From Higman-Sims to Urysohn: a random walk through groups, graphs, designs, and spaces

Peter J. Cameron

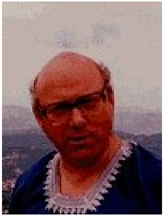
Queen Mary University of London

p.j.cameron@qmul.ac.uk

Ambleside
25 August 2007

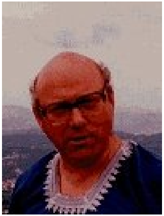
My first reading matter in Oxford

My first reading matter in Oxford

Peter M. Neumann, Leonard L. Scott and Olaf Tamaschke, Primitive permutation groups of degree $3p$, unpublished manuscript.

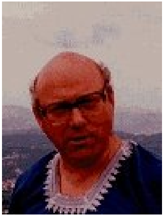
My first reading matter in Oxford

Peter M. Neumann, Leonard L. Scott and Olaf Tamaschke, Primitive permutation groups of degree $3p$, unpublished manuscript.

The group $\mathrm{PSL}(2, 19)$ acts as a primitive permutation group on 57 points.

My first reading matter in Oxford



Peter M. Neumann, Leonard L. Scott and Olaf Tamaschke, Primitive permutation groups of degree $3p$, unpublished manuscript.

The group $\mathrm{PSL}(2, 19)$ acts as a primitive permutation group on 57 points.

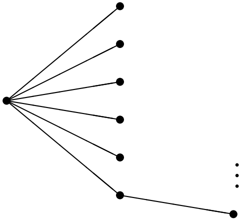
The stabiliser of a point is isomorphic to $\mathrm{PSL}(2, 5)$. It has orbits of sizes $1, 6, 20, 30$, and is 2-transitive on the orbit of size 6.

Orbital graphs

We construct a graph of valency 6 on 57 vertices by joining each point α to the points in the G_α-orbit of size 6.

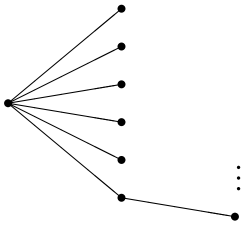
Orbital graphs

We construct a graph of valency 6 on 57 vertices by joining each point α to the points in the G_α-orbit of size 6.



Orbital graphs

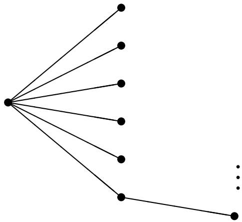
We construct a graph of valency 6 on 57 vertices by joining each point α to the points in the G_α-orbit of size 6.



The automorphism group of the graph is transitive on paths of length 2. So there are no triangles, and the ends of the paths of length 2 starting at α form a single G_α-orbit of size $6 \cdot 5/k$ for some k.

Orbital graphs

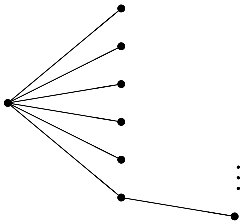
We construct a graph of valency 6 on 57 vertices by joining each point α to the points in the G_α-orbit of size 6.



The automorphism group of the graph is transitive on paths of length 2. So there are no triangles, and the ends of the paths of length 2 starting at α form a single G_α-orbit of size $6 \cdot 5/k$ for some k. Clearly $k = 1$.

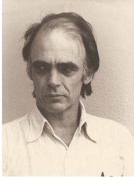
Orbital graphs

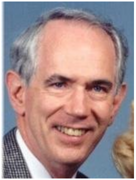
We construct a graph of valency 6 on 57 vertices by joining each point α to the points in the G_α-orbit of size 6.



The automorphism group of the graph is transitive on paths of length 2. So there are no triangles, and the ends of the paths of length 2 starting at α form a single G_α-orbit of size $6 \cdot 5/k$ for some k. Clearly $k = 1$.
Triangle-free graphs with a lot of symmetry will appear very often in this talk!

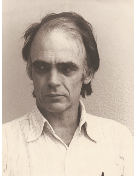
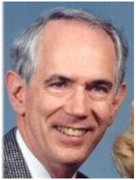
The Higman–Sims group





A better example is the Higman–Sims group.

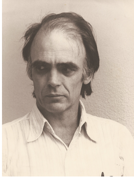
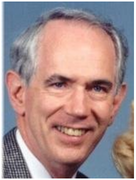
The Higman–Sims group

A better example is the Higman–Sims group.

This is a primitive permutation group on 100 points. The point stabiliser is the Mathieu group M_{22}, having orbits of sizes 1, 22 and 77, and acts 3-transitively on its orbit of size 22.

The Higman–Sims group

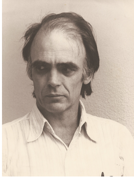
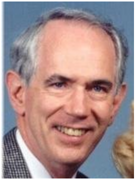




A better example is the Higman–Sims group.

This is a primitive permutation group on 100 points. The point stabiliser is the Mathieu group M_{22}, having orbits of sizes 1, 22 and 77, and acts 3-transitively on its orbit of size 22.

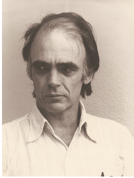
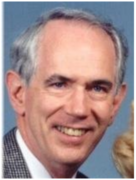
Note that $77 = 22 \cdot 21/6$, so two points at distance 2 in the orbital graph of valency 22 have six common neighbours.

