THE BANACH-TARSKI PARADOX

Bruce Blackadar

The Banach-Tarski Paradox has been called "the most surprising result in theoretical mathematics." (J. Mycielski)

Banach-Tarski Theorem for Spheres: The unit sphere S^2 in $\mathbb{R}^3$ can be decomposed into a finite number of pieces (4 will do) which can be rigidly moved to fit together to form two disjoint spheres of radius 1.

Banach-Tarski Theorem for Balls: The unit ball in $\mathbb{R}^3$ can be decomposed into a finite number of pieces (5 will do) which can be rigidly moved to fit together to form two disjoint balls of radius 1.

The "pieces" are very complicated - dense in the ball; the Axiom of Choice is even needed to define them. They cannot (all) be Lebesgue measurable.

Definition. Two subsets X and Y of $\mathbb{R}^n$ are *equidecomposable* if there are finite partitions $\{X_1, \ldots, X_m\}$ of X and $\{Y_1, \ldots, Y_m\}$ of Y such that X_i and Y_i are congruent for each i, i.e. for each i there is a rigid motion σ_i of $\mathbb{R}^n$ with $Y_i = \sigma_i(X_i)$.

rigid motion
= orientation-preserving isometry
= translation + orthogonal linear transformation of determinant 1
The rigid motions of $\mathbb{R}^n$ form a group SG_n.

SG_n is a Lie group of dimension $\frac{n(n+1)}{2}$, a semidirect product of the additive group $\mathbb{R}^n$ and the special orthogonal group SO_n of orthogonal $n \times n$ matrices of determinant 1.

Equidecomposability should not be confused with *congruence by dissection*, which is usually considered only for nice subsets of $\mathbb{R}^n$ such as polyhedra and which allows the pieces to overlap along a boundary edge or face. The Bolyai-Gerwein Theorem states that any two polygons in $\mathbb{R}^2$ with the same area are congruent by dissection (the equal area condition is also necessary.)

Banach-Tarski Theorem for Spheres: The unit sphere S^2 in $\mathbb{R}^3$ is equidecomposable with the disjoint union $S^2 \coprod S^2$ of two spheres of radius 1.

Banach-Tarski Theorem for Balls: The unit ball in $\mathbb{R}^3$ is equidecomposable with the disjoint union of two balls of radius 1.

Banach-Tarski Theorem, General Version: Any two bounded subsets of $\mathbb{R}^3$ with nonempty interior are equidecomposable. In particular, any two balls in $\mathbb{R}^3$ are equidecomposable.
"A ball the size of a pea can be cut into finitely many pieces which can be reassembled to form a ball the size of the sun."
[Five pieces will not do here: at least 10^{30} pieces are necessary.]
These results hold in $\mathbb{R}^n$ for all $n \geq 3$, but not for $n < 3$.

The first version of the "paradox" was given by F. Hausdorff (1914):
Hausdorff's Paradox: There is a countable subset K of S^2 such that $S^2 \setminus K$ is equidecomposable with the disjoint union of two copies of $S^2 \setminus K$.

Banach and Tarski (1924) showed how to eliminate the countable set K to obtain the sphere verion of the paradox, and how to obtain the ball version from the sphere version. Banach also obtained a "Schröder-Bernstein" theorem for equidecomposability which yields the general version of the paradox.

Outline

1. Preliminary constructions, derivation of the sphere and ball versions from Hausdorff's Paradox
2. The Schröder-Bernstein Theorem, derivation of the general paradox from the ball version
3. Free groups, Axiom of Choice, derivation of Hausdorff's Paradox

Warmup Construction: Can a subset of $\mathbb{R}^n$ be congruent to a proper subset?
Example: $\mathbb{N} = \{1, 2, 3, \dots\} \subseteq \mathbb{R}^1$

What about a bounded subset?
Not possible in $\mathbb{R}^1$ (Exercise), but possible in $\mathbb{R}^2$:
Let θ be an angle which is an irrational multiple of 2π (e.g. $\theta = 1$), and ρ the transformation of rotation counterclockwise around the origin by θ radians. Let p be a point on the unit circle (e.g. $p = (1, 0)$), and let

$$A = \{p, \rho(p), \rho^2(p), \dots\}$$

A is a countable dense subset of the unit circle (the *forward orbit* of p under ρ), and $\rho(A) = A \setminus \{p\}$.

