Weierstraß-Institut
für Angewandte Analysis und Stochastik
Leibniz-Institut im Forschungsverbund Berlin e. V.

Preprint ISSN 2198-5855

The moving frame method for iterated-integrals: Orthogonal invariants

Joscha Diehl[1], Rosa Preiß[2], Michael Ruddy[3], Nikolas Tapia[2,4]

submitted: December 14, 2020

[1] Universität Greifswald
Institut für Mathematik und Informatik
Walther-Rathenau-Str. 47
17489 Greifswald
Germany
E-Mail: joscha.diehl@gmail.com

[2] Institut für Mathematik
Technische Universität Berlin
Fakultät II
Str. des 17. Juni 136
10587 Berlin
Germany
E-Mail: preis@math.tu-berlin.de
tapia@math.tu-berlin.de

[3] The Data Insitute
University of San Francisco
E-Mail: mruddy@usfca.edu

[4] Weierstrass Institute
Mohrenstr. 39
10117 Berlin
Germany
E-Mail: nikolasesteban.tapiamunoz@wias-berlin.de

No. 2796
Berlin 2020

2010 *Mathematics Subject Classification.* 60L10, 14L24.

Key words and phrases. Signature, geometric invariants, moving frame, orthogonal group.

R.P. is supported by the European Research Council through CoG-683164. M.R. was supported in part by the Max Planck Institute for Mathematics in the Sciences. N.T. is supported by the DFG MATH+ Excellence Cluster.

Edited by
Weierstraß-Institut für Angewandte Analysis und Stochastik (WIAS)
Leibniz-Institut im Forschungsverbund Berlin e. V.
Mohrenstraße 39
10117 Berlin
Germany

Fax: +49 30 20372-303
E-Mail: preprint@wias-berlin.de
World Wide Web: http://www.wias-berlin.de/

The moving frame method for iterated-integrals: Orthogonal invariants

Joscha Diehl, Rosa Preiß, Michael Ruddy, Nikolas Tapia

ABSTRACT. We explore the algebraic properties of a generalized version of the iterated-sums signature, inspired by previous work of F. Király and H. Oberhauser. In particular, we show how to recover the character property of the associated linear map over the tensor algebra by considering a deformed quasi-shuffle product of words on the latter. We introduce three non-linear transformations on iterated-sums signatures, close in spirit to Machine Learning applications, and show some of their properties.

1. INTRODUCTION

A central problem in image science is constructing geometrically relevant features of curves that are robust to noise. In this sense, rigid motions of space make up a natural group of 'nuisance' transformations of the data. For this reason, rotation- and translation-invariant features are often desired, for instance, in Human Activity Recognition [33, Section 6] or in matching contours [43]. Classically differential invariants such as curvature have been used [22] for this purpose, and more recently integral invariants of curves have been of interest [12, 15]. In this work we construct a rotation-invariant representation of a curve through its *iterated-integral signature* by applying the *Fels-Olver moving frame method*. We show that this yields sets of integral invariants that characterize the truncated iterated integral signature up to rotation.

In [6,8], the author used the collection of all iterated integrals to characterize smooth curves, and in [31] the author extended this construction to more irregular curves. The modern term for this collection of iterated integrals of a curve is the iterated-integral signature. The iterated-integral signature has since been used in various applications such as constructing features for machine learning tasks (see [9] and references therein) and shape analysis [5, 29].

The Fels-Olver moving frame method, introduced in [14], is a modern generalization of the classical moving frame method formulated by Cartan [3]. In the general setting of a Lie group G acting on a manifold M, a moving frame is defined as a G-equivariant map from M to G. A moving frame can be re-interpreted as a choice of cross-sections to the orbits of G, and hence a unique canonical form for elements of M under G. Thus the moving frame method provides a framework for algorithmically constructing G-invariants on M that characterize orbits and for determining equivalence of submanifolds of M under G.

The moving frame method has been used to construct differential invariants of smooth planar and spatial curves under Euclidean, affine, and projective transformations, and, in certain cases, these differential invariants lead to a *differential signature* which can be used to classify curves under these transformation groups [2]. The differential signature has been applied in a variety of image science applications from automatic jigsaw puzzle assembly [23] to medical imaging [19]. Also in the realm of image science, the moving frame method has been used to construct invariants of grayscale images [1, 42].

We consider the induced action of the orthogonal group of rotations on the log-signature of a curve, which provides a compressed representation of a curve obtained by applying the log transform to the iterated-integral signature, and provide an explicit cross-section for this action. We show that for most curves and any truncation of the curve's log-signature, the orbit is characterized by the value on this cross-section. As a consequence a curve is completely determined up to rigid motions and tree-like extensions by the invariantization of its iterated integral signature induced by this cross-section.

DOI 10.20347/WIAS.PREPRINT.2796 Berlin 2020

This yields a constructive method to compare curves up to rotations and to evaluate rotation invariants that characterize the iterated integral signature under rigid motions. These invariants are constructed from integrals on the curve, and hence are likely to be more noise-resistant than their differential counterparts such as curvature. One can easily set up an artificial example where this is visible. Consider for instance the circle of radius $n^{-3/2}$ given by the parameterization $\gamma : [0,1] \to \mathbb{R}^2$ where

$$\gamma(t) = (x(t), y(t)) = \left(\frac{\cos(2\pi n t)}{n^{3/2}}, \frac{\sin(2\pi n t)}{n^{3/2}}\right),$$

which as $n \to \infty$, converges to the constant curve (at the origin). Now the curvature of this curve does *not* converge (in fact, it blows up). In contrast, the iterated integrals do all converge (to zero) since γ converges in variation norm. Then, also the invariants built out of the iterated-integrals (Section 4) converge to their value on the zero-curve. On this toy example these integral invariants are hence more "stable".

Additionally, in contrast to the methods in [12], the resulting set of integral invariants is shown to uniquely characterize the curve under rotations, and moreover, does so in a minimal fashion. Since the iterated integral signature of a curve is automatically invariant to translations, this provides rigid motion-invariant features of a curve which can be used for applications such as machine learning.

This work is structured as follows. In Section 2 we detail background on the iterated-integral signature and the moving frame method, as well as some facts about algebraic group and invariants. We take a slight detour in Section 3 and consider the orthogonal action on the second order truncation of the log-signature over the complex numbers. Using tools from algebraic invariant theory, we construct the linear space which will form the basis for the cross-section in the following section. We also provide an explicit set of polynomial invariants that characterize the second order truncation of the log-signature under the orthogonal group. In Section 4 we construct the moving frame map for paths in $\mathbb{R}^d$. In particular, in Section 4.1, we outline our procedure and results in simple language for paths in $\mathbb{R}^2$. In Section 5 we detail the moving frame map for planar and space curves, compute some of the resulting integral invariant functions, and illustrate this procedure on particular curve. Finally in Section 6 we discuss some of the interesting questions that arise as a result of our work.

2. Preliminaries

2.1. **The tensor algebra.** Let $d \geq 1$ be an integer. A **word**, or multi-index, over the alphabet $\{\mathtt{1}, \dots, \mathtt{d}\}$ is a tuple $w = (\mathtt{w}_1, \dots, \mathtt{w}_n) \in \{\mathtt{1}, \dots, \mathtt{d}\}^n$ for some integer $n \geq 0$, called its length which is denoted by $|w|$. As is usual in the literature, we use the short-hand notation $w = \mathtt{w}_1 \cdots \mathtt{w}_n$, where the $\mathtt{w}_i$, words of length one, are called **letters**. The **concatenation** of two words v, w is the word $vw := \mathtt{v}_1 \cdots \mathtt{v}_n \mathtt{w}_1 \cdots \mathtt{w}_m$ of length $|vw| = n + m$. Observe that this product is associative and non-commutative. There is a unique element of length zero, called the empty word and denoted by $\mathbf{e}$. It satisfies $w\mathbf{e} = \mathbf{e}w = w$ for all words w. If we denote by $T(\mathbb{R}^d)$ the real vector space spanned by words, the bilinear extension of the concatenation product endows it with the structure of an associative (and non-commutative) algebra. We also note that $T(\mathbb{R}^d)$ admits the direct sum decomposition

$$T(\mathbb{R}^d) = \bigoplus_{k=0}^{\infty} \operatorname{span}_{\mathbb{R}}\{w : |w| = k\}.$$

There is a commutative product on $T(\mathbb{R}^d)$, known as the **shuffle product**, recursively defined by $\mathbf{e} \sqcup\!\sqcup w := w =: w \sqcup\!\sqcup \mathbf{e}$ and

$$v\mathtt{i} \sqcup\!\sqcup w\mathtt{j} := (v \sqcup\!\sqcup w\mathtt{j})\mathtt{i} + (v\mathtt{i} \sqcup\!\sqcup w)\mathtt{j}.$$

The commutator **bracket** $[u, v] := uv - vu$ endows $T(\mathbb{R}^d)$ with the structure of a Lie algebra. The **free Lie algebra over** $\mathbb{R}^d$, denoted by $\mathfrak{g}(\mathbb{R}^d)$, can be realized as the following subspace of $T(\mathbb{R}^d)$,

$$\mathfrak{g}(\mathbb{R}^d) = \bigoplus_{n=1}^{\infty} W_n$$

where $W_1 := \operatorname{span}_{\mathbb{R}}\{\mathtt{1}, \ldots, \mathtt{d}\} \cong \mathbb{R}^d$ and $W_{n+1} := [W_1, W_n]$. There are multiple choices of bases for $\mathfrak{g}(\mathbb{R}^d)$, but we choose to work with the **Lyndon basis**. A **Lyndon word** is a word w such that whenever $w = uv$, with $u, v \neq \mathbf{e}$, then $u < u$ for the lexicographical order. We denote the set of Lyndon words over the alphabet $\{\mathtt{1}, \ldots, \mathtt{d}\}$ by $\mathscr{L}_d$. In particular, w with $|w| \geq 2$ is Lyndon if and only if there exist non-empty Lyndon words u and v such that $u < v$ and $w = uv$. Although there might be multiple choices for this factorization, the one with v as long as possible is called the **standard factorization** of w. The Lyndon basis $b_{\mathtt{w}}$ is recursively defined by setting $b_{\mathtt{i}} = \mathtt{i}$ and $b_w = [b_u, b_v]$ for all Lyndon words w with $|w| \geq 2$, where $w = uv$ is the standard factorization.

Example 2.1. Suppose $d = 2$. The Lyndon words up to length 4, their standard factorizations and the associated basis elements are

w	u	v	b_w
1	—	—	1
2	—	—	2
12	1	2	$[1, 2]$
112	1	12	$[1, [1, 2]]$
122	12	2	$[[1, 2], 2]$
1112	1	112	$[1, [1, [1, 2]]]$
1122	1	122	$[1, [[1, 2], 2]]$
1222	122	2	$[[[1, 2], 2], 2]$

Elements of the dual space $T((\mathbb{R}^d)) := T(\mathbb{R}^d)^*$ can be identified with formal word series. For $F \in T((\mathbb{R}^d))$ we write

$$F = \sum_w \langle F, w\rangle w.$$

In particular, we have no growth requirement for the **coefficients** $\langle F, w\rangle \in \mathbb{R}$. The above expression is meant only as a notation for treating the values of F on words as a single object. This space can be endowed with a multiplication given, for $F, G \in T((\mathbb{R}^d))$, by

$$FG = \sum_w \left(\sum_{uv=w} \langle F, u\rangle \langle G, v\rangle \right) w. \tag{1}$$

Observe that since there is a finite number of pairs of words u, v such that $uv = w$, the coefficients of FG are well defined for all w, so the above formula is an honest element of $T((\mathbb{R}^d))$. It turns out that this product is dual to the **deconcatenation coproduct** $\Delta\colon T(\mathbb{R}^d) \to T(\mathbb{R}^d) \otimes T(\mathbb{R}^d)$ given by

$$\Delta w = \sum_{uv=w} u \otimes v,$$

in the sense that

$$\langle FG, w\rangle = \langle F \otimes G, \Delta w\rangle$$

for all words. This formula is nothing but eq. (1) componentwise.

There are two distinct subsets of $T((\mathbb{R}^d))$ that will be important in what follows. The first one is the subspace $\mathfrak{g}((\mathbb{R}^d))$ of **infinitesimal characters**, formed by linear maps F such that $\langle F, u \sqcup\!\sqcup v\rangle = 0$

whenever u and v are non-empty words, and such that $\langle F, \mathbf{e}\rangle = 0$. It can be identified with the dual space

$$\mathfrak{g}((\mathbb{R}^d)) = \mathfrak{g}(\mathbb{R}^d)^* = \prod_{n=1}^{\infty} W_n.$$

It is a Lie algebra under the commutator bracket $[F, G] = FG - GF$. The second one is the set $\mathcal{G}((\mathbb{R}^d))$ of **characters**, i.e., linear maps F such that $\langle F, u \sqcup\!\sqcup v\rangle = \langle F, u\rangle\langle F, v\rangle$ for all $u, v \in T(\mathbb{R}^d)$.

We may define an exponential map $\exp\colon \mathfrak{g}((\mathbb{R}^d)) \to \mathcal{G}((\mathbb{R}^d))$ by its power series

$$\exp(F) := \sum_{n=0}^{\infty} \frac{1}{n!} F^n.$$

On a single word, the map is given by

$$\langle \exp(F), w\rangle = \sum_{n=0}^{\infty} \frac{1}{n!}\left(\sum_{v_1\cdots v_n = w} \langle F, v_1\rangle \cdots \langle F, v_n\rangle\right),$$

and since F vanishes on the empty word, all terms with $n > |w|$ also vanish, so that the sum is always finite. Therefore, $\exp(F)$ is a well defined element of $T((\mathbb{R}^d))$. It can be shown that the image of exp is equal to $\mathcal{G}((\mathbb{R}^d))$ and that it is a bijection onto its image, with inverse $\log\colon \mathcal{G}((\mathbb{R}^d)) \to \mathfrak{g}((\mathbb{R}^d))$ defined by

$$\log(G) := \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} (G - \varepsilon)^n$$

where ε is the unique linear map such that $\langle \varepsilon, \mathbf{e}\rangle = 1$ and zero otherwise.

Finally, we remark some freeness properties of the tensor algebra and its subspaces. Below,

$$T^+(\mathbb{R}^d) = \bigoplus_{n>0} (\mathbb{R}^d)^{\otimes n}$$

denotes the reduced tensor algebra over $\mathbb{R}^d$. The following result can be found in [16, Corollary 2.1].

Proposition 2.2. *Let $\phi\colon T^+(\mathbb{R}^d) \to \mathbb{R}^e$ be a linear map. There exists a unique extension $\tilde{\phi}\colon T(\mathbb{R}^d) \to T(\mathbb{R}^e)$ such that*

$$(\tilde{\phi} \otimes \tilde{\phi}) \circ \Delta = \Delta \circ \tilde{\phi}$$

and $\pi \circ \tilde{\phi} = \phi$, where $\pi\colon T(\mathbb{R}^e) \to \mathbb{R}^e$ denotes the projection of $T(\mathbb{R}^e)$ onto $\mathbb{R}^e$, orthogonal to $\mathbb{R}\mathbf{e}$ and $\bigoplus_{n>2} \operatorname{span}_{\mathbb{R}}\{w : |w| = n\}$. Moreover, it is given by

$$\tilde{\phi}(w) = \sum_{k=1}^{|w|} \sum_{v_1\cdots v_k = w} \phi(v_1)\cdots\phi(v_k).$$

By transposition, we obtain a unique map $\Phi\colon T((\mathbb{R}^e)) \to T((\mathbb{R}^d))$ such that

$$\Phi(FG) = \Phi(F)\Phi(G)$$

for all $F, G \in T((\mathbb{R}^e))$. In particular,

$$\Phi(F) = \sum_{w}\left(\sum_{k=1}^{|w|} \sum_{v_1\cdots v_k = w} \langle F, \phi(v_1)\cdots\phi(v_k)\rangle\right) w. \tag{2}$$

2.2. **The iterated-integrals signature.** The iterated-integrals signature of (smooth enough) paths was introduced by Chen for homological considerations on loop space, [7]. It played a vital role in the rough path analysis of Lyons, a pathwise approach to stochastic analysis, [32]. Recently it has found applications in statistics and machine learning, where it serves as a method of feature extraction for possibly non-smooth time-dependent data.

Let $X\colon [0,1] \to \mathbb{R}^d$ be a rectifiable path.[1] Given a word $w = \mathtt{w}_1 \cdots \mathtt{w}_n$, define

$$\langle \mathrm{IIS}(X), w\rangle := \int\cdots\int_{0<s_1<\cdots<s_n<1} \dot X_{w_1}(s_1)\cdots \dot X_{w_n}(s_n)\,\mathrm{d}s_1\cdots \mathrm{d}s_n \in \mathbb{R}. \tag{3}$$

This definition has a unique linear extension to $T(\mathbb{R}^d)$. We obtain thus an element $\mathrm{IIS}(X) \in T((\mathbb{R}^d))$, called the **iterated-integrals signature (IIS)** of X.

It was shown by Ree [40] that the coefficients of $\mathrm{IIS}(X)$ satisfy the so-called **shuffle relations**:

$$\langle \mathrm{IIS}(X), v\rangle\langle \mathrm{IIS}(X), w\rangle = \langle \mathrm{IIS}(X), v \sqcup\!\sqcup\, w\rangle.$$

In other words, $\mathrm{IIS}(X) \in \mathscr{G}((\mathbb{R}^d))$.

As a consequence of the shuffle relation one obtains that the **log-signature** $\log(\mathrm{IIS}(X))$ is a **Lie series**, i.e., an element of $\mathfrak{g}((\mathbb{R}^d))$. Moreover, the identity $\mathrm{IIS}(X) = \exp(\log(\mathrm{IIS}(X)))$ holds. The log-signature therefore contains the same amount of information as the signature itself; it in fact is a minimal (linear) depiction of it.[2]

The entire iterated-integrals signature $\mathrm{IIS}(X)$ is an infinite dimensional object, and hence can never actually be numerically computed. We now provide more detail on the truncated, finite-dimensional setting.

For each integer $N \geq 1$, the subspace $I_N \subset T((\mathbb{R}^d))$ generated by formal series such that $\langle F, w\rangle = 0$ for all words with $|w| > N$ is a two-sided ideal, that is, the inclusion

$$I_N T((\mathbb{R}^d)) + T((\mathbb{R}^d)) I_N \subset I_N$$

holds. Therefore, the quotient space $T_{\leq N}((\mathbb{R}^d)) := T((\mathbb{R}^d))/I_N$ inherits an algebra structure from $T((\mathbb{R}^d))$. Moreover, it can be identified with the direct sum

$$T_{\leq N}((\mathbb{R}^d)) \cong \bigoplus_{k=0}^{N} \mathrm{span}_{\mathbb{R}}\{w : |w| = k\}.$$

We denote by $\mathrm{proj}_{\leq N}\colon T((\mathbb{R}^d)) \to T_{\leq N}((\mathbb{R}^d))$ the canonical projection.