The Higman–Sims group

A better example is the Higman–Sims group.
This is a primitive permutation group on 100 points. The point stabiliser is the Mathieu group M_{22}, having orbits of sizes 1, 22 and 77, and acts 3-transitively on its orbit of size 22.
Note that $77 = 22 \cdot 21/6$, so two points at distance 2 in the orbital graph of valency 22 have six common neighbours.
The Higman–Sims group acts transitively on 3-claws, on 4-cycles, and on paths of length 3 not contained in 4-cycles.

The Higman–Sims group

A better example is the Higman–Sims group.
This is a primitive permutation group on 100 points. The point stabiliser is the Mathieu group M_{22}, having orbits of sizes 1, 22 and 77, and acts 3-transitively on its orbit of size 22.
Note that $77 = 22 \cdot 21/6$, so two points at distance 2 in the orbital graph of valency 22 have six common neighbours.
The Higman–Sims group acts transitively on 3-claws, on 4-cycles, and on paths of length 3 not contained in 4-cycles.
(The graph was constructed earlier by Dale Mesner, who never thought to look at its automorphism group. The group was constructed in a different action by Graham Higman.)

Designs

Take a vertex of the Higman–Sims graph. Call its neighbours points and its non-neighbours blocks; a point is incident with a block if they are adjacent in the graph. The structure D satisfies

Designs

Take a vertex of the Higman–Sims graph. Call its neighbours points and its non-neighbours blocks; a point is incident with a block if they are adjacent in the graph. The structure D satisfies

- there are 22 points;

Designs

Take a vertex of the Higman–Sims graph. Call its neighbours points and its non-neighbours blocks; a point is incident with a block if they are adjacent in the graph. The structure D satisfies

- there are 22 points;
- each block is incident with 6 points;

Designs

Take a vertex of the Higman–Sims graph. Call its neighbours points and its non-neighbours blocks; a point is incident with a block if they are adjacent in the graph. The structure D satisfies

- there are 22 points;
- each block is incident with 6 points;
- any 3 points are incident with a unique block.

Designs

Take a vertex of the Higman–Sims graph. Call its neighbours points and its non-neighbours blocks; a point is incident with a block if they are adjacent in the graph. The structure D satisfies

- there are 22 points;
- each block is incident with 6 points;
- any 3 points are incident with a unique block.

In other words, it is a 3-$(22, 6, 1)$ design, the famous Witt design. (This is how Higman and Sims constructed the graph!)

Designs

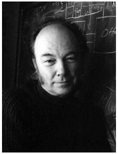
Take a vertex of the Higman–Sims graph. Call its neighbours points and its non-neighbours blocks; a point is incident with a block if they are adjacent in the graph. The structure D satisfies

- there are 22 points;
- each block is incident with 6 points;
- any 3 points are incident with a unique block.

In other words, it is a 3-$(22, 6, 1)$ design, the famous Witt design. (This is how Higman and Sims constructed the graph!)

Note that, if β is a point of the design, then the number of points different from β and the number of blocks incident with β are both 21. In other words, D is an extension of a symmetric design (the projective plane of order 4).

Cameron's Theorem

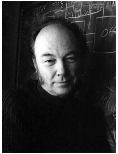
  

Theorem

If a 3-(v, k, λ) design is an extension of a symmetric 2-design then one of the following holds:

- $v = 4(\lambda + 1), k = 2(\lambda + 1)$ (*Hadamard design*);
- $v = (\lambda + 1)(\lambda^2 + 5\lambda + 5), k = (\lambda + 1)(\lambda + 2)$;
- $v = 112, k = 12, \lambda = 1$ (*extension of projective plane of order* 10);
- $v = 496, k = 40, \lambda = 3$.

Cameron's Theorem

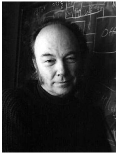

Theorem

If a 3-(v, k, λ) design is an extension of a symmetric 2-design then one of the following holds:

- $v = 4(\lambda + 1), k = 2(\lambda + 1)$ (*Hadamard design*);
- $v = (\lambda + 1)(\lambda^2 + 5\lambda + 5), k = (\lambda + 1)(\lambda + 2)$;
- $v = 112$, $k = 12$, $\lambda = 1$ (*extension of projective plane of order* 10);
- $v = 496$, $k = 40$, $\lambda = 3$.

This is "Cameron's Theorem" in the book *Design Theory* by Hughes and Piper.

Cameron's Theorem

Theorem

If a 3-(v, k, λ) *design is an extension of a symmetric* 2*-design then one of the following holds:*

- $v = 4(\lambda + 1), k = 2(\lambda + 1)$ (*Hadamard design*);
- $v = (\lambda + 1)(\lambda^2 + 5\lambda + 5), k = (\lambda + 1)(\lambda + 2)$;
- $v = 112, k = 12, \lambda = 1$ (*extension of projective plane of order* 10);
- $v = 496, k = 40, \lambda = 3$.

This is "Cameron's Theorem" in the book *Design Theory* by Hughes and Piper.
The only new thing we know now is that there is no projective plane of order 10 (Lam *et al.*).

Fun with permutation groups

Livingstone and Wagner showed that a $(t+1)$-set transitive permutation group of degree $n \geq 2t+1$ is t-set transitive.

