

Sum-free sets and shift automorphisms

Peter J. Cameron



p.j.cameron@qmul.ac.uk

Workshop on Graphs and Asynchronous Systems, 20 May 2008

Cayley graphs

Let G be a group. A *Cayley graph* for G is a graph with vertex set G admitting G (acting by right multiplication) as a group of automorphisms.

Equivalently, it has edge set $\{\{g, sg\} : g \in G, s \in S\}$, where $S = S^{-1}$ (to make it undirected) and $1 \notin S$ (to forbid loops).

We denote this graph by $\text{Cay}(G, S)$.

Sometimes it is assumed that S generates G (equivalently, the graph is connected), but this is not necessarily the case here.

Shift graphs

These are Cayley graphs for the infinite cyclic group \mathbb{Z} . By abuse of notation, we let S denote the set of positive elements in the connection set, and write $\Gamma(S)$ for the graph $\text{Cay}(\mathbb{Z}, S \cup (-S))$.

Thus, $x \sim y$ in $\Gamma(S)$ if and only if $|x - y| \in S$, where $S \subseteq \mathbb{N}$.

The graph $\Gamma(S)$ has a distinguished shift automorphism, the map $x \mapsto x + 1$.

It is easy to show that, if $\Gamma(S)$ is isomorphic to $\Gamma(S')$, then the two corresponding shift automorphisms of this graph are conjugate (in the automorphism group of Γ) if and only if $S = S'$.

The random graph

The following remarkable theorem was proved by Erdős and Rényi in 1963.

Theorem 1. *There is a countable graph R such that, if a random graph X on a fixed countable vertex set is given by selecting edges independently with probability $1/2$, then $\text{Prob}(X \cong R) = 1$.*

Their proof was non-constructive, though explicit constructions are known. I will give one below.

Measure and category

Two familiar techniques for non-constructive existence proofs are:

- Show that the set of all objects is a measure space, in which the “interesting” objects form a set of full measure. (Often the space has measure 1, and the argument can be phrased in terms of probability. This is the case in the Erdős–Rényi theorem.)
- Show that the set of all objects is a complete metric space, in which the interesting sets form a residual set, in the sense of Baire category (the complement of a set of the first category – that is, a set which contains a countable intersection of open dense sets).

In the Erdős–Rényi Theorem, either measure or category can be used: the graph R has measure 1 and is residual in the space of all graphs.

A cautionary tale

The set of all binary sequences is a probability space (recording the outcome of a sequence of coin

tosses) and a metric space (where the distance between two sequences is $1/2^n$ if they first differ in the n th position).

By the Law of Large Numbers, almost all sequences (in the sense of measure) have density $1/2$.

However, sequences with upper density 1 and lower density 0 form a residual set.

Measure and category do agree that almost all sequences are universal (see next slide).

Universal sets

A binary sequence s is *universal* if every finite binary sequence σ occurs as a consecutive subsequence of s (i.e. there exists N such that $s_{N+i} = \sigma_i$ for $i = 0, \dots, l(\sigma) - 1$).

The set of universal sequences has measure 1 and is residual.

A binary sequence is the characteristic function of a subset $S \subseteq \mathbb{N}$. We will say that the set S is *universal* if its characteristic function is universal.

R as shift graph

Proposition 2. For $S \subseteq \mathbb{N}$, the graph $\Gamma(S)$ is isomorphic to R if and only if S is universal.

This shows that almost all shift graphs (in the sense of either measure or category) are isomorphic to R . In addition, since sets of full measure or residual sets have cardinality 2^{\aleph_0} , it follows:

Corollary 3. The graph R has 2^{\aleph_0} cyclic automorphisms, pairwise not conjugate in $\text{Aut}(R)$.

This also gives us an explicit construction of R , by taking an explicit universal set (for example, concatenate the base 2 representations of the natural numbers).

R as Cayley graph

Thus a random Cayley graph for \mathbb{Z} is almost surely R . The same holds for a much wider class of countable groups.

In a group X , a *square-root set* is a set of the form

$$\sqrt{a} = \{x \in X : x^2 = a\};$$

it is *non-principal* if $a \neq 1$.

Theorem 4. Let X be a countable group which is not the union of finitely many translates of non-principal square-root sets. Then the set of Cayley graphs for X which are isomorphic to R is residual and has measure 1.

Many (but not all) countable groups satisfy this condition. For example, in \mathbb{Z} , any element has at most one square root.

