A Formal Proof of the Banach-Tarski Theorem in ACL2(r)

Jagadish Bapanapally
University of Wyoming
jbapanap@uwyo.edu

Ruben Gamboa
University of Wyoming
ruben@uwyo.edu

Abstract

The Banach-Tarski theorem[1] states that a solid ball can be partitioned into a finite number of pieces which can be rotated to form two identical copies of the ball. The proof of the Banach-Tarski theorem involves generating a free group of rotations and then decomposing the ball using these rotations and rearranging them to get two copies of the ball. The key ingredients to the proof are the Hausdorff paradox and the proof that the reals are uncountable. The non-denumerability of the reals has already been proven in ACL2(r)[2], and in this paper we report on a proof in ACL2(r)[3] of the Hausdorff paradox[4]. Currently, we are working to prove the Banach-Tarski theorem for a solid ball centered at the origin with radius 1.

Keywords: ACl2(r), Banach-Tarski

1 Introduction

The result of the Banachi-Tarski theorem is astonishing, but it can be explained because of the existence of non-measurable sets[5] and the axiom of choice [6]. It states that we can break a solid ball and rotate the pieces into two balls which will have the same volume and the shape as of the original sphere. The Hausdorff Paradox is a similar statement, but regarding the unit sphere instead of the unit ball. So far, we have formally proved the Hausdorff Paradox in ACL2(r) and now we are working to prove the Banach-Tarski theorem for the unit ball.

The Hausdorff Paradox states that, except for a countable number of points on the sphere, the sphere can be divided into a finite number of pieces which can be rotated to form two copies of the sphere. The proof involves generating a free group of rotations and then rotating the pieces of the sphere. Except for the poles of the rotations, we can divide the sphere into five pieces, then rotate them to form two copies of the sphere. Finally, we will show that the set of poles is countable.

In section 2, we define the set of reduced words and show that the set satisfies the group properties. In section 3, we show there is a one-to-one mapping between the set of reduced words and a specific set of matrices, and then we'll show that these matrices are rotations. In section 4, we will show the proof of the Hausdorff Paradox.

2 A Free Group of Reduced Words

If we take four characters, say a, a^{-1}, b, and b^{-1}, then a reduced word is a sequence of characters such that a^{-1} doesn't appear before or after a, and b^{-1} doesn't appear before or after b in the sequence. e.g., aab is a reduced word, but aaa^{-1} is not. Lists in ACL2 are used to represent these sequences in our proof, and the recognizer *reducedwordp* returns true if a list of characters satisfies the properties of a reduced word. For example, list (a a b) is a reduced word.

The function, *word-fix* fixes a list with the characters a, a^{-1}, b, and b^{-1} and makes it a reduced word by "cancelling" adjacent "inverses" and the function *compose*, defined below, acts as a group operation over reduced words.

```
(defun compose (x y)
  (word-fix (append x y)))
```

The function, *word-flip* flips each character in the list to its inverse. For example, (*word-flip* (a a b)) = (a^{-1} a^{-1} b^{-1}). The function *word-inverse*, defined below, returns the inverse of the list.

```
(defun word-inverse (x)
  (rev (word-flip x)))
```

The set of these reduced words generates a free group with empty list acting as the identity element of the group. Below are the theorems about group properties of the set of reduced words.

Let's call the set of the reduced words W, lists that start with a as $W(a)$, lists that start with a^{-1} as $W(a^{-1})$, lists that start with b as $W(b)$, and lists that start with b^{-1} as $W(b^{-1})$. Then $W = () \uplus$ [1] $W(a) \uplus W(a^{-1}) \uplus W(b) \uplus W(b^{-1})$ and we have also proved the below two equivalences:

$$W = a^{-1}W(a) \uplus W(a^{-1})$$
$$W = b^{-1}W(b) \uplus W(b^{-1})$$

3 A Free Group of Rotations of rank 2

If we map the below four matrices to the characters a, a^{-1}, b, and b^{-1}, and then associate each list of the reduced words set with matrix multiplication, we get a set

[1] Disjoint union

of 3-d matrices. Let's call this set R.

$$a^{\pm} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{3} & \mp\frac{2\sqrt{2}}{3} \\ 0 & \pm\frac{2\sqrt{2}}{3} & \frac{1}{3} \end{bmatrix} \quad b^{\pm} = \begin{bmatrix} \frac{1}{3} & \mp\frac{2\sqrt{2}}{3} & 0 \\ \pm\frac{2\sqrt{2}}{3} & \frac{1}{3} & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

We can represent the matrices in R using the *array2p* datastructure in ACL2. Matrix multiplication (m-∗), matrix equivalence (m-=) have already been developed and the associative property of m-∗ has also been proved in ACL2 [7].

