Ming Liao

# Decomposition of stochastic flows and Lyapunov exponents 

Received: 19 November 1998 / Revised version: 1 October 1999 /
Published online: 14 June 2000 - (c) Springer-Verlag 2000


#### Abstract

Let $\phi_{t}$ be the stochastic flow of a stochastic differential equation on a compact Riemannian manifold $M$. Fix a point $m \in M$ and an orthonormal frame $u$ at $m$, we will show that there is a unique decomposition $\phi_{t}=\xi_{t} \psi_{t}$ such that $\xi_{t}$ is isometric, $\psi_{t}$ fixes $m$ and $D \psi_{t}(u)=u s_{t}$, where $s_{t}$ is an upper triangular matrix. We will also establish some convergence properties in connection with the Lyapunov exponents and the decomposition $D \phi_{t}(u)=u_{t} s_{t}$ with $u_{t}$ being an orthonormal frame. As an application, we can show that $\psi_{t}$ preserves the directions in which the tangent vectors at $m$ are dilated at fixed exponential rates.


## 1. Introduction

Consider an sde (stochastic differential equation) on a compact connected $d$-dimensional Riemannian manfold $M$ of the following form.

$$
\begin{equation*}
d x_{t}=\sum_{j=1}^{r} X_{j}\left(x_{t}\right) \circ d w_{t}^{j}+X_{0}\left(x_{t}\right) d t \tag{1}
\end{equation*}
$$

where $X_{0}, X_{1}, \ldots, X_{r}$ are (smooth) vector fields on $M, w_{t}=\left(w_{t}^{1}, \ldots, w_{t}^{r}\right)$ is an $r$-dimensional standard Brownian motion defined on a probability space $(\Omega, \mathscr{F}, P)$, and $\circ d$ denotes the Stratonovich stochastic differential. The sde (1) can also be written more concisely as $d x_{t}=\sum_{j=0}^{r} X_{j}\left(x_{t}\right) \circ d w_{t}^{j}$, where $w_{t}^{0}=t$.

Let $\operatorname{Diff}(M)$ be the group of diffeomorphisms: $M \rightarrow M$. A stochastic flow of the sde (1) is a process $\phi_{t}$ in $\operatorname{Diff}(M)$ with $\phi_{0}=\mathrm{id}_{M}$, the identity map on $M$, such that $\forall x \in M, x_{t}=\phi_{t}(x)$ is a solution of (1). The process $x_{t}=\phi_{t}(x)$ is called the one point motion of $\phi_{t}$ and is a diffusion process on $M$.

Let $D \phi_{t}$ be the differential of the random map $\phi_{t}: M \rightarrow M$. For $x \in M$, $D \phi_{t}(x)$ is a linear map: $T_{x} M \rightarrow T_{\phi_{t}(x)} M$. If $u=\left(u_{1}, \ldots, u_{d}\right)$ is a linear frame at $x$, then $D \phi_{t}(x)(u)=\left(D \phi_{t}(x)\left(u_{1}\right), \ldots, D \phi_{t}(x)\left(u_{d}\right)\right)$ is a linear frame at $\phi_{t}(x)$. For simplicity, we may write $D \phi_{t}(u)$ for $D \phi_{t}(x)(u)$. For a $d \times d$ matrix $g=\left\{g_{i j}\right\}$, let $u g=\left(\sum_{i} u_{i} g_{i 1}, \ldots, \sum_{i} u_{i} g_{i d}\right)$. This is a linear frame at $x$ if $g$ is non-singular. Note that $D \phi_{t}(u g)=D \phi_{t}(u) g$.

[^0]Mathematics Subject Classfication (1991): Primary 58G32; Secondary 60H10

Let $I(M)$ be the group of isometries on $M$. This is a Lie group.
Fix a point $m \in M$ and an orthonormal frame $u$ at $m$. Under an additional hypothesis, which is automatically satisfied if $M$ is a sphere, we will show in Section 3 that there is a unique decomposition of $\phi_{t}$ in the form $\phi_{t}=\xi_{t} \circ \psi_{t}$, where $\xi_{t}$ is a process in $I(M)$ and $\psi_{t}$ is a process in $\operatorname{Diff}(M)$ such that $\xi_{0}=\psi_{0}=\mathrm{id}_{M}$, $\psi_{t}(m)=m$ and $D \psi_{t}(u)=u s_{t}$ for some process $s_{t}$ in the group $S$ of upper triangular matrices with positive diagonal elements. Moreover, $\xi_{t}$ is a diffusion process in $I(M)$, and if the stochastic flow $\phi_{t}$ is invariant under $I(M), \xi_{t}$ will be left invariant, so the normalized Haar measure on $I(M)$ will be a stationary measure for $\xi_{t}$.

Let $\lambda_{1} \geq \lambda_{2} \geq \cdots \geq \lambda_{d}$ be the Lyapunov exponents of the stochastic flow $\phi_{t}$. It turns out that the component $\psi_{t}$ not only fixes the point $m$, it also preserves the directions in which the tangent vectors at $m$ are dilated at the fixed exponential rates $\lambda_{i}$. To show this, we will establish some convergence properties in connection to a decomposition of $D \phi_{t}$. This discussion given in sections 4 and 5 will be independent of the decomposition $\phi_{t}=\xi_{t} \psi_{t}$.

Let $O(M)$ be the bundle of orthonormal frames on $M$. Note that $u_{t}=D \xi_{t}(u) \in$ $O(M)$ and $D \phi_{t}(u)=u_{t} s_{t}$. In general, for any $u \in O(M)$, let $u_{t} \in O(M)$ be obtained from $D \phi_{t}(u)$ by performing a standard Gram-Schmidt orthogonalization procedure. Then $D \phi_{t}(u)=u_{t} s_{t}$ with $s_{t} \in S$.

Let $G=G L(d, R)_{+}$be the group of $d \times d$ real matrices of positive determinants and let $K=S O(d)$ be the subgroup of orthogonal matrices. Let $s_{t}=p_{t} a_{t}^{+} k_{t}$ and $s_{t}=a_{t} n_{t}$ be respectively a polar and the Iwasawa decompositions of $s_{t}$, where $p_{t}, k_{t} \in K$, and $a_{t}^{+}, a_{t}$ are diagonal matrices and $n_{t}$ is an upper triangular matrix with diagonal elements all equal to 1 . By Oseledec's multiplicative ergodic theorem and a lemma in linear algebra, we show in Section 4 that if all the Lyapunov exponents are simple, then almost surely, $\lim _{t \rightarrow \infty}(1 / t) \log a_{t}=\lim _{t \rightarrow \infty}(1 / t) \log a_{t}^{+}=$ $\operatorname{diag}\left(e^{\lambda_{1}}, \ldots, e^{\lambda_{d}}\right)$, and both $k_{t}$ and $n_{t}$ converge as $t \rightarrow \infty$. Some of these properties have been mentioned in [6], we provide more complete proofs here.

The component $\psi_{t}$ in the decomposition $\phi_{t}=\xi_{t} \psi_{t}$, defined by a given orthonormal frame $u=\left(u_{1}, \ldots, u_{d}\right)$ at $m \in M$, fixes the point $m$, so $D \psi_{t}$ is a linear map: $T_{m} M \rightarrow T_{m} M$. From the convergence properties mentioned above, when $t$ is large, $D \psi_{t}$ can be regarded as a fixed random linear map, followed by a dilation along each axis $u_{i}$ at the exponential rate $\lambda_{i}$.

