The algebra of an age

Peter J. Cameron

Abstract

Associated with any oligomorphic permutation group G, there is a graded algebra $\mathcal{A}^G$ such that the dimension of its nth homogeneous component is equal to the number of G-orbits on n-sets. I show that the algebra is a polynomial algebra (free commutative associative algebra) in some cases, and pose some questions about transitive extensions.

1 The algebra

Let Ω be an infinite set. Let $\binom{\Omega}{n}$ denote the set of n-element subsets of Ω, V_n the vector space of functions from $\binom{\Omega}{n}$ to $\mathbb{Q}$. Set $\mathcal{A} = \bigoplus_{n\geq 0} V_n$, with multiplication defined as follows: for $f \in V_n$, $g \in V_m$, and $X \in \binom{\Omega}{n+m}$,

$$(fg)(X) = \sum_{Y\in\binom{X}{n}} f(Y)g(X \setminus Y).$$

This is the *reduced incidence algebra* of the poset of finite subsets of Ω (Rota [13]). It is a commutative and associative algebra with identity, but is far from an integral domain: any function with finite support is nilpotent.

Now, if G is any permutation group on Ω, let $\mathcal{A}^G = \bigoplus_{n\geq 0} V_n^G$, where V_n^G consists of the functions in V_n which are G-invariant (where G acts on V_n in the natural way: $f^g(X) = f(Xg^{-1})$). Now a function in V_n is fixed by G if and only if it is constant on the G-orbits. So, if G is *oligomorphic* (that is, G has only finitely many orbits on n-sets for all n), then $\dim(V_n^G) = f_n(G)$ is the number of orbits of G on $\binom{\Omega}{n}$.

If G has a finite orbit, then $\mathcal{A}^G$ contains non-zero nilpotents. I *conjecture* that conversely, if G has no finite orbits, then $\mathcal{A}^G$ is an integral domain. This question arose originally in studying the rate of growth of the numbers $f_n(G)$ for oligomorphic groups. The only evidence for it, apart from the fact that no counterexamples are known, is the following observation. Let $f \in V_n$ and $g \in V_m$ be such that $fg \neq 0$. Let X and Y be sets in the support of f and g respectively. By the Separation Lemma (Neumann [10], Lemma 2.3), if G has no finite orbits, then there is a translate Y' of Y such that $X \cap Y' = \emptyset$. Now we have a non-zero contribution to $(fg)(X \cup Y')$, though this may be cancelled out by other terms in the sum.

There is a stronger form of the conjecture, as follows. Let e be the constant function in V_1 with value 1. It is known that e is a non-zero-divisor in $\mathcal{A}$, and lies in $\mathcal{A}^G$ for any group G. (This implies that multiplication by e is a monomorphism from V_n^G to V_{n+1}^G, and hence that $f_{n+1}(G) \geq f_n(G)$ for any n: see Cameron [1].) I *conjecture* that, if G has no finite orbits, then e is prime in $\mathcal{A}^G$, in the sense that if $e|fg$ then $e|f$ or $e|g$. This would imply that $\mathcal{A}^G$ is an integral domain.

There is a combinatorial version of this algebra, defined as follows. Let $\mathcal{C}$ be a class of finite relational structures closed under isomorphism and under taking induced substructures. Let $V_n(\mathcal{C})$ be the vector space of functions from the isomorphism types of n-element structures in $\mathcal{C}$ to $\mathbb{Q}$, and $\mathcal{A}(\mathcal{C}) = \bigoplus_{n\geq 0} V_n(\mathcal{C})$, with multiplication defined just as before.

The *age* of a relational structure M on Ω is the class of all finite structures embeddable in M as induced substructures. M is *homogeneous* if every isomorphism between finite induced substructures of M extends to an automorphism of M. Now we have:

- If $\mathcal{C}$ is the age of a relational structure M on Ω, then $\mathcal{A}(\mathcal{C})$ is a subalgebra of the reduced incidence algebra $\mathcal{A}$ on Ω (and this is equivalent to $\mathcal{C}$ having the *joint embedding property*, that is, any two members of $\mathcal{C}$ can be simultaneously embedded in a member of $\mathcal{C}$).

- If $\mathcal{C}$ is the age of a homogeneous relational structure M on Ω, then $\mathcal{A}(\mathcal{C}) = \mathcal{A}^G$, where $G = \mathrm{Aut}(M)$ (and this is equivalent to $\mathcal{C}$ having the *amalgamation property*, that is, any amalgam of two members of $\mathcal{C}$ with a common substructure can be embedded in a member of $\mathcal{C}$).