Countable homogeneous graphs

A graph Γ is *homogeneous* if every isomorphism between finite (induced) subgraphs of Γ extends to an automorphism of Γ . (An induced subgraph is a subset of Γ in which both edges and nonedges are the same as in Γ .)

The *age* of a graph Γ is the class of all finite graphs embeddable in Γ (as induced subgraphs).

A theorem of Fraïssé shows that there is at most one countable homogeneous graph with any given age.

Fraïssé's Theorem also gives a necessary and sufficient condition on a class to be the age of a countable homogeneous graph. The crucial condition is the *amalgamation property*: if two elements of the age have isomorphic substructures, they can be glued together along these substructures inside some structure in the age.

The theorem of Lachlan and Woodrow

Theorem 5. A countably infinite homogeneous graph is one of the following:

- a disjoint union of complete graphs of the same size;
- complement of the preceding;
- the unique countable homogeneous graph whose age is the class of finite K_n -free graphs for $n \geq 3$ (this is the Henson graph H_n);
- complement of the preceding;
- the random graph R .

The first two classes are not very interesting!

Cyclic automorphisms of Henson's graphs

Henson showed that H_3 admits cyclic shifts but H_n does not for $n > 3$.

Is H_3 the random triangle-free Cayley graph for \mathbb{Z} ?

Note that the Cayley graph $\Gamma(S)$ is triangle-free if and only if S is *sum-free*, that is, $x, y \in S \Rightarrow x + y \notin S$. For $x, y, x + y \in S$ if and only if $\{0, x, x + y\}$ is a triangle in $\Gamma(S)$.

This leads us to the following definition:

Sum-free sets and sf-universal sets

A subset S of \mathbb{N} is *sf-universal* if and only if

- S is sum-free;
- for any finite binary sequence σ , either
 - there exist $i < j$ with $\sigma_i = \sigma_j = 1$ and $j - i \in S$; or
 - σ occurs as a consecutive subsequence of the characteristic function of S .

In other words, S is a sum-free set in which every subsequence not forbidden by the sum-free condition actually occurs somewhere.

sf-universal sets and Henson's graph

Proposition 6. $\Gamma(S) \cong H_3$ if and only if S is *sf-universal*.

Proposition 7. The *sf-universal* sets are residual in the class of *sum-free* sets.

So H_3 is the generic cyclic triangle-free graph in the sense of Baire category.

What about measure?

Random sum-free sets

There is a simple measure for sum-free sets:

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

The first surprise is that we do not obtain an *sf-universal* set almost surely:

Proposition 8. The probability that S consists entirely of odd numbers is non-zero (it is about 0.218).

Conditioned on S consisting of odd numbers, it is almost surely of the form $2S' + 1$, where S' is universal; that is, $\Gamma(S)$ is almost surely the universal bipartite graph.

Why?

If we are constructing a random sum-free set S and have no even numbers in a long initial segment, then the odd numbers in the segment are random, and so the next even number has high probability of being excluded; but the next odd number still has probability 1/2 of being included.

However, the pattern can change. For example, suppose that we chose 1 and 3 but not 5 or 7. Then we might choose 8 and 10, and the event that all subsequent numbers are congruent to 1, 3, 8 or 10 mod 11 has positive probability.

Other events with positive measure

A subset T of $\mathbb{Z}/(n)$ is *complete sum-free* if it is sum-free, and if for any $z \notin T$ there exist $x, y \in T$ such that $z = x + y$. For example, $\{2, 3\} \bmod 5$ is complete sum-free; so is the set $\{1, 3, 8, 10\} \bmod 11$ we saw on the last slide.

Proposition 9. The probability that S is contained in the set of congruence classes corresponding to a fixed complete sum-free set mod n is strictly positive.

Proposition 10. $\text{Prob}(2 \text{ is the only even number in } S) > 0$.

The last two results have a common generalisation. The class of sum-free sets which fall into a complete sum-free set mod n after some point also has positive probability.

What else?

But it is unlikely that we have yet caught almost all sum-free sets!

Conjecture 1. $\text{Prob}(S \text{ is } sf\text{-universal}) = 0$.

It is not feasible to go on finding classes with positive probability and adding up the probabilities until we get everything! The probability of getting a set of odd numbers is only known to three decimal places.

How many sum-free subsets of $\{1, \dots, n\}$?

