G$ is an integral domain (and even has the stronger property that a specific quotient is an integral domain). I shall say that G is *entire* if $\mathcal{A}^G$ is an integral domain, and *strongly entire* if the stronger property holds. These properties have (rather subtle) consequences for the enumeration problems. The conjecture is still open; but in this paper I prove that, if G is transitive on Ω and the point stabiliser H is (strongly) entire, then G is (strongly) entire.

1 Introduction

A relational structure M such as a graph, digraph or poset is said to be *homogeneous* if any isomorphism between finite substructures of M can be extended to an automorphism of M.

Let M be homogeneous, G the automorphism group of M, and $\mathcal{C}$ the *age* of M, the class of finite structures embeddable in M. Then the number of orbits of G on n-element subsets of M is equal to the number of unlabelled n-element structures in $\mathcal{C}$, and the number of orbits on n-tuples of distinct elements is equal to the number of labelled n-element structures in M. Moreover, a theorem of Fraïssé [4] characterises the ages of (countable) homogeneous structures. So orbit-counting problems for groups are equivalent to combinatorial enumeration problems in *Fraïssé classes*. (See [2] for discussion.)

As a tool for such enumeration problems, I introduced in [1] a commutative, associative graded algebra $\mathcal{A}^G$ associated with a permutation group G, with the property that the dimension of the nth homogeneous component of $\mathcal{A}^G$ is equal to the number of orbits of G on n-sets (if this number is finite — otherwise both quantities are infinite). I conjectured that, if G has no finite orbits, then $\mathcal{A}^G$ is an integral domain. (In fact, a stronger conjecture was given, as will be explained in the next section.) This conjecture would have implications for the rate of growth of the numbers of n-element unlabelled structures in Fraïssé classes under very mild assumptions.

Almost no progress has been made on this conjecture. The purpose of this paper is to prove a theorem which, while not getting any closer to proving it, introduces some techniques which may be useful. The theorem asserts that, if G is a transitive extension of H, and $\mathcal{A}^H$ is an integral domain, then so is $\mathcal{A}^G$ (and the same holds for the stronger condition of the conjecture).

2 The theorem

Let Ω be a set, usually assumed to be countably infinite. The *reduced incidence algebra* (Rota [8]) $\mathcal{A}$ of the poset of finite subsets of Ω is defined as follows. For $n \geq 0$, let V_n be the vector space (over $\mathbb{C}$) of functions from the set $\binom{\Omega}{n}$ of n-element subsets of Ω to $\mathbb{C}$. (Addition and scalar multiplication of functions is defined pointwise.) We define a multiplication from $V_k \times V_l$ to V_{k+l} as follows: for $f \in V_k$, $g \in V_l$, the function $fg \in V_{k+l}$ is given by

$$fg(M) = \sum_{K \in \binom{M}{k}} f(K)g(M \setminus K),$$

for any $M \in \binom{\Omega}{k+l}$.

Let

$$\mathcal{A} = \bigoplus_{n \geq 0} V_n,$$

and extend the multiplication linearly to $\mathcal{A}$. It is easily verified that the multiplication is commutative and associative.

Now suppose that the group G acts on Ω. Let V_n^G be the space of functions in V_n fixed by G, and

$$\mathcal{A}^G = \bigoplus_{n \geq 0} V_n^G,$$

a subalgebra of $\mathcal{A}$, and hence a commutative and associative graded algebra. A function in V_n is fixed by G if and only if it is constant on the orbits of G; so $\dim(V_n^G)$ is equal to the number of orbits on n-sets, if this is finite.

The identity element of $\mathcal{A}$ is the function in V_0 whose value (on the empty set) is 1. We will always use the symbol e for the constant function in V_1 with value 1. It is known that e is not a zero-divisor. (In fact, multiplication of elements of V_n by e is one-to-one as long as $|\Omega| \geq 2n+1$: see [2].)

We say that G is *entire* if $\mathcal{A}^G$ is an integral domain, and that G is *strongly entire* if e is prime (in the sense that, if e divides a product, then it divides one of the factors); equivalently, if $\mathcal{A}^G/e\mathcal{A}^G$ is an integral domain.