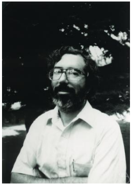
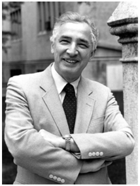
Fun with permutation groups

Livingstone and Wagner showed that a $(t+1)$-set transitive permutation group of degree $n \geq 2t+1$ is t-set transitive.
I showed that such a group is primitive on t-sets, with known exceptions (the most interesting being the Mathieu group M_{24} with $t=4$).

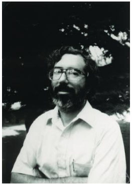
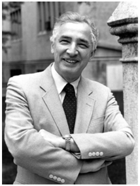
Fun with permutation groups

Livingstone and Wagner showed that a $(t+1)$-set transitive permutation group of degree $n \geq 2t+1$ is t-set transitive.
I showed that such a group is primitive on t-sets, with known exceptions (the most interesting being the Mathieu group M_{24} with $t = 4$).
The proof makes a long detour. First, a counterexample preserves a parallelism of the t-subsets of $\{1, \ldots, n\}$. From this one constructs a symmetric triangle-free graph which is locally like a cube. Then one shows that it is a quotient of a cube by a subspace of $\mathrm{GF}(2)^n$. This subspace turns out to be an extension of a perfect $(t-1)$-error-correcting code; the theorem of van Lint and Tietäväinen identifies the code and hence the group.

The Cameron–Kantor Theorem

The Cameron–Kantor Theorem

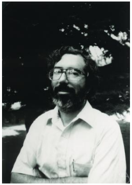
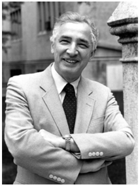
   

In the late 1970s, Bill Kantor and I proved a conjecture of Marshall Hall:

Theorem

A 2-transitive subgroup of $\mathrm{P\Gamma L}(n,q)$ *either contains* $\mathrm{PSL}(n,q)$ *or is* A_7 *inside* $\mathrm{PSL}(4,2) \cong A_8$.

The Cameron–Kantor Theorem

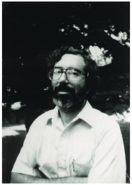
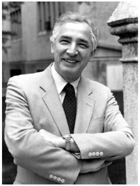

In the late 1970s, Bill Kantor and I proved a conjecture of Marshall Hall:

Theorem

A 2-transitive subgroup of $\mathrm{P\Gamma L}(n,q)$ *either contains* $\mathrm{PSL}(n,q)$ *or is* A_7 *inside* $\mathrm{PSL}(4,2) \cong A_8$.

The proof used a lot of nice geometry, including spreads in projective space and generalised polygons (for which the Feit–Higman theorem applies).

The Cameron–Kantor Theorem

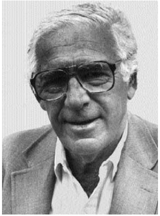
In the late 1970s, Bill Kantor and I proved a conjecture of Marshall Hall:

Theorem

A 2-*transitive subgroup of* $\mathrm{P\Gamma L}(n,q)$ *either contains* $\mathrm{PSL}(n,q)$ *or is* A_7 *inside* $\mathrm{PSL}(4,2) \cong A_8$.

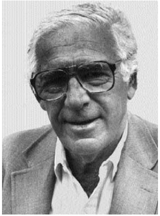
The proof used a lot of nice geometry, including spreads in projective space and generalised polygons (for which the Feit–Higman theorem applies).
But this kind of fun was soon to come to an end!

CFSG



In 1980, the Classification of Finite Simple Groups was announced. The proof was admittedly incomplete (though I think nobody expected it would take a quarter of a century to finish it).

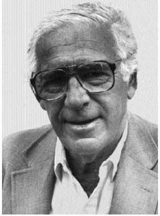
CFSG



In 1980, the Classification of Finite Simple Groups was announced. The proof was admittedly incomplete (though I think nobody expected it would take a quarter of a century to finish it).

But people started using it right away. It has very powerful consequences for the theory of finite permutation groups, some of which appeared in my most cited paper in 1981.

CFSG



In 1980, the Classification of Finite Simple Groups was announced. The proof was admittedly incomplete (though I think nobody expected it would take a quarter of a century to finish it).

But people started using it right away. It has very powerful consequences for the theory of finite permutation groups, some of which appeared in my most cited paper in 1981.

In particular, all 2-transitive groups were now "known" modulo CFSG, so proving theorems like those on the last two slides would no longer bring promotion and pay!

A new direction

A new direction

Livingstone and Wagner had shown that a finite permutation group of degree $n \geq 2t + 1$ which is $(t + 1)$-set transitive is t-set transitive, and is actually t-transitive if $t \geq 5$.

A new direction

Livingstone and Wagner had shown that a finite permutation group of degree $n \geq 2t + 1$ which is $(t + 1)$-set transitive is t-set transitive, and is actually t-transitive if $t \geq 5$.
John McDermott visited Oxford in the 1970s and provoked me into thinking about an infinite version of this result.

A new direction

Livingstone and Wagner had shown that a finite permutation group of degree $n \geq 2t + 1$ which is $(t + 1)$-set transitive is t-set transitive, and is actually t-transitive if $t \geq 5$.
John McDermott visited Oxford in the 1970s and provoked me into thinking about an infinite version of this result.

