Exponential and logarithm maps for orthogonal groups

jason hanson
DigiPen Institute of Technology

June 22, 2006

Abstract

Wherein we discuss the orthogonal decomposition of skew symmetric $n \times n$ matrices. For low dimensions ($n \leq 5$), explicit closed formulae are given. As an application, we give formulae for computing the exponential of a skew symmetric matrix, and the logarithm of a rotation matrix.

1 Notation and formulae

Let $\cdot$ denote the standard Euclidian inner product on $\mathbb{R}^n$, and let $|\,|$ denote Euclidian norm; so that for any $\mathbf{u} \in \mathbb{R}^n$, we have $\mathbf{u} \cdot \mathbf{u} = |\mathbf{u}|^2$.

For $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$, define the **outer product** of $\mathbf{u}$ and $\mathbf{v}$ to be the endomorphism $\mathbf{u} \otimes \mathbf{v} : \mathbb{R}^n \to \mathbb{R}^n$ given by the rule[1]:

$$(\mathbf{u} \otimes \mathbf{v})(\mathbf{w}) \doteq (\mathbf{v} \cdot \mathbf{w})\mathbf{u},$$

for all $\mathbf{w} \in \mathbb{R}^n$. And define the **wedge (or exterior) product** of $\mathbf{u}$ and $\mathbf{v}$ to be the endomorphism

$$\mathbf{u} \wedge \mathbf{v} \doteq \mathbf{u} \otimes \mathbf{v} - \mathbf{v} \otimes \mathbf{u}.$$

For $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathbb{R}^3$, one finds that $(\mathbf{u} \wedge \mathbf{v})(\mathbf{w}) = -(\mathbf{u} \times \mathbf{v}) \times \mathbf{w}$, where $\times$ denotes the usual cross–product on $\mathbb{R}^3$. More generally, the components of

[1] The use of the symbol $\otimes$ here is a little misleading: the outer product is not the tensor product of $\mathbf{u}$ with $\mathbf{v}$, rather it is the tensor product of $\mathbf{u}$ with the *dual* of $\mathbf{v}$.

the skew–symmetric matrix $\mathbf{u} \wedge \mathbf{v}$ are the Plücker coordinates in $\mathbb{R}^{(n-1)n/2}$ of the 2–plane spanned by $\mathbf{u}$ and $\mathbf{v}$.

Theorem 1.1. *For all* $\mathbf{m}, \mathbf{n}, \mathbf{u}, \mathbf{v} \in \mathbb{R}^n$ *and* $\alpha, \beta, \gamma, \delta \in \mathbb{R}$,

i. $(\mathbf{m} \otimes \mathbf{n}) \circ (\mathbf{u} \otimes \mathbf{v}) = (\mathbf{n} \cdot \mathbf{u})\, \mathbf{m} \otimes \mathbf{v}$

ii. $\left(|\mathbf{u}|^2|\mathbf{v}|^2 - (\mathbf{u}\cdot\mathbf{v})^2\right) proj_{\mathbf{uv}} = |\mathbf{v}|^2\mathbf{u}\otimes\mathbf{u} - (\mathbf{u}\cdot\mathbf{v})(\mathbf{u}\otimes\mathbf{v}+\mathbf{v}\otimes\mathbf{u}) + |\mathbf{u}|^2\mathbf{v}\otimes\mathbf{v}$

iii. $(\mathbf{u} \wedge \mathbf{v})^2 = -\left(|\mathbf{u}|^2|\mathbf{v}|^2 - (\mathbf{u} \cdot \mathbf{v})^2\right) proj_{\mathbf{uv}}$

iv. $(\mathbf{u} \wedge \mathbf{v})^3 = -\left(|\mathbf{u}|^2|\mathbf{v}|^2 - (\mathbf{u} \cdot \mathbf{v})^2\right) \mathbf{u} \wedge \mathbf{v}$

v. $(\alpha\mathbf{u} + \beta\mathbf{v}) \wedge (\gamma\mathbf{u} + \delta\mathbf{v}) = (\alpha\delta - \beta\gamma)\mathbf{u} \wedge \mathbf{v}$,

where $proj_{\mathbf{uv}}$ *denotes the orthogonal projection map onto* $\mathbb{R}\{\mathbf{u}, \mathbf{v}\}$, *the 2–plane in* $\mathbb{R}^n$ *spanned by* $\mathbf{u}$ *and* $\mathbf{v}$.

