CONTINUOUS INVERSE AMBIGUOUS FUNCTIONS ON LIE GROUPS

DAVID SCHMITZ, SADMAN RAHMAN, AND ANTHONY KINDNESS

Abstract. In Schmitz (Aequ Math 91:373 - 389, 2017), the first author defines an inverse ambiguous function on a group G to be a bijective function $f : G \to G$ satisfying the functional equation $f^{-1}(x) = f(x^{-1})$ for all $x \in G$. In this paper, we investigate the existence of continuous inverse ambiguous functions on various Lie groups. In particular, we look at tori, elliptic curves over various fields, vector spaces, additive matrix groups, and multiplicative matrix groups.

Contents

1. Introduction 1
2. Tori 2
3. Elliptic Curves 3
4. Vector Spaces and Spheres 6
5. Multiplicative Matrix Groups 8
References 10

1. Introduction

We define an inverse ambiguous function to be a bijective function $f : G \to G$, where G is a group, that satisfies the functional equation

$$f^{-1}(x) = (f(x))^{-1} \tag{1.1}$$

for all $x \in G$. This condition is equivalent to

$$f(f(x)) = x^{-1} \tag{1.2}$$

for all $x \in G$, where x^{-1} denotes the inverse of x in G, which in turn implies that $f(x^{-1}) = f(x)^{-1}$ for all $x \in G$ ([5], Corollary 2.3).

In [5], the first author investigated the existence of inverse ambiguous functions on the additive and multiplicative groups associated to fields, with the added assumption of continuity for topological fields. In [6], the existence of inverse ambiguous functions on some non-abelian groups was studied. For finite groups, we have the following two facts [5, Theorem 3.3 and Theorem 4.1]:

Theorem 1.3. *Let G be a finite group, and let $S(G)$ denote the subset of G consisting of all elements of order 1 or 2. Then*

(1) If $f : G \to G$ is an inverse ambiguous function, then $f(S(G)) = S(G)$.
(2) An inverse ambiguous function exists on G if and only if the number of elements in $G - S(G)$ is a multiple of 4.

In this paper, we focus on the existence of continuous inverse ambiguous functions on topological groups, primarily Lie groups. Recall that a topological group is a topological space endowed with a continuous binary operation satisfying the usual group operations, where the inverse map $x \mapsto x^{-1}$ is continuous. We note that if G is a topological group and $f : G \to G$ is a continuous inverse ambiguous function, then according to Equation (1), the inverse function f^{-1} must also be continuous since it is the composition of two continuous functions. In other words, a continuous inverse ambiguous function is necessarily a homeomorphism. Therefore, if G is a topological group and $\mathrm{Homeo}(G)$ is the associated homeomorphism group (under composition), then the existence of a continuous inverse ambiguous function f on G is more or less equivalent to existence of a "square root of -1", whereby -1 we mean the inversion map $x \mapsto x^{-1}$. To put it a different way, f generates a cyclic subgroup of order 4 in $\mathrm{Homeo}(G)$.

Using algebraic and topological methods, we will consider the question of existence of inverse ambiguous functions on the spherical groups S^1 and S^3, tori, elliptic curves (over various fields), and matrix groups.

2. Tori

We begin with the following lemma.

Lemma 2.1. *There are no continuous inverse ambiguous functions on the circle group, S^1.*

Proof. By way of contradiction, assume that $f : S^1 \to S^1$ is an inverse ambiguous function. By definition, $f \circ f = \iota$, where $\iota(z) = z^{-1}$ for all $z \in S^1$. Since f and ι are homeomorphisms on G, they induce group automorphisms f_* and ι_*, respectively, on the fundamental group $\pi_1(S^1) = \mathbb{Z}$ such that $f_* \circ f_* = \iota_*$. Because ι reverses the direction of loops in S^1, it follows that $\iota_*(n) = -n$ for all $n \in \mathbb{Z}$. However, the only group automorphisms on $\mathbb{Z}$ are the identity map and the map $n \mapsto -n$, and either of these composed with itself produces the identity map, not ι_*. We have reached a contradiction, and so there are no inverse ambiguous functions on S^1. □