The whole unit circle S^1 is not congruent to $S^1 \setminus \{p\}$, but they are equidecomposable: if $B = S^1 \setminus A$, then $\{A, B\}$ is a partition of S^1 and $\{\rho(A), B\}$ is a partition of $S^1 \setminus \{p\}$.

More generally, let K be a countable subset of S^1. The set of angles θ such that rotation by some multiple of θ sends a point of K to another point of K is countable. Thus there is a θ such that the sets K, $\rho(K)$, $\rho^2(K)$, $\dots$ are disjoint. Let

$$A = K \cup \rho(K) \cup \rho^2(K) \cup \cdots$$

A is a countable dense subset of S^1, and $\rho(A) = A \setminus K$.

As before, S^1 is equidecomposable with $S^1 \setminus K$.

If K is a countable subset of S^2, we can find a line through the origin not hitting K, and then rotate around this axis by a suitable angle θ so that sets K, $\rho(K)$, $\rho^2(K)$, $\dots$ are disjoint. As before, set

$$A = K \cup \rho(K) \cup \rho^2(K) \cup \cdots$$

A is a countable dense subset of S^2, and $\rho(A) = A \setminus K$.

Thus S^2 and $S^2 \setminus K$ are equidecomposable.

The situation with the unit disk $\mathbb{D}$ is similar, but with a complication.
Let K be a countable subset of $\mathbb{D}$. Suppose the origin is *not* in K. Then an angle θ can be found so that K, $\rho(K)$, $\rho^2(K)$, etc., are disjoint, and the previous argument shows that $\mathbb{D}$ and $\mathbb{D} \setminus K$ are equidecomposable.
Now suppose K contains the origin. Let $\mathbb{D}_0$ be the unit disk with the origin removed. By the same argument as before, $\mathbb{D}_0$ and $\mathbb{D} \setminus K$ are equidecomposable.
By an identical argument, if $R \subseteq \mathbb{D}$ is a union of a countable number of rays from the origin (including the origin), then $\mathbb{D}_0$ and $\mathbb{D} \setminus R$ are equidecomposable.

$\mathbb{D}$ and $\mathbb{D}_0$ are also equidecomposable: if C is a circle inside D passing through the origin, there is a countable subset A of C containing $(0, 0)$ and an angle θ such that rotation ρ of C around its center by angle θ sends A onto $A \setminus (0, 0)$. If $B = \mathbb{D} \setminus A$, then $\mathbb{D}$ and $\mathbb{D}_0$ are equidecomposable via $\{A, B\}$ and $\{\rho(A), B\}$.

Similarly, if B is the unit ball in $\mathbb{R}^3$, and $B_0 = B \setminus \{(0, 0, 0)\}$, we have:
If K is a countable subset of B not containing the origin, then B and $B \setminus K$ are equidecomposable.
If K is a countable subset of B containing the origin, then B_0 and $B \setminus K$ are equidecomposable.
If $R \subseteq B$ is a union of a countable number of rays from the origin, then B_0 and $B \setminus R$ are equidecomposable.
B and B_0 are equidecomposable.

To conclude that $\mathbb{D}$ and $D \setminus K$, or B and $B \setminus K$, are equidecomposable when K contains the origin, or that B and $B \setminus R$ are equidecomposable, we need to know that equidecomposability is transitive.

Proposition. Equidecomposability is transitive, and thus an equivalence relation.
Proof: Let X, Y, and Z be subsets of $\mathbb{R}^n$. Suppose X and Y are equidecomposable, and that Y and Z are equidecomposable. Then there are partitions $\{A_1, \dots, A_m\}$ of X and $\{B_1, \dots, B_m\}$ of Y and rigid motions σ_i such that $B_i = \sigma_i(A_i)$. There are also partitions $\{C_1, \dots, C_k\}$ of Y and $\{D_1, \dots, D_k\}$ of Z and rigid motions τ_j such that $D_j = \tau_j(C_j)$.
Let $Y_{ij} = B_i \cap C_j$. Then $\{Y_{ij}\}$ is a partition of Y, and $\cup_j Y_{ij} = B_i$ for each i and $\cup_i Y_{ij} = C_j$ for each j. Set $X_{ij} = \sigma_i^{-1}(Y_{ij})$ and $Z_{ij} = \tau_j(Y_{ij})$ for each i, j. Then $\{X_{ij}\}$ is a partition of X, $\{Z_{ij}\}$ is a partition of Z, and Z_{ij} is congruent to X_{ij} via $\tau_j \circ \sigma_i$, so X and Z are equidecomposable.