Proof. Compute! □

In general, the Lie algebra $\mathrm{so}(n)$ of $n \times n$ skew symmetric matrices has an inner product given by

$$f \cdot g \doteq \tfrac{1}{2}\,\mathrm{trace}(f^t g),$$

for $f, g \in \mathrm{so}(n)$, where f^t is the adjoint (transpose) of f. Since this definition amounts to the Euclidian inner product on $\mathbb{R}^{(n-1)n/2}$, the inner product is positive definite. In particular, $\mathbf{u} \wedge \mathbf{v} \in \mathrm{so}(n)$, and from theorem 1.1(iii) it follows by taking traces that

$$|\mathbf{u} \wedge \mathbf{v}|^2 = (\mathbf{u} \wedge \mathbf{v}) \cdot (\mathbf{u} \wedge \mathbf{v}) = |\mathbf{u}|^2|\mathbf{v}|^2 - (\mathbf{u} \cdot \mathbf{v})^2 \tag{1}$$

(recall that the trace of an orthogonal projection onto a subspace is equal to the dimension of that subspace). Thus $|\mathbf{u} \wedge \mathbf{v}| = |\mathbf{u}|\,|\mathbf{v}| \sin\theta$, where θ is the angle between the vectors $\mathbf{u}$ and $\mathbf{v}$.

2 Decomposability and simple rotations

2.1 Two–planes and decomposability

Theorem 2.1. *The vectors* $\mathbf{u}, \mathbf{v}$ *span a 2–plane if and only if* $\mathbf{u} \wedge \mathbf{v} \neq 0$.

Proof. $\mathbf{u} \wedge \mathbf{v} = 0$ if and only if $|\mathbf{u} \wedge \mathbf{v}| = 0$; however the $|\mathbf{u} \wedge \mathbf{v}| = 0$ if and only if $|\mathbf{u}| = 0$, $|\mathbf{v}| = 0$, or the angle between $\mathbf{u}$ and $\mathbf{v}$ is a multiple of π. □

An **orientation** of the 2–plane $\mathbb{R}\{\mathbf{u}, \mathbf{v}\}$ is a choice of ordering of the vectors $\mathbf{u}, \mathbf{v}$. We write $\mathbb{R}\langle \mathbf{u}, \mathbf{v}\rangle$ to denote the 2–plane $\mathbb{R}\{\mathbf{u}, \mathbf{v}\}$ along with the orientation $\mathbf{u} < \mathbf{v}$. For any other vectors $\mathbf{a}, \mathbf{b} \in \mathbb{R}\langle \mathbf{u}, \mathbf{v}\rangle$, say $\mathbf{a} = \alpha\mathbf{u} + \beta\mathbf{v}$ and $\mathbf{b} = \gamma\mathbf{u} + \delta\mathbf{v}$, we may then write $\mathbf{a} < \mathbf{b}$ if they have the same orientation as $\mathbf{u}, \mathbf{v}$; i.e., if $\alpha\delta - \beta\gamma > 0$. From theorem 1.1(v), we have the following.

Theorem 2.2. *Suppose $\mathbb{R}\langle \mathbf{u}, \mathbf{v}\rangle$ is an oriented 2–plane, and $\mathbf{a}, \mathbf{b} \in \mathbb{R}\langle \mathbf{u}, \mathbf{v}\rangle$. Then $\mathbf{a} < \mathbf{b}$ if and only if $(\mathbf{u} \wedge \mathbf{v}) \cdot (\mathbf{a} \wedge \mathbf{b}) > 0$.*

We will say that an endomorphism $f : \mathbb{R}^n \to \mathbb{R}^n$ is **decomposable** if $f = \mathbf{u} \wedge \mathbf{v}$ for some $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$. Observe that if $f = \mathbf{u} \wedge \mathbf{v}$ is non–zero, then image of f is the 2–plane $image(f) = \mathbb{R}\{\mathbf{u}, \mathbf{v}\}$. Moreover, there is a natural orientation for this 2–plane; namely if $\mathbf{a}, \mathbf{b} \in image(f)$, then $\mathbf{a} < \mathbf{b}$ provided that $f \cdot (\mathbf{a} \wedge \mathbf{b}) > 0$.

Theorem 2.3. *The map $f \mapsto image(f)$ gives a one–to–one correspondence between the set of all unit decomposable endomorphisms of $\mathbb{R}^n$ and the set of all oriented 2–planes in $\mathbb{R}^n$.*

Proof. The inverse map is given by $\mathbb{R}\langle \mathbf{u}, \mathbf{v}\rangle \mapsto \mathbf{u} \wedge \mathbf{v}/|\mathbf{u} \wedge \mathbf{v}|$. Details are left to the reader. □

Theorem 2.4. *The 2–planes $\mathbb{R}\{\mathbf{u}, \mathbf{v}\}$ and $\mathbb{R}\{\mathbf{m}, \mathbf{n}\}$ are orthogonal if and only if $(\mathbf{u} \wedge \mathbf{v}) \circ (\mathbf{m} \wedge \mathbf{n}) = 0$.*