The case of multiple exponents requires more elaborate arguments and is treated in Section 5.

## 2. Some geometric preliminaries

Let $X$ be a vector field on $M$. The flow $\eta_{t}$ of $X$ is a smooth family of diffeomorphisms on $M$ indexed by $t \geq 0$ such that $\forall x \in M, y_{t}=\eta_{t}(x)$ is a solution of the ordinary differential equation $(d / d t) y_{t}=X\left(y_{t}\right)$ and $\eta_{0}=\operatorname{id}_{M}$. If $\eta_{t}$ is an isometry for all $t \geq 0$, then $X$ is called an infinitesimal isometry.

Let $L(M)$ be the bundle of linear frames on $M$. A frame $u \in L(M)$ at $x \in M$ is a basis $\left(u_{1}, \ldots, u_{d}\right)$ in $T_{x} M$. We will let $\pi: L(M) \rightarrow M$ be the natural projection given by $\pi(u)=x$. Let $G=G L(d, R)_{+}$be the group of $d \times d$ real
matrices of positive determinant. Its Lie algebra $\mathscr{G}$ is the space of $d \times d$ matrices equipped with the Lie bracket $[A, B]=A B-B A$. For $u=\left(u_{1}, \cdots, u_{d}\right) \in L(M)$ and $g \in G, u g=\left(\sum_{i} u_{i} g_{i 1}, \cdots, \sum_{i} u_{i} g_{i d}\right)$ is a frame at $\pi(u)$. Given $A \in \mathscr{G}$, let $u A=(d / d t)\left[u e^{t A}\right]_{t=0}$, the tangent vector to the curve $t \mapsto u e^{t A}$ in $L(M)$ at $t=0$. Such vectors are called the vertical vectors and they form a subspace $T_{u}^{v} L(M)$ of $T_{u} L(M)$.

For $X \in T_{x} M$, let $z_{t}$ be a curve in $M$ with $\left.(d / d t) z_{t}\right|_{t=0}=X$ and let $u_{t}$ be the parallel displacement of $u$ along $z_{t}$. Let $H(X)(u)=\left.(d / d t) u_{t}\right|_{t=0}$, called the horizontal lift of $X$ to $L(M)$ at $u$. Then $T_{u}^{h} L(M)=\left\{H(X)(u) ; X \in T_{x} M\right\}$ is a subspace of $T_{u} L(M)$ and any element in $T_{u}^{h} L(M)$ is called a horizontal vector at $u$. We have $T_{u} L(M)=T_{u}^{h} L(M) \oplus T_{u}^{v} L(M)$ (direct sum).

Let $K=S O(d)$ be the subgroup of $G$ formed by orthogonal matrices. Its Lie algebra $\mathscr{K}$ is the space of skew-symmetric matrices. Let $O(M)$ be the bundle of orthonormal frames on $M$. Then $O(M) \subset L(M)$. We will let $\pi_{o}: O(M) \rightarrow M$ be the restriction of $\pi: L(M) \rightarrow M$. For $u \in O(M), X \in T_{x} M$ and $A \in \mathscr{K}$, both $H(X)(u)$ and $u A$ are contained in $T_{u} O(M)$. In fact,

$$
T_{u} O(M)=\left\{H(X)(u) ; X \in T_{x} M\right\} \oplus\{u A ; A \in \mathscr{K}\} .
$$

Let $S$ be the subgroup of $G$ formed by upper triangular matrices with positive diagonal elements. Its Lie algebra $\mathscr{S}$ is the space of all upper triangular matrices. Any $g \in G$ can be written uniquely as $g=k s$ with $k \in K$ and $s \in S$. Indeed, this decomposition can be obtained by performing a Gram-Schmidt orthogonalization procedure on the set of column vectors of $g$. At the Lie algebra level, any $A \in \mathscr{G}$ can be written uniquely as $A=A_{\mathscr{K}}+A_{\mathscr{S}}$ with $A_{\mathscr{K}} \in \mathscr{K}$ and $A_{\mathscr{S}} \in \mathscr{S}$.

Let $u \mathscr{S}=\{u A ; A \in \mathscr{S}\}$. For $u \in O(M)$, we have

$$
\begin{equation*}
T_{u} L(M)=T_{u} O(M) \oplus u \mathscr{S} \tag{2}
\end{equation*}
$$

For $Y \in T_{u} L(M)$, let $Y_{O}$ be the $T_{u} O(M)$-component of $Y$ in the above decomposition.

For a vector field $X$ on $M$ with flow $\eta_{t}$, its natural lift to $L(M)$ is a vector field on $L(M)$ defined by $\delta X(u)=\left.(d / d t) D \eta_{t}(u)\right|_{t=0}$. For $Y \in T_{x} M$, let $\nabla_{Y} X=\nabla X(Y)$ be the covariant derivative defined by the Riemannian connection. We may write $\nabla X(u)=\left(\nabla X\left(u_{1}\right), \ldots, \nabla X\left(u_{d}\right)\right)$. Then there is a unique matrix $\tilde{X}(u) \in \mathscr{G}$ such that $\nabla X(u)=u \tilde{X}(u)$. If $u \in O(M)$, then

$$
\begin{equation*}
[\tilde{X}(u)]_{j k}=\left\langle u_{j}, \nabla X\left(u_{k}\right)\right\rangle \tag{3}
\end{equation*}
$$

where $\langle\cdot, \cdot\rangle$ is the Riemannian metric.
Lemma 1. Let $X$ be a vector field on $M$ and $u \in L(M)$. Then

$$
\begin{equation*}
\delta X(u)=H(X)(u)+u \tilde{X}(u)=H(X)(u)+u[\tilde{X}(u)]_{\mathscr{K}}+u[\tilde{X}(u)]_{\mathscr{S}} . \tag{4}
\end{equation*}
$$

Consequently, if $u \in O(M)$, then $[\delta X(u)]_{O}=H(X)(u)+u[\tilde{X}(u)]_{\mathscr{K}}$.

Proof. Let $\eta_{t}$ be the flow of $X$. We may construct a frame field $U$ in a neighborhood of $x=\pi(u)$ with $U=u$ at $x$ such that $D \eta_{t}(U(x))=U\left(\eta_{t}(x)\right)$. Then the Lie bracket $[X, U](x)=\left.(d / d t) D \eta_{t}^{-1}\left[U\left(\eta_{t}(x)\right)\right]\right|_{t=0}=\left.(d / d t) U(x)\right|_{t=0}=0$ and $\nabla_{X} U=\nabla_{U} X+[X, U]=\nabla_{U} X$ at $x$. Let $\Pi_{t}$ denote the parallel displacement along the curve $t \mapsto \eta_{t}(x)$. We have $D \eta_{t}(u)=\Pi_{t}(u) g_{t}$ for some $g_{t} \in G$ with $g_{0}$ equal to the identity matrix, and

$$
\delta X(u)=\frac{d}{d t}\left[\Pi_{t}(u) g_{t}\right]_{t=0}=\frac{d}{d t}\left[\Pi_{t}(u)\right]_{t=0}+\left.\frac{d}{d t}\left(u g_{t}\right)\right|_{t=0} .
$$

The first term on the right hand side of above is $H(X)(u)$ and the second term is

$$
\frac{d}{d t}\left[\Pi_{t}^{-1}\left(D \eta_{t}(u)\right)\right]_{t=0}=\frac{d}{d t}\left[\Pi_{t}^{-1}\left(U\left(\eta_{t}(x)\right)\right)\right]_{t=0}=\nabla_{X} U(x)=\nabla_{U} X(x)=\nabla_{u} X
$$

Recall that $I(M)$ is the isometry group on $M$. Let $\mathscr{I}$ be its Lie algebra. This is a space of vector fields on $M$ which are infinitesimal isometries. It is clear that if $X \in \mathscr{I}$ and $u \in O(M)$, then $\delta X(u) \in T_{u} O(M)$.

