Paradoxical decompositions, amenability and random walks on groups

Richard Sharp
University of Warwick

Warwick Maths Society

23 October 2025

The Banach–Tarski Paradox

The most famous example of a paradoxical decomposition:

Let B be the closed unit ball in three dimensions:

$$B = \{(x, y, z) \in \mathbb{R}^3 : x^2 + y^2 + z^2 \leq 1\}.$$

We can split B into a finite number of disjoint pieces and move them around using Euclidean motions (combinations of rotations and translations) to obtain two copies of B.

The Banach–Tarski Paradox

More formally: there exist sets $B_i \subset B$ and Euclidean motions T_i, $i = 1, \ldots, m, \ldots, m+n$ such that:

- $B_i \cap B_j = \varnothing$ whenever $i \neq j$
- $$\bigcup_{i=1}^{m+n} B_i = B$$
- $$\bigcup_{i=1}^{m} T_i(B_i) = B \quad \text{and} \quad \bigcup_{i=m+1}^{m+n} T_i(B_i) = B$$

Letting $E(3)$ denote the group of three-dimensional Euclidean motions, say that B is $E(3)$-paradoxical.

A nice book

Leonard M. Wapner, *The Pea and the Sun: A Mathematical Paradox*, A. K. Peters/CRC Press, 2005.

The Pea and the Sun?

Another version of the Banach–Tarski Paradox says that a very small ball in $\mathbb{R}^3$, say the size of a pea, may be split into a finite number of disjoint pieces, which can be moved by Euclidean motions to give a very large ball, say the size of the sun.

The Universal Dictionary

(From Ian Stewart, *From Here to Infinity*, OUP, 1996, via Louis Wapner, *The Tea and the Sun*. Stewart calls it the *Hyperwebster*.)

It is the future. The Universal Publishing Company has decided to publish a dictionary that contains all possible words that can be formed from the letters $a, b, \ldots, z$. There will be 26 volumes, arranged so that volume a contains all words starting with a, etc.

But just as they are getting ready to publish, the accountants report some financial problems. Looking for a way to cut costs, they decide they can omit the first letter from each word, as it already appears in the volume title.

Carrying out this procedure, they find that all the volumes now have the same content and that each has the same content as the original dictionary!

Objection!

There is an obvious objection to the Banach–Tarski Paradox. The volume of sets in $\mathbb{R}^3$ is invariant under Euclidean motions. Furthermore, the volume of a disjoint union of sets is the sum of the volumes. So why don't we get the following contradiction?

$$\mathrm{Vol}(B) = \sum_{i=1}^{m+n} \mathrm{Vol}(B_i) = \sum_{i=1}^{m+n} \mathrm{Vol}(T_i(B_i)) = \mathrm{Vol}(B) + \mathrm{Vol}(B)$$

The problem is that assigning size to sets is more complicated than it seems ...

Finitely Additive Measures

To use technical language, a *finitely additive measure* on a collection $\mathcal{A}$ of subsets of a set X is a function $m : \mathcal{A} \to \mathbb{R}_{\geq 0} \cup \{+\infty\}$ such that

- $m(\varnothing) = 0$;
- if $A_1, \dots, A_k$ are pairwise disjoint sets in $\mathcal{A}$ then

$$m(A_1 \cup \cdots \cup A_k) = m(A_1) + \cdots + m(A_k).$$

Tarski's Theorem

Tarski showed the the Banach–Tarski Paradox is equivalent to the following statement:

There is no finitely additive measure m defined on **all** the subsets of $\mathbb{R}^3$ which is $E(3)$-invariant and which has $m(B) = 1$.

(In particular, volume does not give a finitely additive measure defined on *all* subsets of $\mathbb{R}^3$.)

Groups

On an earlier slide we used the term *group* of Euclidean motions. Groups turn out to be very important in this story, so let's define them.

A group is a set G together with an operation $\cdot$ that allows us to "multiply" two elements, with the following properties:

- if $g_1, g_2 \in G$ then $g_1 \cdot g_2 \in G$;
- for all $g_1 . g_2, g_3 \in G$, we have $g_1 \cdot (g_2 \cdot g_3) = (g_1 \cdot g_2) \cdot g_3$;
- G contains an *identity* element e such that $e \cdot g = g \cdot e = g$, for all $g \in G$;
- every $g \in G$ has an *inverse* element $g^{-1} \in G$ such that $g \cdot g^{-1} = g^{-1} \cdot g = e$.

