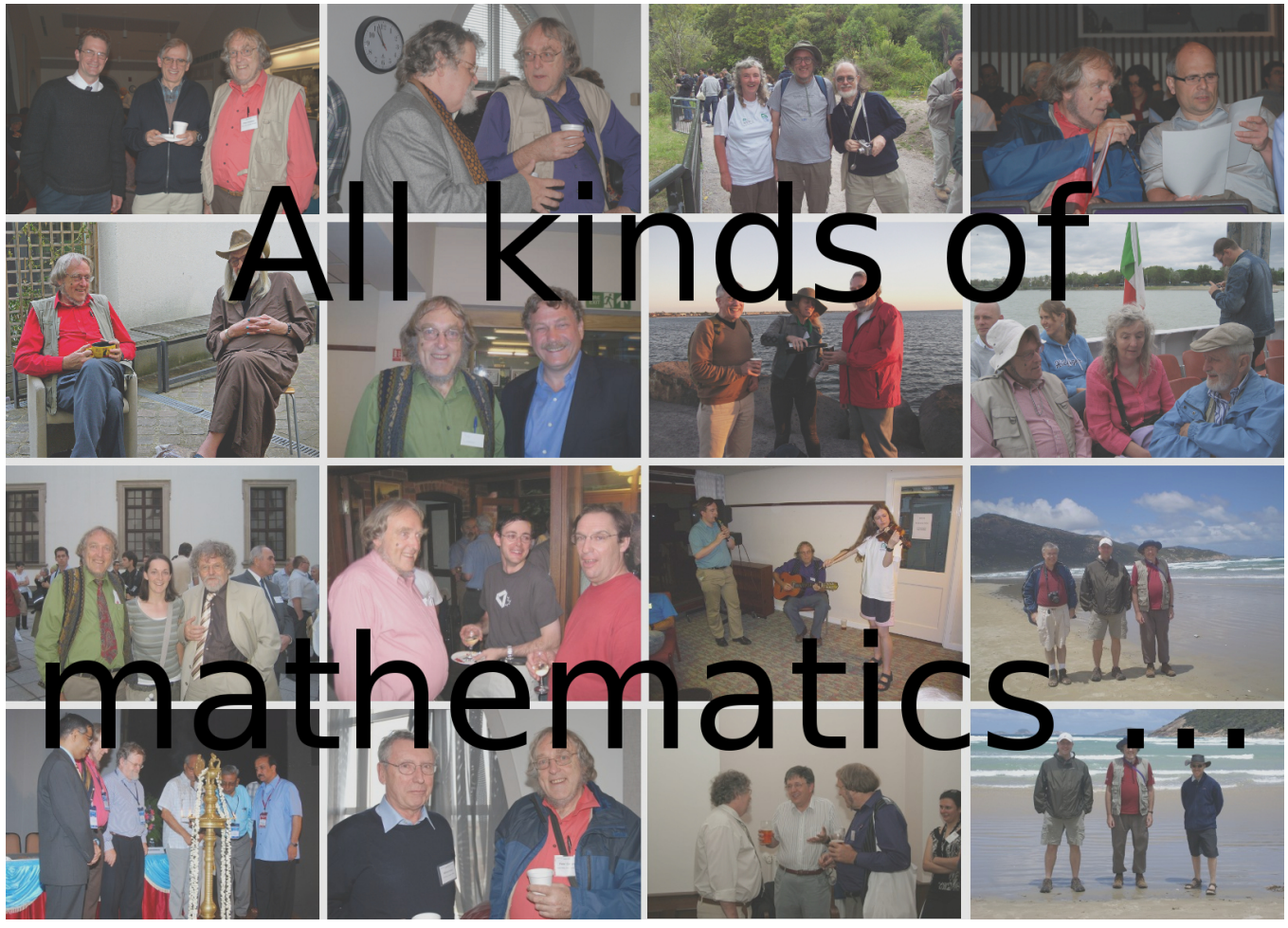
Perchance to dream . . .

Peter J. Cameron
University of St Andrews

All kinds of mathematics. . .
Lisboa, July 2017



Mathematics is what mathematicians do. This conference is not about me, but about you, the friends and colleagues I have done mathematics with, and those that I will do so in the future. My sincerest thanks to you all.

Dreams

The purpose of life is to prove and to conjecture.