Lemma 2. For $u \in O(M)$, the linear map: $\mathscr{I} \rightarrow T_{u} O(M)$ defined by $X \mapsto \delta X(u)$ is injective. Moreover, if $M$ is a sphere, then it is also surjective.

Proof. If $X, Y \in \mathscr{I}$ and $\delta X(u)=\delta Y(u)$, then $X-Y$ is an infinitesimal isometry which fixes $u$, so its flow $\eta_{t}$ will leave all the geodesics starting at $\pi_{o}(u)$ invariant. By the connectedness of $M, \eta_{t}=\mathrm{id}_{M}$ and $X-Y=0$. This proves the injectivity. If $M$ is a sphere, then the differentials of isometries on $M$ are transitive on $O(M)$, hence, $O(M)=\{D \xi(u) ; \xi \in I(M)\}$. From this it follows that $T_{u} O(M)=\{\delta X(u)$; $X \in \mathscr{I}\}$.

## 3. Decomposition of the stochastic flow

Let $m \in M$ and $u \in O(M)$ with $\pi_{o}(u)=m$ be fixed in this section. Recall that $\phi_{t}$ is the stochastic flow of the sde (1) which contains vector fields $X_{0}, X_{1}, \ldots, X_{r}$, and for $Y \in T_{u} L(M), Y_{O}$ is the $T_{u} O(M)$-component of $Y$ in the decomposition (2). Let $\delta \mathscr{I}(u)=\{\delta X(u) ; X \in \mathscr{I}\}$, the image of the map given in Lemma 2. Note that if $X$ is a vector field on $M$ and $\eta \in \operatorname{Diff}(M)$, then $D \eta(X)$ is a vector field on $M$ given by $D \eta(X)(x)=D \eta\left(X\left(\eta^{-1}(x)\right)\right.$ for $x \in M$. We will assume

$$
\begin{equation*}
\forall i=0,1, \ldots, r \text { and } \forall \xi \in \mathscr{I}(M), \quad\left[\delta D \xi\left(X_{j}\right)(u)\right] o \in \delta \mathscr{I}(u) . \tag{5}
\end{equation*}
$$

This hypothesis is automatically satisfied if $M$ is a sphere because then by Lemma 2, $\delta \mathscr{I}(u)=T_{u} O(M)$.

Theorem 1. Under the hypothesis (5), the stochastic flow $\phi_{t}$ of the sde (1) has a unique decomposition $\phi_{t}=\xi_{t} \psi_{t}$, where $\xi_{t}$ is a process in $I(M)$ and $\psi_{t}$ is a process in $\operatorname{Diff}(M)$ such that $\xi_{0}=\psi_{0}=i d_{M}, \psi_{t}(m)=m$ and $D \psi_{t}(u)=u s_{t}$ for some process $s_{t} \in S$. Moreover, $\xi_{t}$ is a diffusion process in $I(M)$ and $\psi_{t}$ is the stochastic flow of an sde on $M$ with random and time dependent vector fields.

Proof. Let $\mathscr{J}$ be the linear space of the vector fields $X$ on $M$ such that $[\delta X(u)]_{o} \in$ $\delta \mathscr{I}(u)$. By (5), $\mathscr{J}$ contains $D \xi\left(X_{j}\right)$ for $j=0,1, \ldots, r$ and $\xi \in I(M)$. By Lemma 2, for any $X \in \mathscr{J}$, there is a unique $J(X) \in \mathscr{I}$ such that

$$
\begin{equation*}
\delta J(X)(u)=[\delta X(u)]_{O} \tag{6}
\end{equation*}
$$

Note that $J(X)(m)=X(m)$. By (6) and Lemma 1,

$$
\begin{equation*}
\delta X(u)=\delta J(X)(u)+u[\tilde{X}(u)] \mathscr{S} \tag{7}
\end{equation*}
$$

By Section I. 4 in [3] (see also [6]), the derivative process $D \phi(u)$ satisfies the following sde on $L(M)$.

$$
\begin{equation*}
d D \phi_{t}(u)=\sum_{j=0}^{r} \delta X_{j}\left(D \phi_{t}(u)\right) \circ d w_{t}^{j} \tag{8}
\end{equation*}
$$

Note that the term $\delta X_{0}\left(D \phi_{t}(u)\right) d t$ is absorbed in the summation with $w_{t}^{0}=t$. The equation (8) can be derived from (1) with $x_{t}$ replaced by $\phi_{t}(x)$ and taking derivatives with respect to $x$ under local coordinates.

For $\xi \in I(M)$ and $Y \in \mathscr{I}$, let $\xi Y$ and $Y \xi$ be respectively the tangent vectors at $T_{\xi} I(M)$ obtained by left and right translations of $Y$. Thus $\xi \mapsto \xi Y(Y \xi)$ may be regarded as a left (right) invariant vector field on $I(M)$.

We may write $X^{J}$ for $J(X)$. Let $\xi_{t}$ be the solution of the following sde on $I(M)$ with $\xi_{0}=\mathrm{id}_{M}$.

$$
\begin{equation*}
d \xi_{t}=\sum_{j=0}^{r} \xi_{t}\left[D \xi_{t}^{-1}\left(X_{j}\right)\right]^{J} \circ d w_{t}^{j} \tag{9}
\end{equation*}
$$

Since the vector fields involved in the above sde depend only on $\xi_{t}$, we see that $\xi_{t}$ is a diffusion process on $I(M)$.