Proof. Using theorem 1.1(i) we compute: $(\mathbf{u} \wedge \mathbf{v}) \circ (\mathbf{m} \wedge \mathbf{n}) = (\mathbf{v} \cdot \mathbf{m})\mathbf{u} \otimes \mathbf{n} - (\mathbf{v} \cdot \mathbf{n})\mathbf{u} \otimes \mathbf{m} - (\mathbf{u} \cdot \mathbf{m})\mathbf{v} \otimes \mathbf{n} + (\mathbf{u} \cdot \mathbf{n})\mathbf{v} \otimes \mathbf{m}$, which is zero if $\mathbb{R}\{\mathbf{u}, \mathbf{v}\}$ and $\mathbb{R}\{\mathbf{m}, \mathbf{n}\}$ are orthogonal. Conversely, if $(\mathbf{u} \wedge \mathbf{v}) \circ (\mathbf{m} \wedge \mathbf{n}) = 0$, then $proj_{\mathbf{uv}} \circ proj_{\mathbf{mn}} = 0$ by theorem 1.1(iii); it follows that $\mathbb{R}\{\mathbf{u}, \mathbf{v}\}$ and $\mathbb{R}\{\mathbf{m}, \mathbf{n}\}$ are orthogonal. □

2.2 Simple rotations

The Lie group $\mathrm{SO}(n)$ consists of all endomorphisms $f : \mathbb{R}^n \to \mathbb{R}^n$ that preserve the inner product: $f(\mathbf{u}) \cdot f(\mathbf{v}) = \mathbf{u} \cdot \mathbf{v}$ for all $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$, and have unit determinant $\det(f) = 1$. Geometrically, $\mathrm{SO}(n)$ is the group of rotations

in $\mathbb{R}^n$. It is well known that exponentiation gives a surjective map from $\mathrm{so}(n)$ to $\mathrm{SO}(n)$:

$$\exp : \mathrm{so}(n) \to SO(n), \quad \exp(f) \doteq \sum_{k=0}^{\infty} \frac{1}{k!} f^k.$$

For a decomposable endomorphism, equations (iii) and (iv) of theorem 1.1 can be used to give closed formula for its exponential.

Theorem 2.5. *For all* $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$,

$$\exp(\mathbf{u} \wedge \mathbf{v}) = id - (1 - \cos|\mathbf{u} \wedge \mathbf{v}|)\, proj_{\mathbf{uv}} + \frac{\sin|\mathbf{u} \wedge \mathbf{v}|}{|\mathbf{u} \wedge \mathbf{v}|} \mathbf{u} \wedge \mathbf{v}.$$

Theorem 2.6. $\exp(\mathbf{u} \wedge \mathbf{v})$ *is counterclockwise rotation by an angle* $|\mathbf{u} \wedge \mathbf{v}|$ *in* $\mathbb{R}\langle \mathbf{u}, \mathbf{v} \rangle$, *and is the identity in the orthogonal complement to* $\mathbb{R}\{\mathbf{u}, \mathbf{v}\}$.

Proof. Choose $\mathbf{a}, \mathbf{b} \in \mathbb{R}\{\mathbf{u}, \mathbf{v}\}$ with $\mathbf{a} < \mathbf{b}$, $\mathbf{a} \cdot \mathbf{b} = 0$ and $|\mathbf{a}| = |\mathbf{b}| = 1$ (so that $|\mathbf{a} \wedge \mathbf{b}| = 1$). By theorem 1.1(v), $\mathbf{u} \wedge \mathbf{v} = |\mathbf{u} \wedge \mathbf{v}| \mathbf{a} \wedge \mathbf{b}$. Thus

$$\begin{aligned} \exp(\mathbf{u} \wedge \mathbf{v})(\mathbf{a}) &= \cos|\mathbf{u} \wedge \mathbf{v}|\mathbf{a} - \sin|\mathbf{u} \wedge \mathbf{v}|\mathbf{b} \\ \exp(\mathbf{u} \wedge \mathbf{v})(\mathbf{b}) &= \sin|\mathbf{u} \wedge \mathbf{v}|\mathbf{a} + \cos|\mathbf{u} \wedge \mathbf{v}|\mathbf{b} \end{aligned}$$

by theorem 2.5. Moreover, if $\mathbf{w}$ is orthogonal to $\mathbb{R}\{\mathbf{u}, \mathbf{v}\}$, then we have $\exp(\mathbf{u} \wedge \mathbf{v})(\mathbf{w}) = \mathbf{w}$, also by theorem 2.5. □

We will call a rotation $R \in \mathrm{SO}(n)$ **simple** if there is a 2–plane $\mathcal{P} \subseteq \mathbb{R}^n$ such that (1) $\mathcal{P}$ is stable under R: $R(\mathcal{P}) = \mathcal{P}$, and (2) the orthogonal complement of $\mathcal{P}$ is fixed by R: if $\mathbf{v} \in \mathcal{P}^\perp$, then $R(\mathbf{v}) = \mathbf{v}$. Theorem 2.6 says that the exponential of a decomposable endomorphism is a simple rotation.

