# Trigonometric Approximation of $\operatorname{SO}(N)$ Loops 

Tatiana Shingel

Received: 23 November 2008 / Revised: 9 December 2009 / Accepted: 12 January 2010 /
Published online: 11 June 2010
© The Author(s) 2010. This article is published with open access at Springerlink.com


#### Abstract

This paper extends previous work on approximation of loops to the case of special orthogonal groups $\mathrm{SO}(N), N \geq 3$. We prove that the best approximation of an $\mathrm{SO}(N)$ loop $Q(t)$ belonging to a Hölder class $\mathrm{Lip}_{\alpha}, \alpha>1$, by a polynomial $\mathrm{SO}(N)$ loop of degree $\leq n$ is of order $\mathcal{O}\left(n^{-\alpha+\epsilon}\right)$ for $n \geq k$, where $k=k(Q)$ is determined by topological properties of the loop and $\epsilon>0$ is arbitrarily small. The convergence rate is therefore $\epsilon$-close to the optimal achievable rate of approximation. The construction of polynomial loops involves higher-order splitting methods for the matrix exponential. A novelty in this work is the factorization technique for $\operatorname{SO}(N)$ loops which incorporates the loops' topological aspects.


Keywords Nonlinearly constrained trigonometric approximation • Jackson-type inequality $\cdot$ Polynomial loops $\cdot$ Lie groups $\cdot$ Higher-order exponential splitting

Mathematics Subject Classification (2000) 41A29 • 41A17 • 42A10 • 22E67

## 1 Introduction

We regard loops as continuous periodic paths from $\mathbb{R}$ to a Lie group, thus identifying their domain with the one-dimensional torus $\mathbb{T}$.

Periodic functions with values in Lie groups can be studied in the framework of infinite-dimensional Lie groups, where they form a class of loop groups. The book of Presley and Segal [10] is a classical reference on the topic of loop groups. In particular, the authors established the density of a subgroup of polynomial loops in the

[^0]loop group $C^{\infty}(\mathbb{T} \rightarrow G)$, where $G$ is any compact semi-simple Lie group $G$. The qualitative aspect of loop approximation is also embodied in the theory of orthogonal wavelet constructions [13], when polyphase symbols are parameterized by $\mathrm{SU}(2)$ valued Laurent polynomials [4,5]. The quantitative approximation of elements of a loop group depending on their smoothness is an interesting theoretical question which also has practical merit. For example, the asymptotic rate of trigonometric approximation of $S U(2)$-valued functions is the key to constructing and operating optical FIR filter architectures for polarization mode dispersion compensation in optical fibres [9].

Here we continue the study of asymptotic properties of trigonometric approximation of loops initiated in [7, 8]. The motivation for this work is mainly theoretical. However, the techniques illustrated below are constructive, which is essential for potential practical applications.

Let $\mathrm{SO}(N)$ denote the Lie group of orthogonal $N \times N$ matrices with determinant one. We consider the space of continuous loops $Q(t) \in C(\mathbb{T} \rightarrow \mathrm{SO}(N))$. Polynomial loops $Q_{n}(t) \in \Pi_{n}(\mathbb{T} \rightarrow \mathrm{SO}(N))$ are defined as corresponding matrix functions with entries from the set of trigonometric polynomials of degree $\leq n$,

$$
\begin{equation*}
\Pi_{n}(\mathbb{T} \rightarrow \mathbb{R}):=\left\{p_{n}(t)=\sum_{k=0}^{n} a_{k} \cos k t+\sum_{k=1}^{n} b_{k} \sin k t, a_{k}, b_{k} \in \mathbb{R}\right\} \tag{1}
\end{equation*}
$$

The main result of the paper is the following Jackson-type estimate for the Hölder classes $\operatorname{Lip}_{\alpha}(\mathbb{T} \rightarrow \mathrm{SO}(N))$ of loops:

Theorem 1 Let $Q(t) \in \operatorname{Lip}_{\alpha}(\mathbb{T} \rightarrow \operatorname{SO}(N))$, with $N \geq 3$ and $\alpha>1$. For any $\epsilon>0$, there exists a sequence of polynomial loops $Q_{n}(t) \in \Pi_{n}(\mathbb{T} \rightarrow \mathrm{SO}(N))$ of degree $\leq n$ such that

$$
\left\|Q-Q_{n}\right\|_{C} \leq C(n+1)^{-\alpha+\epsilon}, \quad n \geq k
$$

where $k:=k(Q) \geq 0$ is an integer determined by topological properties of $Q$, and $C:=C(\alpha, N, Q, \epsilon, k)>0$ is a constant.

In a previous paper [7] we proved that the approximation of an $\mathrm{SU}(N)$-loop belonging to a Hölder-Zygmund class $\operatorname{Lip}_{\alpha}, \alpha>1 / 2$, by a polynomial $\operatorname{SU}(N)$-loop of degree $\leq n$ is of order $\mathcal{O}\left(n^{-\alpha /(1+\alpha)}\right)$ as $n \rightarrow \infty$. This approximation rate was significantly improved when employing higher-order splitting methods [8], at least for $\alpha>1$. In short, the approach to the problem was as follows: by suitable factorization, the problem was reduced to studying $U(t)=e^{X(t)}$, where $X(t) \in \operatorname{Lip}_{\alpha}(\mathbb{T} \rightarrow \mathfrak{s u}(N))$; $X(t)$ was approximated componentwise by linear methods, and then a splitting method for the exponential map was applied to obtain a polynomial $\mathrm{SU}(N)$-valued loop.

In this work we explore loop approximation in conjunction with special orthogonal groups $\mathrm{SO}(N)$-the real counterpart of special unitary groups $\mathrm{SU}(N)$. In establishing the convergence rate, we follow the steps outlined above. However, the real nature of the current problem poses new challenges. For example, we used a generalization of complex Givens rotations for the factorization and reduced the problem
to essentially the case of $\mathrm{SU}(2)$ loops. In the real setting, the Givens rotation blocks are essentially the elements of $\mathrm{SO}(2) \cong S^{1}$, and the only periodic functions with values in the one-dimensional sphere which can be approximated by trigonometric polynomial loops are trigonometric polynomial loops themselves, which makes the approximation question irrelevant. Another obstacle which calls for different methods is the fact that the $\mathrm{SO}(N)$ loop space is not connected. It is natural to aim to reduce the problem to the case of Lie algebra loops, for which we can apply the results of classical approximation theory for linear spaces. This was a routine step in the algorithm in [7], since the loop space $C(\mathbb{T} \rightarrow \mathrm{SU}(N))$ is connected. In the real setting, there exist $\mathrm{SO}(N)$ loops which cannot be contracted to a point, hence the exponential representation is not always feasible. A cornerstone of this work is the factorization algorithm for the elements of $\operatorname{Lip}_{\alpha}(\mathbb{T} \rightarrow \mathrm{SO}(N)), N \geq 3$ which intrinsically deals with the nonconnectivity constraint. The algorithm originates from the generalized polar decomposition for matrices induced by involutive automorphisms on Lie groups [15]. Eventually, the problem is reduced to studying the loops in the exponential form, $\exp (X(t))$, where $X(t) \in \operatorname{Lip}_{\alpha}(\mathbb{T} \rightarrow \mathfrak{s o}(N))$.

The paper is structured as follows. In Sect. 2 we outline the background theory and present some auxiliary results which are easily deduced from classical approximation theory and matrix analysis. Section 3 is dedicated to the construction of a special basis for polynomial loops $X_{n} \in \Pi_{n}(\mathbb{T} \rightarrow \mathfrak{s o}(N))$. The representation of $X_{n}(t)$ as a linear combination of the basis elements taken in a particular order is a working tool for the proof of the main result of the paper. Technical details of the factorization algorithm for loops are presented in Sect. 4. In Sect. 5 we briefly mention some of the facts from splitting methods for the matrix exponential relevant to our theory. The main result of the paper is proved in Sect. 6, followed by some remarks and conclusion (Sect. 7).

## 2 Definitions and Auxiliary Results

We will make use of the theory of matrix Lie groups and Lie algebras. Therefore, familiarity with the main concepts is expected. The reader can refer, for example, to [1] for the extensive treatment of these concepts.

Let $G \subset \mathbb{F}$, where $\mathbb{F}=\mathbb{R}^{N^{2}}$ or $\mathbb{C}^{N^{2}}$, denote a finite-dimensional matrix Lie group with the Lie algebra $\mathfrak{g}$, and let $C(\mathbb{T} \rightarrow \mathcal{M})$ denote a space of continuous maps from the torus $\mathbb{T}$ to $\mathcal{M}$, where $\mathcal{M}$ is either $G$ or $\mathfrak{g}$. We call the elements of this space loops, which geometrically corresponds to closed curves in $\mathcal{M}$. A point-wise composition in $G$ defines a group operation in the corresponding space $C(\mathbb{T} \rightarrow G)$, and the natural choice of topology is the topology of uniform convergence with respect to the Frobenius norm $\|\cdot\|_{F}$ (i.e., Euclidean norm in $\mathbb{F}$ ) or the spectral norm $\|\cdot\|_{2}$ (i.e., the operator norm for linear maps induced by the Euclidean norm in $\mathbb{R}^{N},\left(\mathbb{C}^{N}\right)$ ). One can impose $C(\mathbb{T} \rightarrow G)$ with the manifold structure using the exponential map

$$
\exp : C(\mathbb{T} \rightarrow \mathfrak{g}) \rightarrow C(\mathbb{T} \rightarrow G)
$$

Group multiplication and inversion are smooth, and so $C(\mathbb{T} \rightarrow G)$ is an infinite dimensional Lie group. Similar reasoning holds for the classes of maps of a finite degree of differentiability $k \geq 0, C^{k}(\mathbb{T} \rightarrow \mathcal{M})$.

We will measure distances between the elements of $C(\mathbb{T} \rightarrow \mathcal{M})$ by setting

$$
\operatorname{dist}_{C}\left(Q_{1}, Q_{2}\right):=\left\|Q_{1}-Q_{2}\right\|_{C}:=\max _{t \in \mathbb{T}}\left\|Q_{1}(t)-Q_{2}(t)\right\|_{2}
$$

We drop the subscript in the norm whenever it does not matter which one we use.
Throughout this paper we are concerned with the Hölder classes $\operatorname{Lip}_{\alpha}(\mathbb{T} \rightarrow \mathcal{M}) \subset$ $C(\mathbb{T} \rightarrow \mathcal{M}), \alpha>0$ of loops, defined by the finiteness of the semi-norm

$$
|Q|_{\operatorname{Lip}_{\alpha}}:=\sup _{h>0} h^{-\alpha}\|Q(\cdot+h)-Q(\cdot)\|_{C}, \quad 0<\alpha<1,
$$

and by recursion for $\alpha>1$, requiring $Q(t) \in C^{k}(\mathbb{T} \rightarrow \mathcal{M})$ and setting

$$
|Q|_{\operatorname{Lip}_{\alpha}}:=\left|Q^{(k)}\right|_{\operatorname{Lip}_{\alpha-k}}
$$

where $k$ is the largest integer $k<\alpha$. Obviously, $C^{k}(\mathbb{T} \rightarrow \mathcal{M}) \subset \operatorname{Lip}_{\alpha}(\mathbb{T} \rightarrow \mathcal{M})$. We further let

$$
\|Q\|_{\operatorname{Lip}_{\alpha}}:=\|Q\|_{C}+|Q|_{\mathrm{Lip}_{\alpha}} .
$$

Note that for the matrix groups considered in this paper, the Hölder classes of loops form groups, i.e., the $\mathrm{Lip}_{\alpha}$ property is preserved under multiplication. This fact will be used without further mention.