See, for example, Cameron [3] for discussion.

2 Polynomial algebras

There are only two techniques I know for determining the structure of the algebras $\mathcal{A}^G$ or $\mathcal{A}(\mathcal{C})$. The first is based on the simple observation that, regarding $G \times H$ as a permutation group on the disjoint union of the sets on which G and H act, we have

$$\mathcal{A}^{G\times H} = \mathcal{A}^G \otimes_{\mathbb{Q}} \mathcal{A}^H.$$

Let S denote the symmetric group on an infinite set. Then $\mathcal{A}^S$ is a polynomial ring in one variable (generated by the element e). Hence $\mathcal{A}^{S^n}$ is a polynomial algebra in n variables.

Now let H be a finite permutation group of degree n. Then the *wreath product* $S\mathrm{Wr}H$ is the semidirect product of S^n by H, and so $\mathcal{A}^{S\mathrm{Wr}H}$ consists of the invariants of H in the polynomial algebra (in the classical sense, where H acts as a linear group by permutation matrices). For example, if H is the symmetric group S_n, then $\mathcal{A}^{S\mathrm{Wr}S_n}$ is the polynomial algebra generated by the n elementary symmetric functions, by Newton's Theorem. (Note that $\mathcal{A}^{S\mathrm{Wr}H}$ is always an integral domain, but almost never a polynomial algebra.)

In this case, the numbers $f_n(S \,\mathrm{Wr}\, H)$ can be calculated by Molien's Theorem, which turns out to be a special case of a "cycle index theory" for oligomorphic permutation groups (see [3]).

The second approach requires that the class $\mathcal{C}$ has a "good notion of connectedness", as follows. I will give an axiomatic treatment, since in one of the examples below, words like "connected" and "involvement" have meanings quite different from their usual ones. We require

- a distinguished subclass of $\mathcal{C}$ consisting of "connected" structures;
- a partial order $\leq$ called "involvement" on the class of n-element structures for each n;
- a binary, commutative and associative "composition" $\circ$ such that, if X and Y are structures with n and m points respectively, then $X \circ Y$ is a structure with $n+m$ points.

Assume that the following conditions hold:

A1 Let S be a structure which is partitioned into disjoint induced substructures $S_1, S_2, \ldots$. Then $S_1 \circ S_2 \circ \ldots \leq S$.

A2 Any structure has a unique representation as a composition of connected structures.

Theorem 2.1 *If all the above conditions hold, then $\mathcal{A}(\mathcal{C})$ is a polynomial algebra, generated by the characteristic functions of the connected structures.*

Proof. If $|S| = n$, then S is a disjoint union $S_1 \cup S_2 \cup \ldots$ of connected structures; so we have a bijection between characteristic functions χ_S (the basis elements of $V_n(\mathcal{C})$) and monomials $\phi_S = \chi_{S_1}\chi_{S_2}\ldots$ of total weight n. Consider the matrix expressing the monomials ϕ_S in terms of the basis elements $\chi_{S'}$. The coefficient of χ_S in the row corresponding to ϕ_S is non-zero. Suppose that $\chi_{S'}$ also has non-zero coefficient. Then S' can be partitioned into induced substructures isomorphic to $S_1, S_2, \ldots$; so $S = S_1 \circ S_2 \circ \ldots \leq S'$. Thus the matrix is upper triangular with non-zero diagonal, and hence invertible. So the monomials of weight n form a basis for $V_n(\mathcal{C})$, and the theorem is proved.

Example 1. Let M be the countable "random graph" [4], whose age $\mathcal{C}$ is the class of all finite graphs. Let "connected" have its usual meaning, "involvement" mean "spanning subgraph", and "composition" be disjoint union (with no edges between the parts). Then A1 and A2 hold, and so $\mathcal{A}(\mathcal{C}) = \mathcal{A}^{\mathrm{Aut}(M)}$ is a polynomial algebra, whose generators correspond to the finite connected graphs.

This method works for many other ages, both of homogeneous structures (for example, the class of K_n-free graphs for fixed n [8]), and not (for example, bipartite graphs, N-free graphs [5]).