Theorem 2.7. *If* $R \in \mathrm{SO}(n)$ *is a simple rotation, then* $R = \exp(f)$, *for some decomposable* $f \in \mathrm{so}(n)$. *In fact, we may take*

$$f = \frac{\theta}{2\sin\theta}(R - R^t),$$

where $\theta \doteq \cos^{-1} \frac{1}{2}(trace(R) - n + 2)$.

Proof. First, we may choose a coordinate system for $\mathbb{R}^n$ such that $R = \left(\begin{smallmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{smallmatrix}\right) \oplus id_{n-2}$, where id_{n-2} is the identity on $\mathbb{R}^{n-2}$ and $0 \leq \theta \leq \pi$. Thus $R = \exp(f)$, where $f = -\theta(1, 0, \ldots, 0) \wedge (0, 1, 0, \ldots, 0)$.

Second, write $f = \mathbf{u} \wedge \mathbf{v}$. Observe that id and $proj_{\mathbf{uv}}$ are self–adjoint (symmetric), while $\mathbf{u} \wedge \mathbf{v}$ is skew–symmetric; thus $\exp(\mathbf{u} \wedge \mathbf{v}) - \exp(\mathbf{u} \wedge \mathbf{v})^t = (2 \sin |\mathbf{u} \wedge \mathbf{v}|/|\mathbf{u} \wedge \mathbf{v}|)\mathbf{u} \wedge \mathbf{v}$, by theorem 2.5. Also by theorem 2.5, we have $trace(\exp(\mathbf{u} \wedge \mathbf{v})) = 2 \cos |\mathbf{u} \wedge \mathbf{v}| + n - 2$; the formula in the theorem follows. $\square$

We remark that from the first part of proof of theorem 2.7, we see that the formula for the logarithm of a simple rotation always yields a decomposable endomorphism f whose associated 2–plane $\mathcal{P}$ is oriented in such a fashion that $\exp(f)$ is counterclockwise rotation in $\mathcal{P}$ by an angle less than π.

In two and three dimensions any rotation is necessarily simple and any skew–symmetric endomorphism is necessarily decomposable. Theorems 2.5 and 2.7 thus give a complete recipe for the exponential and logarithm maps in these dimensions. It should be noted that in three dimensions, $R - R^t$ is a multiple of the endomorphism $\Lambda_{\mathbf{u}}$, where $\Lambda_{\mathbf{u}}(\mathbf{v}) \doteq \mathbf{u} \times \mathbf{v}$, and $\mathbf{u}$ is the axis of rotation for R. In matrix form $\Lambda_{\mathbf{u}} = \begin{pmatrix} 0 & -u_z & u_y \\ u_z & 0 & -u_x \\ -u_y & u_x & 0 \end{pmatrix}$, where $\mathbf{u} = (u_x, u_y, u_z)$; thus the components of the axis of rotation can be read off directly from the matrix $R - R^t$.

2.3 Digression: reflections

Reflection in the hyperplane orthogonal to $\mathbf{u} \in \mathbb{R}^n$ is the unique endomorphism $r_{\mathbf{u}} : \mathbb{R}^n \to \mathbb{R}^n$ which satisfies $r_{\mathbf{u}}(\mathbf{u}) = -\mathbf{u}$, and $r_{\mathbf{u}}(\mathbf{v}) = \mathbf{v}$ for all $\mathbf{v}$ orthogonal to $\mathbf{u}$. We can give an explicit formula in terms of the outer product of two vectors:

$$r_{\mathbf{u}} = id - 2\frac{\mathbf{u} \otimes \mathbf{u}}{|\mathbf{u}|^2}. \tag{2}$$

It is well–known that the compositions of two reflections is a rotation, and in fact, a simple rotation. Indeed, computing using theorem 1.1i and 1.1ii, we get the following.

Theorem 2.8. *If* $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$ *are nonzero, then*

$$r_{\mathbf{u}} \circ r_{\mathbf{v}} = id - \frac{2|\mathbf{u} \wedge \mathbf{v}|^2}{|\mathbf{u}|^2|\mathbf{v}|^2} proj_{\mathbf{uv}} + \frac{2(\mathbf{u} \cdot \mathbf{v})}{|\mathbf{u}|^2|\mathbf{v}|^2} \mathbf{u} \wedge \mathbf{v}.$$

Comparison with theorem 2.5 then yields the following.