Paul Erdős

This talk will be about some problems for which I dream of seeing solutions. These are things I have worked on, usually with co-authors, or my friends or students have worked on.

So this is your homework. The hand-in date is by the registration deadline for the next conference in this wonderful series.
Of course, I have many more problems. Feel free to solve one of them instead.

My teachers . . .

Most of what I know I have learnt from my collaborators and students.

Here are my three most prolific co-authors.

. . . and one in particular

I would especially like to thank João Araújo – apart from anything else, for the tremendous work he has done organising this amazing conference.
We have worked together for just the last ten years; in that time we have had ten papers published or accepted for publication, and another (which in our view is certainly one of the best) rejected by one journal and not yet submitted to another. Before this collaboration, I had never done any research on semigroups.
If João survives his current sentence as department head, I hope we can continue this wonderful collaboration for many years!
In the rest of this talk I will speak about some open problems I would like to see solved (or to solve myself). I will begin with two from my joint work with João.

Synchronization

This subject has its roots in automata theory and the infamous Černý conjecture. Unfortunately there is no time to describe the background.

Synchronization theory, as I will describe it here, began in Lisbon, but reached me from several directions: from João via Peter Neumann, from Ben Steinberg via Robert Bailey, and via my own work with Cristy Kazanidis on cores of graphs (for a special volume for Cheryl Praeger).

A permutation group G on Ω is synchronizing if, given any map $a : \Omega \to \Omega$ which is not a permutation, the semigroup $\langle G, a \rangle$ generated by G and a contains a rank 1 element (one whose image consists of a single point).

Translation to graphs

On a visit to St Andrews in 2008, I realised:

Theorem

The permutation group G is non-synchronizing if and only if there is a non-trivial G-invariant graph Γ with clique number equal to chromatic number (that is, with core a complete graph).

There is a closely related property, which can be phrased in terms of graphs as follows (this was not the original form). The transitive permutation group G is non-separating if there is a non-trivial G-invariant graph for which the product of clique number and independence number is equal to the number of vertices. If no such graph exists, then G is separating.

Theorem

2-homogeneous $\Rightarrow$ separating $\Rightarrow$ synchronizing $\Rightarrow$ primitive. None of these implications reverses.

The big problem

The big problem is: *Determine the synchronizing (or separating) permutation groups*.

For one important family (the symmetric group S_n acting on k-sets, for $k < n/2$, we were led to a conjecture which would be a wide extension of Peter Keevash's existence theorem for t-designs. (I have worked on this with Mohammed Aljohani and John Bamberg.)

A Steiner system $S(t,k,n)$ is a collection of k-subsets (called blocks) of a set of n points with the property that any t points lie in a unique block.
If such a system exists, then S_n acting on k-sets is not separating: the blocks of the system form a clique in the graph in which two k-sets are joined if they meet in at most $t-1$ points, and the k-sets containing a fixed t-set form an independent set, such that the product of the sizes of these sets is $\binom{n}{k}$.

The conjecture

Conjecture

There is a function F such that, if $n > F(k)$, then S_n acting on k-sets is non-separating if and only if a Steiner system $S(t,k,n)$ exists for some t with $0 < t < k$.

There are well-known divisibility conditions which are necessary for the existence of a Steiner system: $\binom{k-i}{t-i}$ must divide $\binom{n-i}{t-i}$ for $i = 0, \ldots, t-1$. Keevash showed that, for n sufficiently large, these conditions are also sufficient.

So the conjecture can be re-phrased: for $n > G(k)$, S_n on k-sets is non-separating if and only if the divisibility conditions hold for some t with $0 < t < k$.

And what about synchronizing?

There is a similar conjecture. A large set of Steiner systems $S(t,k,n)$ is a partition of the set of k-subsets of an n-set into Steiner systems. If a large set exists, then S_n on k-sets is not synchronizing.

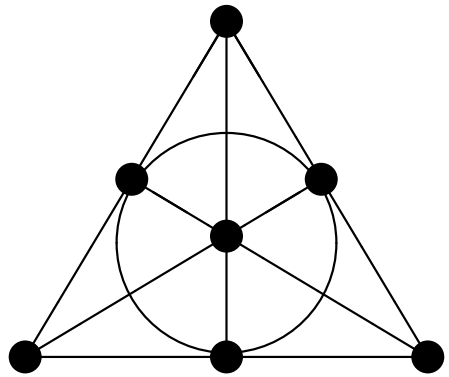
Conjecture

There is a function H such that, for $n > H(k)$, S_n acting on k-sets is non-synchronizing if and only if a large set of Steiner systems $S(t,k,n)$ exists for some t with $0 < t < k$.