We are particularly interested in $G$-valued trigonometric polynomials, also referred to as polynomial loops. For a real matrix Lie group $G$, a polynomial loop $P_{n}(t) \in \Pi_{n}(\mathbb{T} \rightarrow G)$ is a $G$-valued periodic function with entries from the space of trigonometric polynomials (see (1)). Lie group polynomial loops form a nonlinear space, whereas an analogously defined space of polynomial loops $\Pi_{n}(\mathbb{T} \rightarrow \mathfrak{g})$ in the corresponding algebra is obviously linear. For example, for $X_{n}(t) \in \Pi_{n}(\mathbb{T} \rightarrow \mathfrak{s o}(3))$,

$$
X_{n}(t)=\left(\begin{array}{ccc}
0 & -c_{n}(t) & b_{n}(t) \\
c_{n}(t) & 0 & -a_{n}(t) \\
-b_{n}(t) & a_{n}(t) & 0
\end{array}\right),
$$

and $a_{n}(t), b_{n}(t), c_{n}(t) \in \Pi_{n}(\mathbb{T} \rightarrow \mathbb{R})$. It is easy to see that in general, if $X_{n}(t) \in$ $\Pi_{n}(\mathbb{T} \rightarrow \mathfrak{s o}(N))$, the exponential of $X_{n}(t)$ is not a polynomial loop. However, we can decompose $X_{n}(t)$ into a linear combination of polynomial loops, each of which is mapped by the exponential map into a polynomial loop in the group. This aspect will be explored in detail in the next section.

The next two lemmas follow from applying classical theory of univariate trigonometric approximation for $\mathrm{Lip}_{\alpha}$ classes [3].

Lemma 1 Let $X(t) \in \operatorname{Lip}_{\alpha}(\mathbb{T} \rightarrow \mathfrak{s o}(N)), N \geq 3, \alpha>0$. Then there exists $X_{n}(t) \in$ $\Pi_{n}(\mathbb{T} \rightarrow \mathfrak{s o}(N))$ such that

$$
\left\|X-X_{n}\right\|_{C} \leq C_{\alpha}(n+1)^{-\alpha}|X|_{\operatorname{Lip}_{\alpha}}, \quad n \geq 0
$$

and

$$
\left\|X_{n}\right\|_{\operatorname{Lip}_{\alpha}} \leq C_{\alpha}|X|_{\operatorname{Lip}_{\alpha}}, \quad n \geq 0 .
$$

Lemma 2 Let $f(t) \sim \sum_{k \in \mathbb{Z}} c_{k} z^{k} \in \operatorname{Lip}_{\alpha}(\mathbb{T} \rightarrow \mathbb{C}), \alpha>0$. Then

$$
\left\|f-S_{n} f\right\|_{C} \leq C_{\alpha} \frac{\ln (n+2)}{(n+1)^{\alpha}}|f|_{\operatorname{Lip}_{\alpha}}, \quad S_{n} f(t)=\sum_{|k| \leq n} c_{k} z^{k}, \quad n \geq 0
$$

and

$$
\begin{equation*}
\left|c_{n}\right| \leq C_{\alpha} \frac{1}{(n+1)^{\alpha}}\|f\|_{\operatorname{Lip}_{\alpha}}, \quad n \geq 0 \tag{2}
\end{equation*}
$$

Our strategy is to use factorization techniques and splitting methods for the matrix exponential to obtain similar approximation estimates for arbitrary loops $Q(t) \in \operatorname{Lip}_{\alpha}(\mathbb{T} \rightarrow \mathrm{SO}(N))$.

We conclude this section by presenting the following simple but very useful lemma, which will be applied frequently in the proof of the main result of the article:

Lemma 3 For any $Q_{k}(t), \tilde{Q}_{k}(t) \in C(\mathbb{T} \rightarrow \mathrm{SO}(N)), k=1, \ldots, K$, we have

$$
\left\|\prod_{k=1}^{K} \tilde{Q}_{k}-\prod_{k=1}^{K} Q_{k}\right\|_{C} \leq \sum_{k=1}^{K}\left\|\tilde{Q}_{k}-Q_{k}\right\|_{C}
$$

Proof By definition of $\|\cdot\|_{C}$, we have $\|Q\|_{C}=1$ for arbitrary $Q(t) \in C(\mathbb{T} \rightarrow$ $\mathrm{SO}(N))$, and $\left\|\prod_{k} X_{k}\right\|_{C} \leq \prod_{k}\left\|X_{k}\right\|_{C}$ for arbitrary $X_{k}(t) \in C(\mathbb{T} \rightarrow \operatorname{GL}(N))$. Thus,

$$
\begin{aligned}
\left\|\prod_{k=1}^{K} \tilde{Q}_{k}-\prod_{k=1}^{K} Q_{k}\right\|_{C} \leq & \left\|\left(\tilde{Q}_{1}-Q_{1}\right) \prod_{k=2}^{K} \tilde{Q}_{k}\right\|_{C}+\left\|Q_{1}\left(\prod_{k=2}^{K} \tilde{Q}_{k}-\prod_{k=2}^{K} Q_{k}\right)\right\|_{C} \\
\leq & \left\|\tilde{Q}_{1}-Q_{1}\right\|_{C}+\left\|\prod_{k=2}^{K} \tilde{Q}_{k}-\prod_{k=2}^{K} Q_{k}\right\|_{C} \\
& \ldots \\
\leq & \sum_{k=1}^{K}\left\|\tilde{Q}_{k}-Q_{k}\right\|_{C} .
\end{aligned}
$$

## 3 Basis for Polynomial $\mathfrak{s o}(N)$ Loops

Let $\left\{\underline{e}_{i}\right\}$ denote the canonical basis in $\mathbb{R}^{N}$, and introduce

$$
E_{i j}:=\underline{e}_{i} \underline{e}_{j}^{T}-\underline{e}_{j} \underline{e}_{i}^{T}, \quad i=1, \ldots, N-1, j=i+1, \ldots, N
$$

The matrix $E_{i, j}$ has 1 at the entry $(i, j)$ and -1 at the entry $(j, i)$, and the remaining entries are equal to 0 . By definition, $\left\{E_{i j}\right\}$ spans the Lie algebra $\mathfrak{s o}(N)$, which is a linear space isomorphic to $\mathbb{R}^{N(N-1) / 2}$. It is easy to see that a basis for the space of polynomial loops $\Pi_{n}\left(\mathbb{T} \rightarrow \mathbb{R}^{N(N-1) / 2}\right)$ induces a basis for $\Pi_{n}(\mathbb{T} \rightarrow \mathfrak{s o}(N))$ under the same isomorphism.

Next we provide a construction for the following argument: a linear space of polynomial loops $\Pi_{n}\left(\mathbb{T} \rightarrow \mathbb{R}^{m}\right), m \geq 2$, possesses a basis over $\mathbb{R}$ consisting of $m(2 n+1)$ elements.

For $m=2$ we choose the following vectors to be the basis vectors:

$$
\begin{aligned}
& \underline{b}_{1, k}^{T}(t)=(\cos k t, \sin k t), \quad \underline{b}_{3, k}^{T}(t)=(-\cos k t, \sin k t), \quad k=0, \ldots, n, \\
& \underline{b}_{2, k}^{T}(t)=(\sin k t,-\cos k t), \quad \underline{b}_{4, k}^{T}(t)=(\sin k t, \cos k t), \quad k=1, \ldots, n .
\end{aligned}
$$

For $\underline{v}_{n}(t) \in \Pi_{n}\left(\mathbb{T} \rightarrow \mathbb{R}^{2}\right), \underline{v}_{n}(t)=\left(\alpha_{n}(t), \beta_{n}(t)\right)^{T}$, consider

$$
\begin{array}{ll}
\alpha_{n}(t)=\sum_{k=0}^{n} a_{k} \cos k t+\sum_{k=1}^{n} b_{k} \sin k t, & \tilde{\alpha}_{n}(t)=\sum_{k=1}^{n} b_{k} \cos k t-a_{k} \sin k t, \\
\beta_{n}(t)=\sum_{k=0}^{n} c_{k} \cos k t+\sum_{k=1}^{n} d_{k} \sin k t, & \tilde{\beta}_{n}(t)=\sum_{k=1}^{n} d_{k} \cos k t-c_{k} \sin k t,
\end{array}
$$

where the polynomials on the right-hand side are the corresponding conjugate series (see [3]), and $a_{k}, b_{k}, c_{k}, d_{k} \in \mathbb{R}$. Then obviously

$$
\binom{\alpha_{n}(t)}{\beta_{n}(t)}=\binom{\frac{\alpha_{n}(t)+\tilde{\beta}_{n}(t)}{2}}{\frac{\beta_{n}(t)-\tilde{\alpha}_{n}(t)}{2}}+\binom{\frac{\alpha_{n}(t)-\tilde{\beta}_{n}(t)}{2}}{\frac{\beta_{n}(t)+\tilde{\alpha}_{n}(t)}{2}}
$$

and it is easy to verify that

$$
\begin{aligned}
& \binom{\frac{\alpha_{n}(t)+\tilde{\beta}_{n}(t)}{2}}{\frac{\tilde{\beta}_{n}(t)-\alpha_{n}(t)}{2}}=\gamma_{0}+\frac{1}{2} \sum_{k=1}^{n}\left(a_{k}+d_{k}\right) \underline{b}_{1, k}(t)+\frac{1}{2} \sum_{k=1}^{n}\left(b_{k}-c_{k}\right) \underline{b}_{2, k}(t), \\
& \binom{\frac{\alpha_{n}(t)-\tilde{\beta}_{n}(t)}{2}}{\frac{\tilde{\beta}_{n}(t)+\alpha_{n}(t)}{2}}=\gamma_{0}+\frac{1}{2} \sum_{k=1}^{n}\left(d_{k}-a_{k}\right) \underline{b}_{3, k}(t)+\frac{1}{2} \sum_{k=1}^{n}\left(b_{k}+c_{k}\right) \underline{b}_{4, k}(t),
\end{aligned}
$$

where $\gamma_{0}=\left(a_{0} / 2, c_{0} / 2\right)$ is a scalar vector. The basis property follows from above, since $\underline{v}_{n}(t)$ is an arbitrary polynomial loop.