Example 2. Let $\mathcal{C}$ be the age of a homogeneous structure M, and let $G = \mathrm{Aut}(M)$. Let $\mathcal{C}'$ be the class of structures over a language with the relation symbols for $\mathcal{C}$ and one new binary symbol E, in which E is an equivalence relation each of whose classes carries a $\mathcal{C}$-structure (with no instances of relations holding between points in different E-classes). Then $\mathcal{C}'$ is the age of a homogeneous structure consisting of the disjoint union of countably many copies of M, with automorphism group $G\,\mathrm{Wr}\,S$, where S is the symmetric group of countable degree. Now let "connected" mean "only one E-class", "involvement" mean "inclusion of all relations", and "composition" mean "disjoint union". Then A1 and A2 hold.

The conclusion is that $\mathcal{A}^{G\mathrm{Wr}S}$ is always a polynomial algebra; the number of generators of degree n is equal to the number of orbits of G on n-sets.

Example 3. Let A be a fixed alphabet of finite size q, and let $\mathcal{C} = A^*$ be the set of words in A. (Here a word of length n is regarded as an n-set carrying a total order and q unary relations $R_1, \ldots, R_q$, where each element of the set satisfies exactly one of the unary relations; the word $a_1a_2\ldots a_q$ corresponds to the n-set $\{x_1, \ldots, x_n\}$, with $x_1 < x_2 < \ldots < x_n$ and in which x_i satisfies R_{a_i}.) The algebra $\mathcal{A}(A^*)$ is the *shuffle algebra* which arises in the theory of free Lie algebras [12]. The name comes from the fact that the product of two words is the sum of all words which can be obtained by "shuffling" them together, with appropriate multiplicities. For example,

$$(aab) \cdot (ab) = abaab + 3aabab + 6aaabb.$$

Also, A^* is the age of a homogeneous relational structure $M(q)$ which is order-isomorphic to $\mathbb{Q}$ and in which the set of elements satisfying each relation R_i is dense; in other words, a partition of $\mathbb{Q}$ into q dense subsets. Such a partition is unique up to order-isomorphism of $\mathbb{Q}$. Let $G(q) = \mathrm{Aut}(M(q))$.

Take a total order on A, and define the *lexicographic order* on A^* in the usual way: that is, $a_1 \ldots a_m < b_1 \ldots b_n$ if and only if *either*

- $m < n$, and $a_i = b_i$ for $i = 1, \ldots, m$; *or*
- for some $l < \min\{m, n\}$, we have $a_i = b_i$ for $i = 1, \ldots, l$, and $a_{l+1} < b_{l+1}$.

A non-empty word $w \in A^*$ is a *Lyndon word* if, whenever $w = xy$ with x, y non-empty, we have $w < y$; that is, w is less than any proper cyclic shift of itself. The number of Lyndon words of length n is $(1/n)\sum_{d|n}\mu(d)q^{n/d}$, where μ is the Möbius function. (This well-known number counts several other things, for example, irreducible polynomials over $\mathbb{F}_q$ if q is a prime power; see [12].) The following combinatorial properties hold for Lyndon words:

Lemma 2.2 *(i) Any word w has a unique expression in the form $w = w_1w_2\ldots$, where $w_1, w_2, \ldots$ are Lyndon words with $w_1 \geq w_2 \geq \ldots$.*

(ii) Given Lyndon words $w_1, w_2, \ldots$ with $w_1 \geq w_2 \geq \ldots$, the lexicographically greatest shuffle of these words is the concatenation $w_1w_2\ldots$.

Hence, if we let "connected" mean "Lyndon word", "involvement" mean "lexicographic order reversed", and "composition" mean "concatenation in decreasing lexicographic order", then A1 and A2 hold, and we conclude that $\mathcal{A}(A^*) = \mathcal{A}^{G(q)}$ is a polynomial algebra generated by the Lyndon words (a result of Radford [11]).

3 Transitive extensions

Not much is known in general about how the algebra $\mathcal{A}^G$ is affected by group-theoretic or model-theoretic constructions (direct products with product action, wreath products, covers and quotients, etc.). This section contains some comments about transitive extensions.

The permutation group H on Ω is a *transitive extension* of G if H is transitive and the stabiliser H_α of the point α, acting on $\Omega \setminus \{\alpha\}$, is isomorphic to G as permutation group. Note that, in this situation, H is closed if and only if G is closed.