Since $\xi_{t}^{-1} \xi_{t}=\operatorname{id}_{M},\left(\circ d \xi_{t}^{-1}\right) \xi_{t}+\xi_{t}^{-1}\left(o d \xi_{t}\right)=0$. By (9), we obtain an sde for $\xi_{t}^{-1}$.

$$
\begin{equation*}
d \xi_{t}^{-1}=-\sum_{j=0}^{r}\left[D \xi_{t}^{-1}\left(X_{j}\right)\right]^{J} \xi_{t}^{-1} \circ d w_{t}^{j} \tag{10}
\end{equation*}
$$

For $x \in M$, let $x_{t}=\phi_{t}(x)$ and $y_{t}=\xi_{t}^{-1}\left(x_{t}\right)$. By (1) and (10), we have

$$
\begin{aligned}
d y_{t} & =D \xi_{t}^{-1}\left(\circ d x_{t}\right)+\left(\circ d \xi_{t}^{-1}\right)\left(x_{t}\right) \\
& =\sum_{j=0}^{r}\left\{D \xi_{t}^{-1}\left(X_{j}\left(x_{t}\right)\right)-\left[D \xi_{t}^{-1}\left(X_{j}\right)\right]^{J}\left(\xi_{t}^{-1}\left(x_{t}\right)\right)\right\} \circ d w_{t}^{j} \\
& =\sum_{j=0}^{r}\left\{D \xi_{t}^{-1}\left(X_{j}\right)-\left[D \xi_{t}^{-1}\left(X_{j}\right)\right]^{J}\right\}\left(y_{t}\right) \circ d w_{t}^{j}
\end{aligned}
$$

For $X \in \mathscr{J}$, let $X^{H}=X-X^{J}$. Then $X^{H}(m)=0$, and by (7),

$$
\begin{equation*}
\delta X^{H}(u)=u[\tilde{X}(u)]_{\mathscr{C}} . \tag{11}
\end{equation*}
$$

We have proved that $y_{t}$ is a solution of the the following sde on $M$.

$$
\begin{equation*}
d y_{t}=\sum_{j=0}^{r}\left[D \xi_{t}^{-1}\left(X_{j}\right)\right]^{H}\left(y_{t}\right) \circ d w_{t}^{j} \tag{12}
\end{equation*}
$$

The vector fields $\left[D \xi_{t}^{-1}\left(X_{j}\right)\right]^{H}$ of the above sde are random and time dependent, whose natural lifts $\delta\left[D \xi_{t}^{-1}\left(X_{j}\right)\right]^{H}$ can still be defined by fixing $t$ and $\omega$. Since $X^{H}(m)=0$ for any $X \in \mathscr{J}$, it follows that $\left[D \xi_{t}^{-1}\left(X_{j}\right)\right]^{H}(m)=0$, hence, if $y_{0}=m$, then $y_{t}=m$ for all $t>0$.

Let $\psi_{t}=\xi_{t}^{-1} \phi_{t}$. Then $\psi_{t}$ is a process in $\operatorname{Diff}(M)$ and is the stochastic flow of (12) in the sense that $y_{t}=\psi_{t}(y)$ is a solution of (12) for any $y \in M$. The derivative process $D \psi_{t}(u)$ satisfies the sde

$$
\begin{equation*}
d D \psi_{t}(u)=\sum_{j=0}^{r} \delta\left[D \xi_{t}^{-1}\left(X_{j}\right)\right]^{H}\left(D \psi_{t}(u)\right) \circ d w_{t}^{j} \tag{13}
\end{equation*}
$$

This can be proved by the same method used to prove (8).
Since $\psi_{t}(m)=m, D \psi_{t}(u)=u s_{t}$ for some process $s_{t} \in G$. By (13) and (11), we obtain an sde for $s_{t}$.

$$
\begin{equation*}
d s_{t}=\sum_{j=0}^{r}\left\{\left[D \xi_{t}^{-1}\left(X_{j}\right)\right]^{\sim}(u)\right\}_{\mathscr{S}} s_{t} \circ d w_{t}^{j} . \tag{14}
\end{equation*}
$$

Since the vector fields in the above sde are contained in $\mathscr{S}$ and $s_{0}$ is the identity matrix, it follows that $s_{t}$ is a process in $S$.

It remains to prove the uniqueness of the decomposition. Since $D \phi_{t}(u)=$ $D \xi_{t}\left(D \psi_{t}(u)\right)=D \xi_{t}(u) s_{t}$ and $s_{t} \in S$, we see that the orthonormal frame $D \xi_{t}(u)$ $=\left(D \xi_{t}\left(u_{1}\right), \ldots, D \xi_{t}\left(u_{d}\right)\right)$ can be obtained by performing a standard Gram-Schmidt orthogonalization procedure to $D \phi_{t}(u)=\left(D \phi_{t}\left(u_{1}\right), \ldots, D \phi_{t}\left(u_{d}\right)\right)$. It follows that $D \xi_{t}(u)$ is uniquely determined by $D \phi_{t}(u)$. Since $\xi \in I(M)$ is determined by $D \xi(u)$, the theorem is proved.

Remark 1. The uniqueness part of the proof for Theorem 1 in fact shows the uniqueness of decomposition $\phi_{t}=\xi_{t} \psi_{t}$ without assuming $\xi_{0}=\psi_{0}=\mathrm{id}_{M}$. Conversely, given any $\xi_{0} \in I(M)$ and $\psi_{0} \in \operatorname{Diff}(M)$ with $\psi_{0}(m)=m$ and $D \psi_{0}(u)=$ $u s$ for some $s \in S$, we can obtain a decomposition $\phi_{t}=\xi_{t} \psi_{t}$, which has all the properties stated in Theorem 1 except $\xi_{0}=\psi_{0}=\mathrm{id}_{M}$, just by solving (9) with $\xi_{0}$ as the initial point and then setting $\psi_{t}=\xi_{t}^{-1} \phi_{t}$.

Let $M=S^{n-1}$ be the $(n-1)$-dimensional sphere. Then $J(X)$ given by ( 6 ) is defined for any vector field $X$ on $M$. We will now obtain an explicit expression for $J(X)$. Consider $S^{n-1}$ as the unit sphere embedded in $R^{n}$ and let $\left(x_{1}, x_{2}, \ldots, x_{n}\right)$ be the standard coordinates of $R^{n}$. Let $\partial_{i}=\left(\partial / \partial x_{i}\right)$. Fix the point $m=(0, \ldots, 0,1)$ on $S^{n-1}$. Let $u=\left(\partial_{1}, \ldots, \partial_{n-1}\right)$. This is an orthonormal frame at $m$ for $S^{n-1}$. We may express $X$ as

$$
\begin{equation*}
X(x)=\sum_{j=1}^{n} a_{j}(x) \partial_{j} \tag{15}
\end{equation*}
$$

for some smooth functions $a_{j}(x)$ on $S^{n-1}$ satisfying $\sum_{j=1}^{n} x_{j} a_{j}(x)=0$. For $1 \leq i<j \leq n$, let $Z_{i j}=x_{i} \partial_{j}-x_{j} \partial_{i}$. The flow of this vector field is the unit speed rotation in the coordinate plane $\left(x_{i}, x_{j}\right)$. In fact, $\left\{Z_{i j} ; 1 \leq 1<j \leq n\right\}$ is a basis for the Lie algebra $\mathscr{I}$ of infinitesimal isometries on $S^{n-1}$. We will show

$$
\begin{equation*}
J(X)=-\sum_{i=1}^{n-1} a_{i}(m) Z_{i n}+\sum_{1 \leq i<j \leq(n-1)} \partial_{i} a_{j}(m) Z_{i j} \tag{16}
\end{equation*}
$$

Note that for $1 \leq i \leq(n-1), \partial_{i} \in T_{m} S^{n-1}$, so $\partial_{i} a_{j}(m)$ is well defined.
We extend $X$ to a neighborhood of $S^{n-1}$ in $R^{n}$ by setting $X(x)=X(x /|x|)$. Then $\sum_{i=1}^{n} x_{j} a_{j}(x)=0$ for $x$ in this neighborhood, hence,

$$
\begin{equation*}
a_{n}(m)=0 \quad \text { and } \quad a_{i}(m)+\partial_{i} a_{n}(m)=0 \text { for } 1 \leq i \leq(n-1) \tag{17}
\end{equation*}
$$