The fundamental group can similarly be used to show the non-existence of inverse ambiguous functions on tori $\mathbb{T}^n$ when n is odd. For this, we recall the well-known result [1, Proposition 1.12] that for path-connected spaces X_i, $i = 1, \ldots, n$, we have

$$\pi_1\left(\prod_{i=1}^{n} X_i\right) \cong \prod_{i=1}^{n} \pi_1(X_i).$$

Theorem 2.2. *If n is a positive odd integer, then there exist no continuous inverse ambiguous functions on the torus $\mathbb{T}^n$.*

Proof. By way of contradiction, assume that $f : \mathbb{T}^n \to \mathbb{T}^n$ is an inverse ambiguous function, where n is odd. As in the proof of the previous lemma, f and ι are induce group automorphisms f_* and ι_*, respectively, on the fundamental group $\pi_1(\mathbb{T}^n) \cong \mathbb{Z}^n$ such that $f_* \circ f_* = \iota_*$. Under the isomorphism $\pi_1(\mathbb{T}^n) \cong \mathbb{Z}^n$, ι_* becomes the map

$$\iota_* : (m_1, m_2, \ldots, m_n) \mapsto (-m_1, -m_2, \ldots, -m_n).$$

Thus, as an isomorphism of abelian groups (or $\mathbb{Z}$-modules), the map f_* can be associated to an element in $A_f \in GL_n(\mathbb{Z})$ such that $(A_f)^2 = -I_n$, where I_n is the $n \times n$ identity matrix. Taking determinants of both sides, we get $\det(A_f)^2 = (-1)^n = -1$, which is impossible since $\det(A_f)^2$ is an

integer. We have reached a contradiction, and so there are no inverse ambiguous functions on $\mathbb{T}^n$ when n is odd. □

On the other hand, when n is even, there do exist inverse ambiguous functions on $\mathbb{T}^n$. We begin with looking at $\mathbb{T}^2$. Define the function $f : S^1 \times S^1 \to S^1 \times S^1$ by

$$f(z, w) = \left(w, z^{-1}\right).$$

Then, it is easy to verify that f is a homeomorphism from $\mathbb{T}^2$ to itself such that

$$f(f(z, w)) = f\left(w, z^{-1}\right) = \left(z^{-1}, w^{-1}\right) = (z, w)^{-1}$$

for all $z, w \in S^1$. Hence, f is inverse ambiguous. To show the existence of inverse ambiguous functions on other tori $\mathbb{T}^n$ with n even, we can the following, whose proof is straightforward.

Proposition 2.3. *Let G and H be topological groups and suppose that $g : G \to G$ and $h : H \to H$ are continuous inverse ambiguous functions. Then $f = (g, h)$ is a continuous inverse ambiguous function defined on $G \times H$.*

Applying this proposition inductively, we obtain the following result.

Theorem 2.4. *If n is a positive even integer, then there exist continuous inverse ambiguous functions on the torus $\mathbb{T}^n$.*

A specific example of a continuous (smooth, in fact) inverse ambiguous function on $\mathbb{T}^{2n}$ is defined by

$$g : (z_1, w_1; z_2, w_2; \ldots; z_n, w_n) \mapsto \left(w_1, z_1^{-1}; w_2, z_2^{-1}; \ldots; w_n, z_n^{-1}\right).$$

Remark 2.5. More generally, if G is *any* topological group and $H = G^{2n}$ (a direct product of an *even* number of copies of G), then the function g described above is a continuous inverse ambiguous function on H.

3. Elliptic Curves

An elliptic curve E over a field K is a smooth 1-dimensional projective variety of genus 1. Up to isomorphism, an elliptic curve consists of the set of solutions $[x, y, 1] \in \mathbb{P}^2(K)$ of a Weierstrass equation

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6,$$

with coefficients in K, together with the "point at infinity" $O = [0, 1, 0]$. Over fields of characteristic not equal to 2 or 3, a change of variables can transform the Weierstrass equation into the form

$$Y^2 = X^3 + aX + B,$$

with $a, b \in K$. Smoothness is equivalent to the discriminant $\Delta_E = -16(4a^3 + 27b^2)$ being non-zero. (See [7], Chapter 3.) Furthermore, it is not difficult to show (using differential calculus, for example) that Δ_E is positive (resp., negative), when $X^3 + aX + b$ has 1 real root (resp., 3 real roots).

An elliptic curve over $\mathbb{C}$ is isomorphic (as a Lie group) to a complex torus $\mathbb{C}/\Lambda$, where Λ is a lattice generated over $\mathbb{Z}$ by two $\mathbb{R}$-linearly independent complex numbers ω_1, ω_2:

$$\Lambda = \{n_1\omega_1 + n_2\omega_2 \mid n_1, n_2 \in \mathbb{Z}\}.$$

(See [7, Corollary 5.1.1].)