Lemma 1 *If G is strongly entire, then it is entire.*

Proof. Suppose that e is prime in $\mathcal{A}^G$, and that $fg = 0$, with $f, g \neq 0$. By considering the homogeneous components of f and g of least degree, we can assume that f and g are homogeneous; we further assume that the sum of their degrees is minimal. Then $e|fg$, so $e|f$ or $e|g$, say $f = eh$. Now $ehg = 0$, so $hg = 0$ (since e is not a zero-divisor), contradicting the minimality of $\deg(f) + \deg(g)$.

Now the conjecture made in [1] asserts that, if G has no finite orbits on Ω, then G is strongly entire. According to Lemma 1, this would imply that it is entire under the same hypotheses.

The converse of the conjecture is true: for, if G has an orbit Δ with $|\Delta| = n$, and $f \in V_n^G$ takes the value 1 at Δ and 0 elsewhere, then $f^2 = 0$. The conjecture seems to be related to the fact that, if G has no finite orbits, then any two finite sets have disjoint G-images (Lemma 2.3 of Neumann [7]).

These conditions were introduced in order to study the rate of growth of the number $f_n(G)$ of orbits on n-sets of the permutation group G. Subsequently, global results on growth rate were proved, notably by Macpherson [5], using completely different techniques. However, the algebraic method offers the possibility of proving local results. Here is an example.

Proposition 1 *Let G be a permutation group on Ω, and f_n the number of orbits of G on the set of n-subsets of Ω.*

(a) If G is entire, then

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

(b) If G is strongly entire, then

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

PROOF. The dimension of the nth homogeneous component of $\mathcal{A}^G$ is f_n, while the dimension of the nth homogeneous component of $\mathcal{A}^G/e\mathcal{A}^G$ is $f_n - f_{n-1}$ (since e is not a zero-divisor). So the Proposition follows immediately from the following result:

Lemma 2 *Let $\mathcal{A} = \bigoplus V_n$ be a graded algebra over $\mathbb{C}$, with $\dim(V_n) = r_n$. If $\mathcal{A}$ is an integral domain, then*

$$r_{m+n} \geq r_m + r_n - 1.$$

PROOF. Multiplication is a bilinear map from $V_m \times V_n$ to V_{m+n}, and so induces a linear map μ from $V_m \otimes V_n$ to V_{m+n}. Let $U = \ker(\mu)$. Now U contains no rank 1 tensor $v \otimes w$, with $v, w \neq 0$; for $(v \otimes w)\mu = vw \neq 0$, since $\mathcal{A}$ is an integral domain.

Now a subspace of $V_m \otimes V_n$ containing no rank 1 tensor has dimension at most $(r_m - 1)(r_n - 1)$. (For the rank 1 tensors, modulo scalars, form the projective *Segre variety*, with dimension $r_m + r_n - 1$, and this variety intersects any linear subspace whose codimension is smaller than this number: see Shafarevich [9], pp. 56, 71.) So we have

$$\dim(V_{m+n}) \geq r_m r_n - (r_m - 1)(r_n - 1) = r_m + r_n - 1,$$

as claimed.

The permutation group G on Ω is a *transitive extension* of the permutation group H on Δ if

- G is transitive on Ω;
- for $\alpha \in \Omega$, the permutation groups G_α on $\Omega \setminus \{\alpha\}$ and H on Δ are isomorphic, where G_α is the stabiliser of α.

Now we can state the main theorem of the paper.

Theorem 1 *Let G be a transitive extension of H. Then*

(a) if H is entire, then so is G;

(b) if H is strongly entire, then so is G.

3 An easier result

We begin with a simpler result along the same lines, as an introduction to these ideas.

Theorem 2 *Let Ω be an infinite set, and G_1 and G_2 be permutation groups on Ω with $G_1 \leq G_2$.*

(a) If G_1 is entire, then so is G_2.

(b) If G_1 is strongly entire, then so is G_2.

PROOF. (a) This is clear since $\mathcal{A}^{G_2}$ is a subalgebra of $\mathcal{A}^{G_1}$.

(b) Assume that G_1 is strongly entire and let $a, b \in \mathcal{A}^{G_2}$ with $e|ab$. Then e divides either a or b in $\mathcal{A}^{G_1}$; say $a = ec$ with $c \in \mathcal{A}^{G_1}$. For any $g \in G_2$, we have $a^g = e^g c^g$, whence $a = ec^g$, since $a, e \in \mathcal{A}^{G_2}$. So we have

$$e(c - c^g) = 0,$$

whence $c = c^g$, since e is not a zero-divisor. As this holds for all $g \in G_2$, we have $c \in \mathcal{A}^{G_2}$, as required.