Let $\eta(t, x)$ be flow of $X$. For the moment, assume $X(m)=0$. Then $\delta X(u)$ is the same as its vertical component $[\delta X(u)]^{v}$. We have

$$
D \eta(u)=\left(D \eta\left(\partial_{1}\right), \ldots, D \eta\left(\partial_{n-1}\right)\right)=\left(\sum_{i=1}^{n} \partial_{1} \eta_{i} \partial_{i}, \ldots, \sum_{i=1}^{n} \partial_{n-1} \eta_{i} \partial_{i}\right)
$$

Since $(d / d t) \eta_{i}=a_{i}(\eta),(d / d t) \partial_{j} \eta_{i}=\sum_{k=1}^{n} \partial_{k} a_{i}(\eta) \partial_{j} \eta_{k}$ and $(d / d t) \partial_{j} \eta_{i}(0, m)=$ $\partial_{j} a_{i}(m)$. By (17), $\partial_{j} a_{n}(m)=-a_{j}(m)=0$ for $1 \leq j \leq(n-1)$, we have

$$
\delta X(u)=\left.\frac{d}{d t} D \eta(u)\right|_{t=0}=\left(\sum_{i=1}^{n-1} \partial_{1} a_{i}(m) \partial_{i}, \ldots, \sum_{i=1}^{n-1} \partial_{n-1} a_{i}(m) \partial_{i}\right)=u A
$$

where $A$ is the $(n-1) \times(n-1)$ matrix given by $A_{i j}=\partial_{j} a_{i}(m)$. It follows that if $X=x_{j} \partial_{i}$ for $i \leq j$, then $\delta X(u) \in u \mathscr{S}$.

We now remove the assumption that $X(m)=0$. With $x_{n}=\sqrt{1-\sum_{i=1}^{n-1} x_{i}^{2}}$, we may consider $X$ as a function of $x^{\prime}=\left(x_{1}, \ldots, x_{n-1}\right)$ and will find its Taylor expansion at $m$ up to the second order. Let $O\left(\left|x^{\prime}\right|^{2}\right)$ denote any function on $S^{n-1}$ which converges to 0 as $x^{\prime} \rightarrow 0$ (that is, as $x \rightarrow m$ ) in the order of $\left|x^{\prime}\right|^{2}=\sum_{i=1}^{(n-1)} x_{i}^{2}$. We will also use $O\left(\left|x^{\prime}\right|^{2}\right)$ to denote any vector field on $S^{n-1}$ whose components are such functions. Note that if $X=O\left(\left|x^{\prime}\right|^{2}\right)$, then $\delta X(u)=0$. Moreover, $x_{n}=$ $1+O\left(\left|x^{\prime}\right|^{2}\right), \partial_{i} x_{n}=-x_{i} / x_{n}$, and

$$
\partial_{i}\left[a_{j}\left(x_{1}, \ldots, x_{n-1}, \sqrt{1-\left|x^{\prime}\right|^{2}}\right)\right]_{x=m}=\partial_{i} a_{j}(m)
$$

for $1 \leq i \leq(n-1)$. By these comments and (17), we have

$$
\begin{aligned}
X(x) & =\sum_{j=1}^{n} a_{j}(x) \partial_{j} \\
& =\sum_{j=1}^{n-1} a_{j}(m) \partial_{j}+\sum_{i=1}^{n-1} \sum_{j=1}^{n-1} \partial_{i} a_{j}(m) x_{i} \partial_{j}+\sum_{j=1}^{n-1} \partial_{j} a_{n}(m) x_{j} \partial_{n}+O\left(\left|x^{\prime}\right|^{2}\right)
\end{aligned}
$$

$$
\begin{aligned}
= & \sum_{j=1}^{n-1} a_{j}(m)\left[x_{n} \partial_{j}-x_{j} \partial_{n}\right]+\sum_{1 \leq i<j \leq(n-1)} \partial_{i} a_{j}(m)\left[x_{i} \partial_{j}-x_{j} \partial_{i}\right] \\
& +\sum_{j=1}^{n-1} \partial_{j} a_{j}(m) x_{j} \partial_{j}+\sum_{1 \leq i<j \leq(n-1)}\left[\partial_{j} a_{i}(m)+\partial_{i} a_{j}(m)\right] x_{j} \partial_{i}+O\left(\left|x^{\prime}\right|^{2}\right) \\
= & -\sum_{j=1}^{n-1} a_{j}(m) Z_{j n}+\sum_{1 \leq i<j \leq(n-1)} \partial_{i} a_{j}(m) Z_{i j}+\sum_{j=1}^{n-1} \partial_{j} a_{j}(m) x_{j} \partial_{j} \\
& +\sum_{1 \leq i<j \leq(n-1)}\left[\partial_{j} a_{i}(m)+\partial_{i} a_{j}(m)\right] x_{j} \partial_{i}+O\left(\left|x^{\prime}\right|^{2}\right)
\end{aligned}
$$

Now (16) follows from the above and the fact that $\delta\left(x_{j} \partial_{i}\right)(u) \in u \mathscr{S}$ for $i \leq j$.
The diffusion process $\xi_{t}$ on $\mathrm{I}(M)$ is called left invariant if for any $\xi \in \mathrm{I}(M)$, $\xi \xi_{t}$ is equal in distribution to the same diffusion process starting at $\xi \xi_{0}$. It is well known that if $\xi_{t}$ is left invariant, then the normalized Haar measure on $\mathrm{I}(M)$ is a stationary measure of $\xi_{t}$. Recall that a stationary measure of a Markov process is a probability measure on the state space such that if the process started with this measure as the initial distribution, then it will have the same distribution at all time.

The stochastic flow $\phi_{t}$ will be called invariant under $\mathrm{I}(M)$ if for any $\xi \in \mathrm{I}(M)$, $\xi \phi_{t} \xi^{-1} \cong \phi_{t}$ (equal in distribution as processes in $\operatorname{Diff}(M)$ ). Note that $\xi \phi_{t} \xi^{-1}$ is the stochastic flow of the sde $d x_{t}=\sum_{j=0}^{r} D \xi\left(X_{j}\right)\left(x_{t}\right) \circ d w_{t}^{j}$. If $X_{0}=0$ and if for any $\xi \in \mathrm{I}(M), D \xi\left(X_{j}\right)=\sum_{i=1}^{r} \alpha_{i}^{j}(\xi) X_{i}$, where $\alpha(\xi)=\left\{\alpha_{i}^{j}(\xi)\right\}$ is an $r \times r$ orthogonal matrix, then this sde can be written as $d x_{t}=\sum_{j=1}^{r} X_{j}\left(x_{t}\right) \circ d \beta_{t}^{j}$, where $\beta_{t}=\alpha(\xi) w_{t}$ is an $r$-dimensional Brownian motion. Therefore, in this case, $\phi_{t}$ is invariant under $\mathrm{I}(M)$.