Examples

1. The real numbers $\mathbb{R}$ with addition (so $\cdot$ becomes $+$), the integers $\mathbb{Z}$ with addition. In each case, zero is the identity element. (But note that the real numbers under multiplication do not form a group because 0 does not have an inverse.)
2. $\mathbb{R}^n$ and $\mathbb{Z}^n$ with vector addition.
3. $SO(3)$, the group of rotations around the origin in $\mathbb{R}^3$ (with the operation of composition).
4. $E(3)$, the group on Euclidean motions of $\mathbb{R}^3$ (with the operation of composition). (Note that $SO(3)$ is a subgroup of $E(3)$.)

Rotations as matrices

The elements of $SO(3)$ may be represented by 3×3 matrices

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$$

such that $AA^T = I$ and $\det A = 1$, where A^T is the transpose matrix and I is the 3×3 identity matrix:

$$A^T = \begin{pmatrix} a_{11} & a_{21} & a_{31} \\ a_{12} & a_{22} & a_{32} \\ a_{13} & a_{23} & a_{33} \end{pmatrix} \quad \text{and} \quad I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Here, the operation is matrix multiplication and I is the identity element.

Generators and relations

Another way to describe a group is by giving a set of generators and the relations they satisfy.

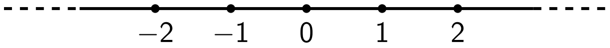
For example

$$\langle R, T \mid R^3 = e,\ T^2 = e \rangle$$

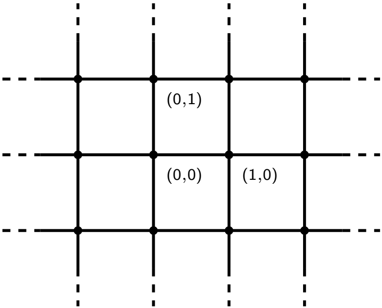
is the group of symmetries of an equilateral triangle. (Here, R is a rotation through $2\pi/3$ radians and T is a reflection in the perpendicular from a vertex to the opposite side.)

Note that we don't write the relations $RR^{-1} = R^{-1}R = e$ and $TT^{-1} = T^{-1}T = e$ explicitly – they are always understood to hold.

Cayley graph for $\mathbb{Z}$



Cayley graph for $\mathbb{Z}^2$



Free groups

Here is another group specified by generators and relations. It will be very important for the rest of the talk.

This group is called F_2. It will have two generators a and b. (Just think of them as abstract symbols.) The elements of F_2 are the identity e and all finite reduced words in a, b and their inverses a^{-1}, b^{-1}, where a reduced word is a finite string of these four elements subject only to the restriction that we cannot follow something by its inverse.

Here are some reduced words (where we use the shorthand $a^2 = aa$, etc.):

$$ab, \; ab^2a^{-1}, \; bab^{-1}a^7b^22a^{-1}$$

Free groups

We still need an operation to make F_2 into a group.

For reduced words w_1 and w_2, we define $w_1 \cdot w_2$ to be the concatenation of w_1 and w_2 with cancellation of adjacent inverses.

Examples:

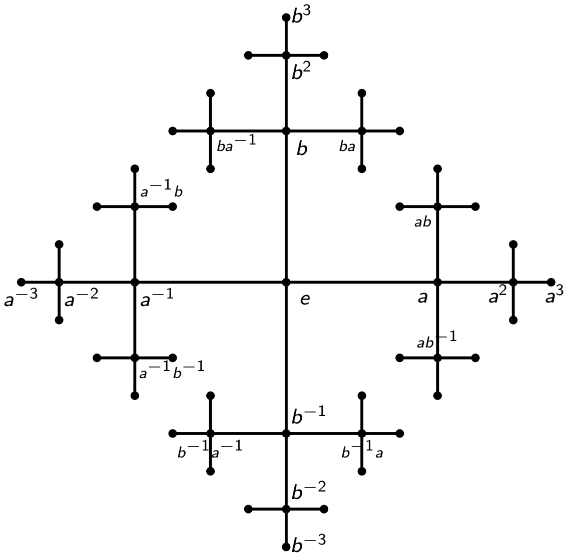
$$a \cdot b = ab$$

$$aba^{-1} \cdot b^3 a^2 = aba^{-1} b^3 a^2$$

$$bab^{-1} a^7 b^2 a^{-1} \cdot ab^2 a^{-1} = bab^{-1} a^7 b^4 a^{-1}$$

Of course, we also define $e \cdot w = w \cdot e = w$ always. (We can think of e as the "empty word".)

Cayley graph for F_2



Free groups

We call F_2 the free group on 2 generators. ("Free" because there are no relations between the generators.)