We will write $X \sim Y$ if X and Y are equidecomposable.

We can now derive the Banach-Tarski Paradoxes for spheres and balls from Hausdorff's Paradox. Let K be a countable subset of S^2 such that $(S^2 \setminus K) \sim (S^2 \setminus K) \coprod (S^2 \setminus K)$. Then

$$S^2 \sim (S^2 \setminus K) \sim (S^2 \setminus K) \coprod (S^2 \setminus K) \sim S^2 \coprod S^2$$

For balls, let K be as above, and let R be the union of all rays in B from the origin to points in K. Then, extending radially the sets in the equidecomposability of $S^2 \setminus K$ and $(S^2 \setminus K) \coprod (S^2 \setminus K)$, we obtain that $B \setminus R$ and $(B \setminus R) \coprod (B \setminus R)$ are equidecomposable. Thus

$$B \sim B_0 \sim B \setminus R \sim (B \setminus R) \coprod (B \setminus R) \sim B \coprod B$$

Another observation: Assume the Banach-Tarski Theorem for balls. By iteration, using transitivity of equidecomposability, the unit ball is equidecomposable with the disjoint union of n balls of radius 1, for any n.

A more general setting is the situation where a group G acts on a set Ω. An *action* of G on Ω is a set

$$\{\alpha_g : g \in G\}$$

of bijections of Ω such that $\alpha_{gh} = \alpha_g \circ \alpha_h$ for $g, h \in G$, i.e. a homomorphism from G to the group of bijections of X. We often write $g \cdot X$ for $\alpha_g(X)$.

Two subsets of Ω can be called *G-congruent* if there is an element of G sending one set to the other. G-Equidecomposability can then be defined in this setting by setting $X \sim_G Y$ if they can be partitioned into disjoint subsets $X_1, \dots, X_m$ and $Y_1, \dots, Y_m$ such that X_k and Y_k are G-congruent for each k. Equidecomposability is the special case where $\Omega = \mathbb{R}^n$ and G is the group of rigid motions. Other interesting settings are where Ω is a metric or topological space and G is a group of isometries or homeomorphisms.

2. The Schröder-Bernstein Theorem

Two sets X and Y are said to *have the same cardinality*, or are *equipotent*, written $|X| = |Y|$, if there is a one-to-one correspondence between them.

We say $|X| \leq |Y|$ if X is equipotent with a subset of Y. A natural question is: if $|X| \leq |Y|$ and $|Y| \leq |X|$, is $|X| = |Y|$? (That is, is $\leq$ a partial order on the equipotence equivalence classes?)

Schröder-Bernstein Theorem. Let X and Y be sets. If $|X| \leq |Y|$ and $|Y| \leq |X|$, then $|X| = |Y|$.

The proof of the Schröder-Bernstein Theorem is a simple but clever "back and forth" argument. Suppose X and Y are sets with $|X| \leq |Y|$ and $|Y| \leq |X|$, so there is a bijection ϕ from X onto a subset of Y, i.e. an injective function $\phi : X \to Y$, and a bijection ψ from Y onto a subset of X (an injective function $\psi : Y \to X$). We must show that there is a bijection $f : X \to Y$.

We will inductively define sequences $(A_1, A_2, \dots)$ of disjoint subsets of X and $(B_1, B_2, \dots)$ of disjoint subsets of Y. Let $A_1 = X \setminus \psi(Y)$ and $B_1 = Y \setminus \phi(X)$. Then, if A_n and B_n have been defined, let $A_{n+1} = \psi(B_n)$ and $B_{n+1} = \phi(A_n)$.

Lemma. The A_n are disjoint, and the B_n are also disjoint.
Proof: A_1 is disjoint from A_n for any $n > 1$ since $A_n \subseteq \psi(Y)$ for $n > 1$. Similarly, B_1 is disjoint from B_n for $n > 1$. Assume $B_1, \dots, B_n$ are disjoint. Then $A_2, \dots, A_{n+1}$ are disjoint since ψ is injective. Similarly, if $A_1, \dots, A_n$ are disjoint, then $B_2, \dots, B_{n+1}$ are disjoint since ϕ is injective. Proceed by induction.