Theorem 3.1. *Every elliptic curve over $\mathbb{C}$ admits a continuous inverse ambiguous function.*

Proof. Using the notation above, the $\mathbb{R}$-linear independence of ω_1 and ω_2 implies that (ω_1, ω_2) is an $\mathbb{R}$-basis of $\mathbb{C}$. Therefore, we can define an $\mathbb{R}$-linear transformation $f : \mathbb{C} \to \mathbb{C}$ by $f(c_1\omega_1 + c_2\omega_2) = -c_2\omega_1 + c_1\omega_2$. This function is a continuous isomorphism of $\mathbb{R}$-vector spaces with the property that

$$f(f(c_1\omega_1 + c_2\omega_2)) = f(-c_2\omega_1 + c_1\omega_2) = -c_1\omega_1 - c_2\omega_2.$$

In other words, $f(f(z)) = -z$ for all $z \in \mathbb{C}$. Moreover, $f(\Lambda) = \Lambda$. Hence, f induces a well-defined homeomorphism $\tilde{f} : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda$ where $\tilde{f}(z + \Lambda) = -z + \Lambda$. In other words, $\tilde{f}$ is a continuous inverse ambiguous function on $\mathbb{C}/\Lambda$. □

It is known that the group of real points of an elliptic curve E over $\mathbb{R}$ is isomorphic (as Lie groups) to either S^1 (which happens when $\Delta_E < 0$) or $S^1 \times \mathbb{Z}_2$ (which happens when $\Delta_E > 0$) [2, Introduction, Proposition 7.2]. In the next theorem, we show that a continuous inverse ambiguous function exists on the elliptic curve in the latter case, but not the former.

Theorem 3.2. *Let $E(\mathbb{R})$ be the Lie group of real points on an elliptic curve over $\mathbb{R}$. Then $E(\mathbb{R})$ admits a continuous inverse ambiguous function if and only if $\Delta_E > 0$.*

Proof. First, suppose that $\Delta_E < 0$, then $E(\mathbb{R}) \cong S^1$. According to Lemma 2.1, no continuous inverse ambiguous functions can exist on $E(\mathbb{R})$.

Next, assume $\Delta_E > 0$. Then $E(\mathbb{R}) \cong S^1 \times \mathbb{Z}_2$. The two connected components of this space are the subgroup $S^1 \times \{0\}$ and its complement $S^1 \times \{1\}$. Therefore, we can define a continuous function on $S^1 \times \mathbb{Z}_2$ that maps points of the form $(z, 0)$ to $(z, 1)$ and points of the form $(w, 1)$ to $(w^{-1}, 0)$. One can easily check that $f(f(z, 0)) = (z^{-1}, 0) = (z, 0)^{-1}$ and $f(f(z, 1)) = (z^{-1}, 1) = (z, 1)^{-1}$ for every $z \in S^1$. This shows that there exists a continuous inverse ambiguous function on $S^1 \times \mathbb{Z}_2$, and so the same is true for $E(\mathbb{R})$. □

In fact, if G is *any* topological group, then the function defined by

$$f((z, 0)) = (z, 1), \qquad \text{and} \qquad f((w, 1)) = \left(w^{-1}, 0\right)$$

is a continuous inverse ambiguous function on $G \times \mathbb{Z}_2$. With a little more effort, we can generalize this construction to some other finite groups H besides $\mathbb{Z}_2$.

Proposition 3.3. *Let G be any topological group and H any finite group satisfying the following two conditions:*

1. *The number of self-invertible elements in H is even.*
2. *The number of non-self-invertible elements in H is a multiple of 4.*

Then $G \times H$ admits a continuous inverse ambiguous function.

This proposition applies, in particular, to A_4, A_5, A_n $(n \geq 8)$, S_n $(n \geq 6)$ (see [6]), and cyclic groups $\mathbb{Z}_n$ with $n \equiv 2 \mod 4$ (see [5]).