Denote with $\mathfrak{g}_{\leq N}((\mathbb{R}^d))$ the **free step-N nilpotent Lie algebra** (over $\mathbb{R}^d$). It can be realized as the following subspace of $T_{\leq N}((\mathbb{R}^d))$, see [17, Section 7.3],

$$\mathfrak{g}_{\leq N}((\mathbb{R}^d)) = \bigoplus_{k=1}^{N} W_k,$$

where, as before $W_1 := \mathrm{span}_{\mathbb{R}}\{\mathtt{i} : i = 1,\ldots,d\} \cong \mathbb{R}^d$ and $W_{n+1} := [W_1, W_n]$. In the case of $N = 2$ this reduces to

$$W_1 \oplus W_2 \cong \mathbb{R}^d \oplus \mathfrak{so}(d,\mathbb{R}),$$

[1] Continuous with finite one-variation.

[2] Minimality follows from Chow's theorem, [17, Theorem 7.28].

where we denote with $\mathfrak{so}(d,\mathbb{R})$ the space of skew-symmetric $d\times d$ matrices. Indeed, an isomorphism is given by

$$\sum_{1\le i\le d} c_{\mathtt{i}}\,\mathtt{i} + \sum_{1\le i<j\le d} c_{\mathtt{ij}}\,[\mathtt{i},\mathtt{j}] \mapsto \left(\begin{pmatrix} c_{1} \\ \vdots \\ c_{\mathtt{d}} \end{pmatrix}, \begin{pmatrix} 0 & c_{12} & \cdots & c_{1\mathtt{d}} \\ -c_{12} & 0 & \cdots & c_{2\mathtt{d}} \\ \cdots & \cdots & \ddots & \cdots \\ -c_{1\mathtt{d}} & -c_{2\mathtt{d}} & \cdots & 0 \end{pmatrix}\right). \tag{4}$$

We remark that the coefficients $c_{\mathtt{i}}$ and $c_{\mathtt{ij}}$ are the coordinates[3] with respect to the Lyndon basis (see Example 2.1).

The linear space $\mathfrak{g}_{\le N}((\mathbb{R}^d))$ is in bijection to its image under the exponential map. This image, denoted $\mathcal{G}_{\le N}(\mathbb{R}^d) := \exp \mathfrak{g}_{\le N}((\mathbb{R}^d))$, is the **free step-$N$ nilpotent group** (over $\mathbb{R}^d$). It is exactly the set of all points in $T_{\le N}(\mathbb{R}^d)$ that can be reached by the truncated signature map, that is (see [17, Theorem 7.28])

$$\mathcal{G}_{\le N}((\mathbb{R}^d)) = \{\mathrm{proj}_{\le N} \operatorname{IIS}(X) \mid X : [0,T] \to \mathbb{R}^d \text{ is rectifiable}\} \subset T_{\le N}((\mathbb{R}^d)).$$

Example 2.3 (Moment curve)**.** We consider the **moment curve** in dimension 3, which is the curve $X : [0,1] \to \mathbb{R}^3$ give as

$$X_t := (t, t^2, t^3).$$

It traces out part of the twisted cubic [20, Example 1.10], see also [26, Sect. 15].

We calculate, as an example,

$$\begin{aligned}\langle \operatorname{ISS}(X), \mathtt{32}\rangle &= \int_0^1 \int_0^s 3r^2 dr 2s ds \\ &= 2\int_0^1 s^4 ds = \frac{2}{5}.\end{aligned}$$

The entire step-2 truncated signature is

$$\mathrm{proj}_{\le 2} \operatorname{IIS}(X) = \left(\begin{pmatrix}1\\1\\1\end{pmatrix}, \begin{pmatrix} \frac{1}{2} & \frac{4}{6} & \frac{3}{4} \\ \frac{2}{6} & \frac{1}{2} & \frac{6}{10} \\ \frac{1}{4} & \frac{4}{10} & \frac{1}{2} \end{pmatrix}\right),$$

and the step-2 truncated log-signature is

$$\mathrm{proj}_{\le 2} \log \operatorname{IIS}(X) = \left(\begin{pmatrix}1\\1\\1\end{pmatrix}, \begin{pmatrix} 0 & \frac{1}{6} & \frac{1}{4} \\ -\frac{1}{6} & 0 & \frac{1}{10} \\ -\frac{1}{4} & -\frac{1}{10} & 0 \end{pmatrix}\right).$$

2.3. **Invariants.** In this work we are interested in functions on paths that factor through the signature that are invariant to a group G acting on the path's ambient space $\mathbb{R}^d$. We will mainly focus on $G = \mathrm{O}_d(\mathbb{R})$, acting linearly on $\mathbb{R}^d$. The action of $A \in G$ on an $\mathbb{R}^d$-valued path X is given by $AX\colon [0,1] \to \mathbb{R}^d$, $t \mapsto AX_t$.

Using Proposition 2.2, we can extend the action of G on $\mathbb{R}^d$ to a **diagonal action** on words. The matrix $A^\top$ acts on single letters by

$$\phi_{A^\top}(\mathtt{i}) = \sum_j a_{ji}\,\mathtt{j},$$

[3] These are often referred to as coordinates of the first kind, see [38]

and we set $\phi_{A^\top}(w) = 0$ whenever $|w| \geq 2$. By Proposition 2.2, this induces an endomorphism $\tilde{\phi}_{A^\top} : T(\mathbb{R}^d) \to T(\mathbb{R}^d)$, satisfying

$$\tilde{\phi}_{A^\top}(\mathtt{w}_1 \cdots \mathtt{w}_n) = \phi_{A^\top}(\mathtt{w}_1) \cdots \phi_{A^\top}(\mathtt{w}_n). \tag{5}$$

In particular, $\tilde{\phi}_{A^\top}(u\mathtt{i}) = \tilde{\phi}_{A^\top}(u)\tilde{\phi}_{A^\top}(\mathtt{i})$ for all words u and letters $\mathtt{i} \in \{1, \dots, \mathtt{d}\}$. In order to be consistent with the notation in [12], we will denote the transpose map just by $A\colon T((\mathbb{R}^d)) \to T((\mathbb{R}^d))$.

Lemma 2.4. *The map $\tilde{\phi}_{A^\top} : T(\mathbb{R}^d) \to T(\mathbb{R}^d)$ is a shuffle morphism, that is,*

$$\tilde{\phi}_{A^\top}(u \sqcup\!\sqcup v) = \tilde{\phi}_{A^\top}(u) \sqcup\!\sqcup \tilde{\phi}_{A^\top}(v)$$

for all words u, v.

Proof. We proceed by induction on $|u| + |v| \geq 0$. If $|u| + |v| = 0$ then necessarily $u = v = \mathbf{e}$, and the identity becomes

$$\tilde{\phi}_{A^\top}(\mathbf{e} \sqcup\!\sqcup \mathbf{e}) = \tilde{\phi}_{A^\top}(\mathbf{e}) = \mathbf{e} = \mathbf{e} \sqcup\!\sqcup \mathbf{e} = \tilde{\phi}_{A^\top}(\mathbf{e}) \sqcup\!\sqcup \tilde{\phi}_{A^\top}(\mathbf{e}),$$

which is true by definition. Now, suppose that the identity is true for all words u', v' with $|u'|+|v'| < n$. If $|u|+|v| = n$ we suppose, without loss of generality, that $u = u'\mathtt{i}$, $v = v'\mathtt{j}$ for some (possibly empty) words u', v' with $|u'| + |v'| < n$. Then

$$\begin{aligned}
\tilde{\phi}_{A^\top}(u \sqcup\!\sqcup v) &= \tilde{\phi}_{A^\top}(u'\mathtt{i} \sqcup\!\sqcup v'\mathtt{j}) \\
&= \tilde{\phi}_{A^\top}(u' \sqcup\!\sqcup v'\mathtt{j})\tilde{\phi}_{A^\top}(\mathtt{i}) + \tilde{\phi}_{A^\top}(u'\mathtt{i} \sqcup\!\sqcup v')\tilde{\phi}_{A^\top}(\mathtt{j}) \\
&= (\tilde{\phi}_{A^\top}(u') \sqcup\!\sqcup \tilde{\phi}_{A^\top}(v'\mathtt{j}))\tilde{\phi}_{A^\top}(\mathtt{i}) + (\tilde{\phi}_{A^\top}(u'\mathtt{i}) \sqcup\!\sqcup \tilde{\phi}_{A^\top}(v'))\tilde{\phi}_{A^\top}(\mathtt{j}) \\
&= \tilde{\phi}_{A^\top}(u'\mathtt{i}) \sqcup\!\sqcup \tilde{\phi}_{A^\top}(v'\mathtt{j}) \\
&= \tilde{\phi}_{A^\top}(u) \sqcup\!\sqcup \tilde{\phi}_{A^\top}(v).
\end{aligned}$$

□

Remark 2.5. Lemma 2.4 is a special case of [10, Theorem 1.2].

Corollary 2.6. *Let $A \in G$.*

1. *The character group is invariant under A, that is, $A \cdot \mathcal{G}((\mathbb{R}^d)) \subset \mathcal{G}((\mathbb{R}^d))$.*
2. *The restriction of A to $\mathfrak{g}((\mathbb{R}^d))$ is a Lie endomorphism. In particular, the free Lie algebra is invariant under A, that is, $A \cdot \mathfrak{g}((\mathbb{R}^d)) \subset \mathfrak{g}((\mathbb{R}^d))$.*
3. *$\log : \mathcal{G}((\mathbb{R}^d)) \to \mathfrak{g}((\mathbb{R}^d))$ is an equivariant map.*

Proof.

1. Let $F \in \mathcal{G}((\mathbb{R}^d))$, and u, v be words. Then
$$\begin{aligned}
\langle A \cdot F, u \sqcup\!\sqcup v\rangle &= \langle F, \tilde{\phi}_{A^\top}(u \sqcup\!\sqcup v)\rangle \\
&= \langle F, \tilde{\phi}_{A^\top}(u) \sqcup\!\sqcup \tilde{\phi}_{A^\top}(v)\rangle \\
&= \langle F, \tilde{\phi}_{A^\top}(u)\rangle\langle F, \tilde{\phi}_{A^\top}(v)\rangle \\
&= \langle A \cdot F, u\rangle\langle A \cdot F, v\rangle,
\end{aligned}$$
that is, $A \cdot F \in \mathcal{G}((\mathbb{R}^d))$.
2. Since $A \cdot (FG) = (A \cdot F)(A \cdot G)$, A is automatically a Lie morphism. Now we check that $A \cdot F \in \mathfrak{g}((\mathbb{R}^d))$ whenever $F \in \mathfrak{g}((\mathbb{R}^d))$. It is clear that $\langle A \cdot F, \mathbf{e}\rangle = \langle F, \mathbf{e}\rangle = 0$. Now, if u, v are non-empty words, then
$$\begin{aligned}
\langle A \cdot F, u \sqcup\!\sqcup v\rangle &= \langle F, \tilde{\phi}_{A^\top}(u \sqcup\!\sqcup v)\rangle \\
&= \langle F, \tilde{\phi}_{A^\top}(u) \sqcup\!\sqcup \tilde{\phi}_{A^\top}(v)\rangle \\
&= 0,
\end{aligned}$$

i.e. $A \cdot F \in \mathfrak{g}((\mathbb{R}^d))$.

3 Let $G \in \mathcal{G}((\mathbb{R}^d))$. Then, since $A \cdot \varepsilon = \varepsilon$ we get

$$\begin{aligned}\log(A \cdot G) &= \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n}(A \cdot G - \varepsilon)^n \\ &= A \cdot \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n}(G - \varepsilon)^n \\ &= A \cdot \log(G).\end{aligned}$$

□

In particular, we easily see that (see also [12, Lemma 3.3])

$$\mathrm{IIS}(A \cdot X) = A \cdot \mathrm{IIS}(X). \tag{6}$$

The same is true for the truncated versions, and we note that, in the special case of $\mathfrak{g}_{\leq 2}((\mathbb{R}^d))$, under the isomorphism in eq. (4), the action has the simple form

$$A \cdot (v, M) = (Av, AMA^\top), \tag{7}$$

where the operations on the right-hand side are matrix-vector resp. matrix-matrix multiplication. It follows from Corollary 2.6 and (6) that $\log(\mathrm{IIS}(AX)) = A \cdot \log(\mathrm{IIS}(X))$. As already remarked, log is a bijection (with inverse exp). To obtain invariant expressions in terms of $\mathrm{IIS}(X)$ it is hence enough to obtain invariant expressions in terms of $\log(\mathrm{IIS}(X))$. Going this route has the benefit of *working on a linear object*. To be more specific, $\mathrm{IIS}(X)$ is, owing to the shuffle relation, highly redundant. As an example in $d = 2$,

$$\left\langle \mathrm{IIS}(X), \mathtt{1} \right\rangle^2 + \left\langle \mathrm{IIS}(X), \mathtt{2} \right\rangle^2 = 2 \left\langle \mathrm{IIS}(X), \mathtt{11} + \mathtt{22} \right\rangle.$$

Now, both of these expressions are invariant to $\mathrm{O}_2(\mathbb{R})$. The left-hand-side is a nonlinear expressions in the signature, whereas the right-hand-side is a linear one. To not have to deal with this kind of redundancy we work with the log-signature. We note that in [12] the *linear* invariants of the signature itself are presented. Owing to the shuffle relation, this automatically yields (all) polynomial invariants. But, as just mentioned, it also yields a lot of redundant information.

Example 2.7. We continue with Example 2.3. The rotation

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix},$$

results in the curve

$$Y_t := AX_t = \begin{pmatrix} t^2 \\ t^3 \\ t \end{pmatrix}.$$

Its step-2 truncated signature is

$$\mathrm{proj}_{\leq 2} \mathrm{IIS}(Y) = \left(\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} \frac{1}{2} & \frac{3}{5} & \frac{1}{3} \\ \frac{2}{5} & \frac{1}{2} & \frac{1}{4} \\ \frac{2}{3} & \frac{3}{4} & \frac{1}{2} \end{pmatrix} \right) = \left(A \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, A \begin{pmatrix} \frac{1}{2} & \frac{4}{6} & \frac{3}{4} \\ \frac{2}{6} & \frac{1}{2} & \frac{6}{10} \\ \frac{1}{4} & \frac{4}{10} & \frac{1}{2} \end{pmatrix} A^\top \right) = A \cdot \mathrm{proj}_{\leq 2} \mathrm{IIS}(X).$$

The step-2 truncated log-signature is

$$\mathrm{proj}_{\leq 2} \log \mathrm{IIS}(Y) = \left(\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 & \frac{1}{10} & -\frac{1}{6} \\ -\frac{1}{10} & 0 & -\frac{1}{4} \\ \frac{1}{6} & \frac{1}{4} & 0 \end{pmatrix} \right) = A \cdot \mathrm{proj}_{\leq 2} \log \mathrm{IIS}(X).$$

DOI 10.20347/WIAS.PREPRINT.2796

In the present work, we consider general, *nonlinear* expressions of the log-signature. That way, we use the economical form of the log-signature, while still providing a complete – in a precise sense – set of nonlinear invariants.

2.4. **Moving frame method.** We now provide a brief introduction to the Fels-Olver moving frame method introduced in [14], a modern generalization of the classical moving frame method formulated by Cartan [4]. For a comprehensive overview of the method and survey of many of its applications see [13,37]. We will assume in this subsection that G is a finite dimensional Lie group acting smoothly on an m-dimensional manifold M.

Definition 2.8. A **moving frame** for the action of G on M is a smooth map $\rho : M \to G$ such that $\rho(g \cdot z) = \rho(z) \cdot g^{-1}$.

In general one can define a moving frame as a smooth G-equivariant map $\rho : M \to G$. For simplicity we assume G acts on itself by right multiplication; this is often referred to as a *right* moving frame. A moving frame can be constructed through the use of a cross-section to the orbits of the action of G on M.

Definition 2.9. A **cross-section** for the action of G on M is a submanifold $\mathcal{K} \subset M$ such that $\mathcal{K}$ intersects each orbit transversally at a unique point.

Definition 2.10. The action of G is **free** if the **stabilizer** G_z of any point $z \in M$ is trivial, i.e.

$$G_z := \{g \in G \,|\, g \cdot z = z\} = \{\mathrm{id}\},$$

where id $\in G$ denotes the identity transformation.

The following result appears in much of the previous literature on moving frames (see, for instance, [36, Thm. 2.4]).

Theorem 2.11. *Assume that Let G be an action on M and assume that*

($*$) The action is free, and around each point $z \in M$ there exists arbitrarily small neighborhoods whose intersection with each orbit is path-wise connected.

If $\mathcal{K}$ is a cross-section, then the map $\rho : M \to G$ defined by sending z to the unique group element $g \in G$ such that $g \cdot z \in \mathcal{K}$ is a moving frame.

Remark 2.12. The equivariance of the map $\rho : M \to G$ such that $\rho(z) \cdot z \in \mathcal{K}$ can be seen from the fact that $\rho(z) \cdot z = \rho(g \cdot z) \cdot (g \cdot z)$ for any $g \in G$. Since G is free this implies that $\rho(z) = \rho(g \cdot z) \cdot g$, and hence ρ satisfies Definition 2.8.

Similarly, in this setting, a moving frame ρ specifies a cross-section defined by $\mathcal{K} = \{\rho(z) \cdot z \in M\}$. This construction can be interpreted as a way to assign a "canonical form" to points $z \in M$ under the action of G, thus producing invariant functions on M under G.