A general question: *Let H be a transitive extension of G. What is the relation between $\mathcal{A}^H$ and $\mathcal{A}^G$?*

We can regard the group induced on Ω by G as the direct product of G (in its given action) with the trivial group of degree 1. For the latter group (K, say), the algebra $\mathcal{A}^K$ is generated by an element k of degree 1 with $k^2 = 0$. In other words, $\mathcal{A}^K \cong T(\mathbb{Q})$, the algebra of 2×2 upper triangular matrices with constant diagonal over $\mathbb{Q}$. Hence, using G^+ for the group induced on Ω by G, we have

$$\mathcal{A}^{G^+} \cong \mathcal{A}^G \otimes_{\mathbb{Q}} T(\mathbb{Q}) \cong T(\mathcal{A}^G).$$

However, we can only say that, since $G^+ \leq H$, the algebra $\mathcal{A}^H$ is a subalgebra of $T(\mathcal{A}^G)$. This does not seem to help to decide, for example, whether $\mathcal{A}^H$ is an integral domain.

There is a special class of transitive extensions for which a bit more can be said. We say that the transitive extension H of G is *curious* if H has a transitive subgroup (on the whole of Ω) which is isomorphic to G. In the case where G and H are closed, this means that H is a reduct of G. If H is a curious transitive extension of G, then $\mathcal{A}^H$ is a subalgebra of $\mathcal{A}^G$; in particular, $\mathcal{A}^H$ is an integral domain if $\mathcal{A}^G$ is. Perhaps it is possible to weave together the embeddings of $\mathcal{A}^H$ in $\mathcal{A}^G$ and in $T(\mathcal{A}^G)$ to get better information.

Example 1 (continued). A *two-graph* on Ω is a set T of 3-element subsets of Ω such that any 4-subset contains an even number of members of T (Seidel [14]).

Given a graph Γ on Ω, let $T(\Gamma)$ be the set of *odd triples* of Γ (those containing an odd number of edges). Then $T(\Gamma)$ is a two-graph on Ω. Every two-graph arises in this way.

Let R be the random graph on Ω_0. Take a new point ∞, and define T to be the two-graph on $\Omega = \Omega_0 \cup \{\infty\}$ derived from R (with ∞ as an isolated vertex). Then $\mathrm{Aut}(T)$ is a transitive extension of $\mathrm{Aut}(R)$. Moreover, it is curious; for the two-graph derived from R without an isolated vertex is clearly a reduct of R, and

is isomorphic to T. (In fact, T is the unique countable universal homogeneous two-graph.) See Thomas [16].
Problem. Is $\mathcal{A}^{\mathrm{Aut}(T)}$ a polynomial algebra?
Remark. Mallows and Sloane [9] showed that the numbers of two-graphs and *even graphs* (graphs with all valencies even) on n points are equal. Hence, if $\mathcal{A}^{\mathrm{Aut}(T)}$ is a polynomial algebra, then its generators are in one-to-one correspondence (preserving degree) with the finite *Eulerian graphs* (the connected even graphs).

Example 3 (continued). Let $G(q)$ be as in Example 3 in the preceding section. Then $G(q)$ has a transitive extension $H(q)$ defined as follows.

On the set of complex roots of unity, put $z_1 \equiv z_2$ if $z_2 z_1^{-1}$ is a qth root of unity. Let Ω be a dense subset containing exactly one member of each equivalence class of this relation. (Such a set is unique up to permutation preserving the cyclic order. If we choose a random member of each class, the resulting set almost surely has this property.) Now define binary relations $R_1, R_2, \ldots, R_q$ by $(z_1, z_2) \in R_j$ if and only if

$$\frac{2\pi(j-1)}{q} < \arg(z_2 z_1^{-1}) < \frac{2\pi j}{q}.$$

The structure $N(q)$ consists of the circular order and the relations $R_1, R_2, \ldots, R_q$. It is $\aleph_0$-categorical. Note that, if $z_1 \neq z_2$, then $(z_1, z_2) \in R_j$ for a unique value of j; and the converse of R_j is R_{q+1-j}. Let $H(q) = \mathrm{Aut}(N(q))$.

Now take $z \in \Omega$. Define a map $\phi : \Omega \setminus \{z\} \to (0,1)$ by letting $\phi(w)$ be the fractional part of $\frac{q}{2\pi}\arg(zw^{-1})$. Then $\phi(\Omega \setminus \{z\}) = (0,1) \cap \mathbb{Q}$. If we give $\phi(w)$ the colour j if $(z, w) \in R_j$, then each colour class is dense. Moreover, the structure $N(q)$ can be recovered uniquely from this information. So $H(q)$ is a transitive extension of $G(q)$.