As we've defined the elements of F_2 are just abstract symbols but we can realise as a group of matrices (in many ways).

Take two distinct axes in $\mathbb{R}^3$ and let α and β be irrational numbers. Let a be a rotation be angle $2\pi\alpha$ around the first axis and let b be a rotation by angle $2\pi\beta$ around the second axis. Then the group generated by a and b is a copy of the free group on 2 generators.

Example:

$$a = \begin{pmatrix} 1/2 & \sqrt{3}/2 & 0 \\ -\sqrt{3}/2 & 1/2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad b = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1/2 & \sqrt{3}/2 \\ 0 & -\sqrt{3}/2 & 1/2 \end{pmatrix}.$$

Paradoxical decompositions again

Let us return to the Banach–Tarski Paradox but consider a more general situation.

Let X be a set and let G be a group action on X. We say that $E \subset X$ is G-paradoxical if there exist pairwise disjoint sets $E_i \subset E$ and $g_i \in G$, $i = 1, \ldots, m, \ldots, m+n$ such that

- $$\bigcup_{i=1}^{m+n} E_i = E$$
- $$\bigcup_{i=1}^{m} g_i(E_i) = E \quad \text{and} \quad \bigcup_{i=m+1}^{m+n} g_i(E_i) = E.$$

von Neumann and amenability

A general version of Tarski's result says that E is *not* G-paradoxical if and only if there is a G-invariant finitely additive measure defined on all the subsets of X such that $m(E) = 1$.

von Neumann realised that this was essentially a property of the group G. Notice that G acts on itself by left multiplication.

Theorem (von Neumann, 1929)

A sufficient condition for there to be a a G-invariant finitely additive measure on X such that $m(E) = 1$ is that there is a left-invariant finitely additive measure μ defined on all the subsets of G with $\mu(G) = 1$.

We call groups with this property *amenable*.

Amenable groups

Clearly finite groups are amenable (just use normalised counting measure). But are there infinite amenable groups?

Yes, but seeing this requires some rather sophisticated mathematics. For example, $\mathbb{Z}$ is amenable.

Why? Define a sequence of measures μ_n on subsets of $\mathbb{Z}$ by

$$\mu_n(A) = \frac{\#(A \cap \{-n, \ldots, n\})}{2n+1}.$$

Then

$$|\mu_n(A+1) - \mu_n(A)| \leq \frac{1}{2n+1}.$$

Then *take a limit along a non-principal ultrafilter* to get an invariant measure.

Ultrafilters?

See Terry Tao's excellent blog post:

Ultrafilters, nonstandard analysis, and epsilon management

Følner's criterion

A similar argument works for $\mathbb{Z}^d$, for any $d \geq 1$.

More generally a (countable) group G is amenable if (and only if) for every finite set $A \subset G$ and every $\epsilon > 0$, there exists a finite set $K \subset G$ such that

$$\frac{\#(K \cap a \cdot K)}{\#K} > 1 - \epsilon, \quad \text{for all } a \in A.$$

This is called Følner's criterion (1950s).

Also note that any subgroup of an amenable group is amenable.

F_2 is not amenable

What about groups which are not amenable? Well, F_2 is not amenable.

We can prove this by contradiction.

F_2 is not amenable

What about groups which are not amenable? Well, F_2 is not amenable.

We can prove this by contradiction. Suppose that μ is an F_2-invariant finitely additive measure defined on all the subsets of F_2.

For the generator a, let $W(a)$ be the set of reduced words that start with an a. Similarly, $W(a^{-1}), W(b)$ and $W(b^{-1})$.

We have the following disjoint unions:

$$\begin{aligned} F_2 &= \{e\} \cup W(a) \cup W(a^{-1}) \cup W(b) \cup W(b^{-1}) \\ &= W(a) \cup aW(a^{-1}) \\ &= W(b) \cup bW(b^{-1}). \end{aligned}$$

F_2 is not amenable

Hence

$$\begin{aligned}\mu(F_2) &= \mu(\{e\}) + \mu(W(a)) + \mu(W(a^{-1})) + \mu(W(b)) + \mu(W(b^{-1}))\\ &= \mu(W(a)) + \mu(aW(a^{-1}))\\ &= \mu(W(b)) + \mu(bW(b^{-1})).\end{aligned}$$

Using invariance and the fact that $\mu(F_2) = 1$, we obtain

$$\begin{aligned}1 &= \mu(\{e\}) + \mu(W(a)) + \mu(W(a^{-1})) + \mu(W(b)) + \mu(W(b^{-1}))\\ &= \mu(W(a)) + \mu(W(a^{-1}))\\ &= \mu(W(b)) + \mu(W(b^{-1})),\end{aligned}$$

giving a contradiction.