Theorem

Let G be an infinite permutation group which is t-set transitive for all natural numbers t. Then either

- *G is t-transitive for all natural numbers t; or*
- *there is a linear or circular order preserved or reversed by G.*

An infinite HS-like graph

An infinite HS-like graph

At the British Combinatorial Conference in London in 1977, I talked about (among other things) the Higman–Sims graph.

An infinite HS-like graph

At the British Combinatorial Conference in London in 1977, I talked about (among other things) the Higman–Sims graph. The next time the Conference was held in London, in 1987, I talked about a countably infinite graph with strikingly similar properties. This graph H was discovered by Ward Henson and characterised by Robert Woodrow.

An infinite HS-like graph

At the British Combinatorial Conference in London in 1977, I talked about (among other things) the Higman–Sims graph. The next time the Conference was held in London, in 1987, I talked about a countably infinite graph with strikingly similar properties. This graph H was discovered by Ward Henson and characterised by Robert Woodrow.

- H is triangle-free;
- every finite triangle-free graph is embeddable in H;
- the automorphism group of H is transitive on induced subgraphs of any given isomorphism type (that is, H is homogeneous).

An infinite HS-like graph

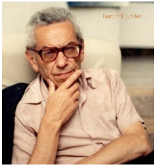
 

At the British Combinatorial Conference in London in 1977, I talked about (among other things) the Higman–Sims graph. The next time the Conference was held in London, in 1987, I talked about a countably infinite graph with strikingly similar properties. This graph *H* was discovered by Ward Henson and characterised by Robert Woodrow.

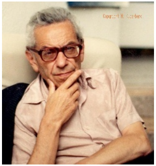
- *H* is triangle-free;
- every finite triangle-free graph is embeddable in *H*;
- the automorphism group of *H* is transitive on induced subgraphs of any given isomorphism type (that is, *H* is homogeneous).

Woodrow showed that, with some trivial exceptions, the first and third properties characterise *H*.

The “random graph”

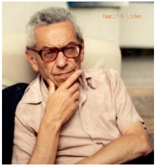


The "random graph"



In fact, there is an even more interesting countable graph R, characterised by Erdős and Rényi and constructed by Rado.

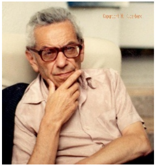
The "random graph"



In fact, there is an even more interesting countable graph R, characterised by Erdős and Rényi and constructed by Rado.

- every finite graph is embeddable in R;
- the automorphism group of H is transitive on induced subgraphs of any given isomorphism type (that is, H is homogeneous).

The "random graph"



In fact, there is an even more interesting countable graph R, characterised by Erdős and Rényi and constructed by Rado.

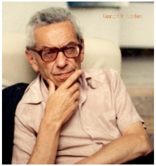
- every finite graph is embeddable in R;
- the automorphism group of H is transitive on induced subgraphs of any given isomorphism type (that is, H is homogeneous).

Erdős and Rényi showed:

Theorem

If a countable random graph is chosen by selecting edges independently with probability $\frac{1}{2}$ from all pairs of vertices, the resulting graph is isomorphic to R with probability 1.

The "random graph"

In fact, there is an even more interesting countable graph R, characterised by Erdős and Rényi and constructed by Rado.

- every finite graph is embeddable in R;
- the automorphism group of H is transitive on induced subgraphs of any given isomorphism type (that is, H is homogeneous).

Erdős and Rényi showed:

Theorem

If a countable random graph is chosen by selecting edges independently with probability $\frac{1}{2}$ from all pairs of vertices, the resulting graph is isomorphic to R with probability 1.

In other words, R is the countable random graph.

Cyclic automorphisms

Henson showed that both the graphs R and H have cyclic automorphisms (permuting all vertices in a single cycle).

Cyclic automorphisms

Henson showed that both the graphs R and H have cyclic automorphisms (permuting all vertices in a single cycle).
Since R is the random graph, we'd like to use random methods to prove this.

Cyclic automorphisms

Henson showed that both the graphs R and H have cyclic automorphisms (permuting all vertices in a single cycle). Since R is the random graph, we'd like to use random methods to prove this.

A graph with a cyclic automorphism is a Cayley graph for $\mathbb{Z}$, say $\mathrm{Cay}(\mathbb{Z}, S \cup (-S))$ for some set S of positive integers; in other words, the vertex set is $\mathbb{Z}$, and we join x and y if and only if $|x - y| \in S$. The cyclic shift $x \mapsto x + 1$ is an automorphism.

Cyclic automorphisms

Henson showed that both the graphs R and H have cyclic automorphisms (permuting all vertices in a single cycle). Since R is the random graph, we'd like to use random methods to prove this.

A graph with a cyclic automorphism is a Cayley graph for $\mathbb{Z}$, say $\mathrm{Cay}(\mathbb{Z}, S \cup (-S))$ for some set S of positive integers; in other words, the vertex set is $\mathbb{Z}$, and we join x and y if and only if $|x - y| \in S$. The cyclic shift $x \mapsto x + 1$ is an automorphism.

Theorem

Choose S at random by including positive integers independently with probability $\frac{1}{2}$. Then, with probability 1, $\mathrm{Cay}(\mathbb{Z}, S \cup (-S)) \cong R$.