Proof. With G and H satisfying the assumptions in the proposition, enumerate the self-invertible elements of H as

$$S(H) = \{a_1, a_2, ..., a_n, b_1, b_2, ..., b_n\}.$$

As in [5, Corollary 3.5], the non-self-invertible elements can be partitioned into subsets of the form $\{c_i, d_i, c_i^{-1}, d_i^{-1}\}$ for $i = 1, ..., m$. Taking advantage of the fact that the subspaces $\{G \times \{x\}\}_{x \in H}$ are

unions of connected components of $G \times H$, we can define a continuous function $f : G \times H \to G \times H$ by the following rules:

$$\begin{array}{rll} f((g,a_i)) & = (g,b_i) & \text{for } i = 1,\dots,n \\ f((g,b_i)) & = (g^{-1},a_i) & \text{for } i = 1,\dots,n \\ f((g,c_j)) & = (g,d_j) & \text{for } j = 1,\dots,m \\ f((g,d_j)) & = (g^{-1},c_j^{-1}) & \text{for } j = 1,\dots,m \\ f((g,c_j^{-1})) & = (g,d_j^{-1}) & \text{for } j = 1,\dots,m \\ f((g,d_j^{-1})) & = (g^{-1},c_j) & \text{for } j = 1,\dots,m. \end{array}$$

It is a straightforward exercise to verify that $f(f((g,h))) = (g^{-1},h^{-1})$ for all elements $(g,h) \in G \times H$. □

Finally, we consider elliptic curves defined over finite fields. For simplicity, we will assume E is defined by a Weierstrass equation of the form

$$Y^2 = X^3 + aX + b \tag{3.4}$$

where $g(X) = X^3 + aX + b \in \mathbb{Z}[X]$. If $\mathbb{F}_q$ (q a power of a prime) is a finite field and $\Delta_E = -16(4a^3 + 27b^2)$ is non-zero in $\mathbb{F}_q$, then the group $E(\mathbb{F}_q)$ is finite, and with respect to the discrete topology, any inverse ambiguous function on $E(\mathbb{F}_q)$ is continuous. Therefore, according to Theorem 1.3, the existence of an inverse ambiguous function on $E(\mathbb{F}_q)$ amounts to showing that the number of non-self-invertible elements in $E(\mathbb{F}_q)$ is a multiple of 4.

The self-invertible elements in $E(\mathbb{F}_q)$ are the point at infinity, O, and the elements of order 2. The latter are known to be of the form $(r,0)$, where r is a root of $g(X)$ ([8], Section 2.1). Under the assumption that $\Delta_E \neq 0$ in $\mathbb{F}_q$, it follows that $g(X)$ has either 0, 1, or 3 roots in $\mathbb{F}_q$. On the other hand, if $s \in \mathbb{F}_q$ is *not* a root of $g(X)$, then the equation $Y = g(s)$ will have either 0 or 2 solutions for Y in $\mathbb{F}_q$. This implies that the number of non-self-invertible elements in $E(\mathbb{F}_q)$ will always be even, and it will be a multiple of 4 if and only if the set

$$N_q = \{s \in \mathbb{F}_q \mid g(s) \text{ is a non-zero square in } \mathbb{F}_q\}$$

has an even number of elements.

Suppose $g(X)$ has 3 roots in $E(\mathbb{F}_q)$. This would mean that $S(E(\mathbb{F}_q))$ is a subgroup of order 4 in $E(\mathbb{F}_q)$, which in turn implies, according to LaGrange's Theorem, that the order of $E(\mathbb{F}_q)$, and hence N_q, is a multiple of 4. We have proved the following:

Proposition 3.5. *Suppose $g(X) = X^3 + aX + b$ has three distinct roots in $\mathbb{F}_q$. Then the elliptic curve defined by the Weierstrass equation $Y^2 = g(X)$ admits a (continuous) inverse ambiguous function.*

We now consider a couple of examples:

Example 3.6. Consider the group of $\mathbb{F}_q$-points on the elliptic curve defined by the Weierstrass equation $Y^2 = X^3 - X$. Then $\Delta_E = 64$, which is non-zero in $\mathbb{F}_q$ for every odd q. For every such q, $g(X) = X^3 - X$ has three distinct roots in $E(\mathbb{F}_q)$, namely $-1, 0, 1$. Therefore, by Proposition 3.5, $E(\mathbb{F}_q)$ admits a (continuous) inverse ambiguous function for every odd q.