4 Proof of the Main Theorem

We assume the hypotheses of the Theorem: G is a transitive extension of H, where G acts on Ω and H on Δ.

We begin with the observation that, if K is a finite set containing α, then there exists $g \in G$ such that Kg does not contain α. (Simply choose g so that αg^{-1} is not in K.) It follows that there is no non-zero homogeneous element in $\mathcal{A}^G$, all of the sets in whose support contain α.

Now $G_\alpha \cong H \times U$ (with the intransitive action of the product), where U is the trivial group on $\{\alpha\}$. Then $\mathcal{A}^U$ is 2-dimensional, generated by an element u of degree 1 satisfying $u^2 = 0$. Hence $\mathcal{A}^{G_\alpha} \cong \mathcal{A}^H \otimes \mathcal{A}^U$, so $\mathcal{A}^{G_\alpha} = \{a + bu : a, b \in \mathcal{A}^H\}$.

Furthermore, $\mathcal{A}^G$ is a subalgebra of $\mathcal{A}^{G_\alpha}$, since G_α is a subgroup of G. Hence we can define a map $\theta : \mathcal{A}^G \to \mathcal{A}^H$ by $(a + bu)\theta = a$.

Lemma 3 *θ is a monomorphism.*

Proof. That θ is a homomorphism follows from the equations

$$\begin{aligned}(a_1 + b_1 u) + (a_2 + b_2 u) &= (a_1 + a_2) + (b_1 + b_2)u,\\ (a_1 + b_1 u) \cdot (a_2 + b_2 u) &= (a_1 a_2) + (a_1 b_2 + a_2 b_1)u.\end{aligned}$$

That it is injective follows from the remark with which we began the proof: for the homogeneous components of an element bu of the kernel would be G-invariant functions, every set in whose support contains α.

Hence $\mathcal{A}^G$ is a subalgebra of $\mathcal{A}^H$, and part (a) of the Theorem follows.

Remark. We have $\mathcal{A}^G = \{a + d(a)u : a \in \mathrm{Im}(\theta)\}$, where d is a *derivation* on $\mathrm{Im}(\theta)$: this is a function satisfying

$$\begin{aligned}d(a + b) &= d(a) + d(b),\\ d(ab) &= ad(b) + d(a)b.\end{aligned}$$

For the proof of part (b), we need the following result.

Lemma 4 *Let f be a function on the n-subsets of $\Omega \setminus \{\alpha\}$, where Ω is infinite. Let G be a transitive permutation group on Ω. Suppose that f takes the same value on n-sets which lie in the same orbit of G. Then f has a unique extension to a G-invariant function on the n-subsets of Ω.*

PROOF. We must define f on n-subsets containing α. If K is such a set, there exists $g \in G$ with $\alpha \notin Kg$, and we must set $f(K) = f(Kg)$. We have to show that this is well-defined and G-invariant.

Suppose that $g_1, g_2 \in G$ with $\alpha \notin Kg_1$ and $\alpha \notin Kg_2$. Then $(Kg_1)(g_1^{-1}g_2) = Kg_2$. By hypothesis, $f(Kg_1) = f(Kg_2)$. So the extension of f is well-defined.

Let K_1 and K_2 be n-sets containing α, and suppose that $K_1h = K_2$ for some $h \in G$. Choose $g \in G$ such that $\alpha \notin (K_1 \cup K_2)g$. Then

$$(K_1g)(g^{-1}hg) = K_1hg = K_2g,$$

and so $f(K_1g) = f(K_2g)$. Thus the extension of f is G-invariant.

Now we return to the proof of (b). Let e denote the element of $\mathcal{A}^H$ of this name. The corresponding element of $\mathcal{A}^G$ is $e+u$. (In the notation of the earlier Remark, $d(e) = 1$.) So we are concerned with divisibility by $e+u$.

We *claim* that

$$e + u \text{ divides } a + d(a)u \text{ in } \mathcal{A}^G \text{ if and only if } e \text{ divides } a \text{ in } \mathcal{A}^H.$$

PROOF. First observe that it suffices to prove the result for homogeneous elements.