Less is known about the existence of large sets, and we do not feel confident enough to conjecture an analogue of Keevash's theorem for them.

The Fano plane

The group S_7 acting on 3-sets is not synchronizing. Take the Fano plane:



This is a 7-clique in the graph in which two 3-sets are joined if they intersect in one point. A 7-colouring of this graph is given by taking one colour for each line of the Fano plane and applying it to that line and the four 3-sets disjoint from it.

A spin-off conjecture

Conjecture

Let q be a prime power greater than 2. Then an independent set of maximum size in the graph whose vertices are the $(q+1)$-sets of a (q^2+q+1)-set, joined if they intersect in one point, consists of all the $(q+1)$-sets containing two given points. In particular, the chromatic number of this graph is strictly greater than its clique number.

This is true for $q = 3, 4$, shown using Leonard Soicher's `GRAPE` software. However, the corresponding groups are not synchronizing, since there are large sets of projective planes of orders 3 and 4 – indeed, Spyros Magliveras conjectures that such sets exist for all prime powers q.

This is an opportunity to thank Leonard for his remarkable programs which have been crucial for studying this problem (and others!).

The road closure property

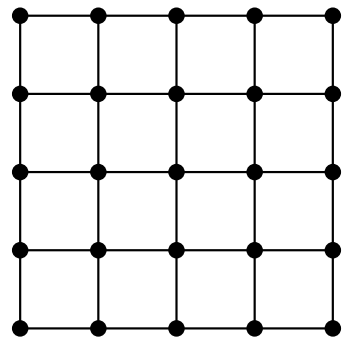
This problem arises from a question about idempotent-generated semigroups, that João and I worked on. At the time, as my St Andrews colleagues will know, there was a long season of road closures in the neighbourhood.

Let G be a transitive permutation group on Ω. A result of Donald Higman (my thesis examiner) asserts that G is primitive if and only if, for every orbit O of G on the set of 2-element subsets of Ω, the orbital graph with vertex set Ω and edge set O is connected.

We say that G has the road closure property if, given any orbit O of G on 2-sets and any (maximal) block of imprimitivity for the action of G on O, the graph $(\Omega, O \setminus B)$ is connected.

An example

Consider the automorphism group of a $m \times m$ grid: two points are joined if they lie in the same row or column. The automorphism group is the wreath product $S_m \wr S_2$ in its product action on m^2 points.



The edges fall into two blocks of imprimitivity under the automorphism group: horizontal and vertical.
If workmen come and dig up all the vertical roads, then it is impossible to get from one row to another. So this primitive group fails to have the road closure property.

The Road Closure Conjecture

In the same way, we see that if G is primitive and non-basic (that is, preserves a Cartesian structure on Ω), then G does not have the road closure property.

Similarly, if G is primitive and has an imprimitive normal subgroup of index 2, then G does not have the road closure property.

We know one more family of groups, arising from $\mathrm{P}\Omega^+(8,q) : S_3$ on the cosets of the parabolic subgroup corresponding to the three leaves of the D_4 diagram.

Conjecture

If G is a basic primitive group, not having an imprimitive subgroup of index 2, and not one of the above examples from triality, then G has the road closure property.

Connection with semigroups

We came to this conjecture from the following problem about idempotent-generated semigroups.

Theorem

Let G be a transitive permutation group on Ω. Then the following conditions on G are equivalent:

- *for every rank 2 map a on Ω, the semigroup*

$$\langle G, a \rangle \setminus G$$

  is idempotent-generated;
- *G has the road closure property.*

So the conjecture would give the complete classification of such groups.

Sum-free sets

My work on sum-free sets grew out of looking at Henson's universal homogeneous triangle-free graph. I worked with Paul Erdős in Cambridge and elsewhere on enumerating them; we made two conjectures (see later).

I stated a problem on sum-free sets at the British Combinatorial Conference in Glasgow in 1985. Neil Calkin took it up, and wrote his PhD thesis on the subject. So I regard Neil as an "honorary student" of mine as well as a collaborator. (Neil was the founding managing editor of the *Electronic Journal of Combinatorics*.)