Application to Banach–Tarski

We've seen that F_2 can be realised as a subgroup of $SO(3)$. Hence $SO(3)$ is not amenable and therefore $E(3)$ is not amenable. This explains why we can have the Banach–Tarski Paradox in dimension 3.

In contrast, $E(2)$, the group of Euclidean motions of $\mathbb{R}^2$, *is* amenable and there is no 2-dimensional version of Banach–Tarski.

Random walks on $\mathbb{Z}$

Now let us think about some probability theory.

Start at $0 \in \mathbb{Z}$. Move $+1$ with probability $1/2$ and -1 with probability $1/2$. We call this process a random walk. We'll denote our position after n steps by S_n.

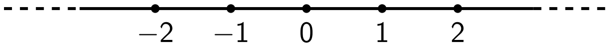
What is the probability that we return to 0 after n steps, i.e. that $S_n = 0$?

First we note that we can only return in an *even* number of steps, so we are interested in $\mathrm{Prob}(S_{2n} = 0)$.

We can easily see that

$$\mathrm{Prob}(S_{2n} = 0) = \frac{1}{2^{2n}} \binom{2n}{n} \asymp \frac{1}{\sqrt{n}}, \quad \text{as } n \to \infty.$$

Cayley graph for $\mathbb{Z}$



Random walks on $\mathbb{Z}^d$

We can generalise the above to higher dimensions.

We can define a random walk on $\mathbb{Z}^d$ as follows. For $i = 1, \ldots, d$, write e_i for the vector with 1 in the ith position and 0s elsewhere (e.g. $e_1 = (1, 0, \ldots, 0)$).

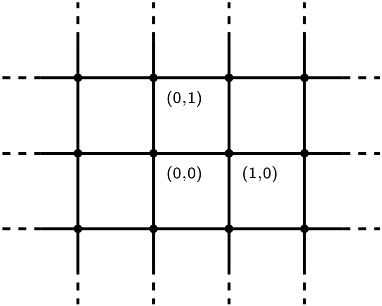
Choose probabilities $p_1, \ldots, p_d, p_{-1}, \ldots, p_{-d} > 0$ such that

$$p_1 + \cdots + p_d + p_{-1} + \cdots + p_{-d} = 1$$

and $p_i = p_{-i}$.

Start at $0 \in \mathbb{Z}^d$. Then jump by e_i with probability p_i and $-e_i$ with probability p_{-i}.

Cayley graph for $\mathbb{Z}^2$



Random walks on $\mathbb{Z}^d$

As before, S_n denotes the position reached after n jumps, and $S_n = 0$ implies that n is even.

We have

$$\text{Prob}(S_{2n} = 0) \asymp \frac{1}{n^{d/2}}, \quad \text{as } n \to \infty.$$

Notice that $\text{Prob}(S_{2n} = 0)$ decays more quickly as d increases but only at a polynomial rate.

Random walks of free groups

Let us consider a random walk on the free group F_2. Remember that this has generators a, b and their inverses a^{-1}, b^{-1}.

Choose probabilities $p_a, p_b, p_{a^{-1}}, p_{b^{-1}} > 0$ such that

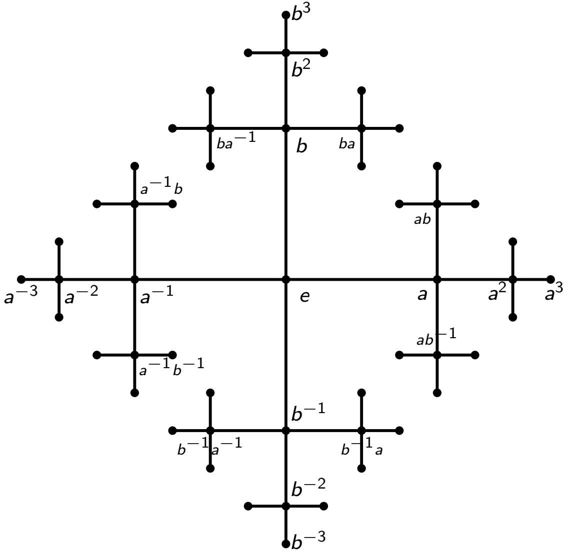
$$p_a + p_b + p_{a^{-1}} + p_{b^{-1}} = 1$$

and $p_a = p_{a^{-1}}$, $p_b = p_{b^{-1}}$.