Example 3.7. Consider the Weierstrass equation $Y^2 = X^3 + X$. Then $\Delta_E = -64$, which is non-zero in $\mathbb{F}_q$ for every odd q. For every such $q = p^n$ for which $p \equiv 1 \mod 4$ or $p \equiv 3 \mod 4$ with n even, $g(X) = X^3 + X$ has three distinct roots in $E(\mathbb{F}_q)$, namely 0 and the 2 square roots of -1. For

these values of q, Proposition 3.5 guarantees that $E(\mathbb{F}_q)$ admits a (continuous) inverse ambiguous function. Therefore, by Proposition 3.5, $E(\mathbb{F}_q)$ admits a (continuous) inverse ambiguous function.

However, if $q = p^n$ with $p \equiv 3 \mod 4$ and n odd, then $g(X)$ has exactly 1 root ($X = 0$) in $\mathbb{F}_q$ because $p^n = X^2 + 1$ has no solution in $\mathbb{Z}$ ([4], Theorem 13.6). Among the non-zero elements of $\mathbb{F}_q$ there are $(q-1)/2$ squares and $(q-1)/2$ non-squares, and the subset of non-squares is collectively the additive inverses of the subset of squares (because -1 is not a square). Because $g(X)$ is an odd polynomial, exactly one of $g(a)$ and $g(-a)$ will be a square in $\mathbb{F}_q$ for each non-zero $a \in \mathbb{F}_q$. Since $(q-1)/2$ is odd, it follows that the $|N_q| \equiv 2 \mod 4$, which means that there are no (continuous) inverse ambiguous functions defined on $E(\mathbb{F}_q)$.

4. Vector Spaces and Spheres

We next look into the existence of continuous inverse ambiguous functions on vectors spaces. Our investigation will consider vector spaces over various fields of scalars. First, if V is an n-dimensional complex vector space, then we see immediately that the linear transformation $f(v) = iv$ is a continuous inverse ambiguous function defined on V.

Next, let V be an n-dimensional vector space over the finite field $\mathbb{F}_q$ where $q = p^r$ for some prime p. Using the fact that the group $\mathbb{F}_q^\times$ is cyclic, it follows that if $q \equiv 1 \mod 4$ or if $p = 2$, then there exists $\alpha \in \mathbb{F}_q$ such that $\alpha^2 = -1$, and so $f : V \to V$ defined by $f(v) = \alpha v$ is a (continuous) inverse ambiguous function on V. Now suppose $q \equiv 3 \mod 4$. Then V has q^n elements, only one of which, 0_V, is self-invertible. Therefore, according to Theorem 1.3, there exists a (continuous) inverse ambiguous function on V if and only if $q^n \equiv 1 \mod 4$, which occurs if and only if n is even. In summary:

Theorem 4.1. *Let V be an n-dimensional vector space over the finite field $\mathbb{F}_q$, where q is a power of a prime p.*

1. *If q is even or $q \equiv 1 \mod 4$, then V admits a (continuous) inverse ambiguous function.*
2. *If $q \equiv 3 \mod 4$, then V admits a (continuous) inverse ambiguous function if and only if n is even.*

We next turn our attention to finite-dimensional real vector spaces. If $V = \mathbb{R}^{2n}$ is even-dimensional, then using Remark 2.5 it follows that

$$f : (x_1, y_1; x_2, y_2; \ldots; x_n, y_n) \mapsto (y_1, -x_1; y_2, -x_2; \ldots; y_n, -x_n) \tag{4.2}$$

is a continuous inverse ambiguous function on V. If V is canonically identified with $\mathbb{C}^n$, then f is the function that multiplies each coordinate by i.

On the other hand, if $V = \mathbb{R}^{2n+1}$ is odd-dimensional, then we will demonstrate that there exists no continuous inverse ambiguous function on V. On the contrary, suppose $f : V \to V$ were such a function. Since 0 is the only self-invertible element in V, we know that $f(0) = 0$. As a homeomorphism of V, f either preserves or reverses the orientation of V (at 0). (See [1], Section 3.3, for example, for a discussion of orientation on manifolds.) In either case, $f \circ f$ must *preserve* the orientation of V (at 0). However, the inverse map $\iota : V \to V$, which is the linear transformation with matrix $-I_{2n+1}$, reverses orientation since $\det(-I_{2n+1}) = -1$. Therefore, $f \circ f = \iota$ is not possible. In summary:

Theorem 4.3. *An n-dimensional vector space V over $\mathbb{R}$ admits a continuous inverse ambiguous function if and only if n is even.*

Since the additive matrix groups $M_n(\mathbb{R})$ and $M_n(\mathbb{C})$ are isomorphic as Lie groups to, respectively, $\mathbb{R}^{n^2}$ and $\mathbb{C}^{n^2}$, we immediately obtain the following result.