The questions that follow are connected to the work with Neil, but stand on their own, I think.

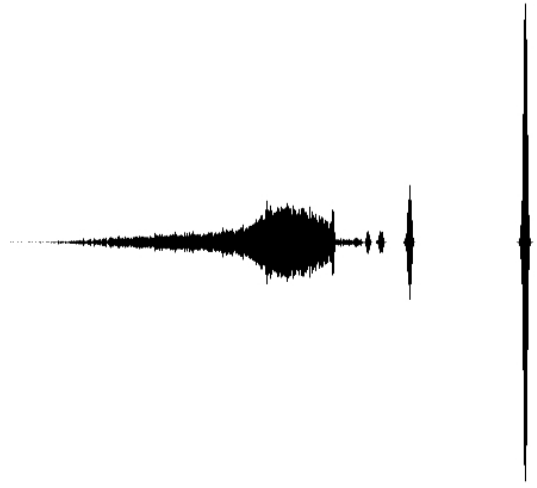
Random sum-free sets

Choose a sum-free subset S of $\mathbb{N}$ as follows: examine each positive integer in turn; if $n = x + y$ where $x, y \in S$, then $n \notin S$; otherwise toss a fair coin.

- **Coin tosses:** HTH...
- **Resulting set:** 1,4,...
- 1 is not a sum, so toss the coin; it's H, so $1 \in S$
- $2 = 1 + 1$, so skip
- 3 is not a sum, so toss the coin; it's T, so $3 \notin S$
- 4 is not a sum, so toss the coin; it's H, so $4 \in S$
- $5 = 1 + 4$, so skip
- ... and so on ...

A simulation

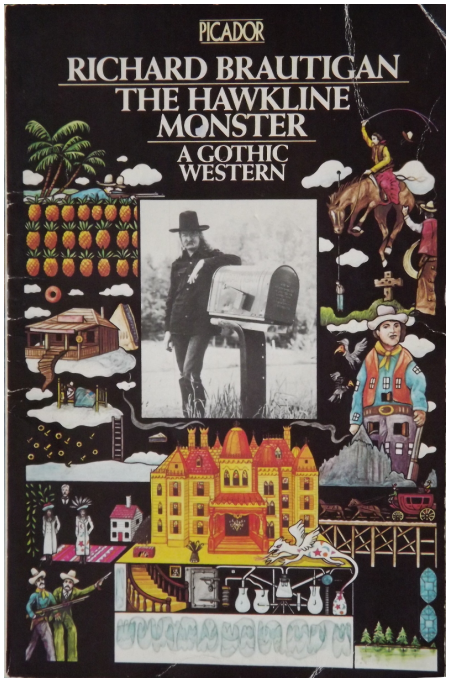
Compute many large sum-free sets and plot their densities.



The "spectral line" at $1/4$ has mass $0.218\ldots$, and corresponds to sets consisting of odd numbers.

- Does a random sum-free set have a density almost surely?
- If so, is the density spectrum discrete or is there a continuous part below $1/6$?
- Is the density almost surely positive?

Counting



"I count a lot of things that theres no need to count," Cameron said. "Just because that's the way I am. But I count all the things that need to be counted."

Richard Brautigan, *The Hawkline Monster: A Gothic Western*

Paul Erdős and I made two conjectures. The first asserted that the number of sum-free subsets of $\{1, \ldots, n\}$ is asymptotically $c_i 2^{n/2}$, where $n \to \infty$ through values congruent to i mod 2 ($i = 0$ or 1). This was proved independently by Ben Green and Sasha Sapozhenko. The second was similar, anc concerned maximal sum-free sets; it was proved by József Balogh, Hong Liu, Maryam Sharifzadeh, and Andrew Treglown.

Growth rates for oligomorphic groups

For a change, the permutation groups in this section act on infinite sets (but you may assume countable without loss of generality).

We say that G on Ω is oligomorphic if, for every natural number n, G has only finitely many orbits on Ω^n (or, equivalently, on the set of n-element subsets of Ω).

The theorem of Engeler, Ryll-Nardzewski and Svenonius from 1959 shows that a countable first-order structure is $\aleph_0$-categorical (that is, it is the unique countable model of its first-order theory) if and only if its automorphism group is oligomorphic.

Thus the automorphism groups of $\aleph_0$-categorical structures are precisely the oligomorphic permutation groups which are closed (in the topology of pointwise convergence in the symmetric group).