Theorem 2.9. *For all nonzero* $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$, $r_{\mathbf{u}} \circ r_{\mathbf{v}}$ *is a simple rotation, and we have*

$$r_{\mathbf{u}} \circ r_{\mathbf{v}} = \exp\left(2\theta \frac{\mathbf{u} \wedge \mathbf{v}}{|\mathbf{u} \wedge \mathbf{v}|}\right)$$

where $\theta \doteq \cos^{-1}((\mathbf{u} \cdot \mathbf{v})/|\mathbf{u}|\,|\mathbf{v}|)$.

Note that the angle of rotation is twice the angle between $\mathbf{u}$ and $\mathbf{v}$, as one expects from the three dimensional case.

3 Strongly orthogonal decomposition

We will say that two endomorphisms $f, g \in \mathrm{so}(n)$ are **strongly orthogonal** if $f \circ g = 0$. Since $f \cdot g = \frac{1}{2} trace(f^t g) = -\frac{1}{2} trace(fg)$, strong orthogonality implies orthogonality. However, the converse is not true. For example, let $\mathbf{e}_i$ $(1 \leq i \leq n)$ denote the standard unit vectors in $\mathbb{R}^n$: at index i the value is unity, and all other indices the value is zero; then $(\mathbf{e}_1 \wedge \mathbf{e}_2) \cdot ((\mathbf{e}_1 + \mathbf{e}_2) \wedge \mathbf{e}_3) = 0$, but $(\mathbf{e}_1 \wedge \mathbf{e}_2) \circ ((\mathbf{e}_1 + \mathbf{e}_2) \wedge \mathbf{e}_3) \neq 0$.

Theorem 3.1. *Every element of* $\mathrm{so}(n)$ *can be expressed as the sum of at most* $\lfloor n/2 \rfloor$ *strongly orthogonal decomposable endomorphisms.*

Proof. We view $f \in \mathrm{so}(n)$ as a skew–hermitian matrix over $\mathbb{C}^n$, so that distinct eigenvectors are orthogonal, and eigenvalues are pure imaginary. Given a nonzero eigenvalue $i\lambda_1$ $(\lambda_1 \in \mathbb{R})$ with corresponding unit eigenvector $\mathbf{v}$, then $-i\lambda_1$ is also an eigenvalue with corresponding unit eigenvector $\bar{\mathbf{v}}$. In this case, set $X_1 \doteq (\mathbf{v} + \bar{\mathbf{v}})/\sqrt{2}$ and $Y_1 \doteq (\mathbf{v} - \bar{\mathbf{v}})/i\sqrt{2}$; thus $X_1, Y_1 \in \mathbb{R}^n$, $|X_1| = 1 = |Y_1|$, $X_1 \cdot Y_1 = 0$, $f(X_1) = -\lambda_1 Y_1$, and $f(Y_1) = \lambda_1 X_1$. Then $f_1 \doteq f - \lambda_1 X_1 \wedge Y_1$, is such that $f_1(X_1) = 0 = f_1(Y_1)$. The construction can be repeated at most a total of $\lfloor n/2 \rfloor$ times before the trivial map is obtained. □

The construction used in the above proof requires us to find (complex–valued) eigenvalues and eigenvectors. Computationally, this can be difficult; one of our goals is to give an alternate way of finding a strong orthogonal decomposition of a skew–symmetric endomorphism. Let us note however, that such a decomposition is not necessarily unique. For example, the endomorphisms $f \doteq \mathbf{e}_1 \wedge \mathbf{e}_2 + \mathbf{e}_3 \wedge \mathbf{e}_4$ admits the alternate strongly orthogonal decomposition $f_1 + f_2$, where $f_1 \doteq \frac{1}{2}(\mathbf{e}_1 + \mathbf{e}_3) \wedge (\mathbf{e}_2 + \mathbf{e}_4)$ and $f_2 \doteq \frac{1}{2}(\mathbf{e}_1 - \mathbf{e}_3) \wedge (\mathbf{e}_2 - \mathbf{e}_4)$.

3.1 Multiple decomposability

We define an endomorphism $f \in \mathrm{so}(n)$ to be **q–decomposable** if we can write f as the sum of exactly q strongly orthogonal decomposable endomorphisms of the same length; i.e., $f = f_1 + \cdots + f_q$, where $|f_1| = \cdots = |f_q|$, and $f_i \circ f_j = 0$ for $i \neq j$.

Theorem 3.2. *Suppose $f \in \mathrm{so}(n)$ is q–decomposable. Then*

i. $f^2 = -\frac{|f|^2}{q} proj_f$,

ii. $f^3 = -\frac{|f|^2}{q} f$,

where $proj_f$ is orthogonal projection onto $image(f)$.