Set $A_\infty = X \setminus \cup_{n=1}^\infty A_n$ and $B_\infty = Y \setminus \cup_{n=1}^\infty B_n$.

Lemma. The function ϕ maps A_∞ bijectively onto B_∞.
Proof: Let $x \in A_\infty$. Since $(B_1, B_2, \dots, B_\infty)$ is a partition of Y, either $\phi(x) \in B_\infty$ or $\phi(x) \in B_n$ for some n. But $\phi(x) \notin B_1$ since $\phi(x) \in \phi(X)$; and $\phi(x) \notin B_n$ for any $n > 1$ since, if $\phi(x) \in B_n$, then $x \in A_{n-1}$ (using the fact that ϕ is injective). Thus ϕ maps A_∞ into B_∞. Now let $y \in B_\infty$. Then $y = \phi(x)$ for some (unique) $x \in X$ since $y \notin B_1$. This x is not in A_n for any n since then we would have $y \in B_{n+1}$, so $x \in A_\infty$.

Similarly, ψ maps B_∞ bijectively onto A_∞, although we will not need this fact. Note that there is no reason to expect that $\psi|_{B_\infty}$ is the inverse of $\phi|_{A_\infty}$.

Now let $X_1 = \cup_{n\,\mathrm{odd}} A_n$, $X_2 = \cup_{n\,\mathrm{even}} A_n$, $X_3 = A_\infty$, $Y_1 = \cup_{n\,\mathrm{even}} B_n$ (note the reversal of even and odd), $Y_2 = \cup_{n\,\mathrm{odd}} B_n$, $Y_3 = B_\infty$. Then ϕ maps X_1 bijectively onto Y_1 and X_3 bijectively onto Y_3, and ψ^{-1} maps X_2 bijectively onto Y_2. Putting these together, we get a bijection from X onto Y.

S. Banach noticed that the proof of the Schröder-Bernstein Theorem really had little to do with cardinality, and applied to sets with an equivalence relation satisfying certain properties.

Banach observed that the essential features of the Schröder-Bernstein argument were that

(1) if $|X| = |Y|$, then there is a bijective function $\phi : X \to Y$ such that $|A| = |\phi(A)|$ for every $A \subseteq X$

(2) if $X_1, X_2, \ldots, X_n$ are disjoint sets, $Y_1, Y_2, \ldots, Y_n$ are disjoint, and $|X_k| = |Y_k|$ for all k, then $|\cup_{k=1}^n X_k| = |\cup_{k=1}^n Y_k|$.

Abstracting the situation, he considered an equivalence relation $\sim$ on sets (to avoid logical difficulties, it is best to fix a universal set Ω and take $\sim$ to be an equivalence relation on the subsets of Ω.) The properties of $\sim$ needed for a Schröder-Bernstein type theorem are:

(1) If $X, Y \subseteq \Omega$ and $X \sim Y$, then there is a bijection $\phi : X \to Y$ such that $A \sim \phi(A)$ for all $A \subseteq X$.

(2) If $X_1, \ldots, X_n$ and $Y_1, \ldots, Y_n$ are families of disjoint subsets of Ω, and $X_k \sim Y_k$ for all k, then $\cup_{k=1}^n X_k \sim \cup_{k=1}^n Y_k$. [It suffices for this to be true for $n = 2$.]

It is easy to see that equidecomposability of subsets of $\mathbb{R}^n$ (for fixed n) satisfies properties (1) and (2). More generally, if a group G acts on a set Ω, G-equidecomposability satisfies (1) and (2).

If $\sim$ is an equivalence relation on the subsets of a set Ω, and $X, Y \subseteq \Omega$, write $X \precsim Y$ if $X \sim Z$ for some $Z \subseteq Y$.

Banach's Schröder-Bernstein Theorem. Let Ω be a set, and $\sim$ an equivalence relation on the subsets of Ω which satisfies (1) and (2). If $X, Y \subseteq \Omega$ with $X \precsim Y$ and $Y \precsim X$, then $X \sim Y$ (i.e. $\precsim$ gives a partial order on the $\sim$-equivalence classes.)