Suppose that a has degree n, and that e divides a, say $a = eb$. Then b is a function on $(n-1)$-subsets of $\Omega \setminus \{\alpha\}$. Also b takes the same value on sets in the same orbit of G. (For suppose that K_1 and K_2 are $(n-1)$-sets in the same orbit of G. Choose $(2n-1)$-sets L_1 and L_2, in the same G-orbit, containing K_1 and K_2 respectively, but not containing α. Then the values of a on corresponding n-subsets of L_1 and L_2 are equal. Since multiplication by e is invertible on functions on the $(n-1)$-subsets of a $(2n-1)$-set, the values of b on corresponding subsets are also equal; that is, $b(K_1) = b(K_2)$.)

By the Lemma, b extends to an element $b + d(b)u$ of $\mathcal{A}^G$. Then

$$(e+u)(b+d(b)u) = eb + (b + ed(b))u = a + d(a)u;$$

so $a + d(a)u$ is divisible by $e+u$, as required. The converse is trivial: if $a + d(a)u = (e+u)(b+d(b)u)$, then $a = eb$.

Now suppose that e is prime in $\mathcal{A}^H$, and that $e+u$ divides $(a+d(a)u)(b+d(b)u)$. Then e divides ab, so e divides a or e divides b, so $e+u$ divides $a+d(a)u$ or $e+u$ divides $b+d(b)u$, as required.

5 Remarks

Previously, the only technique available for showing that G is (strongly) entire involved showing something much stronger, namely, that $\mathcal{A}^G$ is a polynomial algebra. See [3], where sufficient conditions (involving a notion of "connected structure") on a Fraïssé class are given to ensure that, if G is the automorphism group of the corresponding homogeneous structure M, then $\mathcal{A}^G$ is a polynomial ring. Now a polynomial ring is certainly an integral domain; in fact, e is prime, since there is a set of polynomial generators including the element e. So, for example, in each of the following cases (discussed in [3]), $\mathcal{A}^H$ is a polynomial algebra, H is strongly entire:

(a) H is the automorphism group of the random graph;

(b) H is the group of order-preserving permutations of $\mathbb{Q}$ fixing q pairwise disjoint dense subsets whose union is $\mathbb{Q}$.

In each of the cases (a) and (b), H has a transitive extension G. In (a), this is the automorphism group of the countable universal two-graph; in (b), the automorphism group of an appropriate "circular structure". According to the Theorem, in each case G is strongly entire. (This resolves a question posed in [3].) It is unknown whether $\mathcal{A}^G$ is a polynomial algebra.

In this connection, case (a) is interesting. Since the numbers of two-graphs and even graphs on n vertices are equal [6], we see that, if $\mathcal{A}^G$ is a polynomial algebra, then the number of polynomial generators of degree n is equal to the number of connected even (that is, Eulerian) graphs on n vertices. However, I do not know how to choose the correct number of elements to be the polynomial generators.

References

[1] P. J. Cameron, Orbits of permutation groups on unordered sets, II, *J. London Math. Soc.* (2) **23** (1981), 249–265.

[2] P. J. Cameron, *Oligomorphic Permutation Groups*, *London Math. Soc. Lecture Notes* **152**, Cambridge University Press, Cambridge, 1990.

[3] P. J. Cameron, The algebra of an age, pp. 126–133 in *Model Theory of Groups and Automorphism Groups* (ed. David M. Evans), London Mathematical Society Lecture Notes **244**, Cambridge University Press, Cambridge, 1997.

[4] R. Fraïssé, Sur certains relations qui généralisent l'ordre des nombres rationnels, *C. R. Acad. Sci. Paris* **237** (1953), 540–542.

[5] H. D. Macpherson, The action of an infinite permutation group on the unordered subsets of a set, *Proc. London Math. Soc.* (3) **46** (1983), 471–486.

[6] C. L. Mallows and N. J. A. Sloane, Two-graphs, switching classes, and Euler graphs are equal in number, *SIAM J. Appl. Math.* **28** (1975), 876–880.

[7] P. M. Neumann, The lawlessness of finitary permutation groups, *Arch. Math.* **26** (1975), 561–566.

[8] G.-C. Rota, On the foundations of combinatorial theory, I: Theory of Möbius functions, *Z. Wahrscheinlichkeitstheorie* **2** (1964), 340–368.

[9] I. R. Shafarevich, *Basic Algebraic Geometry I: Varieties in Projective Space* (2nd edition), Springer-Verlag, Berlin, 1994.