Proof. Write $f = f_1 + \cdots + f_q$, and set $\theta \doteq |f_1| = \cdots = |f_q|$. From theorem 1.1(iii) and strong orthogonality, we have $f^2 = -\theta^2 \sum_{k=1}^{q} proj_{f_k}$. Thus $|f|^2 = -\frac{1}{2} trace(f^2) = q\theta^2$. Equation (ii) follows from theorem 1.1(iv). □

Theorem 3.3. *For each $f \in \mathrm{so}(n)$, we may write $f = f_1 + \cdots + f_m$, where $m \leq \lfloor n/2 \rfloor$, each f_k is q_k–decomposable, and if $i \neq j$, then $f_i \circ f_j = 0$ and $|f_i|^2/q_i \neq |f_j|^2/q_j$. This decomposition is unique up to reordering of summands.*

Proof. For existence, we use theorem 3.1 and group together summands with the same length. For uniqueness, set $x_k \doteq |f_k|^2/q_k$. Theorem 3.2 then implies $f^{2p+1} = (-1)^p \sum_{k=1}^{m} x_k^p f_k$ for integers $p \geq 0$, from which we obtain the formal matrix equation

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_m \\ \vdots & \vdots & & \vdots \\ x_1^{m-1} & x_2^{m-1} & \cdots & x_m^{m-1} \end{pmatrix} \begin{pmatrix} f_1 \\ f_2 \\ \vdots \\ f_m \end{pmatrix} = \begin{pmatrix} f \\ -f^3 \\ \vdots \\ (-1)^{m-1} f^{2m-1} \end{pmatrix}. \tag{3}$$

The $m \times m$ matrix on the left is a Vandermonde matrix, and is well–known to have determinant $\prod_{i<j}(x_j - x_i)$. Since $x_i \neq x_j$ for $i \neq j$ (by construction), equation (3) is invertable. □

3.2 Finding a strongly orthogonal decomposition

Given $f \in \mathrm{so}(n)$, we wish to find the strongly orthogonal decomposition stated in theorem 3.3: $f = f_1 + \cdots + f_m$. In fact, the proof of that theorem essentially gives a way of doing this. Observe that from theorem 3.2, we have

$$f^{2p} = (-1)^p \sum_{k=1}^{m} x_k^p proj_{f_k} \tag{4}$$

for integers $p \geq 1$, where $x_k \doteq |f_k|^2/q_k$ (q_k is the multiplicity of f_k). Taking traces and rearranging slightly, we get the equations

$$\sum_{k=1}^{m} q_k x_k^p = \frac{(-1)^p}{2} trace(f^{2p}) \tag{5}$$

for $1 \leq p \leq m$. Thus if we can solve these (nonlinear) equations for $(x_1, \ldots, x_m)$, then we can invert equation (3) to get $f_1, \ldots, f_m$. We remark that a special numerical method exists for solving Vandermonde equations such as equation (3), see [NRC].

We do not usually know a priori the value of m, or the multiplicities q_k ($1 \leq k \leq m$); however, we may deduce them as follows. First we solve the equations (5) assuming (for the moment) that $m = \lfloor n/2 \rfloor$ and each $q_k = 1$, which will give us $\lfloor n/2 \rfloor$ numbers $(x'_1, \ldots, x'_{\lfloor n/2 \rfloor})$. Next we remove all zeros and duplicate values to form a new list $(x_1, \ldots, x_m)$. The length of this list is our desired value of m, and the number of times the value x_k occurs in the original list gives the multiplicity q_k. Note that the new list $(x_1, \ldots, x_m)$ is necessarily a solution of equations (5).

3.2.1 Solutions for low dimensions

We give an explicit solution to the recipe given above in the case $m = 2$; i.e., assuming that $f \in \mathrm{so}(n)$ can be written as a sum $f = f_1 + f_2$ of two strongly orthogonal multiply decomposable endomorphisms. In this case, the system of equations (5) can be solved explicitly: one finds the solution $x_1 = x_+$ and $x_2 = x_-$, where

$$x_\pm = \frac{1}{2\delta}\left(-trace(f^2) \pm \sqrt{\eta(2\delta\, trace(f^4) - trace^2(f^2))}\right), \tag{6}$$

where $\delta \doteq q_1 + q_2$, $\eta \doteq q_2/q_1$, and q_k is the multiplicity of f_k. Equation (3) is then be inverted to give

$$f_1 = \frac{1}{x_2 - x_1}(x_2 f + f^3) \qquad \text{and} \qquad f_2 = -\frac{1}{x_2 - x_1}(x_1 f + f^3). \tag{7}$$

In particular, this completely solves the decomposition problem in dimensions $n = 4, 5$: assume that $q_1 = q_2 = 1$ (so that $\delta = 2$ and $\eta = 1$) and apply equation (6); if $x_2 = 0$, or if $4trace(f^4) - trace^2(f^2) = 0$, then f must be multiply decomposable with multiplicity 1 in the former case, 2 in the latter.