Cyclic automorphisms

Henson showed that both the graphs R and H have cyclic automorphisms (permuting all vertices in a single cycle). Since R is the random graph, we'd like to use random methods to prove this.

A graph with a cyclic automorphism is a Cayley graph for $\mathbb{Z}$, say $\mathrm{Cay}(\mathbb{Z}, S \cup (-S))$ for some set S of positive integers; in other words, the vertex set is $\mathbb{Z}$, and we join x and y if and only if $|x-y| \in S$. The cyclic shift $x \mapsto x+1$ is an automorphism.

Theorem

Choose S at random by including positive integers independently with probability $\frac{1}{2}$. Then, with probability 1, $\mathrm{Cay}(\mathbb{Z}, S \cup (-S)) \cong R$.

In other words, R is the random Cayley graph for $\mathbb{Z}$.

Cayley graphs and B-groups

More generally, Ken Johnson and I showed:

Theorem

Let X be a countable group with the property that X cannot be written as the union of finitely many translates of square root sets and a finite set. Then, with probability 1, a random Cayley graph for X is isomorphic to R.

Cayley graphs and B-groups

More generally, Ken Johnson and I showed:

Theorem

Let X be a countable group with the property that X cannot be written as the union of finitely many translates of square root sets and a finite set. Then, with probability 1*, a random Cayley graph for X is isomorphic to R.*

A B-group is a group X with the property that any primitive group G which contains X acting regularly is 2-transitive. Burnside and Schur showed that an cyclic group of prime power, non-prime order is a B-group.

Cayley graphs and B-groups

More generally, Ken Johnson and I showed:

Theorem

Let X be a countable group with the property that X cannot be written as the union of finitely many translates of square root sets and a finite set. Then, with probability 1, a random Cayley graph for X is isomorphic to R.

A B-group is a group X with the property that any primitive group G which contains X acting regularly is 2-transitive. Burnside and Schur showed that an cyclic group of prime power, non-prime order is a B-group.

Problem

Is there a countable B-group?

Cayley graphs and B-groups

More generally, Ken Johnson and I showed:

Theorem

Let X be a countable group with the property that X cannot be written as the union of finitely many translates of square root sets and a finite set. Then, with probability 1, a random Cayley graph for X is isomorphic to R.

A B-group is a group X with the property that any primitive group G which contains X acting regularly is 2-transitive. Burnside and Schur showed that an cyclic group of prime power, non-prime order is a B-group.

Problem

Is there a countable B-group?

Corollary

A countable group satisfying the conditions of the theorem above is not a B-group.

Cyclic automorphisms of H

let S be a set of positive integers. Then $\mathrm{Cay}(\mathbb{Z}, S \cup (-S))$ is triangle-free if and only if S is sum-free, that is, $x, y \in S \Rightarrow x + y \notin S$.

Cyclic automorphisms of H

let S be a set of positive integers. Then $\mathrm{Cay}(\mathbb{Z}, S \cup (-S))$ is triangle-free if and only if S is sum-free, that is, $x, y \in S \Rightarrow x + y \notin S$.

Call a sum-free set S sf-universal if $\mathrm{Cay}(\mathbb{Z}, S \cup (-S)) \cong H$.

Cyclic automorphisms of H

let S be a set of positive integers. Then $\mathrm{Cay}(\mathbb{Z}, S \cup (-S))$ is triangle-free if and only if S is sum-free, that is, $x, y \in S \Rightarrow x + y \notin S$.

Call a sum-free set S sf-universal if $\mathrm{Cay}(\mathbb{Z}, S \cup (-S)) \cong H$. This can be phrased otherwise: any pattern of membership in S of an interval in $\mathbb{N}$, which is not obviously excluded, occurs in S.

Cyclic automorphisms of H

let S be a set of positive integers. Then $\mathrm{Cay}(\mathbb{Z}, S \cup (-S))$ is triangle-free if and only if S is sum-free, that is, $x, y \in S \Rightarrow x + y \notin S$.

Call a sum-free set S sf-universal if $\mathrm{Cay}(\mathbb{Z}, S \cup (-S)) \cong H$. This can be phrased otherwise: any pattern of membership in S of an interval in $\mathbb{N}$, which is not obviously excluded, occurs in S.

Theorem

Almost every sum-free set (in the sense of Baire category) is sf-universal.

Cyclic automorphisms of H

let S be a set of positive integers. Then $\mathrm{Cay}(\mathbb{Z}, S \cup (-S))$ is triangle-free if and only if S is sum-free, that is, $x, y \in S \Rightarrow x + y \notin S$.

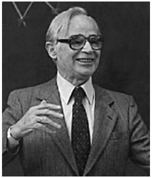
Call a sum-free set S sf-universal if $\mathrm{Cay}(\mathbb{Z}, S \cup (-S)) \cong H$. This can be phrased otherwise: any pattern of membership in S of an interval in $\mathbb{N}$, which is not obviously excluded, occurs in S.

Theorem

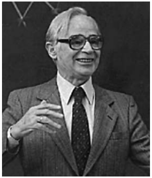
Almost every sum-free set (in the sense of Baire category) is sf-universal.

So H has many cyclic automorphisms.