Definition 2.13. Let $\rho : M \to G$ be a moving frame. The **invariantization** of a function $F : M \to \mathbb{R}$ with respect to ρ is the invariant function $\iota(F)$ defined by

$$\iota(F)(z) = F(\rho(z) \cdot z).$$

Given a moving frame ρ and local coordinates $z = (z_1, \ldots, z_m)$ on M, the invariantization of the coordinate functions $\iota(z_1), \ldots, \iota(z_m)$ are the **fundamental invariants** associated with ρ. In particular we can compute $\iota(F)$ by

$$\iota(F)(z_1, \ldots, z_m) = F(\iota(z_1), \ldots, \iota(z_m)).$$

Since $\iota(I)(z) = I(z)$ for any invariant function I, the fundamental invariants provide a functionally generating set of invariants for the action of G on M. Suppose further that G is an r-dimensional Lie group and that ρ is the moving frame associated to a **coordinate cross-section** $\mathcal{K}$ defined by equations

$$z_1 = c_1, \dots, z_r = c_r$$

for some constants $c_1, \dots, c_r$. Then the first r fundamental invariants are the **phantom invariants** $c_1, \dots, c_r$, while the remaining $m - r$ invariants $\{I_1, \dots, I_{m-r}\}$ form a functionally independent generating set. In this case we can see that two points $z_1, z_2 \in M$ lie in the same orbit if and only if

$$I_1(z_1) = I_1(z_2), \dots, I_s(z_1) = I_s(z_2).$$

Example 2.14. Consider the canonical action of $\mathrm{SO}_2(\mathbb{R})$ on $\mathbb{R}^2\backslash\{(0,0)\}$. This action satisfies the assumptions of Theorem 2.11 and a cross-section to the orbits is given by

$$\mathcal{K} = \{(x, y) \,|\, x = 0, y > 0\}.$$

The unique group element taking a point to the intersection of its orbit with $\mathcal{K}$ is the rotation

$$\rho(x, y) = \begin{bmatrix} \frac{y}{\sqrt{x^2+y^2}} & \frac{-x}{\sqrt{x^2+y^2}} \\ \frac{x}{\sqrt{x^2+y^2}} & \frac{y}{\sqrt{x^2+y^2}} \end{bmatrix}.$$

The fundamental invariants associated with the moving frame $\rho : \mathbb{R}^2\backslash\{(0,0)\} \to \mathrm{SO}_2(\mathbb{R})$ are given by

$$\iota(x) = 0 \quad \iota(y) = \sqrt{x^2 + y^2}.$$

Thus any invariant function for this action can be written as a function of $\iota(y)$, the Euclidean norm. One can check that indeed for an invariant $I(x, y)$, one has $I(x, y) = I(0, \sqrt{x^2 + y^2})$. This additionally implies that two points are related by a rotation if and only if they have the same Euclidean norm.

In practice it is difficult or impossible to find a global cross-section, and thus a global moving frame, to the orbits of G on M. For instance in the above example, the origin was removed from $\mathbb{R}^2$ to ensure freeness of the action. If the action of G on M satisfies condition $(*)$ from Theorem 2.11, then the existence of a **local moving frame** around each point $z \in M$ is guaranteed by [14, Thm. 4.4]. In this case the moving frame is a map $\rho : U \to V$ from a neighborhood $z \in U$ of M to a neighborhood of the identity in $V \subset G$. The fundamental set of invariants produced are also local in nature and thus only guaranteed to be invariant on U for elements $g \in V$.

The condition $(*)$ in Theorem 2.11 can be relaxed in certain cases. In [25, Sec. 1] the authors outline a method to construct a fundamental set of local invariants for actions of G that are only semi-regular, meaning that all orbits have the same dimension. In particular Theorem 1.6 in [25] states that for a semi-regular action of G on M, there exists a *local* coordinate cross-section about every point $z \in M$. In a neighborhood U containing z, such a linear space intersects transversally the connected component containing $\overline{z}$ of the orbit $G \cdot \overline{z}$ at a unique point for each $\overline{z} \in U$.

Remark 2.15. Note that if every sufficiently small neighborhood about z does *not* have path-wise connected intersection with each orbit, a local cross-section about z necessarily intersects some orbit at infinitely-many points. The algebraic actions that we define in the next section are automatically semi-regular on a Zariski-open subset of the target space (Proposition 2.16(c)), and hence a local cross-section exists. Since orbits are algebraic subsets, a local cross-section is a linear space of complementary dimension intersecting transversally each orbit about z transversally, and hence in finitely-many points. Thus a free algebraic group action necessarily satisfies condition $(*)$ from Theorem 2.11.

2.5. **Algebraic groups and Invariants.** In this work, we will be in the setting of an algebraic group G acting rationally on a variety X. In other words G is an algebraic variety equipped with a group structure, and the action of G on X is given by a rational map $\Phi : G \times X \dashrightarrow X$. Here we outline some key facts and results about algebraic group actions and the invariants of such actions, following [39] for much of our exposition. Unless specified otherwise, both G and X are both varieties over the algebraically closed field $\mathbb{C}$.

The orbit $G \cdot p$ of a point $p \in X$ under G is the image of $G \times \{p\}$ under the rational map Φ defining the action, and hence is open in its closure $\overline{G \cdot p}$ under the **Zariski topology**.[4]

The following proposition summarizes a few basic results on orbits of algebraic groups that can be found in [39, Section 1.3].

Proposition 2.16. *For any point $p \in X$, the stabilizer G_p is an algebraic subgroup of G and $G \cdot p$ satisfies the following:*

(a) The orbit $G \cdot p$ is a smooth, Zariski-open subset of $\overline{G \cdot p}$.
(b) The dimension of $G \cdot p$ satisfies $\dim G \cdot p = \dim G - \dim G_p$, where $\dim G_p = \dim T_p(G \cdot p)$.
(c) The dimension of $G \cdot p$ is maximal on a non-empty Zariski-open subset of X.

For an arbitrary field k, the polynomial invariants (for the action of G on the variety X) defined as a form a subring of $k[X]$ defined by

$$k[X]^G = \{f \in k[X] \mid f(g \cdot p) = f(p), \quad \text{for all} \quad g \in G, p \in X\}$$

and the rational invariants form a subfield of $k(X)$ given by

$$k(X)^G = \{f \in k(X) \mid f(g \cdot p) = f(p), \quad \text{for all} \quad g \in G, p \in X\}$$

respectively. Constructing invariant functions and finding generating[5] sets for $\mathbb{C}[X]^G$ is the subject of classical invariant theory [30, 35, 41]. In [21] Hilbert proved his finiteness theorem, showing that for linearly reductive groups acting on a vector space V the polynomial ring $\mathbb{C}[V]^G$ is finitely generated leading him to conjecture in his fourteenth problem that $\mathbb{C}[X]^G$ is always finitely generated. In [34] Nagata constructed a counter-example to this conjecture. For $\mathbb{C}(X)^G$, however, a finite generating set always exists and can be explicitly constructed (see for instance [11, 24]). Furthermore a set of rational invariants is generating if and only if it is also *separating*.

Definition 2.17. A set of rational invariants $\mathcal{I} \subset \mathbb{C}(X)^G$ **separates orbits on a subset** $U \subset X$ if two points $p, q \in U$ lie in the same orbit if and only if $K(p) = K(q)$ for all $K \in \mathcal{I}$. If there exists a non-empty, Zariski-open subset X where $\mathcal{I}$ separates orbits then we say $\mathcal{I}$ is **separating**.

Proposition 2.18. *For the action of G on X, the field $\mathbb{C}(X)^G$ is finitely generated over $\mathbb{C}$. Moreover a subset $\mathcal{I} \subset \mathbb{C}(X)^G$ is generating if and only if it is separating.*

Proof. The backward direction holds by [39, Lem. 2.1]. By [39, Thm. 2.4] there always exists a finite set of separating invariants in $\mathbb{C}(X)^G$, and hence a finite generating set. Additionally this finite set can be rewritten in terms of any generating set, and hence any generating set is also separating. ◻

Under certain conditions the polynomial ring $\mathbb{C}[X]^G$ is also separating, as the following proposition from [39, Prop. 3.4] shows.

[4] The Zariski topology on an affine space k^d is the topology where closed sets are given by subsets of the form $V(f_1, \ldots, f_s) = \{(x_1, \ldots, x_d) \in k^d \mid f_1(x_1, \ldots, x_d) = \ldots = f_s(x_1, \ldots, x_d) = 0\}$ for some collection of polynomials $f_1, \ldots, f_s \in k[x_1, \ldots, x_d]$.

[5] By a **generating set** for $k[X]^G$, we refer to a subset of $k[X]^G$ that generates $k[X]^G$ as a polynomial ring. Similarly a generating set of $k(X)^G$ is a subset that generates $k(X)^G$ as a field.

Proposition 2.19. *Suppose the variety X is irreducible. There exists a finite, separating set of invariants $\mathcal{I} \subset \mathbb{C}[X]^G$ if and only if $\mathbb{C}(X)^G = Q\mathbb{C}[X]^G$ where $Q\mathbb{C}[X]^G = \left\{ \frac{f}{g} \,\middle|\, f, g \in \mathbb{C}[X]^G \right\}$.*

One way to understand the structure of invariant rings is by considering subsets of X that intersect a general orbit.

Definition 2.20. Let $N \subset G$ be a subgroup. A subvariety S of X is a **relative N-section** for the action of G on X if the following hold:

- There exists a non-empty, G-invariant, and Zariski-open subset $U \subset X$, such that S intersects each orbit that is contained in U. In other words, we have that $\overline{\Phi(G \times S)} = X$, where closure is taken in the Zariski topology.
- One has $N = \{n \in G \mid nS = S\}$.

We call the subgroup N the **normalizer** subgroup of S with respect to G. The following proposition summarizes a discussion in [39, Sec. 2.8].

Proposition 2.21. *Let S be a relative N-section for the action of G on X. Then the restriction map*

$$\mathrm{R}_{X\to S} \colon \mathbb{C}(X) \to \mathbb{C}(S),$$

induces a field isomorphism between $\mathbb{C}(X)^G$ and $\mathbb{C}(S)^N$.

Corollary 2.22. *Let S be a relative N-section for the action of G on X and $\mathcal{I} \subset \mathbb{C}(X)^G$ a set such that $\mathrm{R}_{X\to S}(\mathcal{I})$ generates $\mathbb{C}(S)^N$ where $\mathrm{R}_{X\to S}$ is the restriction map from Proposition 2.21. Then $\mathcal{I}$ is a generating set for $\mathbb{C}(X)^G$.*

Relative sections can be used to construct generating sets of rational invariants for algebraic actions as in [18], which the authors refer to as the *slice method*. Similar in spirit to the approach in [25], considerations can be restricted to an algebraic subset of X.

We end the section by considering algebraic actions on varieties defined over $\mathbb{R}$, where the issue is more delicate. For instance Proposition 2.18 no longer holds in this setting (see [28, Rem. 2.7]). Suppose that $X(\mathbb{R})$ and $G(\mathbb{R})$ are real varieties with action given by $\Phi : G(\mathbb{R}) \times X(\mathbb{R}) \dashrightarrow X(\mathbb{R})$ and that X and G are the associated complex varieties. Then Φ defines an action of G on X.

Proposition 2.23. *The field $\mathbb{R}(X(\mathbb{R}))^{G(\mathbb{R})}$ lies in $\mathbb{C}(X)^G$.*

Proof. If $f \in \mathbb{R}(X(\mathbb{R}))^{G(\mathbb{R})}$, then the rational function $f(g \cdot p) - f(p)$ is identically zero on $G(\mathbb{R}) \times X(\mathbb{R})$, and hence is identically zero on $G \times X$. Thus $f \in \mathbb{C}(X)^G$. □

Corollary 2.24. *If $\mathcal{I} = \{I_1, \dots, I_s\} \subset \mathbb{R}(X(\mathbb{R}))^{G(\mathbb{R})}$ generates $\mathbb{C}(X)^G$ then $\mathcal{I}$ generates $\mathbb{R}(X(\mathbb{R}))^{G(\mathbb{R})}$.*

Proof. Suppose that $\mathcal{I}$ generates $\mathbb{C}(X)^G$ and that $f \in \mathbb{R}(X(\mathbb{R}))^{G(\mathbb{R})}$. Then there exists a rational function $g \in \mathbb{C}(y_1, \dots, y_s)$ such that $f = g(I_1, \dots, I_s)$. We can decompose g as $g = \mathrm{Re}(g) + i \cdot \mathrm{Im}(g)$ where $\mathrm{Re}(g), \cdot\mathrm{Im}(g) \in \mathbb{R}(y_1, \dots, y_s)$. Since f is a real rational function

$$2f = [\mathrm{Re}(g) + i \cdot \mathrm{Im}(g)] + [\mathrm{Re}(g) - i \cdot \mathrm{Im}(g)] = 2\mathrm{Re}(g).$$

Thus g must lie in $\mathbb{R}(y_1, \dots, y_s)$ proving the result. □

Proposition 2.25. *Suppose that $\mathbb{R}(X(\mathbb{R}))^{G(\mathbb{R})}$ separates orbits for the action of $G(\mathbb{R})$ on $X(\mathbb{R})$. Then so does any generating set for $\mathbb{R}(X(\mathbb{R}))^{G(\mathbb{R})}$.*

Proof. Suppose that $\mathcal{I} = \{I_1, I_2, \ldots\}$ generates $\mathbb{R}(X(\mathbb{R}))^{G(\mathbb{R})}$ and that $\mathbb{R}(X(\mathbb{R}))^{G(\mathbb{R})}$ separates orbits. Then for any two points $p_1, p_2 \in X(\mathbb{R})$ if

$$I_1(p_1) = I_1(p_2), I_2(p_1) = I_2(p_2), \ldots$$

for all invariants in $\mathcal{I}$, then we also have $I(p_1) = I(p_2)$ for any invariant $I \in \mathbb{R}(X(\mathbb{R}))^{G(\mathbb{R})}$ as $\mathcal{I}$ generates $\mathbb{R}(X(\mathbb{R}))^{G(\mathbb{R})}$. Thus p_1 and p_2 lie in the same orbit under $G(\mathbb{R})$. □

3. Orthogonal invariants on $\mathfrak{g}_{\leq 2}((\mathbb{R}^d))$

In this section we take a closer look at the action of $\mathrm{O}_d(\mathbb{R})$ on $\mathfrak{g}_{\leq 2}((\mathbb{R}^d)) \cong \mathbb{R}^d \oplus \mathfrak{so}(d, \mathbb{R})$. In particular we construct an explicit linear space of complementary dimension intersecting each orbit in a large open subset of this space. To achieve this, we consider the associated action of the *complex* group $\mathrm{O}_d(\mathbb{C})$ on the space $\mathbb{C}^d \oplus \mathfrak{so}(d, \mathbb{C})$ where

$$\mathrm{O}_d(\mathbb{C}) = \{A \in \mathrm{GL}_d(\mathbb{C}) \mid AA^T = \mathrm{id}\}.$$

As described in Section 2.5, we can consider $\mathrm{O}_d(\mathbb{R})$ and $\mathbb{R}^d \oplus \mathfrak{so}(d, \mathbb{R})$ as the real points of the varieties $\mathrm{O}_d(\mathbb{C})$ and $\mathbb{C}^d \oplus \mathfrak{so}(d, \mathbb{C})$.

Remark 3.1. The real Lie group

$$\mathrm{O}_d(\mathbb{R}) := \{A \in \mathbb{R}^{d\times d} : AA^\top = \mathrm{id}\},$$

can be considered as a subset of the Lie group

$$\mathrm{O}_d(\mathbb{C}) := \{A \in \mathbb{C}^{d\times d} : AA^\top = \mathrm{id}\}.$$

We note that $\mathrm{O}_d(\mathbb{C})$ is a complex Lie group, in contradistinction to the Lie group

$$\mathrm{U}_d := \{A \in \mathbb{C}^{d\times d} : A^* A = \mathrm{id}\},$$

where A^* is the conjugate transpose of A. Even though it U_d contains matrices with complex entries it is a real Lie group.

By investigating the associated complex action, we can utilize tools such as the relative sections described in Definition 2.20, and then pass these results down to the real points. As before in (7) the action of $\mathrm{O}_d(\mathbb{C})$ on $\mathbb{C}^d \oplus \mathfrak{so}(d, \mathbb{C})$ is given by

$$A \cdot (v, M) = (Av, AMA^T). \tag{8}$$

Proposition 3.2. *For any $v \in \mathbb{C}^d$ such that $v_1^2 + \ldots + v_d^2 \neq 0$, there exists $A \in \mathrm{O}_d(\mathbb{C})$ such that $\overline{v} = Av$ satisfies $\overline{v}_1 = \ldots = \overline{v}_{d-1} = 0$ and $\overline{v}_d \neq 0$.*

Proof. The function $(d-1)(v_1^2 + \ldots + v_d^2)$ can be written as the sum of all pairwise sum of squares, i.e.

$$(d-1)(v_1^2 + \ldots + v_d^2) = \sum_{i=1}^{d} \sum_{j\neq i} v_i^2 + v_j^2.$$

Suppose that $v_1^2 + \ldots + v_d^2 \neq 0$ and there exists some $v_i \neq 0$ where $1 \leq i \leq d-1$. Otherwise we are done by choosing A as the identity. By the above equation, there exists a pair of coordinates v_i and v_j such that $v_i^2 + v_j^2 \neq 0$ where $1 \leq i < j \leq d$.

Choose the matrix $A \in \mathrm{O}_d(\mathbb{C})$ defined by

$$a_{k\ell} = \begin{cases} 1 & k = \ell \neq i, j \\ \frac{v_j}{w} & k = \ell = i, j \\ -\frac{v_i}{w} & k = i, \ell = j \\ \frac{v_j}{w} & k = j, \ell = i \\ 0 & \text{otherwise} \end{cases}$$

where w is an element of $\mathbb{C}$ that satisfies $w^2 = v_i^2 + v_j^2$. The transformation A is the complex analogue to a Givens Rotation which only rotates two coordinates. Then for $Av = \overline{v}$ we have that $\overline{v}_k = v_k$ for $k \neq i, j$, $\overline{v}_i = 0$, and $\overline{v}_j = w \neq 0$. This process can be repeated until $\overline{v}$ is of the desired form. □

Remark 3.3. The orbits in $\mathbb{C}^d$ under $\mathrm{O}_d(\mathbb{C})$ that satisfy $v_1^2 + \cdots + v_d^2 = 0$ contain the origin in their closure.