4 Exponentials

It is a fact that $\exp(f) \circ \exp(g) = \exp(f + g)$ only if f and g commute; and in particular, when $f, g \in \mathrm{so}(n)$ are strongly orthogonal. We exploit this fact to obtain a method for computing the exponential map.

Theorem 4.1. *Suppose $f \in \mathrm{so}(n)$, and let $f = f_1 + \cdots + f_m$ be a strongly orthogonal decomposition of multiply decomposable endomorphisms, then*

$$\exp(f) = id - \sum_{k=1}^{m} \left((1 - \cos\theta_k) proj_{f_k} - \frac{\sin\theta_k}{\theta_k} f_k \right),$$

where $\theta_k \doteq |f_k|/\sqrt{q_k}$ and q_k is the multiplicity of f_k.

Proof. By strong orthogonality, $(\sum_k f_k)^p = \sum_k (f_k)^p$. The equality now follows by computation using theorem 3.2. □

Thus to compute the exponential of $f \in \mathrm{so}(n)$, we may first decompose f into a sum of strongly orthogonal multiply decomposable endomorphisms: $f = f_1 + \cdots + f_m$. Then we may then apply theorem 4.1 to compute $\exp(f)$. However, to minimize the powers of f used, it is actually better to invert equations (4) for $1 \leq p \leq m$ (also a Vandermonde matrix equation) to obtain the projections used in theorem 4.1.

4.1 Exponentials in low dimensions

The case when $f \in \mathrm{so}(n)$ is multiply decomposable (so that $m = 1$), theorems 4.1 and 3.2 imply that

$$\exp(f) = id + \frac{\sin\theta}{\theta} f + \frac{1 - \cos\theta}{\theta^2} f^2, \tag{8}$$

where $\theta \doteq |f|/\sqrt{q}$ and q is the multiplicity of f. Note that in dimension $n = 2$, $f^2 = -\theta^2 id$ and $q = 1$.

Now consider the case $m = 2$: $f = f_1 + f_2$, where f_1, f_2 are strongly orthogonal multiply decomposable endomorphisms. We already know that f_1 and f_2 are given by equations (6) and (7). Moreover, by inverting the equations (4), we find that

$$\begin{aligned} proj_{f_1} &= -\frac{1}{x_1(x_2 - x_1)}(x_2 f^2 + f^4) \\ proj_{f_2} &= \frac{1}{x_2(x_2 - x_1)}(x_1 f^2 + f^4). \end{aligned} \tag{9}$$

These equations, equation (7), and theorem 4.1 then imply that

$$\exp(f) = id + \frac{1}{x_2 - x_1}(Af + Bf^2 + Cf^3 + Df^4), \tag{10}$$

where x_1, x_2 are as in equation (6) and the coefficients are given by

$$A \doteq \frac{x_2 \sin\sqrt{x_1}}{\sqrt{x_1}} - \frac{x_1 \sin\sqrt{x_2}}{\sqrt{x_2}}, \quad B \doteq \frac{x_2(1 - \cos\sqrt{x_1})}{x_1} - \frac{x_1(1 - \cos\sqrt{x_2})}{x_2},$$
$$C \doteq \frac{\sin\sqrt{x_1}}{\sqrt{x_1}} - \frac{\sin\sqrt{x_2}}{\sqrt{x_2}}, \qquad D \doteq \frac{1 - \cos\sqrt{x_1}}{x_1} - \frac{1 - \cos\sqrt{x_2}}{x_2}.$$

In the special case $n = 4$, we have a slightly simpler formula. In this case, $proj_{f_1} + proj_{f_2} = id$, so that equation (10) may be written as

$$\exp(f) = \frac{1}{x_2 - x_1}(E\, id + Af + Ff^2 + Cf^3), \tag{11}$$

where x_1, x_2 are again as in equation (6), and the coefficients are given by

$$E \doteq (x_2 \cos\sqrt{x_1} - x_1 \cos\sqrt{x_2}), \quad \text{and} \quad F \doteq \cos\sqrt{x_1} - \cos\sqrt{x_2}$$

with A, C as above.