Combinatorial number theory

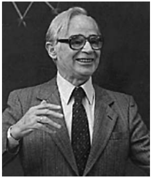
  

Combinatorial number theory



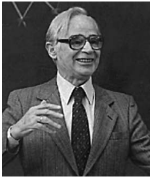
Van der Waerden's theorem states that, if $\mathbb{N}$ is partitioned into finitely many classes, then some class contains arbitrarily long arithmetic progressions.

Combinatorial number theory

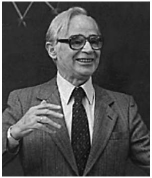
Van der Waerden's theorem states that, if $\mathbb{N}$ is partitioned into finitely many classes, then some class contains arbitrarily long arithmetic progressions.
Szemerédi proved a "density" version of this theorem: a set of natural numbers which does *not* contain arbitrarily long arithmetic progressions must have density zero.

Combinatorial number theory

Van der Waerden's theorem states that, if $\mathbb{N}$ is partitioned into finitely many classes, then some class contains arbitrarily long arithmetic progressions.
Szemerédi proved a "density" version of this theorem: a set of natural numbers which does *not* contain arbitrarily long arithmetic progressions must have density zero.
Schur's theorem states that, if $\mathbb{N}$ is partitioned into finitely many classes, then some class is not sum-free.

Combinatorial number theory

Van der Waerden's theorem states that, if $\mathbb{N}$ is partitioned into finitely many classes, then some class contains arbitrarily long arithmetic progressions.
Szemerédi proved a "density" version of this theorem: a set of natural numbers which does *not* contain arbitrarily long arithmetic progressions must have density zero.
Schur's theorem states that, if $\mathbb{N}$ is partitioned into finitely many classes, then some class is not sum-free.
There is no density version of Schur's theorem. The odd numbers have density $\frac{1}{2}$ and clearly form a sum-free set.

But what if . . . ?

Maybe there is almost a density version of Schur's Theorem.

But what if . . . ?

Maybe there is almost a density version of Schur's Theorem.

Problem

Prove that a sf-universal set has density zero.

But what if . . . ?

Maybe there is almost a density version of Schur's Theorem.

Problem

Prove that a sf-universal set has density zero.

This would imply that almost all sum-free sets (in the sense of Baire category) have density zero.

But what if . . . ?

Maybe there is almost a density version of Schur's Theorem.

Problem

Prove that a sf-universal set has density zero.

This would imply that almost all sum-free sets (in the sense of Baire category) have density zero.
What happens if we use measure instead of category?

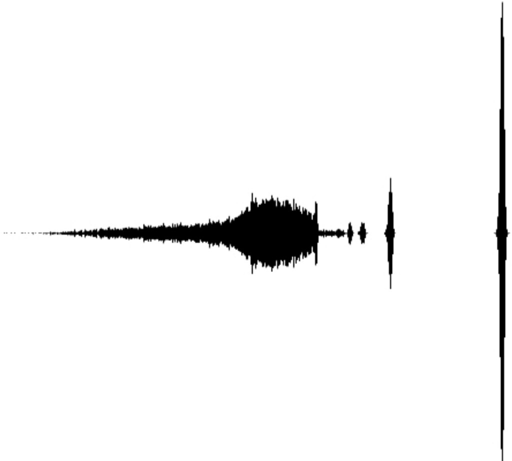
Random sum-free sets

Choose S by considering the natural numbers in turn. When considering n, if $n = x + y$ with $x, y \in S$, then $n \notin S$; otherwise toss a fair coin to decide.

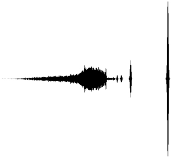
Random sum-free sets

Choose S by considering the natural numbers in turn. When considering n, if $n = x + y$ with $x, y \in S$, then $n \notin S$; otherwise toss a fair coin to decide.

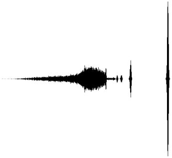
Experimentally, the density of a large random sum-free set looks like this:



Sum-free sets

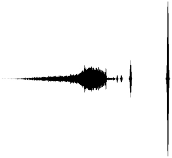


Sum-free sets



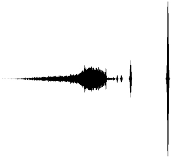
The probability that a random sum-free set consists entirely of odd numbers is non-zero (roughly 0.218 . . .).

Sum-free sets



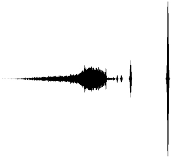
The probability that a random sum-free set consists entirely of odd numbers is non-zero (roughly $0.218\ldots$).
Almost all sum-free sets consisting of odd numbers have density $\frac{1}{4}$. This explains the big spike on the right of the picture.

Sum-free sets



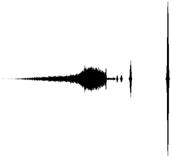
The probability that a random sum-free set consists entirely of odd numbers is non-zero (roughly $0.218\ldots$).
Almost all sum-free sets consisting of odd numbers have density $\frac{1}{4}$. This explains the big spike on the right of the picture.
The next spike comes from sets all of whose elements are congruent to 1 or 4 mod 5, or to 2 or 3 mod 5 (these almost all have density $\frac{1}{5}$. Then come $\{1, 4, 7\}$ mod 8 and $\{3, 4, 5\}$ mod 8, with density $\frac{3}{16}$; and so on.