Theorem 2. Assume $\phi_{t}$ is invariant under $I(M)$. Then $\xi_{t}$ is left invariant.
Proof. It suffices to show that for any $\xi \in I(M)$, if $\xi_{t}^{\prime}$ is the solution of (9) (replacing $\xi_{t}$ by $\xi_{t}^{\prime}$ ) with $\xi_{0}^{\prime}=\xi$, then $\xi_{t}^{\prime} \cong \xi \xi_{t}$ (equal in distribution as processes in $\mathrm{I}(M)$ ). By Remark 1, we have the unique decomposition $\phi_{t} \xi=\xi_{t}^{\prime} \psi_{t}^{\prime}$, where $\psi_{t}^{\prime}$ is a process in $\operatorname{Diff}(M)$ such that $\psi_{t}^{\prime}(m)=m$ and $D \psi_{t}^{\prime}(u)=u s_{t}^{\prime}$ for some $s_{t}^{\prime} \in S$. On the other hand, $\xi \xi_{t} \psi_{t}=\xi \phi_{t}=\xi \phi_{t} \xi^{-1} \xi \cong \phi_{t} \xi$. This proves $\xi \xi_{t} \cong \xi_{t}^{\prime}$ and $\psi_{t} \cong \psi_{t}^{\prime}$.

## 4. Lyapunov exponents

The discussion in this and the next sections will shed light on the decomposition given in Theorem 1, but it will be independent of this decomposition and the hypothesis (5) will not be assumed.

As before, let $\phi_{t}$ be the stochastic flow of the sde (1). We will assume that its one point motion has an ergodic stationary measure $\rho$. This assumption is implied by the following Hörmander type condition: the Lie algebra $\operatorname{Lie}\left(X_{1}, \ldots\right.$, $X_{r}$ ) generated by the vector fields $X_{1}, \ldots, X_{r}$ in (1) spans $T_{x} M$ for any $x \in M$.

By applying the Oseledec Multiplicative Ergodic Theorem to stochastic flows (see [1] or [2]), we can show that for $\rho \times P$-almost all $(x, \omega)$,

$$
\begin{equation*}
\left[D \phi_{t}(x)^{*} D \phi_{t}(x)\right]^{1 / 2 t} \rightarrow \Lambda(x, \omega) \text { as } t \rightarrow \infty \tag{18}
\end{equation*}
$$

where $D \phi_{t}(x)^{*}: T_{\phi_{t}(x)} M \rightarrow T_{x} M$ is the adjoint operator of $D \phi_{t}(x): T_{x} M \rightarrow$ $T_{\phi_{t}(x)} M$ defined relative to the Riemannian metric $\langle\cdot, \cdot\rangle$, and $\Lambda(x, \omega)$ is a selfadjoint operator on $T_{x} M$ with eigenvalues

$$
e^{\lambda_{1}} \geq e^{\lambda_{2}} \geq \cdots \geq e^{\lambda_{d}}
$$

independent of $(x, \omega)$. Let $l$ be the number of distinct eigenvalues. Let $0=i_{0}<$ $i_{1}<i_{2}<\cdots<i_{l}=d$ be the indices so that $\lambda_{i}$ jumps at $i_{k}$ for $1 \leq k \leq(l-1)$, that is,

$$
\begin{equation*}
\lambda_{1}=\cdots=\lambda_{i_{1}}>\lambda_{i_{1}+1}=\cdots=\lambda_{i_{2}}>\lambda_{i_{2}+1} \cdots \cdots \cdot \lambda_{i_{l-1}}>\lambda_{i_{l-1}+1}=\cdots=\lambda_{d} \tag{19}
\end{equation*}
$$

Let $E_{k}(x, \omega)$ be the eigenspace of $\Lambda(x, \omega)$ corresponding to the eigenvalue $e^{\lambda_{i_{k}}}$ and let $V_{k}(x, \omega)=\sum_{j=k}^{l} E_{j}(x, \omega)$ (direct sum). Then for $1 \leq k \leq l$,

$$
\begin{equation*}
\forall Y \in\left[V_{k}(x, \omega)-V_{k+1}(x, \omega)\right], \quad \lim _{t \rightarrow \infty} \frac{1}{t} \log \left\|D \phi_{t}(x)(Y)\right\|=\lambda_{i_{k}}, \tag{20}
\end{equation*}
$$

where $\|\cdot\|=\langle\cdot, \cdot\rangle^{1 / 2}$ and $V_{l+1}(x, \omega)=\{0\}$.
Note that under the Hörmander type condition mentioned earlier, the one point motion $x_{t}=\phi_{t}(x)$ has a positive smooth transition density with respect to the Riemannian measure on $M$. In this case, using the Markov property of $x_{t}$, we can show that the conclusions of the last paragraph in fact hold for all $x \in M$ almost surely.

The numbers $\lambda_{1} \geq \lambda_{2} \geq \cdots \geq \lambda_{d}$ are called the Lyapunov exponents of the stochastic flow $\phi_{t}$, which are exponential rates at which the lengths of the tangent vectors change under the flow and are in fact independent of the Riemannian metric. The number of times an exponent repeats itself in the above list is called its multiplicity. An exponent will be called simple if its multiplicity is equal to 1 . Note that the subspaces $V_{k}(x, \omega)$ form a nested sequence $T_{x} M=V_{1}(x, \omega) \supset \cdots \supset V_{l}(x, \omega)$, called the filtration of $T_{x} M$ determined by the Lyapunov exponents.

We now recall some basic facts about the matrix group $G=G L(d, R)_{+}$. For a general semisimple Lie group, these properties are discussed in great detail in [5], see also [4]. Although $G$ is not semisimple, $G$ is a direct product of the semisimple group $S L(d, R)$ and the multiplication group $R_{+}=(0, \infty)$, where $S L(d, R)$ is the subgroup of $G$ consisting of the $d \times d$ real matrices of determinant 1. Therefore, all these properties hold also for $G$ with $R_{+}$absorbed by the subgroup $A$ to be defined below.

Let $A$ be the subgroup of $G$ formed by the diagonal matrices with positive diagonal elements. This is an abelian group and its Lie algebra $\mathscr{A}$ is the space of all diagonal matrices. For $a \in A$, we will let $\log a$ be the unique element of $\mathscr{A}$ such that $\exp (\log a)=a$. Let $\mathscr{A}_{+}$be the subset of $\mathscr{A}$ consisting of diagonal matrices with strictly descending diagonal elements and let $\overline{\mathscr{A}_{+}}$be its closure.

Let $K=S O(d)$, the subgroup of $G$ consisting of orthogonal matrices of determinant 1 . Any $g \in G$ has a polar decomposition $g=p a^{+} k$ with $a^{+} \in \exp \left(\mathscr{A}_{+}\right)$ and $p, k \in K$. Although $a^{+}$is uniquely determined by $g,(p, k)$ is not. All possible choices for $(p, k)$ are given by ( $p m, m^{-1} k$ ) with $m$ ranging over the centralizer of $a^{+}$in $K$, that is, $m \in K$ with $m a^{+} m^{-1}=a^{+}$.