We construct a sequence of linear subspaces of $\mathbb{C}^d \oplus \mathfrak{so}(d, \mathbb{C})$ given by

$$L_1 = \{(v, M) \in \mathbb{C}^d \oplus \mathfrak{so}(d, \mathbb{C}) \mid v_1 = \cdots = v_{d-1} = 0\},$$
$$L_i = \{(v, M) \in L_{i-1} \mid m_{1(d-i+2)} = \cdots = m_{(d-i)(d-i+2)} = 0\}$$

for $2 \leq i \leq d-1$. In particular the subspace $L := L_{d-1}$ is given by pairs (v, M) of the form

$$v = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ v_d \end{bmatrix} \quad M = \begin{bmatrix} 0 & m_{12} & 0 & \dots & 0 \\ -m_{12} & 0 & m_{23} & \dots & 0 \\ 0 & -m_{23} & 0 & \dots & \vdots \\ \vdots & & & \ddots & m_{(d-1)d} \\ 0 & 0 & \dots & -m_{(d-1)d} & 0 \end{bmatrix}. \tag{9}$$

Example 3.4. For $d = 4$, elements in L_1 are of the form

$$\left(\begin{pmatrix} 0 \\ 0 \\ 0 \\ * \end{pmatrix}, \begin{pmatrix} * & * & * & * \\ * & * & * & * \\ * & * & * & * \\ * & * & * & * \end{pmatrix}\right),$$

elements in L_2 are of the form

$$\left(\begin{pmatrix} 0 \\ 0 \\ 0 \\ * \end{pmatrix}, \begin{pmatrix} * & * & * & 0 \\ * & * & * & 0 \\ 0 & * & * & * \\ 0 & * & * & * \end{pmatrix}\right)$$

and elements in L_3 are of the form

$$\left(\begin{pmatrix} 0 \\ 0 \\ 0 \\ * \end{pmatrix}, \begin{pmatrix} * & * & 0 & 0 \\ * & * & * & 0 \\ 0 & * & * & * \\ 0 & 0 & * & * \end{pmatrix}\right).$$

We will show that these form a sequence of relative sections for the action of $\mathrm{O}_d(\mathbb{C})$ on $\mathbb{C}^d \oplus \mathfrak{so}(d, \mathbb{C})$ (see Definition 2.20), and hence need to specify the normalizer subgroup for each L_i.

The group $\mathrm{O}_i(\mathbb{C})$, for $1 \leq i < d$ appears as a subgroup of $\mathrm{O}_d(\mathbb{C})$ in several natural ways, in particular the subgroup obtained by considering elements that rotate some fixed subset of i coordinates and fix the remaining coordinates. For $B \in \mathrm{O}_i(\mathbb{C})$, denote

$$E(B) = \begin{bmatrix} B & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & \cdots & 1 \end{bmatrix}, \tag{10}$$

a matrix rotating the first i coordinates and fixing the last $d-i$. The set of such $E(B)$ forms a subgroup of $\mathrm{O}_d(\mathbb{C})$ isomorphic to $\mathrm{O}_i(\mathbb{C})$ which we will denote

$$\mathrm{O}_d^i(\mathbb{C}).$$

Note that $\mathrm{O}_d^i(\mathbb{C}) \subset \mathrm{O}_d^{i+1}(\mathbb{C})$.

Proposition 3.5. *Let $1 \leq i < d$ and $B \in \mathrm{O}_i(\mathbb{C})$. The image of the coordinates $m_{1(i+1)}, m_{2(i+1)}, \ldots, m_{i(i+1)}$ under the action of $E(B) \in \mathrm{O}_d^i(\mathbb{C})$ on $(v, M) \in \mathbb{C}^d \oplus \mathfrak{so}(d, \mathbb{C})$ is given by*

$$B \begin{bmatrix} m_{1(i+1)} \\ m_{2(i+1)} \\ \vdots \\ m_{i(i+1)} \end{bmatrix},$$

the standard action of $\mathrm{O}_i(\mathbb{C})$ on a vector in $\mathbb{C}^i$.

Proof. This follows from (8). $\square$

Consider the subgroup

$$W := \Big\{\text{diagonal matrices with diagonal entries lying in } \{-1, 1\}\Big\} \subset \mathrm{O}_d(\mathbb{C}).$$

The action of an element of W changes the sign of various coordinates of $\mathbb{C}^d \oplus \mathfrak{so}(d, \mathbb{C})$. We define the subgroup $N_i(\mathbb{C})$ of $\mathrm{O}_d^i(\mathbb{C})$ as

$$N_i(\mathbb{C}) := \mathrm{O}_d^i(\mathbb{C}) \cdot W = \{g \cdot h \mid g \in \mathrm{O}_d^i(\mathbb{C}), h \in W\}.$$

Note that $N_i(\mathbb{C})$ contains matrices of the form

$$\begin{bmatrix} B & 0 & \cdots & 0 \\ 0 & \pm 1 & \cdots & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & \cdots & \pm 1 \end{bmatrix}, \tag{11}$$

with $B \in \mathrm{O}_d^i(\mathbb{C})$.

Proposition 3.6. *For $1 \leq i < d$, the normalizer of L_i is equal to $N_{d-i}(\mathbb{C})$.*

Proof. It is immediate that $N_{d-1}(\mathbb{C})$ leaves the space L_1 invariant. Considering

$$x = (\begin{pmatrix} 0 \\ \cdots \\ 0 \\ 1 \end{pmatrix}, M) \in L_1,$$

we see that for $g \in \mathrm{O}_d(\mathbb{C})$ to have

$$gx \in L_1,$$

we must have $g_{id} = g_{di} = 0$, $i = 1, \dots, d-1$. This proves the claim for $i = 1$.

Let the statement be true for some $1 \leq i \leq d-2$. First, the normalizer of L_{i+1} is contained in L_i. Diagonal entries of ± 1 leave every L_j invariant, so it remains to investigate the matrix B in (11). Now by Proposition 3.5 B acts by standard matrix multiplication on the vector $(m_{1(i+1)}, \dots, m_{i(i+1)})^\top$. We can hence apply the argument of the case L_1 to deduce that $N_{d-(i+1)}(\mathbb{C})$ is the normalizer of L_{i+1}.

□

We now show that L is a relative W-section, by constructing a sequence of relative sections for the action, drawing in our inspiration from recursive moving frame algorithms (see [27] for instance).

Proposition 3.7. *The linear space L is a relative W-section for the action of $\mathrm{O}_d(\mathbb{C})$ on $\mathbb{C}^d \oplus \mathfrak{so}(d,\mathbb{C})$. In particular there exists a set of rational invariants*

$$\mathcal{I}_d = \{f_1, \dots, f_d\} \subset \mathbb{C}(\mathbb{C}^d \oplus \mathfrak{so}(d,\mathbb{C}))^{\mathrm{O}_d(\mathbb{C})} \tag{12}$$

such that if we define the non-empty, Zariski-open subset

$$U = \left\{ (v, m) \in \mathbb{C}^d \oplus \mathfrak{so}(d,\mathbb{C}) \;\middle|\; \prod_{k=1}^{d} f_k(v, M) \neq 0 \right\} \tag{13}$$

we have that L intersects each orbit that is contained in U. Furthermore we can restrict each invariant to obtain

- $f_1 = v_1^2 + \dots + v_d^2$,
- $f_i|_{L_{i-1}} = m^2_{1(d-i+2)} + \dots + m^2_{(d-i+1)(d-i+2)}$ *for* $2 \leq i < d$.
- $f_d|_L = m_{12}^2$.

Proof. By Proposition 3.2, outside of $f_1 = ||v||^2 = 0$, there exists a rotation $A \in \mathrm{O}_d(\mathbb{C})$ such that $A \cdot (v, M) \in L_1$. Thus, by Proposition 3.6, L_1 is a relative N_{d-1}-section. We also have that $f_1|_{L_1} = v_d^2$. We proceed by induction. Suppose that for each point in $U_i = \{\prod_{k=1}^{i} f_k(p) \neq 0\}$ there exists a rotation $A \in \mathrm{O}_d(\mathbb{C})$ such that $A \cdot (v, M) \in L_i$.

By Proposition 3.6, the linear space L_i is a relative N_{d-i}-section and, by Proposition 2.21, there exists a field isomorphism $\rho_i : \mathbb{C}(\mathbb{C}^d \oplus \mathfrak{so}(d,\mathbb{C}))^{\mathrm{O}_d(\mathbb{C})} \longrightarrow \mathbb{C}(L_i)^{N_{d-i}}$. Using proposition 3.5, one can show that on L_i the polynomial $m^2_{1(d-i+2)} + \dots + m^2_{(d-i+1)(d-i+2)}$ lies in $\mathbb{C}(L_i)^{N_{d-i}}$. Let f_{i+1} be the unique element in $\in \mathbb{C}(\mathbb{C}^d \oplus \mathfrak{so}(d,\mathbb{C}))^{\mathrm{O}_d(\mathbb{C})}$ such that $f_{i+1} = \rho^{-1}(m^2_{1(d-i+2)} + \dots + m^2_{(d-i+1)(d-i+2)})$.

By Proposition 3.2, for any $(v, M) \in L_i$ outside of f_{i+1}, there exists a rotation $A \in N_{d-i}$ such that $A \cdot (v, M) \in L_{i+1}$. Thus for any (v, M) outside of $U_{i+1} = \{\prod_{k=1}^{i+1} f_k(p) \neq 0\}$ there exists a rotation $A \in \mathrm{O}_d(\mathbb{C})$ such that $A \cdot (v, M) \in L_{i+1}$. Using Proposition 3.6, again, we see that L_{i+1} is a relative N_{d-i-1}-section.

We can continue this induction until we have f_{d-1} where $f_{d-1}|_{L_{d-2}} = m_{13}^2 + m_{23}^2$. Finally note that the polynomial m_{12}^2 lies in $\mathbb{C}(L)^W$. Since L is a W-section there exists $f_d \in \mathbb{C}(\mathbb{C}^d \oplus \mathfrak{so}(d,\mathbb{C}))^{\mathrm{O}_d(\mathbb{C})}$ such that $f_d|_L = m_{12}^2$. □

In particular the above proposition implies that L is a relative W-section for the action of $\mathrm{O}_d(\mathbb{C})$ on $\mathbb{C}^d \oplus \mathfrak{so}(d,\mathbb{C})$, and hence the function fields $\mathbb{C}(L)^W$ and $\mathbb{C}(\mathbb{C}^d \oplus \mathfrak{so}(d,\mathbb{C}))^{\mathrm{O}_d(\mathbb{C})}$ are isomorphic.

By examining the action of W on L and the structure of $\mathbb{C}(L)^W$ we can therefore glean information about the action of $\mathrm{O}_d(\mathbb{C})$ on $\mathbb{C}^d \oplus \mathfrak{so}(d,\mathbb{C})$. Consider a diagonal matrix $D \in W$ given by

$$D = \begin{bmatrix} w_1 & 0 & \dots & 0 \\ 0 & w_2 & \dots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & w_d \end{bmatrix}$$

where $w_i \in \{-1, 1\}$ for $1 \le i \le d$. Then the image of a point in $\mathbb{C}^d \oplus \mathfrak{so}(d,\mathbb{C})$ (or in $\mathbb{R}^d \oplus \mathfrak{so}(d,\mathbb{R})$) is $D \cdot (v, M) = (\overline{v}, \overline{M})$ where

(14)
$$v = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ w_d v_d \end{bmatrix} \quad M = \begin{bmatrix} 0 & w_1 w_2 m_{12} & 0 & \dots & 0 \\ -w_1 w_2 m_{12} & 0 & w_2 w_3 m_{23} & \dots & 0 \\ 0 & -w_2 w_3 m_{23} & 0 & \dots & \vdots \\ \vdots & & & \ddots & w_{d-1} w_d m_{(d-1)d} \\ 0 & 0 & \dots & -w_{d-1} w_d m_{(d-1)d} & 0 \end{bmatrix}.$$

Proposition 3.8. *The action of W on $L \cap U$ is free.*

Proof. Suppose that the action is not free. Then there exists $D \in W$ such that $D \cdot (v, M) = (v, M)$ and D is not the identity. Necessarily we have that for some $1 \le i \le d-1$, $w_i = -1$. Since $w_i w_{i+1} m_{i(i+1)} = m_{i(i+1)}$ and $m_{i(i+1)} \neq 0$, then $w_{i+1} = -1$. Using a similar argument, $w_{i+2} = -1$ and so forth. However $w_d v_d = v_d$, where $v_d \neq 0$, implying that $w_d = 1$ which is a contradiction. □

Corollary 3.9. *The action of $\mathrm{O}_d(\mathbb{C})$ on $U \subset \mathbb{C}^d \oplus \mathfrak{so}(d,\mathbb{C})$ is free.*

Proof. By Proposition 3.7, each orbit on U meets the linear subspace L. We show that the stabilizer of a point in $L \cap U$ is identity. This is sufficient to prove the result, as any two points in the same orbit have isomorphic stabilizer groups.

Let $(v, M) \in L$ and consider $g \in G$ such that $g \cdot (v, M) = (v, M)$. By Proposition 3.6 g must lie in W. However, by Proposition 3.8, the only element of W fixing a point in $L \cap U$ is the identity. □

Since we have that $w_i^2 = 1$ for any $1 \le i \le d$, clearly

(15)
$$\mathcal{I}_W := \{v_d^2, m_{d(d-1)}^2, \dots, m_{12}^2\}$$

is a set of invariant functions on $\mathbb{C}(L)^W$.

Proposition 3.10. *The set $\mathcal{I}_W$ separates orbits and is a generating set for $\mathbb{C}(L)^W$.*

Proof. Consider the map $F : L \cap U \to \mathbb{C}^d$ defined by evaluating the invariants in $\mathcal{I}_W$ on $L \cap U$ a non-empty, Zariski-open subset of L. We show that every fiber of this map is exactly an orbit of W. Consider any $(v, M) \in L \cap U$; then set of points in the fiber of its image is given by

$$\begin{aligned} F^{-1}(F(v,M)) &= \{(\tilde{v}, \tilde{M}) \in L \cap U \mid \tilde{v}_d^2 = v_d^2, \tilde{m}_{12}^2 = m_{12}^2, \dots, \tilde{m}_{(d-1)d}^2 = m_{(d-1)d}^2\} \\ &= \{(\tilde{v}, \tilde{M}) \in L \cap U \mid \tilde{v}_d = \pm v_d, \tilde{m}_{12} = \pm m_{12}, \dots, \tilde{m}_{(d-1)d} = \pm m_{(d-1)d}\}. \end{aligned}$$

We can individually change the sign for any coordinate of (v, M). To change the sign of only v_d one can act by the matrix $D \in W$ such that $w_i = -1$ for all $1 \le i \le d$. Similarly for $m_{i(i+1)}$ we can act by the matrix $D \in W$ such that $w_k = -1$ for $1 \le k \le i$ and $w_k = 1$ otherwise. This implies that the above set is exactly the orbit of (v, M) under W, and hence $\mathcal{I}_W$ is separating on $L \cap U$. Then by Proposition 2.18, $\mathcal{I}_W$ generates $\mathbb{C}(L)^W$. □

Corollary 3.11. *The set $\mathcal{I}_d$ in (12) is a minimal generating set of rational invariant functions for $\mathbb{C}(\mathbb{C}^d \oplus \mathfrak{so}(d,\mathbb{C}))^{\mathrm{O}_d(\mathbb{C})}$ and separates orbits.*

Proof. By Proposition 3.7 L is a relative W-section for the action of $\mathrm{O}_d(\mathbb{C})$ on $\mathbb{C}^d \oplus \mathfrak{so}(d,\mathbb{C})$, and $\mathcal{I}_d$ restricts to the set of invariants $\mathcal{I}_W$ in (15) for the action of W on L. By Proposition 3.10, the set $\mathcal{I}_W$ is a generating set for $\mathbb{C}(L)^W$, and hence by Corollary 2.22 $\mathcal{I}_d$ is a generating set for $\mathbb{C}(\mathbb{C}^d \oplus \mathfrak{so}(d,\mathbb{C}))^{\mathrm{O}_d(\mathbb{C})}$. By Proposition 2.18, $\mathcal{I}_d$ also separates orbits.

By Corollary 3.9, the action of $\mathrm{O}_d(\mathbb{C})$ is free on a non-empty, Zariski-open subset of $\mathbb{C}^d \oplus \mathfrak{so}(d,\mathbb{C})$. Thus the maximum dimension of an orbit on $\mathbb{C}^d \oplus \mathfrak{so}(d,\mathbb{C})$ is $\dim(\mathrm{O}_d(\mathbb{C})) = \frac{d(d-1)}{2}$. By [39, Corollary, Section 2.3] the transcendence degree of $\mathbb{C}(\mathbb{C}^d \oplus \mathfrak{so}(d,\mathbb{C}))^{\mathrm{O}_d(\mathbb{C})}$ is $\frac{d(d+1)}{2} - \frac{d(d-1)}{2} = d$, and hence any generating set must be at least of size d, implying that $\mathcal{I}_d$ is minimal. □

Remark 3.12. One can prove similar results for the special Orthogonal group $\mathcal{SO}_d(\mathbb{C})$ using the same procedure. Propositions 3.2 and 3.5 also hold for $\mathcal{SO}_d(\mathbb{C})$. By replacing W with the subgroup $W \cap \mathcal{SO}_d(\mathbb{C})$, it can be shown that L intersects each orbit of $\mathcal{SO}_d(\mathbb{C})$ on U and that the action is free.

The above results for the action of $\mathrm{O}_d(\mathbb{C})$ on $\mathbb{C}^d \oplus \mathfrak{so}(d,\mathbb{C})$ help uncover the structure of the action of $\mathrm{O}_d(\mathbb{R})$ on $\mathbb{R}^d \oplus \mathfrak{so}(d,\mathbb{R})$. First we show that the intersection of the set U defined in (13) with $\mathbb{R}^d \oplus \mathfrak{so}(d,\mathbb{R})$ is a non-empty and well-defined Zariski open subset of $\mathbb{R}^d \oplus \mathfrak{so}(d,\mathbb{R})$.

Proposition 3.13. *The set $\mathcal{I}_d$ in (12) is a subset of $\mathbb{R}(\mathbb{R}^d \oplus \mathfrak{so}(d,\mathbb{R}))^{\mathrm{O}_d(\mathbb{R})}$. In particular*

$$U_{\mathbb{R}} := \left[U \cap \mathbb{R}^d \oplus \mathfrak{so}(d,\mathbb{R})\right],$$

is a well-defined and non-empty Zariski open subset of $\mathbb{R}^d \oplus \mathfrak{so}(d,\mathbb{R})$, and

$$L_{\mathbb{R}} := \left[L \cap \mathbb{R}^d \oplus \mathfrak{so}(d,\mathbb{R})\right]$$

intersects each orbit (under $\mathrm{O}_d(\mathbb{R})$) contained in $U_{\mathbb{R}}$.

Proof. In the proof of Proposition 3.7, each function f_i is obtaining by taking the inverse image of a real invariant function under the field isomorphism $\rho_i : \mathbb{C}(\mathbb{C}^d \oplus \mathfrak{so}(d,\mathbb{C}))^{\mathrm{O}_d(\mathbb{C})} \longrightarrow \mathbb{C}(L_i)^{N_{d-i}}$. The function f_i can be decomposed $f_i = h_1 + \mathcal{I} \cdot h_2$, where h_1 and h_2 are elements of $\mathbb{R}(\mathbb{R}^d \oplus \mathfrak{so}(d,\mathbb{R}))^{\mathrm{O}_d(\mathbb{R})}$, and hence by Proposition 2.23, are elements of $\mathbb{C}(\mathbb{C}^d \oplus \mathfrak{so}(d,\mathbb{C}))^{\mathrm{O}_d(\mathbb{C})}$. Thus $h_1|_{L_i} = f_i|_{L_i}$. Since ρ_i is a field isomorphism, f_i must define the same rational function as h_1, and hence is an element of $\mathbb{R}(\mathbb{R}^d \oplus \mathfrak{so}(d,\mathbb{R}))^{\mathrm{O}_d(\mathbb{R})}$.