Sum-free sets



The probability that a random sum-free set consists entirely of odd numbers is non-zero (roughly $0.218\ldots$).
Almost all sum-free sets consisting of odd numbers have density $\frac{1}{4}$. This explains the big spike on the right of the picture.
The next spike comes from sets all of whose elements are congruent to 1 or 4 mod 5, or to 2 or 3 mod 5 (these almost all have density $\frac{1}{5}$. Then come $\{1,4,7\}$ mod 8 and $\{3,4,5\}$ mod 8, with density $\frac{3}{16}$; and so on.
But that is not all. Neil Calkin and I showed that the event that 2 is the only even number in a random sum-free set has positive (though quite small) probability. There are other similar sets with positive probability.

Sum-free sets



The probability that a random sum-free set consists entirely of odd numbers is non-zero (roughly $0.218\ldots$).

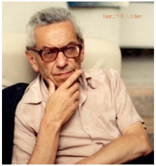
Almost all sum-free sets consisting of odd numbers have density $\frac{1}{4}$. This explains the big spike on the right of the picture.

The next spike comes from sets all of whose elements are congruent to 1 or 4 mod 5, or to 2 or 3 mod 5 (these almost all have density $\frac{1}{5}$. Then come $\{1,4,7\}$ mod 8 and $\{3,4,5\}$ mod 8, with density $\frac{3}{16}$; and so on.

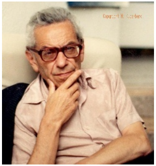
But that is not all. Neil Calkin and I showed that the event that 2 is the only even number in a random sum-free set has positive (though quite small) probability. There are other similar sets with positive probability.

Maybe the density spectrum has a continuous part???

Erdős number 1

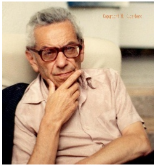


Erdős number 1



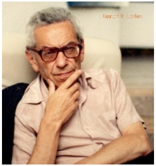
How many sum-free subsets of $\{1, \ldots, n\}$ are there?

Erdős number 1

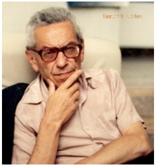
How many sum-free subsets of $\{1, \ldots, n\}$ are there?
Paul Erdős and I conjectured that the number is asymptotically $c_e 2^{n/2}$ or $c_o 2^{n/2}$ as $n \to \infty$ through even or odd values respectively. Moreover, almost all of these sets either consist of odd numbers, or contain no member smaller than $n/3$.

Erdős number 1



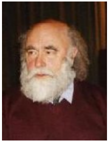

How many sum-free subsets of $\{1, \ldots, n\}$ are there?
Paul Erdős and I conjectured that the number is asymptotically $c_e 2^{n/2}$ or $c_o 2^{n/2}$ as $n \to \infty$ through even or odd values respectively. Moreover, almost all of these sets either consist of odd numbers, or contain no member smaller than $n/3$.
This conjecture was proved by Ben Green, and independently by Sasha Sapozhenko.

Erdős number 1

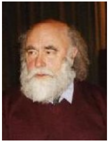
 

How many sum-free subsets of $\{1, \ldots, n\}$ are there?
Paul Erdős and I conjectured that the number is asymptotically $c_e 2^{n/2}$ or $c_o 2^{n/2}$ as $n \to \infty$ through even or odd values respectively. Moreover, almost all of these sets either consist of odd numbers, or contain no member smaller than $n/3$.
This conjecture was proved by Ben Green, and independently by Sasha Sapozhenko.
The numbers $c_e \approx 6.0$ and $c_o \approx 6.8$ are two of "Cameron's sum-free set constants" in Steven Finch's book *Mathematical Constants*.

The Urysohn space

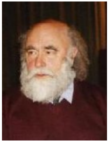


The Urysohn space

In 2000 I lectured about the random graph at the ECM in Barcelona. Anatoly Vershik came to my talk. Afterwards he told me about the Urysohn metric space.

The Urysohn space

In 2000 I lectured about the random graph at the ECM in Barcelona. Anatoly Vershik came to my talk. Afterwards he told me about the Urysohn metric space.

A Polish space is a complete separable metric space. In a posthumous paper in 1927, Urysohn proved:

Theorem

There is a Polish space $\mathbb{U}$ *with the properties*

- $\mathbb{U}$ *is universal (it contains an isometric copy of every Polish space);*
- $\mathbb{U}$ *is homogeneous (any isometry between finite subsets of* $\mathbb{U}$ *can be extended to an isometry of the whole space).*

Moreover, a space with these properties is unique up to isometry.

Metric spaces

A graph of diameter 2 is the same as a metric space in which the metric takes only the values 1 and 2. The graph R is the unique countable homogeneous metric space with these properties.

Metric spaces

A graph of diameter 2 is the same as a metric space in which the metric takes only the values 1 and 2. The graph R is the unique countable homogeneous metric space with these properties.

By the same methods we can construct countable universal homogeneous metric spaces with other sets of values of the metric:

Metric spaces

A graph of diameter 2 is the same as a metric space in which the metric takes only the values 1 and 2. The graph R is the unique countable homogeneous metric space with these properties.

By the same methods we can construct countable universal homogeneous metric spaces with other sets of values of the metric:

- $\{1, 2, \ldots, d\}$ for any $d \geq 2$;

Metric spaces

A graph of diameter 2 is the same as a metric space in which the metric takes only the values 1 and 2. The graph R is the unique countable homogeneous metric space with these properties.