The proof is essentially identical to the previous proof. If Z is the subset of Y equivalent to X, then take $\phi : X \to Z$ to be the function guaranteed by (1), and similarly if $W \subseteq X$ is equivalent to Y, let $\psi : Y \to W$ the corresponding function. The proof is identical through the construction of the X_k and Y_k. By (1), $X_1 \sim Y_1$ and $X_3 \sim Y_3$ by the property of ϕ from (1), and $Y_2 \sim X_2$ by the property of ψ. Thus $X \sim Y$ by (2).

Corollary. Let X and Y be subsets of $\mathbb{R}^n$. If X is equidecomposable with a subset of Y, and Y is equidecomposable with a subset of X, then X and Y are equidecomposable.

It is instructive to explicitly work out the details of the proof in the case of equidecomposability to see exactly how the sets X and Y can be decomposed into congruent pieces.

Example. Let G be the group of *similarities* of $\mathbb{R}^2$, rigid motions followed by scaling. If X is a disk and Y a square (including interior), then each of X and Y is obviously similar to a subset of the other, hence G-equidecomposable with a subset of the other; thus by Banach's Schröder-Bernstein, X and Y are G-equidecomposable.

Problem: Find an explicit G-equidecomposition using 2 pieces. [Solution after break]

To derive the general Banach-Tarski Paradox from the ball form, suppose X and Y are subsets of $\mathbb{R}^n$ ($n \geq 3$). Suppose Y is bounded and that X contains a ball B. Since Y is bounded, it can be covered by a finite number of (overlapping) translates of B, say $B_1, \ldots, B_m$. Thus Y is equidecomposable with a subset of a union of a finite number of disjoint copies of B, say $B'_1, \ldots, B'_m$: move the part of Y in B_1 into B'_1, the part of Y in B_2 but not in B_1 into B'_2, etc.

By the ball version of the paradox, $B'_1 \cup \cdots \cup B'_m$ is equidecomposable with B. Thus Y is equidecomposable with a subset of $B \subseteq X$. If X is also bounded and Y has nonempty interior, then X is equidecomposable with a subset of Y, so X and Y are equidecomposable by the Schröder-Bernstein Theorem.

3. Paradoxical Decompositions

Warmup Example: The Sierpiński-Mazurkiewicz Paradox. There is a nonempty subset X of $\mathbb{R}^2$ which can be partitioned into two disjoint subsets A and B, each congruent to X!

Fix a real number θ such that the complex number $e^{i\theta}$ is transcendental. (This is possible since there are only countably many algebraic complex numbers; in fact, $\theta = 1$ will do. Recall that a complex number is *algebraic* if it is a root of a polynomial with integer coefficients, and a number is *transcendental* if it is not algebraic.) Note that θ is an irrational multiple of 2π.

Let ρ be the rigid motion of $\mathbb{R}^2$ of rotation counterclockwise around the origin by angle θ, and let τ be translation by 1 in the x-direction. If $\mathbb{R}^2$ is identified with $\mathbb{C}$, ρ is multiplication by $e^{i\theta}$ and τ is adding 1.

Let X be the smallest subset of $\mathbb{R}^2 = \mathbb{C}$ containing the origin and closed under ρ and τ. X is a countable dense subset of $\mathbb{R}^2$.

Let $A = \rho(X)$ and $B = \tau(X)$. $A, B \subseteq X$, and A and B are clearly congruent to X. We will show that A and B are disjoint and $A \cup B = X$.

Consider the set of all *words* (strings of symbols) in ρ and τ, including the "empty word". A typical word would be

$$\rho\rho\tau\rho\tau\tau\rho\rho\rho\tau\tau\rho$$

Words can be composed by *concatenation*, for example:

$$(\rho\tau\rho)(\rho\rho\tau\rho\tau) = \rho\tau\rho\rho\rho\tau\rho\tau$$

This operation on words is associative and has an identity, the empty word. The set of words in ρ and τ with this operation is called the *free semigroup* on ρ and τ.

We can identify each word in ρ and τ with a rigid motion of $\mathbb{R}^2$, regarding juxtaposition as composition:

$$\rho\tau\tau\rho\tau \leftrightarrow \rho \circ \tau \circ \tau \circ \rho \circ \tau$$

(this is a homomorphism from the free semigroup on ρ and τ into the group SG_2.)