Note that Proposition 3.2 also holds for any $v \in \mathbb{R}^d$, i.e. by applying Gram-Schmidt to a linearly independent set of d vectors $\{v, v_1, \ldots, v_{d-1}\}$ in $\mathbb{R}^d$. Thus if $f_1(v, M) \neq 0$, there exists a rotation $A \in \mathrm{O}_d(\mathbb{R})$ such that $A \cdot (v, M) \in L_1 \cap \mathbb{R}^d \oplus \mathfrak{so}(d,\mathbb{R})$. Similarly as in the proof of Proposition 3.7 we can proceed by induction. Suppose $(v, M) \in L_i \cap \mathbb{R}^d \oplus \mathfrak{so}(d,\mathbb{R})$ and $f_{i+1}(v, M) \neq 0$. Then we have that

$$m_1^2 + \ldots + m^2 \neq 0.$$

By Proposition 3.5 we can find a rotation $A \in N_{d-i}(\mathbb{C})$ such that $A \cdot (v, M) \in L_{i+1}$. Therefore if $(v, M) \in U_{\mathbb{R}}$, there exists a rotation $A \in \mathrm{O}_d(\mathbb{R})$ such that $A \cdot (v, M) \in L$. □

The following follows directly from Proposition 3.9

Corollary 3.14. *The action of $\mathrm{O}_d(\mathbb{R})$ on $U_{\mathbb{R}} \subset \mathbb{R}^d \oplus \mathfrak{so}(d,\mathbb{R})$ is free.*

Proposition 3.15. *The set $\mathcal{I}_d$ generates the invariant function field $\mathbb{R}(\mathbb{R}^d \oplus \mathfrak{so}(d,\mathbb{R}))^{\mathrm{O}_d(\mathbb{R})}$ and separates orbits on $U_{\mathbb{R}}$.*

Proof. The fact that $\mathcal{I}_d$ generates $\mathbb{R}(\mathbb{R}^d \oplus \mathfrak{so}(d,\mathbb{R}))^{\mathrm{O}_d(\mathbb{R})}$ follows from Propositions 3.7, 3.13 and Corollary 2.24. Using a similar argument as in Proposition 3.10, we can see that $\mathcal{I}_W$ in (15) separates orbits for the action of W on $L_\mathbb{R} \cap U_\mathbb{R}$. By Proposition 3.13, any orbit on $U_\mathbb{R}$ meets $L_\mathbb{R}$, and the $\mathcal{I}_d$ restrict to $\mathcal{I}_W$ on $L_\mathbb{R}$. Thus $\mathcal{I}_d$ is separating on $U_\mathbb{R}$. □

We finish the section by constructing an explicit set of invariant polynomial functions that generate $\mathbb{C}(\mathbb{C}^d \oplus \mathfrak{so}(d,\mathbb{C}))^{\mathrm{O}_d(\mathbb{C})}$. Consider the map

$$\begin{aligned}\phi_k : \mathbb{C}^d \oplus \mathfrak{so}(d,\mathbb{C}) &\to \mathbb{C}^d \\ (v, M) &\mapsto M^k v.\end{aligned}$$

Then for the action of $A \cdot (v, M)$ we have that

$$\phi_k\left(A \cdot (v, M)\right) = \phi_k\left((Av, AMA^T)\right) = (AMA^T)^k Av = AM^k v.$$

Thus the polynomial obtained by the dot-product of ϕ_k with itself is an invariant function on $\mathbb{C}^d \oplus \mathfrak{so}(d,\mathbb{C})$ under $\mathrm{O}_d(\mathbb{C})$. We will show that the set of polynomial invariants (defining $a \cdot b := \sum_i a_i b_i$)

$$\mathcal{I}_M = \left\{v \cdot v,\ M^k v \cdot M^k v, \,|\, 1 \le k < d\right\} \tag{16}$$

generate the field $\mathbb{C}(\mathbb{C}^d \oplus \mathfrak{so}(d,\mathbb{C}))^{\mathrm{O}_d(\mathbb{C})}$ by restricting them to L.

Lemma 3.16. *Consider a matrix M of the form as in (9). Then for $1 \le k < d$, M^k satisfies*

(a) $M^k(d-k, d) = \prod_{i=1}^{k} m_{(d-i)(d-i+1)}$,
(b) $M^k(i, d) = 0$ *for* $i < d - k$,
(c) $M^k(i, d) \in \mathbb{Q}[m_{(d-j)(d-j+1)} \,|\, 1 \le j < k]$ *for* $i > d - k$.

Proof. We proceed by induction. For $k = 1$, $M^1 = M$. Then M^1 satisfies (a)-(c), since $M(d-1, d) = m_{(d-1)(d)}$ and $M(i, d) = 0$ for $i < d - 1$. Now suppose that (a)-(c) hold for M^{k-1}. We have that for $M^k = MM^{k-1}$,

$$\begin{aligned}M^k(1, d) &= m_{12} M^{k-1}(2, d) \\ M^k(i, d) &= -m_{i-1,i} M^{k-1}(i-1, d) + m_{i,i+1} M^{k-1}(i+1, d) \\ M^k(d, d) &= -m_{(d-1)d} M^{k-1}(d-1, d),\end{aligned}$$

where $1 < i < d-1$. Note that $M^k(i, d)$ is linear combination of $M^{k-1}(i-1, d)$ and $M^{k-1}(i+1, d)$. By the induction hypothesis we know that $M^{k-1}(i, d) = 0$ if $i < d - k + 1$, and hence $M^k(i, d) = 0$ when $i + 1 < d - k + 1$, or equivalently when $i < d - k$. This proves (b).

Suppose that $i > d - k$. Then $M^k(i, d)$ is linear in the terms

$$m_{i-1,i}, \quad m_{i,i+1}, \quad M^{k-1}(i-1, d), \quad M^{k-1}(i+1, d),$$

where $m_{i-1,i}$ and $m_{i,i+1}$ are of the form $m_{(d-j)(d-j+1)}$ for $1 \le j < k$. By the induction hypothesis, the latter two terms are polynomials in $m_{(d-j)(d-j+1)}$ where $1 \le j < k - 1$, proving (c).

Finally suppose that $i = d - k$. We have that

$$M^k(d-k,d) = -m_{d-k-1,d-k}M^{k-1}(d-k-1,d) + m_{d-k,d-k+1}M^{k-1}(d-k+1,d).$$

By the induction hypothesis we know that

$$M^{k-1}(d-k+1,d) = \prod_{i=1}^{k-1} m_{(d-i)(d-i+1)} \quad \text{and} \quad M^{k-1}(d-k-1,d) = 0,$$

which proves (a). □

Lemma 3.17. *The polynomials obtained from restricting the functions in $\mathcal{I}_M$ to L generate the invariant rational function field $\mathbb{C}(L)^W$.*

Proof. First note that to restrict the polynomials in $\mathcal{I}_M$ to L, we can assume that (v, M) are of the form in (9) and then compute the inner product. Then we can easily see that

$$v \cdot v|_L = v_d^2 \quad \text{and} \quad Mv \cdot Mv|_L = v_d^2 m_{(d-1)d}^2.$$

This implies that v_d^2 and $m_{(d-1)d}^2$ are rational functions of $v \cdot v|_L$ and $Mv \cdot Mv|_L$. We proceed by induction on i: suppose that $m_{(d-i)(d-i+1)}^2$ is a rational function of $v \cdot v|_L, Mv \cdot Mv|_L, \dots, M^i v \cdot M^i v|_L$ for all $1 \le i < k$. By Lemma 3.16, we know that

$$M^k v \cdot M^k v|_L = v_d^2 \prod_{i=1}^{k} m_{(d-i)(d-i+1)}^2 + v_d^2 \mathcal{I}\left(m_{(d-1)d}, m_{(d-2)(d-1)}, \dots, m_{(d-k+1)(d-k+2)}\right).$$

Since $M^k \cdot M^k v|_L$ is an invariant function, as well as v_d^2 and $m_{(d-i)(d-i+1)}^2$ for $1 \le i < d$, the function $\mathcal{I}$ lies in $\mathbb{C}(W)^L$. By the induction hypothesis and Proposition 3.10, $\mathcal{I}$ is a rational function of

$$v \cdot v|_L,\ Mv \cdot Mv|_L,\ \dots, M^{k-1}v \cdot M^{k-1}v|_L.$$

Thus we can rewrite the above equality to

$$\frac{M^k v \cdot M^k v - v_d^2 \mathcal{I}\left(v \cdot v|_L, Mv \cdot Mv|_L, \dots, M^{k-1}v \cdot M^{k-1}v|_L\right)}{v_d^2 \prod_{i=1}^{k-1} m_{(d-i)(d-i+1)}^2} = m_{(d-k)(d-k+1)}^2.$$

By the induction hypothesis each $m_{(d-i)(d-i+1)}^2$ for $1 \le i < k$ is a rational function of

$$v \cdot v|_L,\ Mv \cdot Mv|_L,\ \dots, M^{k-1}v \cdot M^{k-1}v|_L.$$

This implies that $m_{(d-k)(d-k+1)}^2$ is a rational function of

$$v \cdot v|_L,\ Mv \cdot Mv|_L,\ \dots, M^{k}v \cdot M^{k}v|_L.$$

Therefore each element of $\mathcal{I}_W$ can be written as a rational function of polynomials in $\mathcal{I}_M$ restricted to L. By Proposition 3.10, $\mathcal{I}_M$ restricted to L is a generating set for $\mathbb{C}(L)^W$. □

Proposition 3.18. *The set of polynomial invariants $\mathcal{I}_M$ in (16) generates both $\mathbb{C}(\mathbb{C}^d \oplus \mathfrak{so}(d,\mathbb{C}))^{\mathrm{O}_d(\mathbb{C})}$ and $\mathbb{R}(\mathbb{R}^d \oplus \mathfrak{so}(d,\mathbb{R}))^{\mathrm{O}_d(\mathbb{R})}$ and also separates orbits on $\mathbb{C}^d \oplus \mathfrak{so}(d,\mathbb{C})$ and $\mathbb{R}^d \oplus \mathfrak{so}(d,\mathbb{R})$.*

Example 3.19. By Proposition 3.18 the field of invariants $\mathbb{R}(\mathbb{R}^3 \times \mathfrak{so}(3,\mathbb{R}))^{\mathrm{O}_3(\mathbb{R})}$ is generated by

$$\begin{aligned} v \cdot v &= v_1^2 + v_2^2 + v_3^2 \\ Mv \cdot Mv &= (m_{12}v_1 - m_{23}v_3)^2 + (m_{13}v_1 + m_{23}v_2)^2 + (m_{12}v_2 + m_{13}v_3)^2 \\ M^2v \cdot M^2v &= \left(m_{12}m_{23}v_1 - m_{12}m_{13}v_2 - \left({m_{13}}^2 + {m_{23}}^2\right)v_3\right)^2 \\ &\quad + \left(m_{13}m_{23}v_1 + m_{12}m_{13}v_3 + \left({m_{12}}^2 + {m_{23}}^2\right)v_2\right)^2 \\ &\quad + \left(m_{13}m_{23}v_2 - m_{12}m_{23}v_3 + \left({m_{12}}^2 + {m_{13}}^2\right)v_1\right)^2. \end{aligned}$$

Proof. By Proposition 3.7 L is a relative W-section for the action of $\mathrm{O}_d(\mathbb{C})$ on $\mathbb{C}^d \oplus \mathfrak{so}(d,\mathbb{C})$, and by Proposition 3.10 $\mathcal{I}_W$ is a generating set for $\mathbb{C}(L)^W$. Thus by Lemma 3.17 and Corollary 2.22, $\mathcal{I}_M$ generates $\mathbb{C}(\mathbb{C}^d \oplus \mathfrak{so}(d,\mathbb{C}))^{\mathrm{O}_d(\mathbb{C})}$. By Corollary 2.24 $\mathcal{I}_M$ generates $\mathbb{R}(\mathbb{R}^d \oplus \mathfrak{so}(d,\mathbb{R}))^{\mathrm{O}_d(\mathbb{R})}$.

By Proposition 2.18 $\mathcal{I}_M$ separates orbits on $\mathbb{C}^d \oplus \mathfrak{so}(d,\mathbb{C})$. By Proposition 3.15 there exists a separating set of invariants in $\mathbb{R}(\mathbb{R}^d \oplus \mathfrak{so}(d,\mathbb{R}))^{\mathrm{O}_d(\mathbb{R})}$, and hence $\mathbb{R}(\mathbb{R}^d \oplus \mathfrak{so}(d,\mathbb{R}))^{\mathrm{O}_d(\mathbb{R})}$ separates orbits. Therefore, by Proposition 2.25, $\mathcal{I}_M$ separates orbits on $\mathbb{R}^d \oplus \mathfrak{so}(d,\mathbb{R})$. □

4. $\mathrm{O}_d(\mathbb{R})$-INVARIANT ITERATED INTEGRAL SIGNATURE

4.1. Moving frame on $\mathfrak{g}_{\le n}((\mathbb{R}^2))$.

In this section, we construct a moving frame map for the action of $\mathrm{O}_2(\mathbb{R})$ on $\mathfrak{g}_{\le n}((\mathbb{R}^2))$, and show how this can be used to construct $\mathrm{O}_2(\mathbb{R})$-invariants in $\mathfrak{g}_{\le n}((\mathbb{R}^2))$ and hence in the coefficients of the iterated-integral signature of a curve X.

First consider the action on $\mathfrak{g}_{\le 2}((\mathbb{R}^2)) = \mathbb{R}^2 \oplus [\mathbb{R}^2, \mathbb{R}^2]$. We can denote any element of $\mathfrak{g}_{\le 2}((\mathbb{R}^2))$ as $\mathbf{c}_{\le 2}$ with coordinates c_1, c_2, and c_{12}. Through the isomorphism in (4) we can consider $\mathbf{c}_{\le 2}$ as an element of $\mathbb{R}^2 \oplus \mathfrak{so}(2,\mathbb{R})$,

$$\mathbf{c}_{\le 2} = (v, M) = \left(\begin{pmatrix} c_1 \\ c_2 \end{pmatrix}, \begin{pmatrix} 0 & c_{12} \\ -c_{12} & 0 \end{pmatrix}\right),$$

and with action as in (7). We will now show that $\mathrm{O}_2(\mathbb{R})$ is free on $\mathfrak{g}_{\le 2}((\mathbb{R}^2))$ and the following submanifold

$$\mathcal{K} = \left\{\mathbf{c}_{\le 2} \in \mathfrak{g}_{\le 2}((\mathbb{R}^2)) \mid c_1 = 0; c_2, c_{12} > 0\right\}$$

is a cross-section for the action. Similarly to Example 2.14, we start by defining the group element

$$A(\mathbf{c}_{\le 2}) := \frac{1}{\sqrt{c_1^2 + c_2^2}} \begin{pmatrix} c_2 & -c_1 \\ c_1 & c_2 \end{pmatrix},$$

which is defined outside of $\{c_1 = c_2 = 0\}$. For any such element $\mathbf{c}_{\le 2} \in \mathfrak{g}_{\le 2}((\mathbb{R}^2))$, we have that

$$A(\mathbf{c}_{\le 2}) \cdot \mathbf{c}_{\le 2} = \left(\begin{pmatrix} 0 \\ \sqrt{c_1^2 + c_2^2} \end{pmatrix}, \begin{pmatrix} 0 & c_{12} \\ -c_{12} & 0 \end{pmatrix}\right).$$

Unlike in Example 2.14, the action is not free on $\mathbb{R}^2$, the submanifold defined by $c_1 = 0, c_2 > 0$ is not a cross-section, and $A(\mathbf{c}_{\le 2})$ does not define a moving frame map. This is due to the fact that a reflection about the y-axis will fix v, but change the sign of M. Thus to define a moving frame map we must consider the diagonal action of $\mathrm{O}_2(\mathbb{R})$ on all of $\mathfrak{g}_{\le 2}((\mathbb{R}^2))$, not just the action on $\mathfrak{g}_{\le 1}((\mathbb{R}^2)) = \mathbb{R}^2$. The map $\rho : U \longrightarrow \mathrm{O}_2(\mathbb{R})$ given by

$$\rho(\mathbf{c}_{\leq 2}) = \frac{1}{\sqrt{c_1^2 + c_2^2}} \begin{pmatrix} \operatorname{sgn}(c_{12})c_2 & -\operatorname{sgn}(c_{12})c_1 \\ c_1 & c_2 \end{pmatrix}$$

defines the group element $\rho(\mathbf{c}_{\leq 2})$ such that $\rho(\mathbf{c}_{\leq 2}) \cdot \mathbf{c}_{\leq 2} \in \mathcal{K}$ where

$$U = \left\{ \mathbf{c}_{\leq 2} = (v, M) \mid v \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix}, c_{12} \neq 0 \right\} \subset \mathfrak{g}_{\leq 2}((\mathbb{R}^2)).$$

Note that $\mathcal{K}$ and U are subsets of $L_{\mathbb{R}}$ and $U_{\mathbb{R}}$ respectively, both defined in Proposition 3.13. The (unique) intersection point of the orbit $\mathrm{O}_2(\mathbb{R}) \cdot \mathbf{c}_{\leq 2}$ and $\mathcal{K}$ is $\rho(\mathbf{c}_{\leq 2}) \cdot \mathbf{c}_{\leq 2}$. Since the action is free on $\mathfrak{g}_{\leq 2}((\mathbb{R}^2))$ (Corollary 3.14), the map ρ defines a moving frame with cross-section $\mathcal{K}$. This immediately implies that the coordinates of $\rho(\mathbf{c}_{\leq 2}) \cdot \mathbf{c}_{\leq 2}$ are invariants for the action of $\mathrm{O}_2(\mathbb{R})$ on $\mathfrak{g}_{\leq 2}((\mathbb{R}^2))$[6]:

$$\sqrt{c_1^2 + c_2^2}, \quad |c_{12}|.$$

Furthermore any two elements $\mathbf{c}_{\leq 2}, \tilde{\mathbf{c}}_{\leq 2} \in \mathfrak{g}_{\leq 2}((\mathbb{R}^2))$ are related by element of $\mathrm{O}_2(\mathbb{R})$ if and only if

$$\sqrt{c_1^2 + c_2^2} = \sqrt{\tilde{c}_1^2 + \tilde{c}_2^2} \quad \text{and} \quad |c_{12}| = |\tilde{c}_{12}|.$$

For any path X in $\mathbb{R}^2$, let $\mathbf{c}_{\leq 2}(X)$ denote the element of $\mathfrak{g}_{\leq 2}((\mathbb{R}^2))$ given by $\operatorname{proj}_{\leq 2}(\log(\mathrm{IIS}(X)))$. Then we can define the "invariantized" path $Y := \rho(\mathbf{c}_{\leq 2}(X)) \cdot X$. The above statement implies that for any two paths $X, \tilde{X}$, we have that $\mathbf{c}_{\leq 2}(Y) = \mathbf{c}_{\leq 2}(\tilde{Y})$ if and only if there exists some $g \in \mathrm{O}_2(\mathbb{R})$ such that

$$g \cdot \mathbf{c}_{\leq 2}(X) = \mathbf{c}_{\leq 2}(g \cdot X) = \mathbf{c}_{\leq 2}(\tilde{X}).$$

In particular, since the log map is an equivariant bijection, the same holds true for the IIS of a path under the projection $\operatorname{proj}_{\leq 2}$.