Now coming back to the proof, let the triple (x, y, z) represent the triple $(x_0 \times 3^n/\sqrt{2}, y_0 \times 3^n, z_0 \times 3^n/\sqrt{2})$ where (x_0, y_0, z_0) is the point we get by multiplying the point $(0, 1, 0)$ with a matrix ρ that is one of the elements of R that is mapped to one of the reduced words with length $n > 0$. By induction, it is shown that, x, y and z are integers. If the matrix ρ is identity matrix, then, $(x, y, z) \pmod 3 \equiv (0, 0, 0)$. The function *n-mod3* returns the $\pmod 3$ value of the triple (x, y, z). So, $(\textit{n-mod3}\ \ \rho) = (x, y, z) \pmod 3$. We have proved the below equivalences for the function *n-mod3*:

$$\begin{aligned} (\textit{n-mod3}\ \ (a * \rho)) &\equiv (0, y - z, z - y) \\ (\textit{n-mod3}\ \ (a^{-1} * \rho)) &\equiv (0, y + z, z + y) \\ (\textit{n-mod3}\ \ (b * \rho)) &\equiv (x + y, x + y, 0) \\ (\textit{n-mod3}\ \ (b^{-1} * \rho)) &\equiv (x - y, y - x, 0) \end{aligned}$$

By induction, and using the above equivalences, we have shown that for any matrix m in R that is mapped to a reduced word with length $n > 0$, $(\textit{n-mod3}\ \ m) \not\equiv (0, 0, 0)$. So, m is not an identity matrix; which implies that the set R is a free group of rank 2 with identity matrix acting as the identity element of the group.

We have defined a recognizer *r3-rotationp* which returns true if a 3-d matrix is a rotation. By induction, we have shown that every element of R is a rotation.

Let's say, $R(a)$ is the set of matrices we get by composing the list of reduced words that start with a, $R(b)$ by composing the list of reduced words that start with b, $R(a^{-1})$ by composing the list of reduced words that start with a^{-1}, and $R(b^{-1})$ by composing the list of reduced words that start with b^{-1}, then

$$R = I \uplus R(a) \uplus R(a^{-1}) \uplus R(b) \uplus R(b^{-1})$$

4 Hausdorff Paradox

Since ACL2 does not support infinite sets, we use predicates to reason about infinite sets indirectly, as done in prior work[8]. We have defined a recognizer *s2-def-p* that returns true if a point is on S^2. A recognizer *d-p* that returns true if it is is one of the poles of the rotations in the set R. Let's call the set of poles D. A recognizer, *s2-d-p* that returns true if it is a point belongs to $S^2 - D$. We have shown that if a point, $p \in S^2 - D$ and $\rho \in R$, then $\rho(p) \in S^2 - D$.

The orbit of a point $p \in S^2 - D$ is defined as $\{\rho(p) \mid \rho \in R\}$. Points belong to the same class if they belong to the same orbit. Using *defchoose* with *strengthen* option in ACL2 we can pick one point from these equivalence classes. If we pick two points from the same equivalence class, then because of the *strengthen* option, they both are going to be equal. Let's call the points that we picked from each of the equivalence classes, M. So,

$$S^2 - D = RM = M \uplus R(a)M \uplus R(a^{-1})M \uplus R(b)M \uplus R(b^{-1})M$$

and using the equivalences in section 2 we have proved:

$$\begin{aligned} S^2 - D &= a^{-1}R(a)M \uplus R(a^{-1})M \\ S^2 - D &= b^{-1}R(b)M \uplus R(b^{-1})M \end{aligned}$$

We have proved that the sets M, $R(a)M$, $R(a^{-1})M$, $R(b)M$, $R(b^{-1})M$ are disjoint, sets $a^{-1}R(a)M$, $R(a^{-1})M$ are disjoint and the sets $b^{-1}R(b)M$, $R(b^{-1})M$ are disjoint.

Since, all the rotations are countable and since each rotation has two poles, all the poles are countable; which means the set D is countable.

References

[1] T. Weston, "The Banach-Tarski Paradox," 2003.

[2] R. Gamboa and J. Cowles, "A Cantor Trio: Denumerability, the Reals, and the Real Algebraic Numbers," in *Interactive Theorem Proving*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 51–66.

[3] R. A. Gamboa and M. Kaufmann, "Nonstandard analysis in ACL2," *Journal of automated reasoning*, vol. 27, no. 4, pp. 323–351, 2001.

[4] J. Bapanapally and R. Gamoboa, "A Formal Proof of the Hausdorff Paradox," https://github.com/acl2/acl2/tree/master/books/nonstd/nsa/Banach-Tarski, 2021.

[5] "Non-measurable Set," https://en.wikipedia.org/wiki/Non-measurable_set, accessed: 2021-12-01.

[6] T. J. Jech, *The axiom of choice*. Courier Corporation, 2008.

[7] R. Gamboa, J. Cowles, and J. Baalen, "Using ACL2 Arrays to Formalize Matrix Algebra," in *Fourth International Workshop on the ACL2 Theorem Prover and Its Applications (ACL203)*, vol. 1, 2003.

[8] J. Cowles and R. Gamboa, "Using a First Order Logic to Verify That Some Set of Reals Has No Lesbegue Measure," in *Interactive Theorem Proving*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 25–34.