Theorem. This homomorphism is injective, i.e. distinct words give distinct rigid motions of $\mathbb{R}^2$.

In fact, we can say a little more. Every element of X is obtained by applying some word in ρ and τ to the origin 0. The word is not unique: since $\rho(0) = 0$, any number of ρ's can be added at the end of a word without changing the image of 0. Thus every point $p \neq 0$ of X can be obtained from 0 by applying a word ending in τ.

Theorem. For any $p \neq 0$ in X, there is a *unique* word w in ρ and τ, ending in τ, with $w(0) = p$.

To prove this, first show that if w is any word, then $w(0)$ is a polynomial in $e^{i\theta}$ with natural number coefficients. If distinct words give the same point p, subtract the corresponding polynomials to get a nonzero polynomial with integer coefficients having $e^{i\theta}$ as a root, contradicting the fact that $e^{i\theta}$ is transcendental.

This theorem implies the previous one: if w_1 and w_2 are distinct words giving the same transformation, then $w_1\tau$ and $w_2\tau$ also give the same transformation; but $w_1\tau(0) \neq w_2\tau(0)$, a contradiction.

Thus, if W is the set of words ending in τ, along with the empty word, there is a one-one correspondence between W and X. The transformation ρ corresponds to putting a ρ on the beginning of a nonempty word, and τ corresponds to putting a τ on the beginning of the corresponding word.

A consists of the empty word and words beginning with ρ (and ending in τ), and B consists of the words beginning (and ending) with τ. It is clear that these sets are disjoint and their union is W.

Free Groups

The theory of free groups is a little more subtle than the theory of free semigroups. Suppose a and b are symbols we will use as generators of a free group G. G cannot just consist of words in a and b, since elements of a group must have inverses; so there must also be elements a^{-1} and b^{-1}. We could try taking all words in a, b, a^{-1}, and b^{-1}. But these words cannot all give distinct elements of G: if there is a consecutive a and a^{-1} (in either order), or consecutive b and b^{-1}, the pair can be canceled to reduce the word to a shorter word giving the same group element.

Thus we should take only the set of *reduced words*, ones not containing any canceling pair of consecutive symbols. It is clear that any word can be reduced to a reduced word.

Subtle Problem: In general, a word can be reduced in many ways. How do we know that we always end up with the same reduced word no matter what order we carry out the reductions?

Uniqueness Theorem. Every word is reducible to a *unique* reduced word.

We can thus let G be the set of reduced words, including the empty word. The group operation is concatenation followed by reduction. It it is not hard to show from the Uniqueness Theorem that this operation is well defined and associative. The identity is the empty word, and the inverse is given by taking the inverse of each symbol and reversing the order, e.g.

$$(ab^{-1}aabab^{-1})^{-1} = ba^{-1}b^{-1}a^{-1}a^{-1}ba^{-1}$$

G is called the *free group on two generators*, usually denoted $\mathbb{F}_2$. We can similarly define the free group $\mathbb{F}_n$ on n generators, for any n, and even the free group on an infinite set of generators, using the generators and their formal inverses as the alphabet for the (reduced) words forming the group.

There is an extensive theory of free groups, and they are very important in many parts of mathematics. They have many interesting (and somewhat bizarre) properties. We will only need one key property that free groups have, a *paradoxical decomposition*.

Any group G acts on itself by left translation: $\alpha_g(x) = gx$. If $X \subseteq G$, write gX for $\alpha_g(X)$. gX is the *(left) translation* of the set X by g.

In $\mathbb{F}_2$, let

A_1 = the set of words beginning with a

A_2 = the set of words beginning with a^{-1}

B_1 = the set of words beginning with b

B_2 = the set of words beginning with b^{-1}

A_1, A_2, B_1, and B_2 are disjoint, and

$$A_1 \cup A_2 \cup B_1 \cup B_2 = \mathbb{F}_2 \setminus \{e\}$$

$$A_1 \cap aA_2 = \emptyset \text{ and } A_1 \cup aA_2 = \mathbb{F}_2$$

$$B_1 \cap bB_2 = \emptyset \text{ and } B_1 \cup bB_2 = \mathbb{F}_2$$

Exercise: Modify these sets so that the union is all of $\mathbb{F}_2$.

$\{A_1, A_2, B_1, B_2\}$ is a *paradoxical decomposition* of $\mathbb{F}_2$.