Given a path X starting at the origin, the values of $c_1(X), c_2(X)$ correspond to x and y values of $X(1)$. Similarly the value of $c_{12}(X)$ corresponds to the so-called Lévy area traced by X (see [12, Section 3.2] in the context of classical invariant theory). Thus the moving frame map applied to such a path X, rotates the end point $X(1)$ to the y-axis (and reflects about the y-axis if the Lévy area is negative).

The resulting invariants on $\mathfrak{g}_{\leq 2}((\mathbb{R}^2))$ are perhaps unsurprising, but the above method also yields $\mathrm{O}_2(\mathbb{R})$-invariants on $\mathfrak{g}_{\leq n}((\mathbb{R}^2))$ for an arbitrary truncation order n. We can similarly define a map $\tilde{\rho} : \tilde{U} \subset \mathfrak{g}_{\leq n}((\mathbb{R}^2)) \longrightarrow \mathrm{O}_2(\mathbb{R})$ by

$$\rho(\mathbf{c}_{\leq n}) = \frac{1}{\sqrt{c_1^2 + c_2^2}} \begin{pmatrix} \operatorname{sgn}(c_{12})c_2 & -\operatorname{sgn}(c_{12})c_1 \\ c_1 & c_2 \end{pmatrix}$$

for any $\mathbf{c}_{\leq n} \in \tilde{U}$ where

$$\tilde{U} = \operatorname{proj}^{-1}_{\leq n \to \leq 2}(U) \subset \mathfrak{g}_{\leq n}((\mathbb{R}^2)).$$

Since $\mathrm{O}_2(\mathbb{R})$ acts diagonally on the whole of $\mathfrak{g}_{\leq n}((\mathbb{R}^2))$, $\tilde{\rho}$ is a moving frame map on $\mathfrak{g}_{\leq n}((\mathbb{R}^2))$ with cross-section $\tilde{\mathcal{K}}$ where

$$\tilde{\mathcal{K}} = \operatorname{proj}^{-1}_{\leq n \to \leq 2}(\mathcal{K}) \subset \mathfrak{g}_{\leq n}((\mathbb{R}^2)).$$

Then the resulting coordinate functions of $\rho(\mathbf{c}_{\leq \mathbf{n}}) \cdot \mathbf{c}_{\leq n} \in \mathfrak{g}_{\leq n}((\mathbb{R}^2))$ are also $\mathrm{O}_2(\mathbb{R})$ invariants for the action on $\mathfrak{g}_{\leq n}((\mathbb{R}^2))$ (see Section 5 for a more detailed investigation of these invariants), and hence $\mathrm{O}_2(\mathbb{R})$ invariants for paths in $\mathbb{R}^2$. Furthermore for any truncation order n and paths $X, \tilde{X} \in \mathbb{R}^2$, we have that $\mathbf{c}_{\leq n}(Y) = \mathbf{c}_{\leq n}(\tilde{Y})$ if and only if there exists some element of $\mathrm{O}_2(\mathbb{R})$ such that

[6] The constant functions are referred to as the *phantom invariants*.

$g \cdot \mathbf{c}_{\leq n}(X) = \mathbf{c}_{\leq n}(\tilde{X})$. The following is then true by induction and the fact that the log map is an equivariant bijection.

Proposition 4.1. *Let $X, \tilde{X}$ be paths in $\mathbb{R}^2$ such that $\mathbf{c}_{\leq 2}(X) := \operatorname{proj}_{\leq 2}(\log(\operatorname{IIS}(X))), \mathbf{c}_{\leq 2}(\tilde{X}) := \operatorname{proj}_{\leq 2}(\log(\operatorname{IIS}(\tilde{X})))$ are elements of U. Define*

$$Y := \rho(\mathbf{c}_{\leq 2}(X)) \cdot X, \qquad \tilde{Y} := \rho(\mathbf{c}_{\leq 2}(\tilde{X})) \cdot \tilde{X}.$$

Then $\operatorname{IIS}(Y) = \operatorname{IIS}(\tilde{Y})$ if and only if there exists $g \in \mathrm{O}_2(\mathbb{R})$ such that $\operatorname{IIS}(g \cdot X) = \operatorname{IIS}(\tilde{X})$.

Therefore two paths, starting at the origin are equivalent up to tree-like extensions and action of $\mathrm{O}_2(\mathbb{R})$ if and only if $\operatorname{IIS}(Y) = \operatorname{IIS}(\tilde{Y})$. In this sense, the moving frame map ρ yields a method to invariantize a path X. In the following section, we show that this construction extends to paths in $\mathbb{R}^d$.

4.2. **Moving Frame on $\mathfrak{g}_{\leq n}((\mathbb{R}^d))$.** As for $\mathrm{O}_2(\mathbb{R})$ on $\mathbb{R}^2$, the action of $\mathrm{O}_d(\mathbb{R})$ on paths in $\mathbb{R}^d$ induces an action on its (truncated) signature that coincides with the diagonal action on the ambient space $T_{\leq n}(\mathbb{R}^d)$. The induced action on the log-signature coincides with this diagonal action as well, when considering $\mathfrak{g}_{\leq n}((\mathbb{R}^d))$ as a subspace of $T_{\leq n}(\mathbb{R}^d)$.

Let $\mathbf{c}_{\leq n}$ be an element of $\mathfrak{g}_{\leq n}((\mathbb{R}^d))$ with coordinates given by $c_{\mathtt{i}_1\mathtt{i}_2\ldots\mathtt{i}_m}$ for $m \leq n$. We define the following submanifold $\mathcal{K}$ of $\mathfrak{g}_{\leq n}((\mathbb{R}^d))$:

(17) $$\mathcal{K} = \left\{c_{\mathtt{i}} = 0, c_{\mathtt{j}(\mathtt{i}+1)} = 0, c_{\mathtt{d}} > 0,\ c_{\mathtt{i}(\mathtt{i}+1)} > 0 \,|\, 1 \leq i \leq d-1, 1 \leq j < i\right\} \subset \mathfrak{g}_{\leq n}((\mathbb{R}^d))$$

Let $\operatorname{proj}_{\leq 2} : \mathfrak{g}_{\leq n}((\mathbb{R}^d)) \to \mathfrak{g}_{\leq 2}((\mathbb{R}^d))$ be the projection onto the first two levels (Section 2.2).The projection of this submanifold onto $\mathfrak{g}_{\leq 2}((\mathbb{R}^d))$, $\operatorname{proj}_{\leq 2}(\mathcal{K})$ is analogous to the real, positive points of L in (9) where

$$\left(\begin{pmatrix} c_{\mathtt{1}} \\ \vdots \\ c_{\mathtt{d}} \end{pmatrix}, \begin{pmatrix} 0 & c_{\mathtt{12}} & \ldots & c_{\mathtt{1d}} \\ -c_{\mathtt{12}} & 0 & \ldots & c_{\mathtt{2d}} \\ \ldots & \ldots & \ddots & \ldots \\ -c_{\mathtt{1d}} & -c_{\mathtt{2d}} & \ldots & 0 \end{pmatrix}\right) = (v, M).$$

Similarly we can define the analogue to U in (13). Consider the rational functions on $\mathfrak{g}_{\leq n}((\mathbb{R}^d))$ given by

$$F_i(\mathbf{c}_{\leq n}) := f_i(v, M)|_{v_j = c_{\mathtt{j}}\ m_{k\ell} = c_{\mathtt{k}\ell}}$$

for $1 \leq i \leq d$ where $f_i(v, M)$ is given in Proposition 3.7. By Proposition 3.13, the functions F_i are rational functions on $\mathfrak{g}_{\leq 2}((\mathbb{R}^d))$ with real coefficients. Then the following is a Zariski-open subset of $\mathfrak{g}_{\leq n}((\mathbb{R}^d))$,

$$U_n^d := \left\{\mathbf{c}_{\leq n} \in \mathfrak{g}_{\leq n}((\mathbb{R}^d)) \mid F_i(\mathbf{c}_{\leq n}) \neq 0, \forall i, 1 \leq i \leq d\right\},$$

where $\operatorname{proj}_{\leq 2}(U_n^d) = U$ if we identify $\mathbf{c}_{\leq 2}$ with (v, M) as above. In particular, both U_n^d and $\mathcal{K}$ are completely characterized by $\operatorname{proj}_{\leq 2}(\mathbf{c}_{\leq n})$, i.e.

$$U_n^d = \operatorname{proj}^{-1}_{\leq n \to \leq 2}\left(\operatorname{proj}_{\leq 2}(U_n^d)\right) \subset \mathfrak{g}_{\leq n}((\mathbb{R}^2))$$
$$\mathcal{K} = \operatorname{proj}^{-1}_{\leq n \to \leq 2}\left(\operatorname{proj}_{\leq 2}(\mathcal{K})\right) \subset \mathfrak{g}_{\leq n}((\mathbb{R}^2)).$$

We now show that on the subset $U_n^d \subset \mathfrak{g}_{\leq n}((\mathbb{R}^d))$ the submanifold $\mathcal{K}$ is a cross-section, which induces a moving frame.

Lemma 4.2. *For $n = 2$ and any point $\mathbf{c}_{\leq 2} \in \mathcal{K} \cap U_2^d$, the orbit $\mathrm{O}_d(\mathbb{R}) \cdot \mathbf{c}_{\leq 2}$ and $\mathcal{K}$ intersect transversally.*

Proof. First, we recall that $\mathrm{O}_d(\mathbb{R}) \cdot \mathbf{c}_{\leq 2}$ and $\mathcal{K}$ intersect transversally if and only if, at every point q in the intersection, the tangent spaces $T_q(\mathrm{O}_d(\mathbb{R}) \cdot \mathbf{c}_{\leq 2})$ and $T_q\mathcal{K}$ generate the whole ambient space $\mathfrak{g}_{\leq 2}((\mathbb{R}^d))$.

Now, at a point $q = A \cdot \mathbf{c}_{\leq 2} = (Av, AMA^\top)$ in the orbit, the tangent space has the form

$$T_q\Big(\mathrm{O}_d(\mathbb{R}) \cdot \mathbf{c}_{\leq 2}\Big) = \{(HAv, [H, AMA^\top]) : H \in \mathfrak{so}(d, \mathbb{R})\}, \tag{18}$$

and the tangent space to the cross section is

$$T_q\mathcal{K} = \{c_{\mathtt{i}} = 0, c_{\mathtt{j(i+1)}} = 0 : 1 \leq i \leq d-1, 1 \leq j < i\}.$$

We note that

$$\dim T_q\mathcal{K} = d, \quad \dim T_q\Big(\mathrm{O}_d(\mathbb{R}) \cdot \mathbf{c}_{\leq 2}\Big) = \frac{d(d-1)}{2},$$

so that $\dim T_q\mathcal{K} + \dim T_q\Big(\mathrm{O}_d(\mathbb{R}) \cdot \mathbf{c}_{\leq 2}\Big) = \dim \mathfrak{g}_{\leq 2}((\mathbb{R}^d))$. Therefore, we only need to show that $T_q\mathcal{K} \cap T_q\Big(\mathrm{O}_d(\mathbb{R}) \cdot \mathbf{c}_{\leq 2}\Big) = \{0\}$ for all $q \in \mathcal{K} \cap \mathrm{O}_d(\mathbb{R}) \cdot \mathbf{c}_{\leq 2}$.

Let $(\Gamma_{i,j} : 1 \leq i < j \leq d)$ be the standard basis of $\mathfrak{so}(d, \mathbb{R})$, that is, $(\Gamma_{i,j})_{k,l} = \delta_{i,k}\delta_{j,l} - \delta_{j,k}\delta_{i,l}$. It is not hard to show that the commutation relations

$$[\Gamma_{i,j}, \Gamma_{k,(k+1)}] = \Gamma_{(k+1),j}\delta_{i,k} + \Gamma_{i,(k+1)}\delta_{j,k} - \Gamma_{k,j}\delta_{i,(k+1)} - \Gamma_{i,k}\delta_{j,(k+1)} \tag{19}$$

hold for all $1 \leq k < d$ and $1 \leq i < j \leq d$. By eq. (18), a generic element $p \in T_q\Big(\mathrm{O}_d(\mathbb{R}) \cdot \mathbf{c}_{\leq 2}\Big)$ has the form $p = (HAv, [H, AMA^\top])$ with

$$H = \sum_{1 \leq i < j \leq d} h_{i,j}\Gamma_{i,j} \in \mathfrak{so}(d, \mathbb{R}).$$

But since $q = (Av, AMA^\top) \in \mathcal{K}$,

$$Av = \alpha e_d, \quad AMA^\top = \sum_{k=1}^{d-1} \beta_k \Gamma_{k,k+1}$$

with $\alpha > 0$, and $\beta_k > 0$ for all $k \in \{1, \ldots, d-1\}$. If p also belongs to $T_q\mathcal{K}$, then we have in particular that

$$HAv = \sum_{i=1}^{d-1} h_{i,d} e_i = \alpha' e_d,$$

for some $\alpha' \in \mathbb{R}$, thus $h_{i,d} = 0$ for all $i \in \{1, \ldots, d-1\}$. Now we show that $h_{i,j} = 0$ for all $1 \leq i < j \leq d-1$ by induction on $r := d - 1 - j$. By eq. (19), we see that

$$[H, AMA^\top] = \sum_{1 \leq i < j \leq d-1} \sum_{k=1}^{d-1} h_{i,j}\beta_k(\Gamma_{(k+1),j}\delta_{i,k} + \Gamma_{i,(k+1)}\delta_{j,k} - \Gamma_{k,j}\delta_{i,(k+1)} - \Gamma_{i,k}\delta_{j,(k+1)}),$$

so that

$$[H, AMA^\top]_{i,d-1} = h_{i,d-1}\beta_{d-1} = 0.$$

for $i \in \{1, \ldots, d-2\}$. Therefore, $h_{i,d-1} = 0$ for all $i \in \{1, \ldots, d-2\}$, and the claim is proven when $r = 0$. Suppose it is true for all $r' < r$. Then

$$[H, AMA^\top]_{i,d-1-r} = h_{i,d-1-r}\beta_{d-1-r} = 0$$

for $i \in \{1, \ldots, d-2-r\}$, hence $h_{i,d-1-r} = 0$ for all $i \in \{1, \ldots, d-2-r\}$. Finally, we have $H = 0$ thus $p = (HAv, [H, AMA^\top]) = 0$.

We have shown that if $q \in \mathrm{O}_d(\mathbb{R}) \cdot \mathbf{c}_{\le 2} \cap \mathcal{K}$ then $\dim T_q\Big(\mathrm{O}_d(\mathbb{R}) \cdot \mathbf{c}_{\le 2}\Big) + \dim T_q\mathcal{K} = \dim \mathfrak{g}_{\le 2}((\mathbb{R}^d))$ and $T_q\Big(\mathrm{O}_d(\mathbb{R}) \cdot \mathbf{c}_{\le 2}\Big) \cap T_q\mathcal{K}$ is trivial. It follows that if $q \in \mathrm{O}_d(\mathbb{R}) \cdot \mathbf{c}_{\le 2} \cap \mathcal{K}$, then

$$\mathfrak{g}_{\le 2}((\mathbb{R}^d)) = T_q\Big(\mathrm{O}_d(\mathbb{R}) \cdot \mathbf{c}_{\le 2}\Big) \oplus T_q\mathcal{K},$$

and in particular $\mathrm{O}_d(\mathbb{R}) \cdot \mathbf{c}_{\le 2}$ and $\mathcal{K}$ intersect transversally. □

Theorem 4.3. *The submanifold $\mathcal{K}$ in (17) is a cross-section for the action of $\mathrm{O}_d(\mathbb{R})$ on $U_n^d \subset \mathfrak{g}_{\le n}((\mathbb{R}^d))$. In particular $\mathcal{K}$ induces a moving frame map.*

Proof. We first claim that $\mathcal{K}$ intersects each orbit in U_n^d at a unique point. Denote the linear span of $\mathcal{K}$ as

$$K := \left\{c_{\mathtt{i}} = 0, c_{\mathtt{j(i+1)}} = 0 \mid 1 \le i \le d-1, 1 \le j < i\right\} \subset \mathfrak{g}_{\le n}((\mathbb{R}^d)).$$

Note that the action on $\mathrm{proj}_{\le 2}\, \mathfrak{g}_{\le n}((\mathbb{R}^d)) = \mathfrak{g}_{\le 2}((\mathbb{R}^d))$ is isomorphic to the action on $\mathbb{R}^d \oplus \mathfrak{so}(d,\mathbb{R})$ given in (7). Thus for any $\mathbf{c}_{\le n} \in U_n^d$, by Proposition 3.13 and the diagonality of the action (see Section 2.3), there exists an element of $g \in \mathrm{O}_d(\mathbb{R})$ such that $g \cdot \mathbf{c}_{\le n} = \tilde{\mathbf{c}}_{\le n} \in K$.