When $m=3$, the basis for $\Pi_{n}\left(\mathbb{T} \rightarrow \mathbb{R}^{3}\right)$ consists of the vectors

$$
\begin{array}{ll}
\underline{b}_{1, k}^{T}(t)=(\cos k t, \sin k t, 0), & \underline{b}_{2, k}^{T}(t)=(\sin k t,-\cos k t, 0), \\
\underline{b}_{3, k}^{T}(t)=(\cos k t, 0, \sin k t), & \underline{b}_{4, k}^{T}(t)=(\sin k t, 0,-\cos k t), \\
\underline{b}_{5, k}^{T}(t)=(0, \cos k t, \sin k t), & \underline{b}_{6, k}^{T}(t)=(0, \sin k t,-\cos k t),
\end{array}
$$

where $k=0, \ldots, n$ for $\underline{b}_{1, k}, \underline{b}_{3, k}, \underline{b}_{5, k}$, and $k=1, \ldots, n$ for $\underline{b}_{2, k}, \underline{b}_{4, k}, \underline{b}_{6, k}$. The proof for this is analogous to the case $m=2$, i.e., an arbitrary polynomial loop $\underline{v}_{n}(t) \in$ $\Pi_{n}\left(\mathbb{T} \rightarrow \mathbb{R}^{3}\right)$ is decomposed into a sum of vector-functions with entries represented as linear combinations of the entries of the original loop and their conjugates. From
this representation one can deduce the coefficients $c_{l, k} \in \mathbb{R}$, such that

$$
\underline{v}_{n}(t)=\sum_{l^{\prime}=1}^{3}\left(\sum_{k=0}^{n} c_{2 l^{\prime}-1, k} \underline{b}_{2 l^{\prime}-1, k}(t)+\sum_{k=1}^{n} c_{2 l^{\prime}, k} \underline{b}_{2 l^{\prime}, k}(t)\right) .
$$

It remains to note that for $m>3$, we can decompose the space $\Pi_{n}\left(\mathbb{T} \rightarrow \mathbb{R}^{m}\right)$ into a direct sum of spaces of dimension 2 and 3. Therefore, any basis element is essentially one of the elements in the systems given above for $m=2$ and $m=3$ (under the corresponding projection map), and it is easy to see that there are in total $m(2 n+1)$ basis elements.

Let $\mathcal{B}_{n}=\left\{B_{l, k}\right\}$ denote the basis over $\mathbb{R}$ for the space $\Pi_{n}(\mathbb{T} \rightarrow \mathfrak{s o}(N))$ consisting of $N(N-1)(2 n+1) / 2$ elements as follows from above. Intuitively, up to $\pm$ sign before each of the summands, the basis elements can be parameterized as follows:

$$
\begin{align*}
B_{2 l^{\prime}-1, k}(t) & =\cos k t E_{\lambda \mu}+\sin k t E_{\xi \eta}, & & k=0, \ldots, n,  \tag{3}\\
B_{2 l^{\prime}, k}(t) & =\sin k t E_{\lambda \mu}-\cos k t E_{\xi \eta}, & & k=1, \ldots, n,
\end{align*}
$$

for some $\lambda \leq \xi \leq \mu \leq \eta$ and $l^{\prime}=1, \ldots, N(N-1) / 2$. The dependence of the parameters $\lambda, \mu, \xi, \eta$ on $l^{\prime}$ is determined by the choice of the isomorphism map between $\Pi_{n}\left(\mathbb{T} \rightarrow \mathbb{R}^{N(N-1) / 2}\right)$ and $\Pi_{n}(\mathbb{T} \rightarrow \mathfrak{s o}(N))$. Furthermore, observe that for an $N \times N$ matrix, there are at most $N(N-1) / 2$ submatrices of rank 2 . Hence, there exists an isomorphism from $\Pi_{n}\left(\mathbb{T} \rightarrow \mathbb{R}^{N(N-1) / 2}\right)$ to $\Pi_{n}(\mathbb{T} \rightarrow \mathfrak{s o}(N))$ such that any basis polynomial loop is a rank 2 matrix. With respect to the notation in (3), this means that two out of four parameters $\lambda, \mu, \xi, \eta$ are always equal. Let us consider the case when $\lambda=\xi$. Then we can write

$$
\begin{align*}
B_{2 l^{\prime}-1, k}(t)=\cos k t E_{\lambda \mu}+\sin k t E_{\lambda \eta} & =\cos k t\left(\underline{e}_{\lambda} \underline{e}_{\mu}^{T}-\underline{e}_{\mu} \underline{e}_{\lambda}^{T}\right)+\sin k t\left(\underline{e}_{\lambda} \underline{e}_{\eta}^{T}-\underline{e}_{\eta} \underline{e}_{\lambda}^{T}\right) \\
& =\underline{e}_{\lambda} \underline{x}_{k}^{T}(t)-\underline{x}_{k}(t) \underline{e}_{\lambda}^{T} \tag{4}
\end{align*}
$$

where $\underline{x}_{k}^{T}(t)=(\ldots, \cos k t, \ldots, \sin k t, \ldots)$ is a vector-valued function which has only two nonzero coordinates, $\cos k t$ and $\sin k t$, at positions $\mu$ and $\eta$, respectively. An analogous formula can be derived for $B_{2 l^{\prime}, k}(t)$. From now on we will always assume the representation (4). The following lemma establishes some of the important properties of the basis $\mathcal{B}_{n}$ :

Lemma 4 For any basis element $B_{l, k}$ and for any $c \in \mathbb{R}$,

$$
\begin{equation*}
e^{c B_{l, k}}=I+\sin c B_{l, k}+(1-\cos c) B_{l, k}^{2}, \quad l=1, \ldots, N(N-1), \tag{5}
\end{equation*}
$$

which is a polynomial loop in $\mathrm{SO}(N)$. Furthermore,

$$
\begin{equation*}
\prod_{j=1}^{J} e^{c_{j} B_{l, k_{j}}(t)} \in \Pi_{2 n}(\mathbb{T} \rightarrow \mathrm{SO}(N)), \quad l=1, \ldots, N(N-1) \tag{6}
\end{equation*}
$$

for any product of this form with $0<k_{1} \leq \cdots \leq k_{J} \leq n$.

Proof For simplicity, in what follows we only consider

$$
B_{1, k}(t)=\underline{e}_{1} \underline{x}_{k}^{T}(t)-\underline{x}_{k}(t) \underline{e}_{1}^{T},
$$

where $\underline{e}_{1}$ is the first canonical basis vector in $\mathbb{R}^{N}$ and $\underline{x}_{k}^{T}(t)=(0, \cos k t, \sin k t, 0, \ldots)$. For any other $B_{l, k}$ the same reasoning holds, which easily follows from (4).

Further, let $c \in \mathbb{R}$, and note that $\left\|\underline{x}_{k}(t)\right\|=1$ for any $t \in \mathbb{T}$, where $\|\cdot\|$ denotes the Euclidean norm. By applying the power-series formula for matrix exponential, we obtain

$$
\begin{aligned}
\exp \left(c B_{1, k}(t)\right)= & I+\frac{\sin \left\|c \underline{x}_{k}\right\|}{\left\|c \underline{x}_{k}\right\|}\left(c \underline{e}_{1} \underline{x}_{k}^{T}-c \underline{x}_{k}^{T} \underline{e}_{1}\right) \\
& +\frac{1-\cos \left\|c \underline{x}_{k}\right\|}{\left\|c \underline{x}_{k}\right\|^{2}}\left(-\left\|c \underline{x}_{k}\right\|^{2} \underline{e}_{1} \underline{e}_{1}^{T}-c^{2} \underline{x}_{k} \underline{x}_{k}^{T}\right) \\
= & I+\sin c B_{1, k}(t)+(1-\cos c) B_{1, k}^{2}(t),
\end{aligned}
$$

and the property (5) follows.
In order to establish the property (6), it is enough to verify that $\prod_{j=1}^{J} B_{1, k_{j}}(t)$ is a polynomial loop of degree at most $2 n$, for $0<k_{1} \leq \cdots \leq k_{J} \leq n, J>0$. Here we allow nonstrict inequalities among $k_{j}$ s to include the case when we have factors of the basis elements to the second power. Note that

$$
B_{1, k_{j}} B_{1, k_{i}}=-e_{1}\left(\underline{x}_{j}^{T} \underline{x}_{i}\right) e_{1}^{T}-\underline{x}_{j} \underline{x}_{i}^{T},
$$

where for simplicity we let $\underline{x}_{s}^{T}(t)=\left(0, \cos k_{s} t, \sin k_{s} t, 0, \ldots\right), s=i, j$. Inductively, we deduce for even $J=2 J^{\prime}$,

$$
\begin{aligned}
\prod_{j=1}^{J} B_{1, k_{j}} & =\prod_{j=1}^{2 J^{\prime}}\left(e_{1} \underline{x}_{j}^{T}-\underline{x}_{j} e_{1}^{T}\right)=(-1)^{J^{\prime}}\left(e_{1}\left(\prod_{j=1}^{J^{\prime}} \underline{x}_{2 j-1}^{T} \underline{x}_{2 j}\right) e_{1}^{T}+\prod_{j=1}^{J^{\prime}} \underline{x}_{2 j-1} \underline{x}_{2 j}^{T}\right) \\
& =(-1)^{J^{\prime}}\left(\left(\prod_{j=1}^{J^{\prime}} \underline{x}_{2 j-1}^{T} \underline{x}_{2 j}\right) e_{1} e_{1}^{T}+\left(\prod_{j=1}^{J^{\prime}-1} \underline{x}_{2 j}^{T} \underline{x}_{2 j+1}\right) \underline{x}_{1} \underline{x}_{2 J^{\prime}}^{T}\right)
\end{aligned}
$$

Observe that $\underline{x}_{j}^{T}(t) \underline{x}_{i}(t)=\cos \left(k_{j}-k_{i}\right) t$. Therefore,

$$
\begin{aligned}
\prod_{j=1}^{J} B_{1, k_{j}}(t)= & (-1)^{J^{\prime}} \prod_{j=1}^{J^{\prime}} \cos \left(k_{2 j}-k_{2 j-1}\right) t e_{1} e_{1}^{T} \\
& +(-1)^{J^{\prime}} \prod_{j=1}^{J^{\prime}-1} \cos \left(k_{2 j+1}-k_{2 j}\right) t \underline{x}_{1} \underline{x}_{2 J^{\prime}}^{T}
\end{aligned}
$$

The degree of the first component is obviously less than the degree of the second component. If we denote the degree of the second component by $m$, then $0<m=$ $\sum_{j=1}^{J^{\prime}-1}\left(k_{2 j+1}-k_{2 j}\right)+k_{1}+k_{J} \leq k_{J-1}+k_{J}<2 n$.