Excursion: Which groups have paradoxical decompositions?

Theorem: A group has a paradoxical decomposition if and only if it is not amenable.

Amenable groups are a class of "nicely-behaved" groups. There are a great many equivalent characterizations of amenable groups, and they are extremely important. Some basic facts (the Axiom of Choice is needed for some of these):

Every finite group is amenable.

Every abelian group is amenable.

Every subgroup or quotient of an amenable group is amenable.

An extension of amenable groups is amenable. In particular, every solvable group is amenable, and a Cartesian product of amenable groups is amenable.

$\mathbb{F}_2$ is not amenable, nor is any group containing a subgroup isomorphic to $\mathbb{F}_2$.

A famous long-standing open question was: does every nonamenable group contain a copy of $\mathbb{F}_2$?

Ol'shanskii 1990: There is a nonamenable group G in which every element has finite order, so G cannot contain a copy of $\mathbb{F}_2$.

The term "amenable" is a pun: an amenable group is a group with an invariant mean. But the name is appropriate: the various characterizations show that the class of amenable groups is precisely the class of groups whose structure is amenable to precise understanding.

Orbits

If a group G acts on a set X, and $p \in X$, then the *orbit* of p under G is

$$\{g \cdot p : g \in G\}$$

The orbit of p is all points reachable from p by the action of G.

Basic fact: if $p, q \in X$, then the orbits of p and q are either identical or disjoint.

So X partitions into a disjoint union of orbits.

An action of G on X is *free* if no element of G except the identity leaves any point of X fixed.

If G acts freely on X and $p \in X$, then the orbit of p can be identified with G: $g \mapsto g \cdot p$ is a bijection from G onto the orbit of p [If $g \cdot p = h \cdot p$, then $(h^{-1}g) \cdot p = p$, so $h^{-1}g = e$, $g = h$.]

Free Actions of $\mathbb{F}_2$

Suppose $\mathbb{F}_2$ acts freely on X. Each orbit can then be identified with $\mathbb{F}_2$. Since each point of X lies in a unique orbit, each point of X is identified with a group element, and the action of $\mathbb{F}_2$ is just left translation.

Define four subsets of X: let X_1 be the set of all elements of X identified with elements of $A_1 \subseteq \mathbb{F}_2$, and similarly X_2 the points identified with elements of A_2, Y_1 the points identified with B_1, and Y_2 the points identified with B_2. Then

X_1, X_2, Y_1, and Y_2 are disjoint

$X_1 \cup X_2 \cup Y_1 \cup Y_2 = X$

X_1 and $a \cdot X_2$ are disjoint and $X_1 \cup a \cdot X_2 = X$

Y_1 and $b \cdot Y_2$ are disjoint and $Y_1 \cup b \cdot Y_2 = X$

So $X_1 \cup X_2$ and $Y_1 \cup Y_2$ are each $\mathbb{F}_2$-equidecomposable with X. So we have

Theorem. If $\mathbb{F}_2$ acts freely on a set X, then X is a disjoint union of two subsets, each $\mathbb{F}_2$-equidecomposable with X.

Corollary. If X is a bounded subset of $\mathbb{R}^n$, and $\mathbb{F}_2$ acts freely on X by rigid motions, then X is equidecomposable with the union of two disjoint copies of X.

Thus, to prove the Hausdorff paradox, we just have to find a free action of $\mathbb{F}_2$ on $S^2 \setminus K$ by rigid motions, for some countable subset K of S^2.

Not So Fast!

We have glossed over a substantial subtlety in the construction. In order to identify an orbit with $\mathbb{F}_2$, we must pick a point in the orbit (which will be identified with the identity of $\mathbb{F}_2$.) It does not matter which point is chosen; any point will do equally well. But choice of a different point will give a different identification. Thus we must choose a point out of each of the orbits, and there are typically many orbits (uncountably many in our applications.)

How do we know we can make such a choice? We must use the *Axiom of Choice*. There are many equivalent formulations of the Axiom of Choice. One which is relevant for us is:

Axiom of Choice. If $\{X_i : i \in I\}$ is a collection of disjoint nonempty sets, there is a set $\{p_i : i \in I\}$ with $p_i \in X_i$ for all i.