Consider the subgroup $W_{\mathbb{R}} \subset \mathrm{O}_d(\mathbb{R})$ of diagonal matrices w with diagonal entries $w_{jj} \in \{-1,1\}$, $1 \le j \le d$. By Proposition 3.6 any element of $W_{\mathbb{R}}$ sends a point in K to K. For any $\tilde{\mathbf{c}}_{\le n} \in K$, the action of $W_{\mathbb{R}}$ on the coordinates $\mathrm{proj}_{\le 2}(\mathbf{c}_{\le n}) = \mathbf{c}_{\le 2}$ is given by the following (see (14)):

$$c_{\mathtt{d}} \mapsto w_{dd} c_{\mathtt{d}}, \quad c_{\mathtt{i(i+1)}} \mapsto w_{ii} w_{(i+1)(i+1)} c_{\mathtt{i(i+1)}}.$$

The element $w \in W_{\mathbb{R}}$ such that $w_{jj} = -1$ for $1 \le j \le d$ changes only the sign on $c_{\mathtt{d}}$. The element $w \in W_{\mathbb{R}}$ where $w_{jj} = -1$ for $1 \le j \le i$ and $w_{jj} = 1$ for $i < j \le d$ changes only the sign of $c_{\mathtt{i(i+1)}}$. Thus there exists $g \in W_{\mathbb{R}}$ such that $g \cdot \tilde{\mathbf{c}}_{\le n} \in \mathcal{K}$, implying $\mathcal{K}$ intersects each orbit in U_n^d.

Now suppose that for some $\mathbf{c}_{\le n} \in \mathcal{K}$, $g \in \mathrm{O}_d(\mathbb{R})$ we have $g \cdot \mathbf{c}_{\le n} \in \mathcal{K}$. We show that this implies $g = \mathrm{id}$. Since the action of $\mathrm{O}_d(\mathbb{R})$ on $T_1(\mathbb{R}^d)$ is isomorphic to the canonical action on $\mathbb{R}^d$, $g \in \mathrm{O}_d^{d-1}(\mathbb{R})$ (recall the notation after (10)). By Proposition 3.5, the action of $\mathrm{O}_d^{d-1}(\mathbb{R})$ on the coordinates $c_{\mathtt{1d}}, c_{\mathtt{2,d}}, \dots, c_{\mathtt{(d-1)d}}$ of $\mathbf{c}_{\le n}$ is isomorphic to the canonical action on $\mathbb{R}^{d-1}$. Thus we deduce that g must be in $\mathrm{O}_d^{d-2}(\mathbb{R})$. Iterating, we obtain that g must be the identity, as claimed, implying that $\mathcal{K}$ intersects each orbit in U_n^d exactly once.

We now show that the intersection with each orbit is transverse. By Corollary 3.14 the action is free on U_2^d, and thus on U_n^d. Since the action is free on U_n^d, each orbit $\mathrm{O}_d(\mathbb{R}) \cdot \mathbf{c}_{\le n}$ is smooth and of dimension $n(n-1)/2$ (see Proposition 2.16). Let $\mathbf{c}_{\le n}$ be a point in $\mathcal{K}$. Since $\mathcal{K}$ is on open subset of the linear space K, we have $T_{\mathbf{c}_{\le n}}\mathcal{K} = K$. Since $\mathcal{K}$ and $\mathrm{O}_d(\mathbb{R}) \cdot \mathbf{c}_{\le n}$ are of complementary dimension, $\mathcal{K}$ intersects $\mathrm{O}_d(\mathbb{R}) \cdot \mathbf{c}_{\le n}$ transversally if and only if the span of their tangent spaces is equal to the dimension of U_n^d.

Since $\mathrm{O}_d(\mathbb{R})$ acts diagonally we have that

$$\begin{aligned}\mathrm{proj}_{\le 2}(T_{\mathbf{c}_{\le n}}\mathcal{K} + T_{\mathbf{c}_{\le n}}(\mathrm{O}_d(\mathbb{R}) \cdot p)) &= \mathrm{proj}_{\le 2}(T_{\mathbf{c}_{\le n}}\mathcal{K}) + \mathrm{proj}_{\le 2}(T_{\mathbf{c}_{\le n}}(\mathrm{O}_d(\mathbb{R}) \cdot \mathbf{c}_{\le n})) \\ &= T_{\mathrm{proj}_{\le 2}(\mathbf{c}_{\le n})}\, \mathrm{proj}_{\le 2}(\mathcal{K}) + T_{\mathrm{proj}_{\le 2}(\mathbf{c}_{\le n})}\left(\mathrm{O}_d(\mathbb{R}) \cdot \mathrm{proj}_{\le 2}(\mathbf{c}_{\le n})\right),\end{aligned}$$

where $V + W$ denotes the span of two subspaces V, W. Then by Lemma 4.2

$$\mathrm{proj}_{\le 2}(T_{\mathbf{c}_{\le n}}\mathcal{K} + T_{\mathbf{c}_{\le n}}(\mathrm{O}_d(\mathbb{R}) \cdot \mathbf{c}_{\le n})) = \mathfrak{g}_{\le 2}((\mathbb{R}^d)).$$

Since for any vector $v \in T_{\mathrm{proj}_{\le 2}(\mathbf{c}_{\le n})}\, \mathrm{proj}_{\le 2}(\mathcal{K})$, $\langle v \rangle \oplus \mathfrak{g}_{\le \ge 3}((\mathbb{R}^d))$ is a subspace of $T_{\mathbf{c}_{\le n}}\mathcal{K}$, we have that $T_{\mathbf{c}_{\le n}}\mathcal{K} + T_{\mathbf{c}_{\le n}}(\mathrm{O}_d(\mathbb{R}) \cdot \mathbf{c}_{\le n}) = \mathfrak{g}_{\le n}((\mathbb{R}^d))$. Thus $\mathcal{K}$ and $\mathrm{O}_d(\mathbb{R}) \cdot p$ intersect transversally.

Therefore $\mathcal{K}$ intersects transversally each orbit of U_n^d at a unique point, and hence by definition is a cross-section for this action. The free and algebraic action of $\mathrm{O}_d(\mathbb{R})$ on U_n^d satisfies the hypothesis of Theorem 2.11 (see Remark 2.15), and hence there exists a moving frame map $\rho : U^d_n \to \mathrm{O}_d(\mathbb{R})$ taking each element of U^d_n to the unique intersection point of its orbit and $\mathcal{K}$. □

Remark 4.4. By a similar argument as above, together with Remark 3.12, one can construct a cross-section for the action of $\mathrm{SO}_d(\mathbb{R})$ from $\mathcal{K}$. For certain dimensions d, one may have to adjust the restriction that $c_{12} > 0$.

The proof of Proposition 3.7 provides a road-map for explicitly finding the element of $\mathrm{O}_d(\mathbb{R})$ taking any point $\mathbf{c}_{\leq n} \in U^d_n$ to $\mathcal{K}$, and hence $\rho(\mathbf{c}_{\leq n}) \cdot \mathbf{c}_{\leq n}$. By successively applying rotations, one can bring $\mathbf{c}_{\leq n}$ to the cross-section $\mathcal{K}$. For an example of doing this in practice see Example 5.2.

An important consequence of Theorem 4.3 is the following corollary.

Corollary 4.5. *Two elements $\mathbf{c}_{\leq n}, \tilde{\mathbf{c}}_{\leq n} \in U^d_n$ lie in the same orbit if and only if they take the same value on the cross-section $\mathcal{K}$, i.e. if and only if $\rho(\mathbf{c}_{\leq n}) \cdot \mathbf{c}_{\leq n} = \rho(\tilde{\mathbf{c}}_{\leq} n) \cdot \tilde{\mathbf{c}}_{\leq n}$.*

Thus to find a unique representative of the orbit of $\mathbf{c}_{\leq n} \in U^n_d$ we can "invariantize" $\mathbf{c}_{\leq n}$ by computing $\rho(\mathbf{c}_{\leq n}) \cdot \mathbf{c}_{\leq n}$, and the smooth functions defining the non-zero coordinates of $\mathcal{K} \cap \mathrm{O}_d(\mathbb{R}) \cdot \mathbf{c}_{\leq n}$ are invariant functions which characterize the orbit. Note that the cross-section $\mathcal{K}$ and the moving frame only depend on the $\mathfrak{g}_{\leq 2}((\mathbb{R}^d))$ coordinates. In particular we have that for any path X such that $\mathbf{c}_{\leq n}(X) = \mathrm{proj}_{\leq n}(\log(\mathrm{IIS}(X))) \in U^d_n$

$$\rho(\mathbf{c}_{\leq n}(X)) = \rho(\mathrm{proj}_{\leq 2}(\mathbf{c}_{\leq n}(X))) := \rho(\mathbf{c}_{\leq 2}(X))$$

which implies that the "invariantization" of a path $Y := \rho(\mathbf{c}_{\leq 2}(X)) \cdot X$ is well-defined. This is due to the diagonal nature of the action of $\mathrm{O}_d(\mathbb{R})$ on $\mathfrak{g}_{\leq n}((\mathbb{R}^d))$, and the fact that $\dim(\mathrm{O}_d(\mathbb{R})) < \dim(\mathfrak{g}_{\leq 2}((\mathbb{R}^d)))$. Since the action of the coordinates on $\mathfrak{g}_{\leq 2}((\mathbb{R}^d))$ is not affected by the higher level coordinates, we can define a cross-section on $\mathfrak{g}_{\leq 2}((\mathbb{R}^d))$ that extends naturally to $\mathfrak{g}_{\leq n}((\mathbb{R}^d))$. For higher-dimensional groups one may have to consider a cross-section on $\mathfrak{g}_{\leq 3}((\mathbb{R}^d))$ or higher.

As a consequence, the infinite log signature (and thus the iterated integral signature) of a path X under the action of $\mathrm{O}_d(\mathbb{R})$ is characterized by its value on the cross-section.

Theorem 4.6. *For any two paths $X, \tilde{X}$ in $\mathbb{R}^d$ such that $\mathbf{c}_{\leq 2}(X) := \mathrm{proj}_{\leq 2}(\log(\mathrm{IIS}(X))), \mathbf{c}_{\leq 2}(\tilde{X}) := \mathrm{proj}_{\leq 2}(\log(\mathrm{IIS}(\tilde{X})))$ are elements of U^d_2, define*

$$Y := \rho\left(\mathbf{c}_{\leq 2}(X)\right) X, \qquad \tilde{Y} := \rho\left(\mathbf{c}_{\leq 2}(\tilde{X})\right) \tilde{X}.$$

Then $\mathrm{IIS}(Y) = \mathrm{IIS}(\tilde{Y})$ if and only if there exists $g \in \mathrm{O}_d(\mathbb{R})$ such that $\mathrm{IIS}(g \cdot X) = \mathrm{IIS}(\tilde{X})$.

5. Invariants of planar and spatial curves

5.1. **Planar curves.** In Section 4.1 we detailed a moving frame construction for $\mathfrak{g}_{\leq n}((\mathbb{R}^2))$ under $\mathrm{O}_2(\mathbb{R})$ for any truncation order n. In particular on the subset

$$U^2_n = \left\{\mathbf{c}_{\leq n} \in \mathfrak{g}_{\leq n}((\mathbb{R}^2)) \mid (c_1, c_2) \neq (0,0), c_{12} \neq 0\right\},$$

the map $\rho : U^2_n \to \mathrm{O}_2(\mathbb{R})$ defined by

$$\rho(\mathbf{c}_{\leq n}) = \frac{1}{\sqrt{c_1^2 + c_2^2}} \begin{pmatrix} \mathrm{sgn}(c_{12})c_2 & -\mathrm{sgn}(c_{12})c_1 \\ c_1 & c_2 \end{pmatrix}$$

for $\mathbf{c}_{\leq n} \in \mathfrak{g}_{\leq n}((\mathbb{R}^2))$ is a moving frame map bring any element of $\mathfrak{g}_{\leq n}((\mathbb{R}^2))$ to the intersection of its orbit with the cross-section

$$\mathcal{K} = \left\{\mathbf{c}_{\leq n} \in \mathfrak{g}_{\leq n}((\mathbb{R}^2)) \mid c_1 = 0, c_2, c_{12} > 0\right\}.$$

Any path X in $\mathbb{R}^2$ defines an element $\mathbf{c}_{\le n}(X) = \mathrm{proj}_{\le n}(\log(\mathrm{IIS}(X))) \in \mathfrak{g}_{\le n}((\mathbb{R}^2))$. Since $\rho(\mathbf{c}_{\le n}) = \rho(\mathbf{c}_{\le 2})$, we can define the invariantization of X with respect to $\mathrm{O}_2(\mathbb{R})$ as $Y := \rho(\mathbf{c}_{\le 2}(X)) \cdot X$. The coordinates of $\log(\mathrm{IIS}(Y))$ as functions of the coordinates of $\log(\mathrm{IIS}(X))$ are invariant functions for paths under $\mathrm{O}_2(\mathbb{R})$.

A basis for $\mathfrak{g}_{\le 4}((\mathbb{R}^2))$ is given by the coordinates (see Example 2.1)

$$\mathbf{c}_4 = (c_1, c_2, c_{12}, c_{112}, c_{122}, c_{1112}, c_{1122}, c_{1222}).$$

As detailed before in Section 4.1, we have that

$$c_1(Y) = 0, \quad c_2(Y) = \sqrt{c_1(X)^2 + c_2(X)^2}, \quad c_{12}(Y) = |c_{12}(X)|.$$

Using the action as defined in Section 2.3, one can compute

$$\begin{aligned}
c_{112}(Y) &= \frac{c_1(X)c_{122}(X) + c_{112}(X)c_2(X)}{\sqrt{c_1(X)^2 + c_2(X)^2}} \\
c_{122}(Y) &= \mathrm{sgn}(c_{12}) \left(\frac{-c_1(X)c_{112}(X) + c_{122}(X)c_2(X)}{\sqrt{c_1(X)^2 + c_2(X)^2}} \right) \\
c_{1112}(Y) &= \mathrm{sgn}(c_{12}) \left(\frac{c_1(X)^2 c_{1222}(X) + c_1(X)c_2(X)c_{1122}(X) + c_2(X)^2 c_{1112}(X)}{c_1(X)^2 + c_2(X)^2} \right) \\
c_{1122}(Y) &= \frac{-c_1(X)^2 c_{1122}(X) + 2c_1(X)c_2(X)(c_{1222}(X) - c_{1112}(X)) + c_2(X)^2 c_{1122}(X)}{c_1(X)^2 + c_2(X)^2} \\
c_{1222}(Y) &= \mathrm{sgn}(c_{12}) \left(\frac{c_1(X)^2 c_{1112}(X) - c_1(X)c_2(X)c_{1122}(X) + c_2(X)^2 c_{1222}(X)}{c_1(X)^2 + c_2(X)^2} \right).
\end{aligned}$$

As before, for any two paths X and $\tilde{X}$ starting at the origin, we have that $\mathbf{c}_4(X)$ is related to $\mathbf{c}_4(\tilde{X})$ under $\mathrm{O}_2(\mathbb{R})$ if and only if $\mathbf{c}_4(Y) = \mathbf{c}_4(\tilde{Y})$. By inspection, we see that a simpler set of *polynomial* invariants also determine the equivalence class of the image of a path X in $\mathfrak{g}_{\le 4}((\mathbb{R}^2))$.

$$\begin{aligned}
p_1(X) &= c_1(X)^2 + c_2(X)^2 \\
p_2(X) &= c_{12}(X)^2 \\
p_3(X) &= c_1(X)c_{122}(X) + c_{112}(X)c_2(X) \\
p_4(X) &= c_{12}(X)\left(-c_1(X)c_{112}(X) + c_{122}(X)c_2(X)\right) \\
p_5(X) &= c_{12}(X)\left(c_1(X)^2 c_{1222}(X) + c_1(X)c_2(X)c_{1122}(X) + c_2(X)^2 c_{1112}(X)\right) \\
p_6(X) &= -c_1(X)^2 c_{1122}(X) + 2c_1(X)c_2(X)(c_{1222}(X) - c_{1112}(X)) + c_2(X)^2 c_{1122} \\
p_7(X) &= c_{12}(X)\left(c_1(X)^2 c_{1112}(X) - c_1(X)c_2(X)c_{1122}(X) + c_2(X)^2 c_{1222}(X)\right)
\end{aligned}$$

The value of X on the above invariant set determines the value of $\mathbf{c}_4(Y)$. Thus they provide a simpler invariant representation for $\mathbf{c}_4(X) = \mathrm{proj}_{\le 4}(\log(\mathrm{IIS}(X)))$.

Remark 5.1. It is an interesting fact that by adding the invariants $c_{1112}(Y)$ and $c_{1222}(Y)$, we get the much simpler invariant

$$c_{1112}(Y) + c_{1222}(Y) = \mathrm{sgn}(c_{12})(c_{1112}(X) + c_{1222}(X)).$$

In the polynomial invariant set, one can likewise replace either p_4 or p_7 by

$$p_4'(X) = c_{12}(X)(c_{1112}(X) + c_{1222}(X)).$$

5.2. **Spatial curves.** We can define a moving frame similarly for $\mathfrak{g}_{\leq n}((\mathbb{R}^3))$. Theorem 4.3 indicates that the subset of $\mathfrak{g}_{\leq n}((\mathbb{R}^3))$ defined by

$$\mathcal{K} = \{c_1 = c_2 = c_{12} = 0, c_3, c_{13}, c_{23} > 0\}$$

is a cross-section for the action of $\mathrm{O}_3(\mathbb{R})$ on a Zariski-open subset of $\mathfrak{g}_{\leq n}((\mathbb{R}^3))$. Define the polynomials in basis elements of $\mathfrak{g}_{\leq 2}((\mathbb{R}^3))$,

$$\begin{aligned}
p_1(\mathbf{c}_{\leq n}) &= c_1^2 + c_2^2 + c_3^2\\
p_2(\mathbf{c}_{\leq n}) &= c_1^2(c_{12}^2 + c_{13}^2) + 2c_1c_{23}(c_{13}c_2 - c_{12}c_3) + c_2^2(c_{12}^2 + c_{23}^2) + 2c_{12}c_{13}c_2c_3 + c_3^2(c_{13}^2 + c_{23}^2)\\
p_3(\mathbf{c}_{\leq n}) &= c_1c_{23} - c_2c_{13} + c_3c_{12}.
\end{aligned}$$

Then one can check that the group element $A \in \mathrm{O}_3(\mathbb{R})$ defined by

$$A(\mathbf{c}_{\leq n}) = B(\mathbf{c}_{\leq n})C(\mathbf{c}_{\leq n}) \tag{20}$$

where

$$B(\mathbf{c}_{\leq n}) = \begin{pmatrix} \operatorname{sgn}(p_2(\mathbf{c}_{\leq n})p_3(\mathbf{c}_{\leq n})) & 0 & 0\\ 0 & \operatorname{sgn}(p_2(\mathbf{c}_{\leq n})) & 0\\ 0 & 0 & 1 \end{pmatrix}$$

and

$$C(\mathbf{c}_{\leq n}) = \begin{pmatrix} \frac{c_1(-c_{13}c_2+c_{12}c_3)-c_{23}(c_2^2+c_3^2)}{\sqrt{p_1(\mathbf{c}_{\leq n})|p_2(\mathbf{c}_{\leq n})|}} & \frac{c_1^2c_{13}+c_1c_2c_{23}+c_3(c_{12}c_2+c_{13}c_3)}{\sqrt{p_1(\mathbf{c}_{\leq n})|p_2(\mathbf{c}_{\leq n})|}} & -\frac{c_1^2c_{12}-c_1c_{23}c_3+c_2(c_{12}c_2+c_{13}c_3)}{\sqrt{p_1(\mathbf{c}_{\leq n})|p_2(\mathbf{c}_{\leq n})|}}\\ \frac{c_{12}c_2+c_{13}c_3}{\sqrt{|p_2(\mathbf{c}_{\leq n})|}} & \frac{-c_1c_{12}+c_{23}c_3}{\sqrt{|p_2(\mathbf{c}_{\leq n})|}} & \frac{-c_1c_{13}-c_2c_{23}}{|\sqrt{p_2(\mathbf{c}_{\leq n})}|}\\ \frac{c_1}{\sqrt{p_1(\mathbf{c}_{\leq n})}} & \frac{c_2}{\sqrt{p_1(\mathbf{c}_{\leq n})}} & \frac{c_3}{\sqrt{p_1(\mathbf{c}_{\leq n})}} \end{pmatrix}$$

brings any element $\mathbf{c}_{\leq n} \in \mathfrak{g}_{\leq n}((\mathbb{R}^3))$ such that $p_1(\mathbf{c}_{\leq n}), p_2(\mathbf{c}_{\leq n}) \neq 0$ to $\mathcal{K}$. In particular the moving frame map $\rho : U_n^3 \to \mathrm{O}_3(\mathbb{R})$ is defined on the Zariski-open set $U_n^3 = \{p_1(\mathbf{c}_{\leq n}), p_2(\mathbf{c}_{\leq n}) \neq 0\} \subset \mathfrak{g}_{\leq n}((\mathbb{R}^3))$.