Start at the identity e and jump by $s \in \{a, b, a^{-1}, b^{-1}\}$ with probability p_s.

The simplest case is $p_a = p_b = p_{a^{-1}} = p_{b^{-1}} = 1/4$.

Cayley graph for F_2



Random walks of free groups

In this situation, it is much harder to return to the identity.

In the simplest case where all jump probabilities are $1/4$, a not so simple calculation gives that

$$\mathrm{Prob}(S_{2n} = e) \asymp \frac{1}{n^{3/2}} \left(\frac{2\sqrt{2}}{3} \right)^{2n}, \quad \text{as } n \to \infty.$$

In particular,

$$\frac{2\sqrt{2}}{3} \approx 0.94 < 1,$$

so $\mathrm{Prob}(S_{2n} = e)$ decays exponentially fast, as $n \to \infty$.

Random walks of free groups

For more general probabilities $\mathbf{p} = (p_a, p_b, p_{a^{-1}}, p_{b^{-1}})$, we have

$$\mathrm{Prob}(S_{2n} = e) \asymp \frac{1}{n^{3/2}} \lambda(\mathbf{p})^{2n}, \quad \text{as } n \to \infty,$$

for some $0 < \lambda(\mathbf{p}) < 1$, so we still have exponential decay.

More general set-up

Let G be a countable group with a finite set of generators S. To simplify notation, we assume that S contains all its inverses, i.e. $s \in S$ if and only if $s^{-1} \in S$.

Choose probabilities $p_s > 0$, $s \in S$, such that

$$\sum_{s \in S} p_s = 1$$

and $p_s = p_{s^{-1}}$. Let $\mathbf{p} = (p_s)_{s \in S}$.

Then define a random walk on G by staring at the identity and jumping by $s \in S$ with probability p_s.

Exponential decay

Question: When does $\mathrm{Prob}(S_n = e)$ decay exponentially fast?

Set

$$\lambda(G, \mathbf{p}) := \limsup_{n\to\infty} \mathrm{Prob}(S_n = e)^{1/n} \leq 1.$$

Theorem (Kesten, 1958)

For a **symmetric** *random walk on a group G as above,*

$$\lambda(G, \mathbf{p}) < 1$$

if and only if G is not amenable.

Non-symmetric random walks?

Without symmetry ($p_s = p_{s^{-1}}$), Kesten's theorem is **false**.

Even for random walks on $\mathbb{Z}$, we get $\lambda < 1$ if there is a preference for some direction.

Example: $p_1 = 3/2$, $p_{-1} = 1/3$.

Non-symmetric random walks?

However, there is a natural replacement of Kesten's result. This requires the notion of the **abelianization** of a group.

Recall that a group is *abelian* if it is commutative (i.e. $g \cdot h = h \cdot g$ always).

The *abelianization* G^{ab} of a group G is the group obtained from G by adding the relations $g \cdot h = h \cdot g$ for every pair of elements $g, h \in G$.

Alternatively, G^{ab} is the largest abelian quotient group of G, i.e. the largest abelian group for which there exists a surjective homomorphism $\phi : G \to G^{\mathrm{ab}}$.

Abelianization

If G is finitely generated then G^{ab} is isomorphic to

$$\mathbb{Z}^k \times A,$$

with $k \geq 0$ and A a finite abelian group.

Example: $F_2^{\text{ab}} = \mathbb{Z}^2$.

A random walk $\mathbf{p} = (p_s)_{s \in S}$ on G gives a random walk $\overline{\mathbf{p}} = (\overline{p}_\sigma)_{\sigma \in \Sigma}$ on G^{ab} by the formula

$$\overline{p}_\sigma = \sum_{\phi(s)=\sigma} p_s,$$

where $\Sigma = \phi(S)$.

A non-symmetric Kesten criterion

The next theorem is joint work with Rhiannon Dougall (Durham University).

We first note that we always have $\lambda(G, \mathbf{p}) \leq \lambda(G^{\mathrm{ab}}, \overline{\mathbf{p}})$.

Theorem (Dougall and Sharp, 2024)

For a random walk on a group G as above,

$$\lambda(G, \mathbf{p}) < \lambda(G^{ab}, \overline{\mathbf{p}})$$

if and only if G is not amenable.
Furthermore, $\lambda(G^{ab}, \overline{\mathbf{p}}) = 1$ if and only if for every homomorphism $\chi : G^{ab} \to \mathbb{R}$ we have

$$\sum_{\sigma \in \Sigma} \overline{p}_\sigma \chi(\sigma) = 0.$$

Thank you for listening!