For odd $J=2 J^{\prime}+1$,

$$
\begin{aligned}
& \prod_{j=1}^{J} B_{1, k_{j}}(t) \\
&=(-1)^{J^{\prime}}\left(\left(\prod_{j=1}^{J^{\prime}} \underline{x}_{2 j-1}^{T} \underline{x}_{2 j}\right) e_{1} e_{1}^{T}+\left(\prod_{j=1}^{J^{\prime}-1} \underline{x}_{2 j}^{T} \underline{x}_{2 j+1}\right) \underline{x}_{1} \underline{x}_{2 J^{\prime}}^{T}\right) \\
& \times\left(e_{1} \underline{x}_{2 J^{\prime}+1}^{T}-\underline{x}_{2 J^{\prime}+1} e_{1}^{T}\right) \\
&=(-1)^{J^{\prime}}\left(\left(\prod_{j=1}^{J^{\prime}} \underline{x}_{2 j-1}^{T} \underline{x}_{2 j}\right) e_{1} \underline{x}_{2 J^{\prime}+1}^{T}-\left(\prod_{j=1}^{J^{\prime}} \underline{x}_{2 j}^{T} \underline{x}_{2 j+1}\right) \underline{x}_{1} e_{1}^{T}\right) \\
&=(-1)^{J^{\prime}} \prod_{j=1}^{J^{\prime}} \cos \left(k_{2 j}-k_{2 j-1}\right) t e_{1} \underline{x}_{2 J^{\prime}+1}^{T}+(-1)^{J^{\prime}} \prod_{j=1}^{J^{\prime}} \cos \left(k_{2 j+1}-k_{2 j}\right) t \underline{x}_{1} e_{1}^{T} .
\end{aligned}
$$

Similarly, $0<m^{\prime}=\sum_{j=1}^{J^{\prime}}\left(k_{2 j}-k_{2 j-1}\right)+k_{2 J^{\prime}+1} \leq k_{J-1}-k_{1}+k_{J}<2 n$ and $0<$ $m^{\prime \prime}=\sum_{j=1}^{J^{\prime}}\left(k_{2 j+1}-k_{2 j}\right)+k_{1} \leq k_{J} \leq n$. Consequently, the degree of the above polynomial loop is $m=\max \left\{m^{\prime}, m^{\prime \prime}\right\}<2 n$. This concludes the proof of the lemma.

## 4 Factorization of SO(N) Loops

Recall that the fundamental group $\pi_{1}(\mathrm{SO}(N)), N \geq 3$, which is a group of homotopy classes of loops in $\mathrm{SO}(N)$, is isomorphic to $\mathbb{Z}_{2}$ (see [11] for details). The fact that the fundamental group $\pi_{1}(\mathrm{SO}(N))$ is nontrivial also means that $\mathrm{SO}(N)$ is not simply connected. An immediate consequence is that the corresponding loop group $C(\mathbb{T} \rightarrow \mathrm{SO}(N)$ ) is not (path) connected (in general the notions connected and path connected are distinct, but it can be shown that they are equivalent for manifolds). Consequently, $C(\mathbb{T} \rightarrow \mathrm{SO}(N))$ has two connected components. The connected component containing the identity element of the group is referred to as the identity or principal component (a unique open connected subgroup of $C(\mathbb{T} \rightarrow \mathrm{SO}(N))$ ).

In order to use the tools represented in the previous section, we would like to factorize an arbitrary loop into essentially a product of the exponentials of the algebra loops. Any element in the principal component can be represented as a product of exponentials of the algebra loops using, for example, a simple homotopy argument (cf. [8]). As the group theory suggests, any connected component of a group is a coset of the identity component. Hence, any loop in the second connected component in $C(\mathbb{T} \rightarrow \mathrm{SO}(N)$ ) can be decomposed into a product of a "bad" (i.e., which cannot be contracted to a point) loop and a "good" loop. If we choose the "bad" loop to be a polynomial loop, the "good" loop can be dealt with using again the homotopy argument. However, this approach is not constructive and initially requires analysis on the topology of a loop, which is cumbersome even for the $N=3$ case. Instead, we propose a uniform factorization algorithm for elements of $C(\mathbb{T} \rightarrow \mathrm{SO}(N)), N \geq 3$,
which constructively deals with the nonconnectivity constraint whenever necessary. The central idea is to "slice" the loops which are the exponentials of $\mathfrak{s o}(N)$ loops, such that the remaining loop is essentially an $\mathrm{SO}(N-1)$ loop. The algorithm stops when the $2 \times 2$ block is reached. Since by construction the last multiple has only two eigenvalues which are not identically one for all $t \in \mathbb{T}$, it can be identified with the element of the first nontrivial loop group (from the point of view of polynomial loop approximation), which is an SO (3) loop. Topological properties of the last factor define the topological properties of the initial loop. However, the analysis is straightforward due to its simple form. Finally, we decompose the last factor into the product of a polynomial loop and an exponential of the corresponding algebra loop. Remarkably, the loops in the decomposition carry the same smoothness properties as the original loop.

Theorem 2 For any $Q(t) \in \operatorname{Lip}_{\alpha}(\mathbb{T} \rightarrow \mathrm{SO}(N)), N \geq 3, \alpha>1 / 2$,

$$
\begin{equation*}
Q(t)=\left(\prod_{j=1}^{N-2} Q_{0, j} e^{X_{j}(t)}\right) \hat{P}_{k}(t) e^{\Delta(t) \hat{\Phi}} \tag{7}
\end{equation*}
$$

where $Q_{0, j}$ are constant orthogonal matrices, some of which are the identity matrices

$$
\begin{equation*}
X_{j}(t) \in \operatorname{Lip}_{\alpha}(\mathbb{T} \rightarrow \mathfrak{s o}(N)), \quad j=1, \ldots, N-2, \tag{8}
\end{equation*}
$$

and

$$
\left\|X_{j}\right\|_{\operatorname{Lip}_{\alpha}} \leq C(\alpha, N, Q)\|Q\|_{\operatorname{Lip}_{\alpha}}, \quad j=1, \ldots, N-2
$$

The loop $\left(\prod_{j=1}^{N-2} e^{-X_{j}(t)} Q_{0, j}^{T}\right) Q(t)$ is isomorphic to a function from $\mathbb{T}$ to $\mathbb{T}$. For $k$ denoting the winding number of this function,

$$
\hat{P}_{k}(t)=\left(\begin{array}{cc}
I_{N-3} & \mathbf{0}^{T}  \tag{9}\\
\mathbf{0} & P_{k}(t)
\end{array}\right), \quad P_{k}(t)=\left(\begin{array}{ccc}
1 & 0 & 0 \\
0 & \cos k t & -\sin k t \\
0 & \sin k t & \cos k t
\end{array}\right)
$$

where $I_{s}$ denotes the $s \times s$ identity matrix. Finally,

$$
\hat{\Phi}=\left(\begin{array}{cc}
O_{N-3} & \mathbf{0}^{T} \\
\mathbf{0} & \Phi
\end{array}\right), \quad \Phi=\left(\begin{array}{ccc}
0 & 0 & 0 \\
0 & 0 & -1 \\
0 & 1 & 0
\end{array}\right),
$$

where $O_{s}$ denotes the $s \times s$ zero matrix, and $\Delta(t) \in \operatorname{Lip}_{\alpha}(\mathbb{T} \rightarrow \mathbb{R})$.

Proof of Theorem 2 The proof of the theorem comprises several auxiliary results.

Lemma 5 Let $Q(t) \in \operatorname{Lip}_{\alpha}(\mathbb{T} \rightarrow \operatorname{SO}(N)), \alpha>1 /(N-1)$ and $N \geq 3$. Then

$$
\begin{equation*}
Q(t)=Q_{0} \exp (X(t)) P(t) \tag{10}
\end{equation*}
$$

where $X(t)$ and $P(t)$ satisfy the same Lipschitz condition as $Q(t)$ with norms governed by constants depending on $Q(t)$, and $Q_{0}$ is a scalar matrix. In particular,

$$
X(t)=\left(\begin{array}{cccc}
0 & -x_{2}(t) & \ldots & -x_{N}(t)  \tag{11}\\
x_{2}(t) & 0 & \ldots & 0 \\
\vdots & \vdots & \ldots & \vdots \\
x_{N}(t) & 0 & \ldots & 0
\end{array}\right)=\underline{x}(t) \underline{e}_{1}^{T}-\underline{e}_{1} \underline{x}(t)^{T},
$$

where $\underline{x}: \mathbb{T} \rightarrow \mathbb{R}^{N}$ is the vector-valued function with the first coordinate $x_{1}(t) \equiv 0$ and the vector $\underline{e}_{1}$ is the first canonical basis vector in $\mathbb{R}^{N}$. The coordinates of the vector-valued function $\underline{x}(t)$ can be found from the first column vector of the matrix $\underline{\tilde{Q}}_{1}(t):=Q_{0}^{T} Q(t)$ via the following formulas:

$$
\begin{align*}
& \|\underline{x}(t)\|=\arccos \tilde{Q}_{11}(t), \\
& x_{k}(t)=\frac{\|\underline{x}(t)\|}{\sin \|\underline{x}(t)\|} \tilde{Q}_{k 1}(t) \quad \text { for } k=2, \ldots, N, \tag{12}
\end{align*}
$$

and the scalar matrix $Q_{0}$ can be chosen to ensure that the above formulas are welldefined, i.e., $\left|\tilde{Q}_{11}(t)\right| \leq \epsilon<1$ for any $t \in \mathbb{T}$ and some small $\epsilon>0$. Finally,

$$
\begin{gather*}
P(t)=\exp (-X(t)) Q(t)=\left(\begin{array}{cc}
1 & 0 \\
0 & \tilde{P}(t)
\end{array}\right) \\
\text { where } \tilde{P}(t) \in \operatorname{Lip}_{\alpha}(\mathbb{T} \rightarrow \mathrm{SO}(N-1)) \tag{13}
\end{gather*}
$$

Proof As was mentioned in the introduction, this factorization originates from the generalized polar decomposition for the matrix exponential induced by an involutive automorphism acting on the group (cf. [15]). In particular, the authors proposed a so-called "peel-down" approach, for which a particular automorphism is chosen such that when applied consecutively, every factor belongs to the subgroup of lower dimension. Based on their results, we assume that there exists a decomposition such as (10), where the matrix $P(t)$ is essentially an $\mathrm{SO}(N-1)$ loop and $X(t)$ is a rank 2 matrix (11). We then derive each of the factors by algebraic manipulations.