This extension is also curious. If we repeat the above construction, but with z a point on the unit circle which is not a root of unity, we obtain a bijection from all of Ω to a countable dense subset of $(0,1)$ partitioned into q dense subsets.
Problem. Is $\mathcal{A}^{H(q)}$ a polynomial algebra?
Remark. For $q = 2$, the relations R_1 and R_2 are a converse pair of tournaments, each of which is isomorphic to the countable universal homogeneous *local order* [2], *locally transitive tournament* [7], or *vortex-free tournament* [6]: these are three alternative names for a tournament having no subtournament consisting of a directed 3-cycle dominating or dominated by a vertex. This structure is further discussed in the lectures of Evans, Ivanov and Macpherson.

Orbits of $H(q)$ on n-sets are parametrised by two-way infinite "shift register sequences" (x_i) with elements in $\{1, \ldots, q\}$ satisfying $x_i + n \equiv x_i + 1 \pmod{q}$ for all i. For $q = 2$, the sequences counting these orbits is listed as M0324 in the *Encyclopedia of Integer Sequences* [15], where further references can be found.

On the assumption that $\mathcal{A}^{H(2)}$ is a polynomial algebra, it is possible to compute the numbers of generators of each degree. The resulting sequence appears to be "unknown"; in particular, it is not in the Encyclopedia [15].

The group $H(2)$ does not have a transitive extension. Nevertheless, the following occurrence is suggestive.

Knuth [6] defines a *CC-structure* to be a set with a ternary relation satisfying five universal axioms, of which the first three assert that the induced structure on any 3-set is a circular order. The letters CC stand for "counter-clockwise"; and, given a set Ω of points in the Euclidean plane with no three collinear, the relation R such that $R\alpha\beta\gamma$ holds if and only if the points α, β, γ occur in the counter-clockwise sense, is a CC-structure. Such a CC-structure is called *representable*. There is a countable universal representable CC-structure, defined by choosing a countable dense set of points in the Euclidean plane with no three collinear. It is not homogeneous; indeed, the class of CC-structures (or of representable CC-structures) does not have the amalgamation property.

Given a ternary relation R on Ω whose restriction to any 3-set is a circular order, there is a derived tournament R_α on $\Omega \setminus \{\alpha\}$ defined by $R_\alpha\beta\gamma \Leftrightarrow R\alpha\beta\gamma$. Knuth's fifth axiom for CC-structures implies that R_α is a local order for any point α. Indeed, if we take the universal representable CC-structure above, and project $\Omega \setminus \{\alpha\}$ radially onto the unit circle with centre α, we obtain the homogeneous local order $N(2)$.

Problem. Do there exist countable CC-structures (or representable ones) with large automorphism groups, or with other nice model-theoretic properties?

Acknowledgment. I am grateful to R. A. Bailey, R. M. Bryant and D. G. Fon-Der-Flaass for their help with the contents of this paper.

References

[1] P. J. Cameron, Transitivity of permutation groups on unordered sets, *Math. Z.* **48** (1976), 127–139.

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

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

[4] P. J. Cameron, The random graph, pp. 333–351 in *The Mathematics of Paul Erdős, II* (ed. R. L. Graham and J. Nešetřil), Algorithms and Combinatorics **14**, Springer, Berlin, 1997.

[5] J. Covington, A universal structure for N-free graphs, *Proc. London Math. Soc.* (3), **58** (1989), 1–16.

[6] D. E. Knuth, *Axioms and Hulls*, Lecture Notes in Computer Science **606**, Springer, Berlin, 1992.

[7] A. H. Lachlan, Countable homogeneous tournaments, *Trans. Amer. Math. Soc.* **284**, 431–461.

[8] A. H. Lachlan and R. E. Woodrow, Countable ultrahomogeneous undirected graphs, *Trans. Amer. Math. Soc.* **262** (1980), 51–94.

[9] 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.

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

[11] D. E. Radford, A natural ring basis for the shuffle algebra and an application to group schemes, *J. Algebra* **58** (1979), 432–454.

[12] C. Reutenauer, *Free Lie Algebras*, London Math. Soc. Monographs (New Series) **7**, Oxford University Press, 1993.

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

[14] J. J. Seidel, A survey of two-graphs, pp. 481–511 in *Proc. Int. Colloq. Teorie Combinatorie*, Accad. Naz. Lincei, Roma, 1977.

[15] N. J. A. Sloane and S. Plouffe, *The Encyclopedia of Integer Sequences*, Academic Press, New York, 1995.

[16] S. R. Thomas, Reducts of the random graph, *J. Symbolic Logic* **56** (1991) 176–181.

Author's address:
School of Mathematical Sciences,
Queen Mary and Westfield College,
London E1 4NS,
England.
e-mail: P.J.Cameron@qmw.ac.uk