Corollary 4.4.

(1) For every positive integer n, the topological group $M_n(\mathbb{C})$ admits a continuous inverse ambiguous function, one example being $A \mapsto iA$.
(2) The topological group $M_n(\mathbb{R})$ admits a continuous inverse ambiguous function if and only if n even.

Corollary 4.5.

(1) For every positive integer n, the subspace of all matrices in $M_n(\mathbb{C})$ having trace 0 admits a continuous inverse ambiguous function.
(2) The subspace of all matrices in $M_n(\mathbb{R})$ having trace 0 admits a continuous inverse ambiguous function if and only if n is odd.

Proof. This follows from the previous corollary in light of the fact that the subspace of trace-0 matrices has codimension 1. □

Consideration of orientation can also be used to determine existence or non-existence of continuous inverse ambiguous functions on n-spheres. The only spheres that are connected Lie groups are S^1 and S^3 (see [1], Section 3.C). We saw earlier that there are no continuous ambiguous functions defined on S^1 (Theorem 2.1). It turns out the same holds for S^3. The multiplicative group S^3 can be identified with the unit quaterions $\mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$, where $i^2 = j^2 = k^2 = 1$ and $ijk = -1$. Now, if $f : S^3 \to S^3$ were continuous and inverse ambiguous, then $f \circ f$ would preserve the orientation of S^3. However, the group inverse map ι fixes 1 and maps each of i, j, and k to their additive inverses $-i$, $-j$, and $-k$. Therefore, with respect to the ordered basis $\{1, i, j, k\}$, ι is given by the matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix},$$

which has determinant -1. Therefore, ι is orientation reversing, and this implies that $f \circ f = \iota$ is not possible. Hence:

Theorem 4.6. *No continuous inverse ambiguous functions are defined on S^3.*

Finally, even though S^n does not have a group structure for all n, the symmetry of each sphere (as a subspace of Euclidean space) allows us to consider homeomorphisms $f : S^n \to S^n$ such that

$$f(f(z)) = -z \qquad \text{for all } z \in S^n. \tag{4.7}$$

(In other words, $f \circ f$ is the antipodal map on S^n.) The linear map $\iota : z \mapsto -z$ on $\mathbb{R}^{n+1}$ has matrix $-I_{n+1}$. If n even, then $\det(-I_{n+1}) = -1$, which indicates that ι is orientation reversing on $\mathbb{R}^{n+1}$, and thus also on S^n. As a result, $f \circ f$ cannot equal ι for any homeomorphism of S^n to itself since,

as noted before, the composition $f \circ f$ would be orientation preserving regardless of whether f is orientation preserving or reversing. On the other hand, if $m = 2n - 1$ is odd, it is easily verified that the function defined in Equation (4.2) restricts to a homeomophism from S^m to itself that satisfies Equation (4.7). This completes the proof of the following:

Theorem 4.8. *There exists a homeomorphism $f : S^n \to S^n$ satisfying the equation $f(f(z)) = -z$ for all $z \in S^n$ if and only if n is odd.*

5. Multiplicative Matrix Groups

In this final section, we begin an investigation of the multiplicative group $G = GL_n(\mathbb{R})$ and some of its subgroups. We observe that G has two connected components, namely $GL_n^+(\mathbb{R})$, the normal subgroup of all matrices in G with a positive determinant, and $GL_n^-(\mathbb{R})$, the subset of all matrices in G with a negative determinant. Moreover, the orthogonal group

$$O(n) = \{A \in G \mid AA^T = I_n\}$$

is a closed subgroup of G whose components are $SO(n) = O^+(n)$ and its complement.

When n is odd, we can use the disconnectedness of G to define a continuous inverse ambiguous function on G.

Theorem 5.1. *Assume n is positive odd integer. Then the function $f : GL_n(\mathbb{R}) \to GL_n(\mathbb{R})$ defined by*

$$f(A) = \begin{cases} -A & \text{if } A \in GL_n^+(\mathbb{R}) \\ -A^{-1} & \text{if } A \in GL_n^-(\mathbb{R}) \end{cases}$$

is continuous and inverse ambiguous. Furthermore, this function restricts to a continuous inverse ambiguous function from $O(n)$ to $O(n)$.