Let us assume for now that the absolute value of the leading diagonal coefficient of the loop $Q(t)$ stays away from 1 , so $Q_{0}$ can be set to be the identity matrix. The following closed formula holds for $X(t)$ :

$$
\begin{equation*}
\exp (X)=I+\frac{\sin \|\underline{x}\|}{\|\underline{x}\|}\left(\underline{x e}_{1}^{T}-\underline{e}_{1} \underline{x}^{T}\right)+\frac{1-\cos \|\underline{x}\|}{\|\underline{x}\|^{2}}\left(-\|\underline{x}\|^{2} \underline{e}_{1} \underline{e}_{1}^{T}-\underline{x x^{T}}\right) \tag{14}
\end{equation*}
$$

The proof follows immediately by the definition of the matrix exponential applied to any matrix of the form (11). Further, assuming $\tilde{P}(t)$ has the form (13), the first column of the matrix $Q$ is determined by the equation,

$$
\underline{Q}_{1}=Q \underline{e}_{1}=\exp (X) \underline{e}_{1}
$$

Using (14) we obtain

$$
\underline{Q}_{1}=\cos \|\underline{x}\| \underline{e}_{1}+\frac{\sin \|\underline{x}\|}{\|\underline{x}\|} \underline{x} .
$$

The formulas (12) follow from this equality. The matrix $P(t)$ is then obtained by computing $P(t)=\exp (-X(t)) Q(t)$.

It remains to consider the case when $Q_{11}(t)$ passes through $1 \mathrm{and} /$ or -1 for some $t \in \mathbb{T}$. Let $\underline{Q}_{1}(t)$ be the first column of the matrix $Q(t)$, which is a $\operatorname{Lip}_{\alpha}\left(\mathbb{T} \rightarrow S^{N-1}\right)$ loop in the unit sphere $S^{N-1} \subset \mathbb{R}^{N}$. The existence of the matrix $Q_{0}$ such that the leading coefficient of $Q_{0}^{T} Q(t)$ does not pass through $\pm 1$ is equivalent to the statement that the set

$$
\Gamma=\left\{\underline{Q}_{0,1} \in S^{N-1}: \underline{Q}_{0,1}^{T} \cdot \underline{Q}_{1}(t) \neq \pm 1 \text { for any } t \in \mathbb{T}\right\}
$$

is nonempty. For this it is sufficient to prove that the complement $\Gamma^{c}=S^{N-1} \backslash \Gamma$, which is in fact the union of the curves $\underline{Q}_{1}$ and $-\underline{Q}_{1}$, has zero surface measure. The loop $\underline{Q}_{1}(t) \in \operatorname{Lip}_{\alpha}\left(\mathbb{T} \rightarrow S^{N-1}\right)$ can be covered by $n$ spherical caps

$$
\mathcal{C}\left(r, \underline{q}_{m}\right):=\left\{\underline{Q} \in S^{N-1}:\left\|\underline{Q}-\underline{q}_{m}\right\| \leq r\right\}, \quad m=1, \ldots, n
$$

with $r \leq C n^{-\alpha}$ and $\underline{q}_{m}=\underline{Q}_{1}(2 \pi m / n)$. The measure of each cap is bounded by $C r^{N-1}$ for $r \rightarrow 0$. Therefore, the curve is contained in the union of the caps with total measure $\leq C n r^{N-1} \leq C^{\prime} n^{1-(N-1) \alpha}$, which is zero for $n \rightarrow \infty$ when $\alpha>1 /(N-1)$. The union of two sets of measure zero is again a set of measure zero. The remaining columns of $Q_{0}$ should be chosen such that the matrix becomes orthogonal with determinant one. It can easily be done, for example, by taking arbitrary unit vectors and then applying the Gram-Schmidt process.

The proof of the $\mathrm{Lip}_{\alpha}$ property for the factors follows from the fact that the transformations from $Q(t)$ to $X(t)$ and $P(t)$ are diffeomorphisms. Since the transformations are nonlinear, the constants in general depend on $Q$.

Let us apply the above lemma to $Q(t) \in \operatorname{Lip}_{\alpha}(\mathbb{T} \rightarrow \mathrm{SO}(3))$ :

$$
Q(t)=Q_{0} \exp (X(t)) P(t), \quad P(t)=\left(\begin{array}{ccc}
1 & 0 & 0  \tag{15}\\
0 & a(t) & -b(t) \\
0 & b(t) & a(t)
\end{array}\right)
$$

where $a^{2}(t)+b^{2}(t)=1$ for any $t \in \mathbb{T}$ and the constant matrix $Q_{0}$ can be the identity. Note that $P(t)$ is isomorphic to a loop $\lambda(t):=a(t)+i b(t) \in \operatorname{Lip}_{\alpha}(\mathbb{T} \rightarrow \mathbb{T})$, and one can construct a function $\Delta(t) \in \operatorname{Lip}_{\alpha}([0,2 \pi] \rightarrow \mathbb{R})$ such that $a(t)=\cos \Delta(t)$ and $b(t)=\sin \Delta(t)$. We are interested in the winding number $W(\lambda)$ for the function $\lambda$ (cf. [2]). It is easy to see that if $\Delta(2 \pi)=\Delta(0)$, the winding number $W(\lambda)$ is zero. In this case we can write

$$
P(t)=\exp (\Delta(t) \Phi), \quad \Phi=\left(\begin{array}{ccc}
0 & 0 & 0  \tag{16}\\
0 & 0 & -1 \\
0 & 1 & 0
\end{array}\right)
$$

and $\Delta(t) \Phi \in \operatorname{Lip}_{\alpha}(\mathbb{T} \rightarrow \mathfrak{s o}(3))$. The second case is when $\Delta(2 \pi)=\Delta(0)+2 \pi k$ for some $k \in \mathbb{Z}, k \neq 0$, which corresponds to $W(\lambda)=k$. Then the loop $P(t)$ cannot be represented as an exponential of a loop in the corresponding algebra. However, let

$$
P_{k}(t):=\left(\begin{array}{ccc}
1 & 0 & 0  \tag{17}\\
0 & \cos k t & -\sin k t \\
0 & \sin k t & \cos k t
\end{array}\right) .
$$

Then the product $P_{k}^{T}(t) P(t)$ is equal to

$$
\left(\begin{array}{ccc}
1 & 0 & 0  \tag{18}\\
0 & \cos (\Delta(t)-k t) & -\sin (\Delta(t)-k t) \\
0 & \sin (\Delta(t)-k t) & \cos (\Delta(t)-k t)
\end{array}\right) .
$$

We define $\hat{\Delta}(t):=\Delta(t)-k t$. Note that $\hat{\Delta}(t) \in \operatorname{Lip}_{\alpha}(\mathbb{T} \rightarrow \mathbb{R})$, and hence we can write (18) in the exponential form as in (16). For simplicity, we further refer to $k$ as the winding number of the loop $P(t)$ in (15).

From the topological point of view, if the degree $k$ is even, $P_{k}(t)$ and $e^{\hat{\Delta}(t) \Phi}$ belong to the identity component of the loop group $\operatorname{Lip}_{\alpha}(\mathbb{T} \rightarrow \mathrm{SO}(3))$, and so does their product. For odd $k$, the product $P_{k}(t) e^{\hat{\Delta}(t) \Phi}$ belongs to the second connected component, and it illustrates the fact that this connected component is a coset of the identity component. To summarize, we have established the following result:

Lemma 6 For any $Q(t) \in \operatorname{Lip}_{\alpha}(\mathbb{T} \rightarrow \operatorname{SO}(3)), \alpha>1 / 2$,

$$
\begin{equation*}
Q(t)=Q_{0} e^{X(t)} P_{k}(t) e^{\Delta(t) \Phi} \tag{19}
\end{equation*}
$$

where $Q_{0} \in \mathrm{SO}(3)$ can also be the identity, and $X(t) \in \operatorname{Lip}_{\alpha}(\mathbb{T} \rightarrow \mathfrak{s o}(3))$ is found using (11), (12). The absolute value of the winding number $k$ of the loop $e^{-X(t)} Q_{0}^{T} Q(t)$ (which is isomorphic to a loop $\lambda(t) \in \operatorname{Lip}_{\alpha}(\mathbb{T} \rightarrow \mathbb{T})$ ) determines the degree of the polynomial loop $P_{k}(t)$ given by (17). Note that for $k=0, P_{k}(t) \equiv I$. Further, $\Delta(t) \in \operatorname{Lip}_{\alpha}(\mathbb{T} \rightarrow \mathbb{R})$ is determined from the equation

$$
P_{k}^{T}(t) e^{-X(t)} Q_{0}^{T} Q(t)=e^{\Delta(t) \Phi}
$$

where $\Phi \in \mathfrak{s o}$ (3) is the same as in (16).
In general, we can repeatedly factorize the loops $P(t)$ in (13) until we obtain the loop isomorphic to an $\mathrm{SO}(3)$ loop, for which we apply Lemma 6. The lower bound on $\alpha$ follows from Lemma 5, since $1 / 2$ is the largest value, obtained at the last factorization step. This establishes the proof of Theorem 2.

## 5 Facts from Splitting Methods

Here we briefly outline the idea of splitting methods. It is well known that the exponential $e^{\lambda\left(A_{1}+\cdots+A_{m}\right)}$, where $\left\{A_{k}\right\} \in \mathfrak{s o}(N)$, can be approximated by the splitting formula $F\left(\left\{\lambda A_{j}\right\}_{j=1, \ldots, m}\right)=e^{\lambda A_{1}} \cdots e^{\lambda A_{m}}$ of order one, i.e., $e^{\lambda\left(A_{1}+\cdots+A_{m}\right)}=$
$F\left(\left\{\lambda A_{j}\right\}_{j=1, \ldots, m}\right)+\mathcal{O}\left(\lambda^{2}\right)$. Furthermore, the error estimate is

$$
\begin{equation*}
\left\|e^{\lambda\left(A_{1}+\cdots+A_{m}\right)}-F\left(\left\{\lambda A_{j}\right\}_{j=1, \ldots, m}\right)\right\|_{2} \leq \frac{\lambda^{2}}{2} \sum_{k=1}^{m-1}\left\|\left[A_{k}, \sum_{j=k+1}^{m} A_{j}\right]\right\|_{2} \tag{20}
\end{equation*}
$$

A second-order approximation can be achieved using, for example, a symmetric splitting formula

$$
S\left(\left\{\lambda A_{j}\right\}_{j=1, \ldots, m}\right)=e^{(\lambda / 2) A_{1}} \cdots e^{(\lambda / 2) A_{m-1}} e^{\lambda A_{m}} e^{(\lambda / 2) A_{m-1}} \cdots e^{(\lambda / 2) A_{1}}
$$

and the magnitude of the error for this splitting in the case of skew-symmetric matrices can be estimated as follows:

$$
\begin{equation*}
\left\|e^{\lambda \sum_{k=1}^{m} A_{k}}-S\left(\left\{\lambda A_{j}\right\}_{j=1, \ldots, m}\right)\right\|_{2} \leq \lambda^{3} \Delta\left(A_{1}, \ldots, A_{m}\right) \tag{21}
\end{equation*}
$$

where $\Delta\left(A_{1}, \ldots, A_{m}\right)=\sum_{k=1}^{m-1} \Delta_{2}\left(A_{k}, A_{k+1}+\cdots+A_{m}\right)$, and

$$
\Delta_{2}(X, Y)=\frac{1}{12}\left\{\|[[X, Y], Y]\|_{2}+\frac{1}{2}\|[[X, Y], X]\|_{2}\right\} .
$$