Rapid and smooth growth?

Let $f_n(G)$ be the number of orbits of G on n-element subsets of Ω. A meta-conjecture states that the numbers $f_n(G)$ grow rapidly and smoothly.

In particular, Dugald Macpherson showed that, if G is primitive, then either $f_n(G) = 1$ for all n (so G is highly homogeneous) or it grows at least exponentially with n.

- Show that $f_n(G)^{1/n}$ tends to a limit as $n \to \infty$. (If so, call such a limit a growth rate.)
- Macpherson showed that a growth rate greater than 1 for a primitive group is at least $\sqrt[5]{2}$; Francesca Merola improved this to $1.324\ldots$.
- Is it true that the smallest growth rate is 2?
- What is the largest number α for which there are only finitely many growth rates smaller than α?

Isbell's Conjecture

Isbell's conjecture is nearly 60 years old (older than the Černý conjecture) and still open. I would like to see it settled. It arose originally in game theory.

Conjecture

Given a prime p, there is a function f_p such that, if $n = p^a.b$ with $p \nmid b$ and $a > f_p(b)$, then any transitive permutation group of degree n contains a fixed-point-free element of p-power order.

The conjecture is surely true. Jordan showed that a transitive permutation group of degree greater than 1 contains a fixed-point-free element, and Fein, Kantor and Schacher (using CFSG) showed that there is a fixed-point-free element of prime power order (but without specifying which prime).

You can't ask for more

Pablo Spiga worked on this problem.

I had been rash enough to make a stronger conjecture, which looked more attackable. I conjectured the existence of a function g_p such that, if a p-group P has b orbits each of size at least $p^{g_p(b)}$, then P must contain a fixed-point-free element.

This conjecture easily implies Isbell's conjecture. However, it was refuted by Pablo and Eleanora Crestani, using a nice "profinite" construction.

Related problems

To me, the result of Fein, Kantor and Schacher cries out for a proof not using CFSG.

A related question is whether a fixed-point-free (fpf) element in a transitive group can be found efficiently. Arjeh Cohen and I showed that at least a fraction $1/n$ of the elements of G are fpf; so choosing nm random elements of G, we will get a fpf element with probability about $1 - 1/e^m$. Is there a deterministic algorithm?

Emil Vaughan observed that the Fein–Kantor–Schacher proof gives a polynomial-time algorithm to find a fpf element; but it is rather complicated, and CFSG is needed to prove its correctness!

Then in 2013, Vikraman Arvind from Chennai gave a beautifully simple argument "derandomizing" the random algorithm above.

Generating sets

With Colva Roney-Rougal I worked on an exchange property for group generating sets. Andrea Lucchini got interested when I talked about it in Budapest (at the birthday conference for P^3).

For a natural number m, call two elements x and y of a group G m-equivalent if y can be substituted for x in any m-element generating set for G; that is, $G = \langle x, z_1, \ldots, z_{m-1} \rangle$ if and only if $G = \langle y, z_1, \ldots, z_{m-1} \rangle$.

Could this be true?

The equivalence relation of m-equivalence gets finer as m increases, and so in a finite group it stabilises at some value; call this value $\psi(G)$.

It is clear that $\psi(G) \geq d(G)$, where $d(G)$ is the minimal number of generators of G. We have some evidence (and no counterexamples) for the following:

Conjecture

For any finite group G, either $\psi(G) = d(G)$ or $\psi(G) = d(G) + 1$.

This would give an interesting dichotomy for finite groups.

There might be a similar analysis for other algebraic structures ...

A few more conjectures

Here are a few more conjectures I would like to see settled.

- Every primitive permutation group of diagonal type preserves a non-trivial association scheme. (Association schemes, of course, consist of symmetric relations; otherwise it would be trivially true.)
- The second row of a (uniform) random Latin square of order n tends very rapidly to a (uniform) random derangement of the first as $n \to \infty$.
- The $\alpha + n$ conjecture (devised by participants at the Isaac Newton Institute programme on Combinatorics and Statistical Mechanics, along with David Wallace and Vladimir Dokchitser): if α is any algebraic integer, there is a natural number n such that $\alpha + n$ is a root of the chromatic polynomial of a graph.

. . . for coming, for all I have learned from you, and for the wonderful experience of working with many of you (and I hope to work with the rest of you before next time).