Some of my favourite problems

Peter J. Cameron
University of St Andrews

Old Codgers Combinatorics Colloquium
Reading, 2 November 2016

Problems are the lifeblood of mathematics.
I have a collection of problems accessible from my QMUL webpage. Some of them have been solved, and I am hoping to edit and update them with comments in the coming months.
Please take a look, and if you have any information or comments about any of the problems, send it to me!
Today I am going to talk about a few fairly substantial problems in different parts of combinatorics.

First problem: Extensions of Keevash's Theorem

This problem comes from the synchronization project, though I don't have time to talk about the connection here.

A Steiner system $S(t,k,n)$ consists of an n-set X and a collection $\mathcal{B}$ of k-element subsets of X with the property that every t-element subset of X is contained in a unique member of $\mathcal{B}$.

A necessary condition for the existence of an $S(t,k,n)$ is that

$$\binom{k-i}{t-i} \text{ divides } \binom{n-i}{t-i} \text{ for } i = 0, \ldots, t-1.$$

Peter Keevash showed the remarkable result that these necessary conditions are asymptotically sufficient (that is, they are sufficient for all but finitely many n, given t and k).

Cliques and cocliques

Let $\omega(G)$ and $\alpha(G)$ be the clique number and independence number of the graph G.
The following easy result may partly motivate the problem coming up.

Theorem

If the graph G on n vertices is vertex-transitive, then $\omega(G)\alpha(G) \leq n$; equality implies that every maximum clique intersects every maximum independent set.

Now let n and k be integers with $n \geq 2k$, and $I \subseteq \{0, \ldots, k-1\}$. Define a graph $G(n, k, I)$ as follows: the vertices are the k-element subsets of $\{1, \ldots, n\}$; two vertices are joined if the size of their intersection belongs to I.

Theorems

Theorem (Erdős–Ko–Rado)

Let $I = \{t, t+1, \ldots, k-1\}$ for some $t < k$. Then, for sufficiently large n, a clique in $G(n, k, I)$ has size at most $\binom{n-t}{k-t}$, with equality if and only if it consists of all k-sets containing a fixed t-set.

Theorem

Let $I = \{t, t+1, \ldots, k-1\}$ for some $t < k$. Then an independent set in $G(n, k, I)$ has size at most $\binom{n}{k} \Big/ \binom{n-t}{k-t}$, with equality if and only if it is the set of blocks of a Steiner system $S(t, k, n)$.

Theorem (Keevash)

For sufficiently large n, a Steiner system $S(t, k, n)$ exists if and only if $\binom{k-i}{t-i}$ divides $\binom{n-i}{t-i}$ for $i = 0, \ldots, t-1$.

So, for sufficiently large n, the graph $G = G(n, k, \{t, \ldots, k-1\}$ has $\omega(G)\alpha(G) = |VG|$ if and only if a Steiner system exists, that is, if and only if the divisibility conditions hold.

A conjecture

These theorems give asymptotic necessary and sufficient conditions for the clique–independent set bound to be attained in $G(n,k,I)$ for this particular I. The next conjecture is a generalisation to arbitrary subsets I.

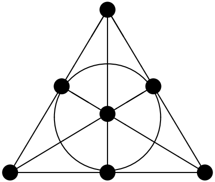
Conjecture

Let k be given, and I a subset of $\{0,\ldots,k-1\}$. Then the following are equivalent for all sufficiently large n:

- *the graph $G = G(n,k,I)$ satisfies $\omega(G)\alpha(G) = \binom{n}{k}$;*
- *$I = \{t,\ldots,k-1\}$ or $I = \{0,\ldots,t-1\}$ for some t, and*

$$\binom{k-i}{t-i} \text{ divides } \binom{n-i}{t-i} \text{ for } i = 0,\ldots,t-1.$$

An example



The Fano plane shows that the graphs $G(7,3,\{1\})$ and $G(8,3,\{1\})$ have clique number (at least) 7.

These graphs have independence numbers (at least) 5 and 8 respectively. (For $G(7,3,\{1\})$, take a 3-set and the four 3-sets disjoint from it; for $G(8,3,\{1\})$, partition the vertices into two 4-sets, and take the 3-sets contained in a part of the partition.)

So equality holds throughout, and these two graphs meet the clique–independent set bound.

It is not too hard to show that this bound is not attained by $G(n,3,\{1\})$ for $n > 8$. So the conjecture is true for $k = 3$.