There are $2^{\lceil n/2 \rceil}$ sets consisting of odd numbers.

There are the same number of subsets of $\{\lceil n/2 \rceil, \dots, n\}$. These two classes have only a small overlap.

This is more or less all:

Theorem 11. *The number of sum-free subsets of $\{1, \dots, n\}$ is asymptotically $c_e 2^{n/2}$ or $c_o 2^{n/2}$ as $n \rightarrow \infty$ through even or odd values. Almost all of them are either sets of odd numbers or have smallest element at least $n/2 - w(n)$, for any $w(n) \rightarrow \infty$ as $n \rightarrow \infty$.*

This was conjectured by Paul Erdős and me, and proved by Ben Green and independently by Sasha Sapozhenko.

Note that the other sets of positive measure that we saw do not contribute asymptotically.

Completing the square

A subset of \mathbb{N} is AP-free if it fails to contain arbitrarily long arithmetic progressions.

Theorem 12. • (Schur) \mathbb{N} cannot be partitioned into finitely many sum-free sets.

- (van der Waerden) \mathbb{N} cannot be partitioned into finitely many AP-free sets.
- (Szemerédi) An AP-free set must have density zero.

The “fourth statement” is false, since the odd numbers are sum-free and have density 1/2. But perhaps almost all sum-free sets have density zero ...

Density

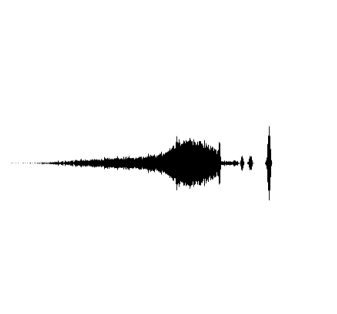
Conjecture 2. *The density of a sf-universal set is zero.*

Since almost all sum-free sets are sf-universal (in the sense of Baire category), this would be a substitute for the missing “density version” of Schur’s Theorem.

Direct constructions of sf-universal sets always proceed by allowing longer and longer empty gaps between the small pieces where the action is, and so have density zero.

Density of a random sum-free set

Empirically the density of a random sum-free set has spectrum like this:



The sets of odd numbers, and of subsets of $\{2, 3\}$ or $\{1, 4\} \pmod 5$, are clearly visible.

Perhaps the density is discrete above 1/6 but has a continuous part to its distribution below this value ...

Henson’s graphs as Cayley graphs

Henson’s triangle-free graph H_3 , like R , is a Cayley graph for a fairly large class of countable groups.

For $n > 3$, we observed that H_n is not a Cayley graph for \mathbb{Z} . More generally, it is not a normal Cayley graph for any countable group X (this is a graph invariant under left and right multiplication; equivalently, one in which the connection set S is closed under conjugation).

Problem 1. *Is H_n a Cayley graph for $n > 3$?*

Cyclic metric spaces

There are many homogeneous metric spaces (those for which any isometry between finite subsets extends to a global isometry), and no classification.

Among these are countable universal metric spaces for the following sets of values of the metric:

- all positive integers up to k , for some fixed k ;
- all positive integers;
- all positive rational numbers.

The first for $k = 2$ is the random graph (distance 1 is adjacency, distance 2 non-adjacency); this has a cyclic shift automorphism. It is not known whether there is such an automorphism for $k > 2$.

The second and third types do have cyclic shift automorphisms.

The Urysohn space

There is a unique (up to isometry) homogeneous universal *Polish space* (complete separable metric space), the celebrated *Urysohn space*.

Note that interesting Polish spaces cannot be countable; separability replaces countability here.

The Urysohn space is the completion of the countable homogeneous universal metric space with rational distances. (This space is sometimes called the “rational Urysohn space”.)

Anatoly Vershik has shown that the Urysohn space is the “random Polish space” (in a fairly general sense) and also the “residual Polish space”.

Cyclic shifts of the Urysohn space

The cyclic shift of the rational Urysohn space extends to an isometry of the (real) Urysohn space all of whose orbits are dense.

The closure of the group it generates is an Abelian group acting transitively on the points of the Urysohn space. So this space has an Abelian group structure (indeed many such structures).

It is not known which isomorphism types of Abelian groups can act transitively on the Urysohn space. The Abelian group of exponent 2 can, while that of exponent 3 cannot. As a special case, it is not known which isomorphism types arise as closures of cyclic shifts of the rational Urysohn space.