Let $\Theta$ be a subset of $\{1,2, \ldots,(d-1)\}$ and let $i_{1}<i_{2}<\cdots<i_{l}$ be the integers in $\{1,2, \ldots, d\}$ which are not contained in $\Theta$. Then $i_{l}=d$. Let $K_{\Theta}$ be the subgroup of $K$ which leaves the following subspaces of $R^{d}$ invariant.

$$
\begin{align*}
& E_{1}=\operatorname{span}\left(e_{1}, \ldots, e_{i_{1}}\right), \quad E_{2}=\operatorname{span}\left(e_{i_{1}+1}, \ldots, e_{i_{2}}\right), \ldots, \\
& E_{l}=\operatorname{span}\left(e_{i_{l-1}+1}, \ldots, e_{d}\right), \tag{21}
\end{align*}
$$

where $\left\{e_{1}, e_{2}, \ldots, e_{d}\right\}$ is the standard basis of $R^{d}$. The non-zero elements of a matrix in $K_{\Theta}$ are contained in $l$ sub-matrices arranged along the diagonal. Note that if $\Theta \subset \Theta^{\prime}$, then $K_{\Theta} \subset K_{\Theta^{\prime}}$, and $K_{\emptyset}$ is the subgroup of $K$ formed by the diagonal matrices with diagonal elements equal to $\pm 1$, where $\emptyset$ is the empty set.

From now on, unless explicitly stated otherwise, we will let $\Theta$ be the set of integers $i$ with $1 \leq i \leq(d-1)$ such that $\lambda_{i}=\lambda_{i+1}$. Then $K_{\Theta}$ is the centralizer of $\operatorname{diag}\left(e^{\lambda_{1}}, \ldots, e^{\lambda_{d}}\right)$ in $K$, and the integers $i_{k}$ coincide with those given by (19).

Let $u \in L(M)$ with $x=\pi(u)$. We may think $u$ as a linear map: $R^{d} \rightarrow T_{x} M$ defined by $\eta=\left(\eta_{1}, \ldots, \eta_{d}\right) \mapsto u \eta=\sum_{i} u_{i} \eta_{i}$. The adjoint map $u^{*}: T_{x} M \rightarrow R^{d}$ is defined by $\left\langle u^{*} Y, \eta\right\rangle_{0}=\langle Y, u \eta\rangle$ for $Y \in T_{x} M$ and $\eta \in R^{d}$, where $\langle\cdot, \cdot\rangle_{0}$ is the usual Euclidean inner product. It is easy to check that if $u \in O(M)$, then $u^{*}=u^{-1}$.

For $u \in O(M)$, the frame $D \phi_{t}(u)$ is in general not orthonormal, but by performing a standard Gram-Schmidt orthogonalization procedure to $D \phi_{t}(u)$, we obtain $D \phi_{t}(u)=u_{t} s_{t}$, where $u_{t} \in O(M)$ and $s_{t} \in S$. We may regard the matrix $s_{t}$ as a linear map: $R^{d} \rightarrow R^{d}$ as usual. Then $D \phi_{t}(x)=D \phi_{t}(u) u^{-1}=u_{t} s_{t} u^{-1}$. Let $s_{t}=p_{t} a_{t}^{+} k_{t}$ be a polar decomposition of $s_{t}$. We may write $U_{t}(u, \omega), s_{t}(u, \omega)$, $a_{t}^{+}(u, \omega)$ and $k_{t}(u, \omega)$ for $u_{t}, s_{t}, a_{t}^{+}$and $k_{t}$ to indicate their dependence on the initial frame $u$ and $\omega$. Note that although $k_{t}(u, \omega)$ is not uniquely determined by $s_{t}(u, \omega)$, the left coset $K_{\Theta} k_{t}(u, \omega)$ is when $t$ is large because then $K_{\Theta}$ contains the centralizer of $a_{t}^{+}$in $K$.

Lemma 3. For almost all $(x, \omega) \in M \times \Omega$ and all $u \in \pi_{o}^{-1}(x)$,

$$
\begin{equation*}
\lim _{t \rightarrow \infty} \frac{1}{t} \log a_{t}^{+}(u, \omega)=\operatorname{diag}\left\{\lambda_{1}, \lambda_{2}, \ldots, \lambda_{d}\right\} \tag{22}
\end{equation*}
$$

and $K_{\Theta} k_{t}(u, \omega) \rightarrow K_{\Theta} k_{\infty}(u, \omega)$ in the left coset space $K_{\Theta} \backslash K$ as $t \rightarrow \infty$ for some $k_{\infty}(u, \omega) \in K$. Moreover, the map $\Lambda: T_{x} M \rightarrow T_{x} M$ defined by (18) is given by

$$
\Lambda(u, \omega)=u k_{\infty}^{*}(u, \omega) \operatorname{diag}\left(e^{\lambda_{1}}, \ldots, e^{\lambda_{d}}\right) k_{\infty}(u, \omega) u^{-1}
$$

Proof. Since $D \phi_{t}(x)=u_{t} s_{t} u^{-1}, D \phi_{t}(x)^{*}=\left(u^{*}\right)^{-1} s_{t}^{*} u_{t}^{*}$, where $s_{t}^{*}$ is the matrix transpose of $s_{t}$. It follows that $D \phi_{t}(x)^{*} D \phi_{t}(x)=u\left(s_{t}^{*} s_{t}\right) u^{-1}$. By (18), for $\rho \times P$ almost all $(x, \omega)$ and all $u \in \pi_{o}^{-1}(x),\left[s_{t}(u, \omega)^{*} s_{t}(u, \omega)\right]^{1 / 2 t}$ converges to some symmetric matrix with eigenvalues $\left\{e^{\lambda_{1}}, e^{\lambda_{2}}, \ldots, e^{\lambda_{d}}\right\}$. This symmetric matrix may
be diagonalized with an orthogonal matrix, we have, $\left[s_{t}(u, \omega)^{*} s_{t}(u, \omega)\right]^{1 / 2 t} \rightarrow$ $k_{\infty}^{*} \operatorname{diag}\left(e^{\lambda_{1}}, \ldots, e^{\lambda_{d}}\right) k_{\infty}$ as $t \rightarrow \infty$, for some $k_{\infty} \in K$.

Since $s_{t}^{*} s_{t}=k_{t}^{*}\left(a_{t}^{+}\right)^{2} k_{t}$, we have $\left[s_{t}^{*} s_{t}\right]^{1 / 2 t}=k_{t}^{*} \exp \left[(1 / t) \log a_{t}^{+}\right] k_{t}$. Let $b$ and $k_{\infty}^{\prime}$ be respectively limiting points of $(1 / t) \log a_{t}^{+}$and $k_{t}$ as $t \rightarrow \infty$. Then

$$
k_{\infty}^{\prime *} \exp (b) k_{\infty}^{\prime}=k_{\infty}^{*} \exp \left[\operatorname{diag}\left(\lambda_{1}, \ldots, \lambda_{d}\right)\right] k_{\infty}^{*}
$$

By the uniqueness of the polar decomposition, $b=\operatorname{diag}\left(\lambda_{1}, \ldots, \lambda_{d}\right)$ and $k_{\infty}^{\prime} \in$ $K_{\Theta} k_{\infty}$.

Corollary 1. For $\rho \times P$-almost all $(x, \omega)$ and all $u \in \pi_{o}^{-1}(x)$, the eigenspace of $\Lambda(x, \omega)$ corresponding to the eigenvalue $\exp \left(\lambda_{i_{k}}\right)$ is given by $E_{k}(x, \omega)=$ $u k_{\infty}^{-1}(u, \omega) E_{k}$ for $1 \leq k \leq l$, where $E_{k}$ are subspaces of $R^{d}$ given by (21).