5 Logarithms

To compute the logarithm of $R \in \mathrm{SO}(n)$, we find m multiply decomposable endomorphisms $f_1, \ldots, f_m$, each strongly orthogonal to the other, such that

$R = \exp(f_1 + \cdots + f_m)$. Since the identity and projection mappings are symmetric, while a decomposable endomorphism is antisymmetric, theorem 4.1 implies

$$\tfrac{1}{2}(R - R^t) = \sum_{k=1}^{n} \frac{\sin\theta_k}{\theta_k} f_k,$$

where $\theta_k \doteq |f_k|/\sqrt{q_k}$ and f_k has multiplicity q_k. Moreover, by strong orthogonality and theorem 3.2, we get

$$\left(\frac{R - R^t}{2}\right)^{2p} = (-1)^p \sum_{k=1}^{m} \sin^{2p}\theta_k \, proj_k \tag{12}$$

$$\left(\frac{R - R^t}{2}\right)^{2p-1} = (-1)^p \sum_{k=1}^{m} \frac{\sin^{2p-1}\theta_k}{\theta_k} f_k \tag{13}$$

for integers $p \geq 1$. In particular, equation (12) implies

$$\sum_{k=1}^{m} q_k y_k^p = \frac{(-1)^p}{2} trace \left(\frac{R - R^t}{2}\right)^{2p} \tag{14}$$

for all $p \geq 1$, where $y_k \doteq \sin^2\theta_k$.

We may use equations (13) and (14) to find our strongly orthogonal decomposition in so(n). Namely, we first find a solution $(y_1, \ldots, y_m)$ to the m equations (14) with $1 \leq p \leq m$. Using this solution, we invert the formal matrix equation formed from equations (13) for $1 \leq p \leq m$ (which may be cast into a Vandermonde matrix equation) to obtain $f = f_1 + \cdots + f_m$.

On the other hand, the above solution, as it involves inverting the sine function to obtain θ_k, is only valid for a compound rotation composed of simple rotations by angles less than $\pi/2$. With a little more work, it is possible to do better. Using theorem 4.1, it is possible to show that

$$R^p = id + \sum_{k=1}^{m} \left(\frac{\sin p\theta_k}{\theta_k} f_k - (1 - \cos p\theta_k) proj_k\right)$$

for all integers $p \geq 0$. Consequently since f_k is antisymmetric, for such p we have

$$\sum_{k=1}^{m} q_k \cos p\theta_k = \frac{1}{2}\left(trace(R^p) - n + 2\sum_{k=1}^{m} q_k\right) \tag{15}$$

We may now use these equations, for $1 \leq p \leq m$, in conjunction with equation (13) to find a strongly orthogonal decomposition for $\log(R)$. Note that since $\cos n\theta = 2\cos(n-1)\theta\,\cos\theta - \cos(n-2)\theta$ for $n \geq 2$, $\cos p\theta_k$ can be expressed as a polynomial of degree p in $z_k \doteq \cos\theta_k$; so solving equations (15), with $1 \leq p \leq m$, amounts to solving a system of algebraic equations.

5.1 Low dimensional formulae

Suppose $R \in \mathrm{SO}(n)$. If $m = 1$, then we obtain the same formula for $\log(R)$ as in theorem 2.7: $f = (\theta/2\sin\theta)(R - R^t)$, except with θ now given by $\theta = \cos^{-1}\frac{1}{2}\big(trace(R) - n + 2q\big)/2$, where q is the multiplicity of f.

In the case $m = 2$, the system of equations (15) can be recast in the form

$$q_1 z_1 + q_2 z_2 = \tfrac{1}{2}\big(trace(R) - n\big) + \delta \quad \text{and} \quad q_1 z_1^2 + q_2 z_2^2 = \tfrac{1}{4}\big(trace(R^2) - n\big) + \delta,$$

where $z_k = \cos\theta_k$ and $\delta \doteq q_1 + q_2$. These equations have the solution $z_1 = z_+$, $z_2 = z_-$, where

$$\begin{aligned} z_\pm &= \frac{1}{2\delta}\big(trace(R) - n + 2\delta \pm \sqrt{H}\big), \\ H &\doteq \eta\big(\delta\, trace(R^2) - trace(R)^2 + 2(n - 2\delta)\, trace(R) + 3n\delta - n^2\big), \end{aligned} \tag{16}$$

with $\delta \doteq q_1 + q_2$ and $\eta \doteq q_2/q_1$. The strongly orthogonal decomposition for $\log(R) = f_1 + f_2$ is then given by

$$\begin{aligned} f_1 &= \frac{\theta_1}{\sin\theta_1}\frac{1}{\sin^2\theta_1 - \sin^2\theta_2}\left(\sin^2\theta_2\frac{R - R^t}{2} + \big(\frac{R - R^t}{2}\big)^3\right) \\ f_2 &= \frac{\theta_2}{\sin\theta_2}\frac{1}{\sin^2\theta_2 - \sin^2\theta_1}\left(\sin^2\theta_1\frac{R - R^t}{2} + \big(\frac{R - R^t}{2}\big)^3\right) \end{aligned} \tag{17}$$

where $\theta_k = \cos^{-1}(z_k)$ $(k = 1, 2)$.

References

[NRC] *Numerical recipes in C*, by W. H. Press, B. B. Flannery, S. A. Teukolsky, and W. T. Vetterling; published by Cambridge University Press, 1988; ISBN: 0521431085.