The bounds (20), (21) were established in [12, 14]. Similar bounds also hold in the general setting when $\left\{A_{k}\right\}$ are noncommuting operators in a Banach space. Let $f_{j}(\lambda)$, $j=1, \ldots, r$ be first, second or in general $k$ th-order approximants for the original exponential operator $e^{\lambda\left(A_{1}+\cdots+A_{m}\right)}$. Then a splitting formula of order $s$ can be given in the form

$$
\begin{equation*}
F_{S}\left(\left\{\lambda A_{j}\right\}_{j=1, \ldots, m}\right)=f_{1}\left(\left\{\tau_{1} \lambda A_{j}\right\}_{j=1, \ldots, m}\right) \cdots f_{r}\left(\left\{\tau_{r} \lambda A_{j}\right\}_{j=1, \ldots, m}\right), \tag{22}
\end{equation*}
$$

where the parameters $\tau_{j}$ are determined by the requirement

$$
e^{\lambda\left(A_{1}+\cdots+A_{m}\right)}=F_{s}\left(\left\{\lambda A_{j}\right\}_{j=1, \ldots, m}\right)+\mathcal{O}\left(\lambda^{s+1}\right)
$$

For example, if $r$ is even, and $f_{2 j}\left(\left\{\lambda A_{j}\right\}_{j=1, \ldots, m}\right)=f_{j}^{-1}\left(\left\{-\lambda A_{j}\right\}_{j=1, \ldots, m}\right)$, where $f_{j}=F$ is the standard first-order splitting mentioned above, we obtain the wellknown symmetric Yoshida-Suzuki splitting formula (see [6] for an overview), for which the parameters $p_{j}$ can be determined via a straightforward recursive procedure. The idea of Yoshida and Suzuki was as follows: splitting methods of order 2(s'+1) can be constructed from a given method of order $2 s^{\prime}$ via the formula

$$
\begin{aligned}
& S_{2\left(s^{\prime}+1\right)}\left(\left\{A_{j}\right\}_{j=1, \ldots, m}\right) \\
& \quad=S_{2 s^{\prime}}\left(\left\{a_{s^{\prime}} A_{j}\right\}_{j=1, \ldots, m}\right) S_{2 s^{\prime}}\left(\left\{b_{s^{\prime}} A_{j}\right\}_{j=1, \ldots, m}\right) S_{2 s^{\prime}}\left(\left\{a_{s^{\prime}} A_{j}\right\}_{j=1, \ldots, m}\right)
\end{aligned}
$$

if one chooses the constants

$$
a_{s^{\prime}}=\left(2-2^{1 /\left(2 s^{\prime}+1\right)}\right)^{-1}, \quad b_{s^{\prime}}=-2^{1 /\left(2 s^{\prime}+1\right)}\left(2-2^{1 /\left(2 s^{\prime}+1\right)}\right)^{-1}
$$

In theory, Yoshida-Suzuki splitting can be of arbitrarily high order. The practical constraint is however that the number of stages increases exponentially (let $f_{j}=S$, then $r=3^{s^{\prime}-1}$ for the method of order $2 s^{\prime}$ ).

Many other symmetric and nonsymmetric decompositions can be obtained from (22). Generally, finding the parameters $p_{j}$ is a challenging task, which involves computation of higher-order terms of the Baker-Campbell-Hausdorf formula [6]. In principle, for the same order $s$, the number of states $r$ varies. For our purposes we assume that $r$ is a fixed function of $s$.

For any of these methods to be applicable to our theory, we would like to know the magnitude of the error term $e^{\lambda\left(A_{1}+\cdots+A_{m}\right)}-F_{S}\left(\left\{\lambda A_{j}\right\}_{j=1, \ldots, m}\right)$. The following lemma gives a rough estimate of the accuracy of an arbitrary splitting method. We formulate it in conjunction with special orthogonal groups only for convenience, since similar results hold in a general setting.

Lemma 7 For $A_{j} \in \mathfrak{s o}(N), j=1, \ldots, m$, and $0<\lambda<\lambda_{\max }$, let

$$
F_{S}\left(\left\{\lambda A_{j}\right\}_{j=1, \ldots, m}\right)=\prod_{i=1}^{r} e^{\tau_{i 1} \lambda A_{1}} \cdots e^{\tau_{i m} \lambda A_{m}}
$$

be an order s splitting formula. Then

$$
\left\|e^{\lambda\left(A_{1}+\cdots+A_{m}\right)}-F_{s}\left(\left\{\lambda A_{j}\right\}_{j=1, \ldots, m}\right)\right\|_{2} \leq C_{s} \lambda^{s+1}\left(\left\|A_{1}\right\|_{2}+\cdots+\left\|A_{m}\right\|_{2}\right)^{s+1}
$$

where $C_{s}>0$ depends on the order $s, \lambda_{\max }$, and $\sum_{j=1}^{m}\|A\|_{2}$.
Proof Obviously,

$$
\left\|e^{\lambda\left(A_{1}+\cdots+A_{m}\right)}-F_{s}\left(\left\{\lambda A_{j}\right\}_{j=1, \ldots, m}\right)\right\|_{2}=\left\|e^{-\lambda\left(A_{1}+\cdots+A_{m}\right)} F_{s}\left(\left\{\lambda A_{j}\right\}_{j=1, \ldots, m}\right)-I\right\|_{2}
$$

If we consider the Taylor series expansion for the exponential functions in the expression on the right, we obtain the matrix power series in terms of $\lambda A_{j}$, where all the terms involving $\lambda^{k}, k \leq s$, should cancel out due to the choice of the parameters $\left\{\tau_{i j}\right\}_{i=1, \ldots, r ; j=1, \ldots, m}$. Further, we would like to make use of the so-called projection operator $\Psi_{s}$, which in the case of scalar functions $f(t)=\sum_{k=0}^{\infty} \alpha_{k} t^{k}$ is defined as follows: $\Psi_{s}(f(t)):=\sum_{k=s+1}^{\infty} \alpha_{k} t^{k}$. This operator can be applied to matrix power series in a straightforward way. Therefore,

$$
\begin{aligned}
& \left\|e^{-\lambda\left(A_{1}+\cdots+A_{m}\right)} F_{S}\left(\left\{\lambda A_{j}\right\}_{j=1, \ldots, m}\right)-I\right\|_{2} \\
& \quad=\left\|\Psi_{s}\left(e^{-\lambda\left(A_{1}+\cdots+A_{m}\right)} F_{S}\left(\left\{\lambda A_{j}\right\}_{j=1, \ldots, m}\right)\right)\right\|_{2} .
\end{aligned}
$$

Next observe that

$$
\begin{aligned}
\left\|\Psi_{s}\left(e^{-\lambda\left(A_{1}+\cdots+A_{m}\right)} F_{s}\left(\left\{\lambda A_{j}\right\}_{j=1, \ldots, m}\right)\right)\right\|_{2} & \leq \Psi_{s}\left(e^{|\lambda|\left(\sum_{k=1}^{m}\left\|A_{k}\right\|\left(1+\sum_{j=1}^{r}\left|\tau_{j k}\right|\right)\right)}\right) \\
& \leq C_{s}|\lambda|^{s+1}\left(\left\|A_{1}\right\|_{2}+\cdots+\left\|A_{m}\right\|_{2}\right)^{s+1}
\end{aligned}
$$

where the first inequality follows from repeatedly applying the triangle inequality to the matrix power series, and the second is the crude estimate of the corresponding Taylor series by its leading term. From here the statement of the lemma follows.

So far we were neither able to derive nor could we find in the literature an error bound for a splitting formula of order greater than two, where the participating factors were involved in commutator relations similar to those in (20), (21).

## 6 Proof of Theorem 1

We are finally ready to prove the main result of this paper. Note that the constants in the estimates below in general depend on $Q, \alpha, N, s$, and $k$, but they are independent of other parameters, in particular, of the final degree $n$ of the polynomial loop $Q_{n}$.

Recall that an arbitrary loop $Q(t) \in \operatorname{Lip}_{\alpha}(\mathbb{T} \rightarrow \mathrm{SO}(N)), N \geq 3, \alpha>1 / 2$, can be factorized as follows:

$$
Q(t)=\left(\prod_{j=1}^{N-2} Q_{0, j} e^{X_{j}(t)}\right) \hat{P}_{k}(t) e^{X_{N-1}(t)} .
$$

The polynomial loop $\hat{P}_{k}(t)$ is defined according to (9), and we assigned $X_{N-1}(t):=$ $\Delta(t) \hat{\Phi}$ to keep the notation uniform $(\Delta(t)$ and $\hat{\Phi}$ are defined in Theorem 2). The approximation can be carried out factor by factor. In more detail, suppose we have constructed the polynomial loops $P_{j}(t)$ of degree $\leq n$ in $\mathrm{SO}(N)$ such that

$$
\left\|e^{X_{j}(t)}-P_{j}(t)\right\|_{C} \leq \epsilon, \quad j=1, \ldots, N-1 .
$$

Then

$$
P(t):=\left(\prod_{j=1}^{N-2} Q_{0, j} P_{j}(t)\right) \hat{P}_{k}(t) P_{N-1}(t)
$$

is a polynomial loop in $\Pi_{n}(\mathbb{T} \rightarrow \mathrm{SO}(N))$ of degree $\leq(N-1) n+k$, $(k$ is the degree of the polynomial $\hat{P}_{k}(t)$ ), and $P(t)$ satisfies the estimate

$$
\begin{equation*}
\|Q(t)-P(t)\|_{C} \leq(N-1) \epsilon, \tag{23}
\end{equation*}
$$

which is easily obtained using Lemma 3. Therefore, we further concentrate on how one should construct a polynomial $P_{j}(t)$.