Some progress

The conjecture concerns cliques and cocliques, not in any old graph, but in a graph which is a union of classes in an association scheme, namely the Johnson scheme $J(n,k)$, whose elements are the k-subsets of $\{1,\ldots,n\}$, two subsets being ith associates if they intersect in $k-i$ points, for $i=0,\ldots,k$.

In this situation, a number of bounds are available, in particular Delsarte's linear programming bound, for the sizes of cliques and independent sets.

Using these techniques, John Bamberg and I have been able to prove the conjecture for small values of k. I cannot give a definitive result, since this is work in progress, but we hope to reach somewhere round $k=10$.

Can these bounds be used to prove the conjecture in general?

First extension: chromatic number

Question

When does the graph $G(n,k,I)$ have clique number equal to chromatic number?

If a vertex-transitive graph G has $\omega(G) = \chi(G)$, then in a minimal colouring all colour classes have size $n/\omega(G)$, and so the clique–independent set bound is attained.

We cannot partition the k-sets into subsets each consisting of all k-sets containing a fixed t-set. So $G(n,k,\{0,\ldots,t-1\})$ does not have clique number equal to chromatic number.

The complement graph $G(n,k,\{t,\ldots,k-1\})$ has clique number equal to chromatic number if and only if there is a partition of the k-sets into Steiner systems $S(t,k,n)$, that is, a large set of Steiner systems.

Thus a solution to this question involves proving the earlier conjecture and deciding whether, for given t, k, n, there exists a large set of Steiner systems $S(t, k, n)$.
The existence of a large set is known in two general cases:

- the case $t = 1$, k divides n: by Baranyai's theorem, a large set always exists;
- the case $t = 2, k = 3, n \equiv 1$ or $3 \pmod 6$: a large set of Steiner triple systems exists if and only if $n > 7$ (Lu, Teirlinck).

Second extension: a q-analogue

We obtain a related class of problems by using instead the graph $G_q(n,k,I)$, for prime power q, whose vertices are the k-dimensional subspaces of an n-dimensional vector space over $\mathbb{F}_q$, two vertices joined if the dimension of their intersection lies in the set I.

The general set-up is as before: a maximum clique in $G(n,k,\{0,\ldots,t-1\})$ consists of all k-subspaces containing a t-subspace (if n is large enough), while a maximum coclique is a q-Steiner system (a set of k-subspaces with the property that any t-subspace is contained in a unique member of the collection).

But here we do not have the analogue of Keevash's theorem: there is only one known parameter set with $1 < t < k$, several $S(2,3,13)$s over $\mathbb{F}_2$ constructed by Braun, Etzion, Östergård, Vardy and Wasserman.

So it would be rash to make the analogous conjecture here …

Second problem: random derangements and Latin squares

This problem arises in the study of multiplication groups of loops. Again, I won't give the background.

Given a Latin square of order n (an $n \times n$ array with symbols from $\{1, \ldots, n\}$ so that each symbol occurs once in each row and once in each column), we can normalise by permuting the columns so that the first row is $(1, 2, \ldots, n)$. Then the second row is a derangement of the symbols (a permutation with no fixed points).

For $n = 4$, there are two types of derangements: a cyclic permutation, or the product of two transpositions. In the first case, the two rows can be completed to a Latin square in just two different ways; in the second case, in four ways.

How does the ratio of maximum to minumum number of completions of two rows to a Latin square behave as n increases? We'd like to know that it doesn't grow too fast …

The cases $n = 7, 8$

The values for $n = 7, 8$ are:

$[7]$	6566400
$[5, 2]$	6604800
$[4, 3]$	6543360
$[3, 2, 2]$	6635520

$[8]$	181519810560
$[6, 2]$	182125854720
$[5, 3]$	181364244480
$[4, 2, 2]$	183299604480
$[4, 4]$	182052126720
$[3, 3, 2]$	181813248000
$[2, 2, 2, 2]$	186042286080

Conjecture

The ratio of the maximum to the minimum number of completions of two rows to a Latin square tends very rapidly to 1 *as* $n \to \infty$.

A more general conjecture?

Conjecture

For "suitable", "fairly large" subsets of an $n \times n$ grid, any conflict-free way of filling these positions with symbols has approximately the same number of extensions to a Latin square.

I do not know how to make this conjecture precise. Taking a $2 \times n - 1$ rectangle would not work since we might omit the same symbol in both rows.

However, there should be a result along these lines. For example, it should hold for a $k \times n$ rectangle, where k is not too large compared to n.

Other structures

There are other structures for which similar results may be true. But I have no body of evidence to support either of these. Here, “approximately the same” means that the ratio of the greatest to the smallest number of completions tends rapidly to 1 as $n \to \infty$.