By the same methods we can construct countable universal homogeneous metric spaces with other sets of values of the metric:

- $\{1, 2, \ldots, d\}$ for any $d \geq 2$;
- the positive integers;

Metric spaces

A graph of diameter 2 is the same as a metric space in which the metric takes only the values 1 and 2. The graph R is the unique countable homogeneous metric space with these properties.

By the same methods we can construct countable universal homogeneous metric spaces with other sets of values of the metric:

- $\{1, 2, \ldots, d\}$ for any $d \geq 2$;
- the positive integers;
- the positive rationals.

Metric spaces

A graph of diameter 2 is the same as a metric space in which the metric takes only the values 1 and 2. The graph R is the unique countable homogeneous metric space with these properties.

By the same methods we can construct countable universal homogeneous metric spaces with other sets of values of the metric:

- $\{1, 2, \ldots, d\}$ for any $d \geq 2$;
- the positive integers;
- the positive rationals.

In the first two cases we can modify the construction to produce the analogue of Henson's graph (i.e. no equilateral triangles with side 1), or a bipartite graph (all triangles have even perimeter).

Problem

What are the countable homogeneous metric spaces?

The Urysohn space

The Urysohn space $\mathbb{U}$ can be defined to be the completion of the countable homogeneous universal rational metric space. Despite different language, this is not so different from Urysohn's original construction.

The Urysohn space

The Urysohn space $\mathbb{U}$ can be defined to be the completion of the countable homogeneous universal rational metric space. Despite different language, this is not so different from Urysohn's original construction.

Vershik showed that "almost all" Polish spaces are isomorphic to $\mathbb{U}$, in each of two senses. A Polish space is the completion of a countable metric space, and the latter can be constructed by adding points one at a time, so the notions of Baire category and measure can both be applied to the product space. Now $\mathbb{U}$ is residual in the sense of Baire category, and is the random Polish space for any of a wide variety of measures on the set of possible points that can be added at each stage.

Isometries of $\mathbb{U}$

Any isometry of the universal rational metric space $Q\mathbb{U}$ can be extended to an isometry of its completion $\mathbb{U}$.

Isometries of $\mathbb{U}$

Any isometry of the universal rational metric space $Q\mathbb{U}$ can be extended to an isometry of its completion $\mathbb{U}$.

There is an isometry σ of $Q\mathbb{U}$ permuting all its points in a single cycle (analogous to the cyclic automorphism of the random graph).

Isometries of $\mathbb{U}$

Any isometry of the universal rational metric space $Q\mathbb{U}$ can be extended to an isometry of its completion $\mathbb{U}$.

There is an isometry σ of $Q\mathbb{U}$ permuting all its points in a single cycle (analogous to the cyclic automorphism of the random graph).
The isometry of $\mathbb{U}$ induced by σ has the property that all its orbits are dense.

Isometries of $\mathbb{U}$

Any isometry of the universal rational metric space $Q\mathbb{U}$ can be extended to an isometry of its completion $\mathbb{U}$.

There is an isometry σ of $Q\mathbb{U}$ permuting all its points in a single cycle (analogous to the cyclic automorphism of the random graph).
The isometry of $\mathbb{U}$ induced by σ has the property that all its orbits are dense.

Problem

What other countable groups have this property?

Isometries of $\mathbb{U}$

Any isometry of the universal rational metric space $Q\mathbb{U}$ can be extended to an isometry of its completion $\mathbb{U}$.

There is an isometry σ of $Q\mathbb{U}$ permuting all its points in a single cycle (analogous to the cyclic automorphism of the random graph).
The isometry of $\mathbb{U}$ induced by σ has the property that all its orbits are dense.

Problem

What other countable groups have this property?

All we know is that the elementary abelian 2-group has this property but the elementary abelian 3-group does not.

Abelian group structure of $\mathbb{U}$

The closure of $\langle \sigma \rangle$ is an abelian group acting transitively on $\mathbb{U}$ (so $\mathbb{U}$ has an abelian group structure).

Abelian group structure of $\mathbb{U}$

The closure of $\langle \sigma \rangle$ is an abelian group acting transitively on $\mathbb{U}$ (so $\mathbb{U}$ has an abelian group structure).
There are many such σ, and so the abelian group structure of $\mathbb{U}$ is not canonical.

Abelian group structure of $\mathbb{U}$

The closure of $\langle \sigma \rangle$ is an abelian group acting transitively on $\mathbb{U}$ (so $\mathbb{U}$ has an abelian group structure).
There are many such σ, and so the abelian group structure of $\mathbb{U}$ is not canonical.

Problem

What isomorphism types of abelian groups can occur as the closure of $\langle \sigma \rangle$?

Abelian group structure of $\mathbb{U}$

The closure of $\langle \sigma \rangle$ is an abelian group acting transitively on $\mathbb{U}$ (so $\mathbb{U}$ has an abelian group structure).
There are many such σ, and so the abelian group structure of $\mathbb{U}$ is not canonical.

Problem

What isomorphism types of abelian groups can occur as the closure of $\langle \sigma \rangle$*?*

The closure of the countable elementary abelian 2-group with dense orbits is an elementary abelian 2-group acting transitively on U.