Proof. Suppose n is odd. First, we see that if $\det(A) > 0$, then

$$\det(-A) = (-1)^n \det(A) = -\det(A) < 0.$$

Similarly, if $\det(A) < 0$, then

$$\det(-A^{-1}) = (-1)^n \det(A^{-1}) = -\det(A) > 0.$$

This shows that f is well-defined. The continuity of f is clear, as is the fact that $f(f(A)) = A^{-1}$ for all A. The last statement follows from the fact that $A \in O(n)$ if and only if $-A$ and A^{-1} belong to $O(n)$. □

If n is even, then the strategy used to define the function in the above theorem does not work since $\det(-A) = (-1)^n \det(A) = \det(A)$. In other words, A and $-A$ belong to the same connected component. In fact, as we will demonstrate, when $n = 2$, the strategy of defining a continuous inverse ambiguous function that swaps components of $GL_2(\mathbb{R})$ is not possible.

Lemma 5.2. *In $GL_2^+(\mathbb{R})$, there are exactly 2 self-invertible elements, while in $GL_2^-(\mathbb{R})$ there are infinitely many self-invertible elements.*

Proof. Suppose $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ satisfies $A^2 = I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Then

$$a^2 = 1 - bc = d^2, \qquad \text{and} \qquad b(a + d) = 0 = c(a + d)$$

are necessary and sufficient conditions for the entries of A.

If $a, d \neq 0$, then the first equation gives us $a = \pm d$. If, further, $a = d$, then $a + d \neq 0$, which implies that $b = c = 0$, and hence $a^2 = 1 - 0 = d^2$, or $a = d = \pm 1$. The resulting matrices are $\pm I_2$, both of which have determinant 1. If, $a = -d \neq 0$, then any real numbers b, c satisfying $bc = 1 - a^2$ (for which there are infinitely many combinations for any value of a) will give a solution for A. In this case, $\det(A) = ad - bc = -a^2 - bc = -1$. Finally, if $a = d = 0$, then $1 - bc = 0 = ad$, and so $\det(A) = ad - bc = 0 - bc = -1$. □

Remark 5.3. The two self-invertible elements in $GL_2^+(\mathbb{R})$ are the identity matrix and the matrix representing a half turn about the origin. Among the self-invertible elements in $GL_2^-(\mathbb{R})$ are matrices representing reflections across lines through the origin. Because a self-invertible matrix in $GL_n(\mathbb{R})$ must have determinant ± 1, the lemma also shows that $SO(2)$ (resp. $O(2) - SO(2)$) has exactly 2 (resp. infinitely many) self-invertible elements.

In light of this lemma and Theorem 1.3, we see that any continuous inverse ambiguous function $f : GL_2(\mathbb{R}) \to GL_2(\mathbb{R})$ must map $GL_2^+(\mathbb{R})$ to $GL_2^+(\mathbb{R})$ and $GL_2^-(\mathbb{R})$ to $GL_2^-(\mathbb{R})$. More specifically, either f fixes I_2 and $-I_2$ or transposes them. Similarly, any continuous inverse ambiguous function $f : O(2) \to O(2)$ would necessarily restrict to a continuous inverse ambiguous function on $SO(2)$. However, $SO(2)$ is isomorphic to S^1 as Lie groups, and S^1 admits no continuous inverse ambiguous functions (Lemma 2.1). This proves the following:

Theorem 5.4. *There are no continuous inverse ambiguous functions defined on $O(2)$ or on $SO(2)$.*

We next consider the special linear group $SL_n(\mathbb{R})$, which is the Lie subgroup of $GL_n(\mathbb{R})$ consisting of all matrices with determinant equal to 1. Our investigation will consider orientations as we did in the previous section. We first establish a lemma.