Question

Is it true that, for n even, the number of completions of two disjoint 1*-factors of* K_n *to a* 1*-factorisation is approximately the same for any choice of the two* 1*-factors?*

Question

Is it true that, for n odd, the number of completions of two disjoint Hamiltonian cycles of K_n *to a Hamiltonian decomposition is approximately the same for any choice of the two Hamiltonian cycles?*

Third problem: Sum-free sets

Here is a machine for constructing sum-free sets. We represent a subset of $\mathbb{N}$ by its characteristic function, a zero-one sequence. The machine takes as input an arbitrary sequence ι and outputs a sequence o by the following rule. When it is looking at position n in the output, it first checks whether $n = x + y$ for some x, y with $o(x) = o(y) = 1$; if so, then set $o(n) = 0$, and advance the writing head to $n + 1$; otherwise, copy the next element of ι to o and advance the reading and writing heads. For example, if ι is the all-1 sequence, then o is the characteristic function of the odd numbers.

We define a random sum-free set to be the output produced from a random input sequence (an infinite sequence of tosses of a fair coin).

Complete modular sum-free sets

A subset T of $\mathbb{Z}_n$ (the integers mod n) is a *complete sum-free set mod n* if

- T is sum-free (in the additive group of $\mathbb{Z}_n$);
- if $z \notin T$, then $z = x + y$ for some $x, y \in T$.

Examples include $\{1\} \pmod 2$, and $\{1, 4\} \pmod 5$, and $\{2, 3\} \pmod 5$.

Theorem

If T is a complete sum-free set mod n, then the event that the random sum-free set S lies in the union of the congruence classes in T (mod n) has non-zero probability.

Random sum-free sets

Random sum-free sets S have a rich structure which is not well understood. For example, each of the events "S contains no even numbers" has non-zero probability (approximately 0.218); nothing is known about the properties of this number, and it is known only to three places of decimals. Neil Calkin and I showed that the event "2 is the only even number in S" also has non-zero probability (though much smaller).

A zero-one sequence o is ultimately periodic if there exist N and $d > 0$ such that $o(n) = o(n + d)$ for all $n \geq N$.

Question

Is it true that, with probability 1*, a random sum-free set is contained in an almost-periodic sum-free set?*

Density

Conjecture

(a) *A random sum-free set S almost surely has a density (that is, $\lim_{n\to\infty} |S \cap \{1,\ldots,n\}|/n$ exists with probability 1).*

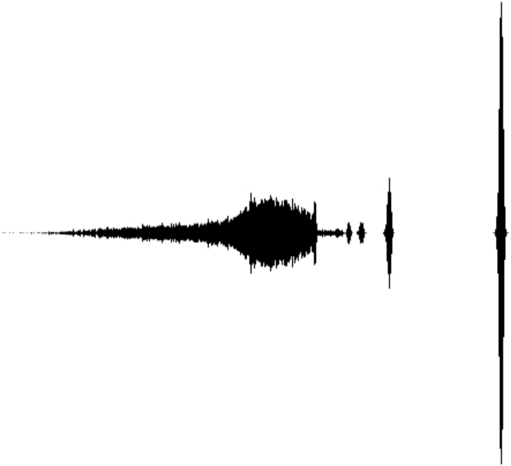
(b) *The density is almost surely positive.*

(c) *The density spectrum is discrete above $1/6$: more precisely, conditioned on density greater than $1/6$, the density is almost surely of the form $k/2(3k-1)$ for some $k \in \mathbb{N}$.*

The displayed densities arise from the complete sum-free set $\{k,\ldots,2k-1\} \pmod{3k-1}$ or transforms of it. For $k = 1$, this is sets of odd numbers; for $k = 2$, sets of integers contained in $\{2,3\} \pmod 5$ or $\{1,4\} \pmod 5$.

A picture

Here is a plot of densities of long finite sum-free sets. The “spectral lines” at 1/4, 1/5 and 3/8 are clearly visible, as is an apparent change of behaviour at 1/6.



Ultimately periodic?

Question

Is it true that the sum-free set machine, given an ultimately periodic input, produces an ultimately periodic output?

Neil Calkin and I did extensive computation on this. For many periodic or ultimately constant inputs, the output is indeed ultimately periodic. But there are a few cases which were tracked for millions of steps without becoming periodic.

We are inclined to conjecture that the answer to the question is "no", but this may be difficult to show.

Related problems

One could ask similar questions for many other types of set (just look among examples considered by Paul Erdős for inspiration!).
This subject is completely open. I have no idea what structure to expect, or what the good problems will be.

Thank you for your attention!