For any $m>1$, we can approximate $X_{j}(t) \in \operatorname{Lip}_{\alpha}(\mathbb{T} \rightarrow \mathfrak{s o}(N)), j=1, \ldots$, $N-1$, by an $\mathfrak{s o}(N)$-valued polynomial loop $X_{j, m}(t)$ of degree $\leq m$ at the optimal rate (say, by applying the de la Vallée Poussin means componentwise), i.e.,

$$
\begin{equation*}
\left\|e^{X_{j}(t)}-e^{X_{j, m}(t)}\right\|_{C} \leq \frac{C_{\alpha}}{m^{\alpha}}\left|X_{j}\right|_{\operatorname{Lip}_{\alpha}}, \quad m>0 \tag{24}
\end{equation*}
$$

(see Lemma 1), and

$$
\begin{equation*}
X_{j, m}(t):=\sum_{l=1}^{L} A_{m, l}(t):=\sum_{l=1}^{L} \sum_{k=0}^{m} c_{l, k} B_{l, k}(t), \quad L=N(N-1), \tag{25}
\end{equation*}
$$

where $\left\{B_{l, k}(t)\right\}_{l=1, \ldots, L ; k=0, \ldots, m}$ is the designated basis over $\mathbb{R}$ for the linear space of polynomial loops $\Pi_{m}(\mathbb{T} \rightarrow \mathfrak{s o}(N)$ ) (see Sect. 3 for the details on the construction of the basis). For simplicity of notation, the dependence of the coefficients $c_{l, k}$ in (25) on $j$ and $m$ is not made explicit. Moreover, for even $l$ the terms with $k=0$ are redundant. We group the basis elements of the same type $l$ into $A_{m, l}(t)$ in order to apply the property (6). For any $l$, the entries of the polynomial loop $A_{m, l}(t)$ are derived from the entries of the initial loop $X_{j, m}(t)$ by separating even and odd parts of the trigonometric polynomials and their conjugates and taking their linear combinations, analogous to the proof of the basis property for $\left\{B_{l, k}(t)\right\}_{l=1, \ldots, L ; k=0, \ldots, m}$ given in Sect. 3. The remaining effort goes into approximating $\exp \left(X_{j, m}(t)\right)$, for which we will use higher-order splitting methods. Since the same approximation procedure is carried out for each $j$, we henceforth drop the index $j$.

We define

$$
F\left(\left\{A_{m, l}(t) / M\right\}_{l=1, \ldots, L}\right):=e^{\frac{1}{M} A_{m, 1}(t)} e^{\frac{1}{M} A_{m, 2}(t)} \cdots e^{\frac{1}{M} A_{m, L}(t)}
$$

In conjunction with (22), we can construct

$$
\begin{aligned}
& F_{S}\left(\left\{A_{m, l}(t) / M\right\}_{l=1, \ldots, L}\right) \\
& \quad:=F\left(\left\{\tau_{1} A_{m, l}(t) / M\right\}_{l=1, \ldots, L}\right) \cdots F\left(\left\{\tau_{r} A_{m, l}(t) / M\right\}_{l=1, \ldots, L}\right),
\end{aligned}
$$

which is the order $s$ splitting formula for $e^{\sum_{l=1}^{L} A_{m, l}(t) / M}$, i.e.,

$$
e^{\sum_{l=1}^{L} A_{m, l}(t) / M}=F_{s}\left(\left\{A_{m, l}(t) / M\right\}_{l=1, \ldots, L}\right)+\mathcal{O}\left(M^{-(s+1)}\right)
$$

and we assume that the appropriate conditions on the parameters $\tau_{i}, i=1, \ldots, r$ are satisfied. We use Lemma 3 and Lemma 7 to obtain the estimate

$$
\begin{align*}
& \left\|e^{\sum_{l=1}^{L} A_{m, l}(t)}-\left(F_{S}\left(\left\{A_{m, l}(t) / M\right\}_{l=1, \ldots, L}\right)\right)^{M}\right\|_{C} \\
& \quad=\left\|\left(e^{\sum_{l=1}^{L} A_{m, l}(t) / M}\right)^{M}-\left(F_{s}\left(\left\{A_{m, l}(t) / M\right\}_{l=1, \ldots, L}\right)\right)^{M}\right\|_{C} \\
& \quad \leq M\left\|e^{\frac{1}{M} \sum_{l=1}^{L} A_{m, l}(t)}-F_{s}\left(\left\{A_{m, l}(t) / M\right\}_{l=1, \ldots, L}\right)\right\|_{C}<\frac{C}{M^{s}} \tag{26}
\end{align*}
$$

Next we consider each of the factors $F\left(\left\{\tau_{i} A_{m, l}(t) / M\right\}_{l=1, \ldots, L}\right)$. By construction,

$$
F\left(\left\{\tau_{i} A_{m, l}(t) / M\right\}_{l=1, \ldots, L}\right)=\prod_{l=1}^{L} e^{\left(\tau_{i} / M\right) A_{m, l}(t)}=\prod_{l=1}^{L} e^{\left(\tau_{i} / M\right) \sum_{k=0}^{m} c_{l, k} B_{l, k}(t)} .
$$

Let us define

$$
P^{l}\left(\left\{\tau_{i} c_{l, k} B_{l, k}(t) / M\right\}_{k=0, \ldots, m}\right):=\prod_{k=0}^{m} e^{\left(\tau_{i} / M\right) c_{l, k} B_{l, k}(t)}
$$

Note that $P^{l}$ is already a polynomial loop in the group of degree $2 m$ according to (6). We again make use of the higher-order splitting formula (22), this time in conjunction
with $P^{l}\left(\left\{\tau_{i} c_{l, k} B_{l, k}(t) / M\right\}_{k=0, \ldots, m}\right)$,

$$
\begin{aligned}
P_{s}^{l} & \left(\left\{\tau_{i} c_{l, k} B_{l, k}(t) / M\right\}_{k=0, \ldots, m}\right) \\
& =P^{l}\left(\left\{\tau_{i 1} c_{l, k} B_{l, k}(t) / M\right\}_{k=0, \ldots, m}\right) \cdots P^{l}\left(\left\{\tau_{i r} c_{l, k} B_{l, k}(t) / M\right\}_{k=0, \ldots, m}\right)
\end{aligned}
$$

which generates the polynomial loop in the group of degree $\leq 2 \mathrm{rm}$. Next we apply Lemma 7 to $e^{\left(\tau_{i} / M\right) \sum_{k=0}^{m} c_{l, k} B_{l, k}(t)}$ to obtain the inequality

$$
\begin{align*}
& \left\|e^{\left(\tau_{i} / M\right) \sum_{k=0}^{m} c_{l, k} B_{l, k}(t)}-P_{s}^{l}\left(\left\{\tau_{i} c_{l, k} B_{l, k}(t) / M\right\}_{k=0, \ldots, m}\right)\right\|_{C} \\
& \quad \leq \frac{C}{M^{s+1}}\left(\sum_{k=0}^{m}\left|c_{l, k}\right|\left\|B_{l, k}(t)\right\|_{C}\right)^{s+1} . \tag{27}
\end{align*}
$$

Recall that $c_{l, k}$ can be obtained as linear combinations of the coefficients of trigonometric polynomials approximating the functions from the Hölder class $\operatorname{Lip}_{\alpha}(\mathbb{T} \rightarrow \mathbb{C})$ (Sect. 3), and therefore should decay with order $1 /(k+1)^{\alpha}$ (as in (2)). Hence,

$$
\sum_{k=0}^{m}\left|c_{l, k}\right|\left\|B_{l, k}(t)\right\|_{C} \leq C \sum_{k=0}^{m}(k+1)^{-\alpha} \leq C^{\prime},
$$

where the constant $C^{\prime}>0$ is independent of the number of splitting terms $m$ if the corresponding series is convergent, which holds for Hölder classes of loops with $\alpha>1$. By the same reasoning, the constant in (27) can be uniformly bounded with respect to the number of splitting terms $m$. Note that the restriction on $\alpha$ comes from the lack of more precise error estimates for higher-order splitting methods.

With these preparations, we can write down the final formula for the approximation of $e^{X_{j}(t)}$ :

$$
P_{j}(t):=\left(\prod_{i=1}^{r} \prod_{l=1}^{L} P_{s}^{l}\left(\left\{\tau_{i} c_{l, k} B_{l, k}(t) / M\right\}_{k=0, \ldots, m}\right)\right)^{M} .
$$

Note that the degree of the polynomial $P_{j}(t)$ does not exceed $2 L r^{2} m M$ (or when substituting the value of $L, 2 N(N-1) r^{2} m M$, resp.). We apply Lemma 3 repeatedly to deduce that

$$
\begin{aligned}
\| & \left(F_{S}\left(\left\{A_{m, l}(t) / M\right\}_{l=1, \ldots, L}\right)\right)^{M}-P_{j}(t) \|_{C} \\
= & \|\left(\prod_{i=1}^{r} \prod_{l=1}^{L} e^{\left(\tau_{i} / M\right) \sum_{k=0}^{m} c_{l, k} B_{l, k}(t)}\right)^{M} \\
& -\left(\prod_{i=1}^{r} \prod_{l=1}^{L} P_{s}^{l}\left(\left\{\tau_{i} c_{l, k} B_{l, k}(t) / M\right\}_{k=0, \ldots, m}\right)\right)^{M} \|_{C}
\end{aligned}
$$

$$
\begin{align*}
& \leq M r L \max _{i, l}\left\|e^{\left(\tau_{i} / M\right) \sum_{k=0}^{m} c_{l, k} B_{l, k}(t)}-P_{s}^{l}\left(\left\{\tau_{i} c_{l, k} B_{l, k}(t) / M\right\}_{k=0, \ldots, m}\right)\right\|_{C} \\
& \leq \frac{C}{M^{s}} \tag{28}
\end{align*}
$$

Note that here the constant depends on the order of the splitting method $s$ as well as the number of stages of the splitting method $r$, which is also a function of $s$. Combining this result with (26) and using the triangle inequality,

$$
\begin{aligned}
\left\|e^{\sum_{l=1}^{L} A_{m, l}(t)}-P_{j}(t)\right\|_{C} \leq & \left\|e^{\sum_{l=1}^{L} A_{m, l}(t)}-\left(F_{s}\left(\left\{A_{m, l}(t) / M\right\}_{l=1, \ldots, L}\right)\right)^{M}\right\|_{C} \\
& +\left\|\left(F_{s}\left(\left\{A_{m, l}(t) / M\right\}_{l=1, \ldots, L}\right)\right)^{M}-P_{j}(t)\right\|_{C} \leq \frac{C}{M^{s}}
\end{aligned}
$$

Finally, using (24) and the above estimate, we obtain

$$
\left\|e^{X_{j}(t)}-P_{j}(t)\right\|_{C} \leq\left\|e^{X_{j}(t)}-e^{X_{j, m}(t)}\right\|_{C}+\left\|e^{X_{j, m}(t)}-P_{j}(t)\right\|_{C} \leq C\left(\frac{1}{m^{\alpha}}+\frac{1}{M^{s}}\right)
$$

Therefore, substitution into (23) yields

$$
\begin{equation*}
\|Q(t)-P(t)\|_{C} \leq(N-1) \max _{j}\left\|e^{X_{j}(t)}-P_{j}(t)\right\|_{C} \leq C\left(\frac{1}{m^{\alpha}}+\frac{1}{M^{s}}\right) \tag{29}
\end{equation*}
$$

In order for the degree of the polynomial $P(t)$ to satisfy

$$
\begin{equation*}
2 N(N-1)^{2} r^{2} m M+k \leq n, \quad \text { for } n>k \tag{30}
\end{equation*}
$$

we must choose $m$ to be the integer part of $(n-k)^{\frac{s}{\alpha+s}}$ and $M$ to be the integer part of $\left(2 N(N-1)^{2} r^{2}\right)^{-1}(n-k)^{\frac{\alpha}{\alpha+s}}$. With this notation, (29) becomes

$$
\|Q(t)-P(t)\|_{C} \leq \frac{C}{(n-k)^{s \alpha /(\alpha+s)}}=\frac{C}{(n-k)^{\alpha-\alpha^{2} /(\alpha+s)}}
$$

Hence,

$$
\|Q(t)-P(t)\|_{C} \leq \frac{C}{n^{\alpha-\epsilon}}, \quad \epsilon=\alpha^{2} /(\alpha+s)
$$

where the constant $C$ now also depends on $k$. This establishes the claim of the theorem, if for given $\alpha>1$ and $\epsilon>0$, we choose the order $s$ of the splitting method large enough.