Lemma 5.5. *If $\iota : GL_n(\mathbb{R}) \to GL_n(\mathbb{R})$ is the inverse map, then the differential of ι at the identity matrix I_n is $-I^{n^2}$.*

Proof. For each $1 \leq i, j \leq n$, denote by e_{ij} the $n \times n$ matrix with all 0 entries except for a 1 in the ij^{th} position. Consider the n^2 curves in $GL_n(\mathbb{R})$, defined for $t \in \mathbb{R}$ and each passing through I_n at $t = 0$:

$$\gamma_{ij}(t) = I_n + t \cdot e_{ij}.$$

One can check that

$$\iota(\gamma_{ij}(t)) = \begin{cases} I_n - t \cdot e_{ij} & \text{if } i \neq j \\ I_n - \dfrac{t}{t+1} \cdot e_{ii} & \text{if } i = j. \end{cases}$$

Differentiating each of these image curves and evaluating at $t = 0$, we get $d\iota|_{I_n}(e_{ij}) = -e_{ij}$ for all i, j. This implies that $d\iota|_{I_n} = -I_{n^2}$, as desired. □

Now, the determinant of $d\iota|_{I_n}$ is $(-1)^{n^2}$, which indicates that ι is orientation preserving (resp. reversing) on $GL_n^+(\mathbb{R})$ when n is even (resp. odd). Thus, we do *not* arrive at the usual orientation-related contradiction that would rule out the existence of a continuous inverse ambiguous function on $GL_n^+(\mathbb{R})$ when n is even. However, we can deduce the following:

Theorem 5.6. *There are no continuous inverse ambiguous functions on $GL_n^+(\mathbb{R})$ when n is odd.*

Consequently, the only continuous inverse ambiguous functions on $GL_n(\mathbb{R})$ for odd n must map each of its two connected components to the other one (as demonstrated in Theorem 5.1).

Now consider the connected, $n^2 - 1$ dimensional, Lie subgroup $SL_n(\mathbb{R})$ of $GL_n(\mathbb{R})$. (See [1], Example 5.27.) Because $SL_n(\mathbb{R})$ is an embedded submanifold of the general linear group, $d\iota|_{I_n}$ on the tangent space of $SL_n(\mathbb{R})$ is simply the restriction of $d\iota|_{I_n}$ from the tangent space of $GL_n(\mathbb{R})$ [1, Chapter 5]. In other words, for $SL_n(\mathbb{R})$, $d\iota|_{I^n} = -I_{n^2-1}$, which has determinant -1 if and only if n is even. Hence, whether f is a orientation preserving or reversing continuous inverse ambiguous function on $SL_n(\mathbb{R})$ (n even), then $f \circ f$ is orientation preserving but ι is orientation reversing. Therefore,

Theorem 5.7. *If n is even, there are no continuous inverse ambiguous functions on $SL_n(\mathbb{R})$.*

Likewise, since $SO(n)$ is a connected, $\binom{n}{2}$-dimensional embedded Lie subgroup of $GL_n(\mathbb{R})$ [1, Example 5.42], then a similar argument shows that whenever $\binom{n}{2} = \frac{1}{2}(n)(n-1)$ is odd, then there are no continuous inverse ambiguous functions defined on $SO(n)$. More simply,

Theorem 5.8. *If $n \equiv 2$ or $3 \mod 4$, then there are no continuous inverse ambiguous functions on $SO(n)$.*

When the group inverse map is orientation preserving and the matrix group is connected, our methods do not lead to the non-existence of continuous inverse ambiguous functions. If further results are to be obtained for groups like $GL_n^+(\mathbb{R})$ (n even), $SL_n(\mathbb{R})$ (n odd), $SO(n)$ (n congruent to 0 or 1 modulo 4), and $GL_n(\mathbb{C})$ (any $n > 1$), other tools will need to be developed.

References

[1] Hatcher, A.: Algebraic Topology, copyright by A. Hatcher (2001)
[2] Husemoller: Ellpitic Curves, Second Edition (GTM 111), Springer-Verlag, New York 20 (2004)
[3] Lee, J. M.: Introduction to Smooth Manifolds Gaughan, 2nd Edition (GTM 218), Springer, New York (2013).
[4] Rosen, K. H.: Elementary Number Theory and Its Applications, 5th Edition, Pearson (2005)
[5] Schmitz, D.: Inverse ambiguous functions on fields. Aequ. Math. **91**, 373-359 (2017)
[6] Schmitz, D. and Gallagher, K.: Inverse ambiguous functions on some finite non-abelian groups. Aequ. Math. **92**, 963-975 (2018)
[7] Silverman, J. H.: The Arithmetic of Elliptic Curves (GTM 106), Springer-Verlag, New York (1986)
[8] Silverman, J. H. and Tate, J. T.: Rational Points on Elliptic Curves, 2nd edition (UTM), Springer, Switzerland (2015)

Department of Mathematics, North Central College, Naperville, IL.