Then for any path $X \in \mathbb{R}^3$ and $Y := \rho(\mathbf{c}_{\leq 2}(X)) \cdot X$, the non-zero coordinates of $\mathbf{c}_{\leq 2}(Y)$ are invariant functions given by[7]

$$\begin{aligned}
c_3(Y) &= \sqrt{p_1(\mathbf{c}_{\leq 2}(X))},\\
c_{12}(Y) &= \frac{|p_3(\mathbf{c}_{\leq n}(X))|}{\sqrt{p_1(\mathbf{c}_{\leq 2}(X))}},\\
c_{23}(Y) &= \sqrt{\frac{|p_2(\mathbf{c}_{\leq n}(X))|}{p_1(\mathbf{c}_{\leq 2}(X))}}.
\end{aligned}$$

From this we can conclude that the polynomial invariants $p_1(\mathbf{c}_{\leq n}(X)), p_2(\mathbf{c}_{\leq n}(X))^2$, and $p_3(\mathbf{c}_{\leq n}(X))^2$ characterize the equivalence class of $\mathbf{c}_{\leq 2}(X)$ under $\mathrm{O}_3(\mathbb{R})$.

Example 5.2. Continuing with our running example, the moment curve, we have already seen (Example 2.3) that

$$\operatorname{proj}_{\leq 2}\log \operatorname{IIS}(X) = \left(\begin{pmatrix}1\\1\\1\end{pmatrix}, \begin{pmatrix} 0 & \frac{1}{6} & \frac{1}{4}\\ -\frac{1}{6} & 0 & \frac{1}{10}\\ -\frac{1}{4} & -\frac{1}{10} & 0 \end{pmatrix}\right)$$

[7] We note that $p_3(\mathbf{c}_{\leq n}(X))$ is the "signed volume" of the curve, compare [12, Lemma 3.17].

The matrix

$$A = \begin{pmatrix} \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} & -\sqrt{\frac{2}{3}} \\ -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} \end{pmatrix}$$

is such that

$$A \cdot \mathrm{proj}_{\leq 2} \log \mathrm{IIS}(X) = \left(\begin{pmatrix} 0 \\ 0 \\ \sqrt{3} \end{pmatrix}, \begin{pmatrix} 0 & \frac{1}{60\sqrt{3}} & \frac{7}{20\sqrt{2}} \\ -\frac{1}{60\sqrt{3}} & 0 & -\frac{29}{60\sqrt{6}} \\ -\frac{7}{20\sqrt{2}} & \frac{29}{60\sqrt{6}} & 0 \end{pmatrix} \right).$$

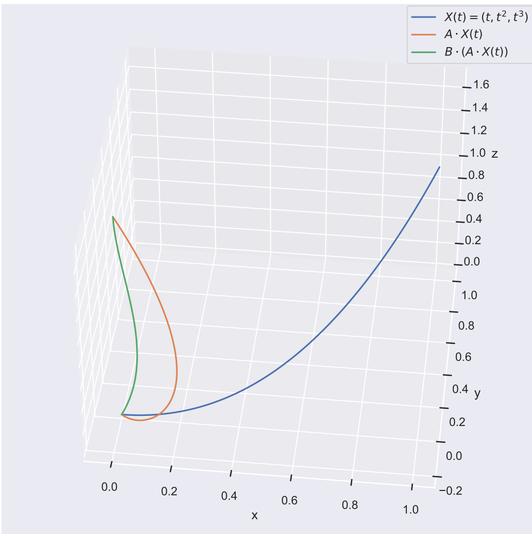
Finally, the matrix

$$B = \begin{pmatrix} -\frac{29}{2\sqrt{541}} & -\frac{21\sqrt{3}}{2\sqrt{541}} & 0 \\ \frac{21\sqrt{3}}{2\sqrt{541}} & -\frac{29}{2\sqrt{541}} & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

is such that

$$B \cdot (A \cdot \mathrm{proj}_{\leq 2} \log \mathrm{IIS}(X)) = \left(\begin{pmatrix} 0 \\ 0 \\ \sqrt{3} \end{pmatrix}, \begin{pmatrix} 0 & \frac{1}{60\sqrt{3}} & 0 \\ -\frac{1}{60\sqrt{3}} & 0 & \frac{\sqrt{541}}{30\sqrt{6}} \\ 0 & -\frac{\sqrt{541}}{60\sqrt{6}} & 0 \end{pmatrix} \right) \in \mathcal{K}.$$

The figure below shows the effects of these transformations on the path itself.

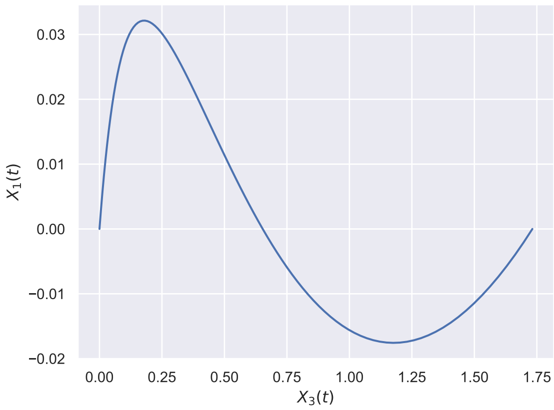


In this sense, this two step process is similar to the iterative process outlined in the proof of Proposition 3.7 of bringing an element of $\mathfrak{g}_{\leq 2}((\mathbb{R}^d))$ to successively smaller linear spaces. The transformation A brings $\mathbf{c}_{\leq 2}(X)$ to L_1, then finally to L_2 by a transformation B. In principle, given a procedure to rotate an element of $\mathbb{R}^d$ to a particular axis, this iterative process is quite easy to perform to bring any $\mathbf{c}_{\leq 2}(X)$ for any path X to $\mathcal{K}$, and hence invariantize any path.

Alternatively one can directly use the moving frame map in (20); note that this is equivalent to the single action by the matrix

$$\rho(\mathbf{c}_2(X)) = BA = \begin{pmatrix} \frac{17}{\sqrt{3246}} & -23\sqrt{\frac{2}{1623}} & \frac{29}{\sqrt{3246}} \\ \frac{25}{\sqrt{1082}} & -2\sqrt{\frac{2}{541}} & -\frac{21}{\sqrt{1082}} \\ \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} \end{pmatrix}.$$

The next figure shows the projection of $\rho(\mathbf{c}_2(X)) \cdot X$ onto the (x, z) plane. One can check that the total area under the curve vanishes.



6. Discussion and open problems

We conclude with a discussion of some interesting questions arising from this work. We presented a method to construct $\mathrm{O}_d(\mathbb{R})$ invariants for a path X from the coordinates of the log signature (or iterated integral signature) in a way that completely characterizes the orbit of $\mathrm{proj}_n(\log(\mathrm{IIS}(X))$ (or $\mathrm{proj}_n(\mathrm{IIS}(X)))$ under $\mathrm{O}_d(\mathbb{R})$. This procedure also furnishes a quick method to compare equivalence classes of paths under $\mathrm{O}_d(\mathbb{R})$ without computing the full set of invariants (see Example 5.2).

In particular Theorem 4.6 is similar in spirit to [12, Conjecture 7.2], where the authors characterize all *linear* $\mathrm{SO}_d(\mathbb{R})$-invariants in the coordinates of $\mathrm{IIS}(X)$ and ask if these determine a path up to $\mathrm{SO}_d(\mathbb{R})$ and tree-like extensions. The invariant sets we construct are smooth functions in the coordinates of $\log(\mathrm{IIS}(X))$, though in many cases we can, by inspection, find an equivalently generating polynomial set (see Section 5). Polynomials in coordinates of $\log(\mathrm{IIS}(X))$ correspond to polynomial invariants in the coordinates of $\mathrm{IIS}(X)$, which yield linear $\mathrm{O}_d(\mathbb{R})$-invariants by the shuffle relations. Thus the conjecture remains open, and more broadly the connection between the two sets of invariants should be explored.

In Section 3, we investigate sets of separating sets of rational and polynomial invariants for the action of $\mathrm{O}_d(\mathbb{R})$ on $\mathfrak{g}_{\leq 2}((\mathbb{R}^d))$. An open question is whether the polynomial invariants we construct, generate the *ring* of polynomial invariants for this action. In even more generality questions remain about the relationship between the polynomial invariants we construct and the ring of polynomial invariants for the action of $\mathrm{O}_d(\mathbb{R})$ on $\mathfrak{g}_{\leq n}((\mathbb{R}^d))$.

Additionally we only consider $\mathrm{O}_d(\mathbb{R})$-invariants (and to a lesser extend $\mathrm{SO}_d(\mathbb{R})$) in this work. The dimension of $\mathrm{O}_d(\mathbb{R})$ implies that to construct a cross-section for the action, one only has to consider the action on $\mathfrak{g}_{\leq 2}((\mathbb{R}^d))$. For larger groups like $\mathrm{GL}_d(\mathbb{R})$ one may have to construct a cross-section using coordinates on $\mathfrak{g}_{\leq 3}((\mathbb{R}^d))$.

The cross section $\mathcal{K}$ in Section 4.2 can also be used as a starting point for groups containing $\mathrm{O}_d(\mathbb{R})$, since any element of $\mathfrak{g}_{\leq 2}((\mathbb{R}^d))$ can be brought to $\mathcal{K}$ by an element of $\mathrm{O}_d(\mathbb{R})$. For instance if one considers scaling transformations in addition to orthogonal transformations, changing the conditions of $c_{\mathtt{d}}, c_{\mathtt{i(i+1)}} > 0$ on $\mathcal{K}$ to $c_{\mathtt{d}} = c_{\mathtt{i(i+1)}} = 0$, for $1 \leq i < d$, likely yields a cross-section.

As mentioned in the introduction, there are many applications of the iterated-integral signature of paths where finding $\mathrm{O}_d(\mathbb{R})$-invariant features could be advantageous. It would be interesting to see if the sets of integral invariants constructed, or "invariantization" procedure outlined can be useful for such applications.

References

[1] M. Boutin, *The pascal triangle of a discrete image: Definition, properties and application to shape analysis*, Symmetry, Integrability and Geometry: Methods and Applications (2013).

[2] E. Calabi, P. J. Olver, C. Shakiban, A. Tannenbaum, and S. Haker, *Differential and numerically invariant signatures curves applied to object recognition*, Int. J. Computer vision **26** (1998), Paper 107,135.

[3] E. Cartan, *La méthode du repère mobile, la théorie des groupes continus, et les espaces généralisés*, Exposés de Géométrie, vol. 5, Hermann, Paris, 1935.

[4] E. Cartan, *La théorie des groupes finis et continus et la géométrie différentielle, traitées par la méthode du repere mobile. leçons professées à la sorbonne.*, tgfc (1951).

[5] E. Celledoni, P. I. E. Lystad, and N. Tapia, *Signatures in shape analysis: an efficient approach to motion identification*, Geometric science of information, Lecture Notes in Comput. Sci., vol. 11712, Springer, Cham, 2019, pp. 21–30.

[6] K.-T. Chen, *Iterated integrals and exponential homomorphisms*, Proceedings of the London Mathematical Society **s3-4** (1954), no. 1, 502–512.

[7] ______, *Iterated integrals and exponential homomorphisms*, Proc. London Math. Soc. **s3-4** (1954), no. 1, 502–512.

[8] ______, *Integration of paths—a faithful representation of paths by non-commutative formal power series*, Trans. Amer. Math. Soc. **89** (1958), 395–407.

[9] I. Chevyrev and A. Kormilitzin, *A primer on the signature method in machine learning*, 2016, `arXiv:1603.03788 [stat.ML]`.

[10] L. Colmenarejo and R. Preiß, *Signatures of paths transformed by polynomial maps*, Beitr. Algebra Geom. **61** (2020), no. 4, 695–717.

[11] H. Derksen and G. Kemper, *Computational invariant theory*, Springer, 2015.

[12] J. Diehl and J. Reizenstein, *Invariants of Multidimensional Time Series Based on Their Iterated-Integral Signature*, Acta Appl. Math. **164** (2019), 83–122.

[13] M. Fels and P. J. Olver, *Moving coframes: I. a practical algorithm*, Acta Applicandae Mathematica **51** (1998), no. 2, 161–213.

[14] M. Fels and P. J. Olver, *Moving Coframes. II. Regularization and Theoretical Foundations*, Acta Appl. Math. **55** (1999), 127–208.

[15] S. Feng, I. Kogan, and H. Krim, *Classification of curves in 2d and 3d via affine integral signatures*, Acta Applicandae Mathematicae **109** (2008), no. 3, 903–937.

[16] L. Foissy, F. Patras, and J.-Y. Thibon, *Deformations of shuffles and quasi-shuffles*, Ann. Inst. Fourier (Grenoble) **66** (2016), no. 1, 209–237.

[17] P. K. Friz and N. B. Victoir, *Multidimensional stochastic processes as rough paths: theory and applications*, vol. 120, Cambridge University Press, 2010.

[18] P. Görlach, E. Hubert, and T. Papadopoulo, *Rational invariants of even ternary forms under the orthogonal group*, Foundations of Computational Mathematics **19** (2018), no. 6, 1315–1361.

[19] A. Grim and C. Shakiban, *Applications of signature curves to characterize melanomas and moles*, Applications of computer algebra, Springer Proc. Math. Stat., vol. 198, Springer, Cham, 2017, pp. 171–189.

[20] J. Harris, *Algebraic geometry: a first course*, vol. 133, Springer Science & Business Media, 2013.

[21] D. Hilbert, *Ueber die theorie der algebraischen formen*, Mathematische Annalen **36** (1890), no. 4, 473–534.

[22] D. J. Hoff and P. J. Olver, *Extensions of invariant signatures for object recognition*, J. Math. Imaging Vision **45** (2013), no. 2, 176–185.

[23] ______, *Automatic solution of jigsaw puzzles*, J. Math. Imaging Vision **49** (2014), no. 1, 234–250.

[24] E. Hubert and I. A. Kogan, *Rational invariants of a group action. construction and rewriting*, Journal of Symbolic Computation **42** (2007), no. 1-2, 203–217.

[25] E. Hubert and I. A. Kogan, *Smooth and algebraic invariants of a group action: local and global constructions*, Found. Comput. Math. **7** (2007), no. 4, 455–493.

[26] S. Karlin and L. S. Shapley, *Geometry of moment spaces*, no. 12, American Mathematical Soc., 1953.

[27] I. A. Kogan, *Two algorithms for a moving frame construction*, Canadian Journal of Mathematics **55** (2003), no. 2, 266–291.

[28] I. A. Kogan, M. Ruddy, and C. Vinzant, *Differential signatures of algebraic curves*, SIAM Journal on Applied Algebra and Geometry **4** (2020), no. 1, 185–226.

[29] D. Lee and R. Ghrist, *Path signatures on lie groups*, 2020, `arXiv:2007.06633 [cs.CV]`.

[30] D. E. Littlewood, G. B. Gurevich, J. R. M. Radok, and A. J. M. Spencer, *Foundation of the theory of algebraic invariants*, The Mathematical Gazette **49** (1965), no. 369, 346.

[31] T. Lyons, *Differential equations driven by rough signals*, Revista Matemática Iberoamericana **14** (1998), 215–310.
[32] T. J. Lyons, *Differential equations driven by rough signals*, Revista Matemática Iberoamericana **14** (1998), no. 2, 215–310.
[33] J. Morales and D. Akopian, *Physical activity recognition by smartphones, a survey*, Biocybernetics and Biomedical Engineering **37** (2017), no. 3, 388–400.
[34] M. Nagata, *On the 14-th problem of hilbert*, American Journal of Mathematics **81** (1959), no. 3, 766.
[35] P. J. Olver, *Classical invariant theory*, Cambridge University Press, January 1999.
[36] ______, *Joint invariant signatures*, Foundations of Computational Mathematics **1** (2001), no. 1, 3–68.
[37] P. J. Olver, *Lectures on Moving Frames*, (2018).
[38] B. Owren and A. Marthinsen, *Integration methods based on canonical coordinates of the second kind*, Numerische Mathematik **87** (2001), no. 4, 763–790.
[39] V. L. Popov and E. B. Vinberg, *Invariant theory*, Algebraic geometry IV, Springer, 1994, pp. 123–278.
[40] R. Ree, *Lie elements and an algebra associated with shuffles*, Ann. Math. (2) **68** (1958), no. 2, 210–220 (English).
[41] B. Sturmfels, *Algorithms in invariant theory*, Springer Science & Business Media, 2008.
[42] S. L. Tuznik, P. J. Olver, and A. Tannenbaum, *Equi-affine differential invariants for invariant feature point detection*, European Journal of Applied Mathematics **31** (2019), no. 2, 277–296.
[43] Y. Zhang, K. Li, X. Chen, S. Zhang, and G. Geng, *A multi feature fusion method for reassembly of 3d cultural heritage artifacts*, Journal of Cultural Heritage **33** (2018), 191–200.