## 7 Concluding Remarks

There are several remarks regarding Theorem 1. A shortcoming of the result is that the constant $C(\alpha, N, Q, \epsilon)$ depends on $Q$ in a nonspecified way. In particular, it also depends on the order of a splitting method $s$. However, the latter is less of a problem. In fact, specifying a splitting method and optimizing the estimate in (29) with respect
to $s$ leads to sharper results about the convergence rate. It follows from (28) that the right-hand side in (29) can be further estimated by

$$
C(\alpha, N, Q)\left(\frac{1}{m^{\alpha}}+\frac{r(s) C(s)}{M^{s}}\right),
$$

where $C(\alpha, N, Q), C(s)>0$ are constants depending on the listed parameters and $r(s)$ is the number of stages in the splitting method. Recall that $r(s)=3^{s^{\prime}-1}$ for the Yoshida-Suzuki splitting of order $2 s^{\prime}$. We can assume that asymptotically $C(s) \sim$ $r(s)$ and rewrite the expression in parenthesis as follows:

$$
\begin{equation*}
\frac{1}{m^{\alpha}}+\frac{R(s)}{M^{s}}, \quad R(s)=r^{2}(s) \tag{31}
\end{equation*}
$$

We would like to minimize the above expression with respect to the parameters $m, M$ which satisfy the following constraint:

$$
\begin{equation*}
R(s) m M \leq n, \quad R(s)=r^{2}(s) . \tag{32}
\end{equation*}
$$

Note that the above condition is analogous to (30). Here the degree $n$ is rescaled by a constant depending only on $N$ and shifted by $k$, which has no effect on the asymptotic behavior we are interested in when $n \rightarrow \infty$. Letting $m$ to be the integer part of $R(s)^{-\frac{s+1}{\alpha+s}} n^{\frac{s}{\alpha+s}}$ and $M$ the integer part of $R(s)^{-1+\frac{s+1}{\alpha+s}} n^{\frac{\alpha}{\alpha+s}}$ fulfills the condition (32). Also, (31) becomes

$$
\frac{2}{m^{\alpha}}=\frac{2}{n^{\alpha}}\left(R(s)^{\frac{s+1}{\alpha+s}} n^{\frac{\alpha}{\alpha+s}}\right)^{\alpha} \leq \frac{2}{n^{\alpha}}\left(R(s) n^{\alpha / s}\right)^{\alpha}, \quad \alpha>1 .
$$

Therefore, the problem is reduced to minimizing $R(s) n^{\alpha / s}$ with respect to $s$. In particular, after substituting $R(s)=3^{s}$, it is easy to verify that $\ln \left(3^{s} n^{\alpha / s}\right)$ (and hence $\left.3^{s} n^{\alpha / s}\right)$ achieves its minimum at $s=\sqrt{\frac{\alpha}{\ln 3} \ln n}$. Then $\min _{s} 3^{s} n^{\alpha / s}=n^{\frac{C^{\prime}(\alpha)}{\sqrt{\ln n}}}$, where $C^{\prime}(\alpha)$ is some constant depending on $\alpha$, and hence

$$
C(\alpha, N, Q)\left(\frac{1}{m^{\alpha}}+\frac{r(s) C(s)}{M^{S}}\right) \leq C(\alpha, N, Q) \frac{n^{\frac{C^{\prime}(\alpha)}{\sqrt{1 n} n}}}{n^{\alpha}} .
$$

Finally, we observe that $(\ln n)^{\gamma} \ll n^{\frac{\beta}{\sqrt{\ln n}}} \ll n^{\epsilon}$ for any choice of the positive constants $\epsilon, \beta, \gamma$.

Another important remark is that the restriction $\alpha>1$ arises from the use of the crude error estimate in Lemma 7. For example, a more accurate error bound for the second-order method (21), if applied to the set $\left\{c_{j, k} B_{j, k}(t)\right\}_{k=1, \ldots, m}$, would lead to the estimate of the right-hand side in (21) by a sum of the form $\sum_{k=1}^{m}(\log k)^{2} k^{-3 \alpha}$ (see Lemma 2), which is uniformly bounded for $\alpha>1 / 3$. In contrast, using the estimate in Lemma 7 with $s=2$ leads to the constant factor of the form $\left(\sum_{k=1}^{m} k^{-\alpha}\right)^{3}$, and the uniform bound exists for $\alpha>1$. Unfortunately, error estimates for splitting methods of order greater than 2 in terms of iterated commutator relations are currently not known. Note also that the bound $\alpha>1 / 2$ follows from the particular choice of the
factorization method we used for loops. Generalizing the problem to the case of $\alpha>0$ would probably require a different approach.

In our approach we had to deal with topological properties of loops, which led to setting the lower bound $k$ on the degree of the polynomial loops. As we are interested in the asymptotic behavior for $n \rightarrow \infty$, this does not pose any problems. From a practical point of view, large $k$ can be undesirable. So far we can only bridge this gap by choosing $P(t)=I$, which gives the trivial bound $\|Q(t)-I\|_{C} \leq 2$.

Approximation of loops can be pursued for unit spheres $S^{N-1} \in \mathbb{R}^{N}, N \geq 3$. Recall that the rotation group $\mathrm{SO}(N)$ acts transitively on $S^{N-1}$. Consider $\underline{q}(t) \in$ $\operatorname{Lip}_{\alpha}\left(\mathbb{T} \rightarrow S^{N-1}\right)$. It is possible to construct a loop $Q(t) \in \operatorname{Lip}_{\alpha}(\mathbb{T} \rightarrow \mathrm{SO}(N))$ such that the first column of $Q(t)$ equals $q(t)$, i.e., $Q(t) \underline{e}_{1}=\underline{q}(t)$. Here is the sketch of the construction of $Q(t) \in \operatorname{Lip}_{\alpha}(\mathbb{T} \rightarrow \mathrm{SO}(N))$ :

1. There exists a point $v \in S^{N-1}$ and $r>0$ such that $\underline{q}(t) \cap C(v, r)=\varnothing$ for any $t \in \mathbb{T}$, where $C(v, r)$ is a spherical cap of radius $r$ (the argument for finding $v$ and $r$ is similar to that in Lemma 5).
2. Define $u(t):=\frac{q(t)-v}{\|\underline{q}(t)-v\|} \in \operatorname{Lip}_{\alpha}\left(\mathbb{T} \rightarrow S^{N-1}\right)$, with which we associate the Householder matrix $H_{u}(t)=I-u(t) u(t)^{T}$. We construct $\tilde{Q}(t) \in \operatorname{Lip}_{\alpha}(\mathbb{T} \rightarrow \operatorname{SO}(N))$ from $H_{u}(t)$ by multiplying the last column by -1 .
3. $Q(t):=\tilde{Q}(t) V$, were $V \in \operatorname{SO}(N)$ satisfies $V \underline{e}_{1}=v$.

Further, we construct a sequence of $Q_{n} \in \Pi_{n}(\mathbb{T} \rightarrow \mathrm{SO}(N))$, which approximate $Q(t)$ with known rate as $n \rightarrow \infty$. It remains to observe that the first columns of $Q_{n}(t)$ are trigonometric loops in $\Pi_{n}\left(\mathbb{T} \rightarrow S^{N-1}\right)$, which approximate $\underline{q}(t)$ with the same rate.

Open Access This article is distributed under the terms of the Creative Commons Attribution Noncommercial License which permits any noncommercial use, distribution, and reproduction in any medium, provided the original author(s) and source are credited.

## References

1. Adams, F.: Lectures on Lie Groups. University of Chicago Press, Chicago (1982)
2. Deimling, K.: Nonlinear Functional Analysis. Springer, New York (1985)
3. DeVore, R.A., Lorentz, G.G.: Constructive Approximation. Springer, Berlin (1993)
4. Lawton, W.M.: Conjugate quadrature filters. In: Lau, K.-S. (ed.) Advances in Wavelets, pp. 103-119. Springer, Berlin (1999)
5. Lawton, W.M.: Hermite interpolation in loop groups and conjugate quadrature filter approximation. Acta Appl. Math. 84, 315-349 (2004)
6. McLachlan, R.I., Quispel, G.R.W.: Splitting methods. Acta Numer. 11, 341-434 (2002)
7. Oswald, P., Shingel, T.: Splitting methods for $\operatorname{SU}(\mathrm{N})$ loop approximation. J. Approx. Theory 161, 174-186 (2009)
8. Oswald, P., Shingel, T.: Close-to-optimal bounds for $\mathrm{SU}(\mathrm{N})$ loop approximation. J. Approx. Theory (2008). doi:10.1016/j.jat.2010.04.006
9. Oswald, P., Madsen, C.K., Konsbruck, R.L.: Analysis of scalable PMD compensators using FIR filters and wevelength-dependent optical measurements. J. Lightwave Technol. 22(2), 647-657 (2004)
10. Presley, A., Segal, G.: Loop Groups. Oxford Univ. Press, London (1986)
11. Rossmann, W.: Lie Groups: An Introduction Through Linear Groups. Oxford Univ. Press, London (2002)
12. Sheng, Q.: Global error estimates for exponential splitting. IMA J. Numer. Anal. 14, 27-57 (1993)
13. Strang, G., Nguyen, T.: Wavelets and Filter Banks. Cambridge University Press, Cambridge (1996)
14. Suzuki, M.: Decomposition formulas of exponential operators and Lie exponentials with some applications to quantum mechanics and statistical physics. J. Math. Phys. 26, 601-612 (1985)
15. Zanna, A., Munthe-Kaas, H.Z.: Generalized polar decompositions for the approximation of the matrix exponential. SIAM J. Matrix Anal. Appl. 23(3), 840-862 (2002)

[^0]:    Communicated by Erik Koelink.
    The work was done while at the University of Cambridge.
    T. Shingel ( $\boxtimes$ )

    University of California, San Diego, USA
    e-mail: tshingel@math.ucsd.edu