This is often stated informally as "Given a collection of nonempty sets, you can choose an element from each set." The phrase "you can choose" should really be interpreted to mean "there exists a choice," not that there is any procedure for actually making such a choice.

The Axiom of Choice may at first seem obvious, but with more thought the less obvious it becomes. In fact, it is independent of the other (ZF) axioms of set theory! (That is, neither the Axiom of Choice nor its negation can be proved from the other set theory axioms, so it is consistent to assume the Axiom of Choice is true, or that it is false.)

Most mathematicians, especially analysts, accept the Axiom of Choice since many important theorems can only be proved using it. But we usually try to be careful to note which results are dependent on the Axiom of Choice.

The theorem about paradoxical decompositions of sets with a free $\mathbb{F}_2$-action requires the Axiom of Choice (in some form), i.e. it is not a theorem of ZF set theory. Some form of the Axiom of Choice can be shown to be necessary for the Banach-Tarski Paradox, i.e. it is also not a theorem of ZF set theory.

So is the Axiom of Choice the culprit in the paradox? If we reject the Axiom of Choice, the paradox disappears, but other counterintuitive consequences appear, for example:

Without the Axiom of Choice, there are two sets X and Y, such that neither is equipotent with a subset of the other (i.e. $|X| \not\leq |Y|$ and $|Y| \not\leq |X|$.)

Without some form of the Axiom of Choice, it cannot be proved that a countable union of countable sets is countable.

It cannot even be shown without some form of the Axiom of Choice that every infinite set contains a sequence of distinct elements! (The *Axiom of Dependent Choice* suffices for this.)

So we should not be too quick to reject the Axiom of Choice. In fact, the world of set theory, and the rest of mathematics, is arguably much more bizarre without it, even without the Banach-Tarski Paradox.

Hausdorff's Paradox

The group SO_3 of rigid motions of $\mathbb{R}^3$ fixing the origin sends S^2 onto itself, hence restricts to an action on S^2. So any subgroup of SO_3 also acts naturally on S^2.

Theorem. SO_3 contains a subgroup isomorphic to $\mathbb{F}_2$.

Hausdorff gave an explicit pair of elements in SO_3 generating a free subgroup (rotations around two axes where the angle θ between the axes has $\cos 2\theta$ transcendental). Simpler pairs have since been found. In fact, "almost all" pairs of elements in SO_3 generate a free subgroup: the set of pairs which do not is a set of first category in $SO_3 \times SO_3$.

However, this does not finish the paradox, since this subgroup does not act freely on S^2. In fact, every element of SO_3 has a pair of diametrically opposed fixed points on S^2 (it is easy to prove that every element of SO_3 has 1 as an eigenvalue, hence a one-dimensional space of fixed vectors). In fact, every element of SO_3 is a rotation around some axis.

But if G is a subgroup of SO_3 isomorphic to $\mathbb{F}_2$, then G is countable, so the set K of points in S^2 left fixed by some nonidentity element of G is countable. It is easy to see that K is invariant under G, and hence $S^2 \setminus K$ is also invariant; and the restriction of the G-action to $S^2 \setminus K$ is free.

Thus $S^2 \setminus K$ is equidecomposable with two disjoint copies of itself, yielding the Hausdorff Paradox and thus the Banach-Tarski Paradox.

The construction in $\mathbb{R}^n$, $n > 3$, is similar. SO_n contains a copy of SO_3 and hence a free group. (The generalization to $\mathbb{R}^n$ is not completely straightforward: a free group must be found in SO_n which has a "small" set of fixed points.)

Can this be done in $\mathbb{R}^2$? No; the reason is that SG_2 is a solvable group (SO_2 is abelian), hence any subgroup is amenable and has no paradoxical decomposition. In fact, a theorem of Tarski implies:

Theorem. Lebesgue measure on $\mathbb{R}^2$ can be extended to a finitely additive measure on all subsets of $\mathbb{R}^2$ which is invariant under rigid motions.

Corollary. If X and Y are Lebesgue measurable subsets of $\mathbb{R}^2$ which are equidecomposable (even using nonmeasurable pieces), then X and Y have the same Lebesgue measure.

The Banach-Tarski Paradox shows that there is no such extension for Lebesgue measure on $\mathbb{R}^3$.

Reference:

Stan Wagon, *The Banach-Tarski Paradox.* Second Edition, Cambridge University Press, 1994.