The process $u_{t}$ is a diffusion process in $O(M)$. As in [6], using Lemma 1 and (8), we can write down sde's satisfied by $u_{t}$ and $s_{t}$,

$$
\begin{equation*}
d u_{t}=\sum_{j=0}^{r}\left\{H\left(X_{j}\right)\left(u_{t}\right)+u_{t}\left[\tilde{X}_{j}\left(u_{t}\right)\right]_{\mathscr{K}}\right\} \circ d w_{t}^{j} \tag{23}
\end{equation*}
$$

and

$$
\begin{equation*}
d s_{t}=\sum_{j=0}^{r}\left[\tilde{X}_{j}\left(u_{t}\right)\right] \mathscr{\mathscr { S }} s_{t} \circ d w_{t}^{j} \tag{24}
\end{equation*}
$$

Note that $\left[\tilde{X}_{j}\left(u_{t}\right)\right] \mathscr{\mathscr { S }} s_{t}$ may be regarded as a matrix product.
Let $N$ be the subgroup of $G$ formed by the upper triangular matrices with diagonal elements all equal to 1 . We have the Iwasawa decomposition $G=K A N$ in the sense that the map $(h, a, n) \mapsto g=$ han is a diffeomorphism: $K \times A \times N \rightarrow G$. Note that $S=A N$, so if $s \in S$, then its Iwasawa decomposition $s=a n$ does not have a $K$-component. We will let $s_{t}=a_{t} n_{t}$ be the Iwasawa decomposition of the process $s_{\tilde{t}}$.

Let $\tilde{N}$ be the subgroup of $G$ formed by the lower triangular matrices with diagonal elements all equal to 1 . Both $N$ and $\tilde{N}$ are nilpotent subgroups of $G$. It is known that $\tilde{P}_{\Theta}=\tilde{N} A K_{\Theta}$ is a closed subgroup of $G$, called a boundary subgroup or parabolic subgroup. Note that the non-zero elements of a matrix in $\tilde{P}_{\Theta}$ are confined in the region on and below the "stairs" along the diagonal as shown in the following figure, where $0=i_{0}<i_{1}<i_{2}<\cdots<i_{l-1}<i_{l}=d$ are the indices given by (19).


It is known that $\tilde{P}_{\Theta} N$ is an open subset of $G$ whose complement has a positive co-dimension. Moreover, $Q_{\Theta}=\left\{k \in K ; k \in \tilde{P}_{\Theta} N\right\}$ is an open subset of $K$ (in relative topology) whose complement has a lower dimension in $K$.

The following lemma is just Lemme (2.23) in [4] which is valid for a general non-compact type semisimple Lie group $G$. Note that a different Iwasawa decomposition, namely $G=N A K$, is used in [4]. To get the lemma in the present form, we just need to take an inverse.

Lemma 4. Let $g_{j}$ be a sequence in $G$ with a polar decomposition $g_{j}=p_{j} a_{j}^{+} k_{j}$ and the Iwasawa decomposition $g_{j}=h_{j} a_{j} n_{j}$. Assume $K_{\Theta} k_{j} \rightarrow K_{\Theta} k_{\infty}$ in $\left(K_{\Theta} \backslash K\right)$ for some $k_{\infty} \in Q_{\Theta}, \forall i \in \Theta,\left(a_{j}^{+}\right)_{i} /\left(a_{j}^{+}\right)_{i+1} \leq C$ for some constant $C>0$, and $\forall i \notin \Theta$ with $1 \leq i \leq(d-1),\left(a_{j}^{+}\right)_{i} /\left(a_{\tilde{\tilde{P}}}^{+}\right)_{i+1} \rightarrow \infty$ as $j \rightarrow \infty$, where $\left(a_{j}^{+}\right)_{i}$ is the $i$-th diagonal element of $a_{j}^{+}$. Then $\tilde{P}_{\Theta} n_{j} \rightarrow \tilde{P}_{\Theta} k_{\infty}$ in $\left(\tilde{P}_{\Theta} \backslash G\right), a_{j}\left(a_{j}^{+}\right)^{-1}$ is contained in a compact subset of $A$, and $h_{j}=p_{j} p_{j}^{\prime}$ with $p_{j}^{\prime} \in K$ satisfying $p_{j}^{\prime} K_{\Theta} \rightarrow K_{\Theta}$ in $K / K_{\Theta}$.

For $x \in M$, the fiber $\pi_{0}^{-1}(x)$ may be identified with $K$ via the map $k \mapsto u k$ for some fixed $u \in \pi_{o}^{-1}(x)$, hence, the normalized Haar measure on $K$ induces a measure on $\pi_{o}^{-1}(x)$, which is independent of the choice of $u$. In the sequel, when we say something holds for almost all $u \in \pi_{o}^{-1}(x)$, it is this measure we are referring to.

Theorem 3. For $u \in O(M)$, let $D \phi_{t}(u)=u_{t} s_{t}$, where $u_{t} \in O(M)$ with $u_{0}=u$ and $s_{t} \in S$. Let $s_{t}=p_{t} a_{t}^{+} k_{t}$ and $s_{t}=a_{t} n_{t}$ be respectively a polar and the Iwasawa decompositions of $s_{t}$. Assume all the Lyapunov exponents are simple. Then for $\rho \times P$-almost all $(x, \omega) \in M \times \Omega$ and almost all $u \in \pi_{o}^{-1}(x)$,

$$
\begin{equation*}
\lim _{t \rightarrow \infty} \frac{1}{t} \log a_{t}^{+}(u, \omega)=\lim _{t \rightarrow \infty} \frac{1}{t} \log a_{t}(u, \omega)=\operatorname{diag}\left(e^{\lambda_{1}}, \ldots, e^{\lambda_{d}}\right) \tag{25}
\end{equation*}
$$

Moreover, as $t \rightarrow \infty, \quad K_{\emptyset} k_{t}(u, \omega) \rightarrow K_{\emptyset} k_{\infty}(u, \omega)$ for some $k_{\infty}(u, \omega) \in Q_{\emptyset}$, $n_{t}(u, \omega) \rightarrow n_{\infty}(u, \omega)$ for some $n_{\infty}(u, \omega) \in \tilde{P}_{\emptyset} k_{\infty}(u, \omega)$, and $p_{t}(u, \omega) K_{\emptyset} \rightarrow K_{\emptyset}$.

Proof. For any $k \in K, s_{t} k=k_{t}^{\prime} s_{t}^{\prime}$ for $k_{t}^{\prime} \in K$ and $s_{t}^{\prime} \in S$. On the other hand, $s_{t} k=p_{t} a_{t}^{+} k_{t} k$, hence, $s_{t}^{\prime}=\left(k_{t}^{\prime-1} p_{t}\right) a_{t}^{+}\left(k_{t} k\right)$ is a polar decomposition of $s_{t}^{\prime}$. Since $D \phi_{t}(u k)=u_{t} s_{t} k=\left(u_{t} k_{t}^{\prime}\right) s_{t}^{\prime}$ and $u_{t} k_{t}^{\prime} \in O(M)$, it follows that $k_{t}(u k, \omega)=$ $k_{t}(u, \omega) k$. Because all the Lyapunov exponents are simple, $\Theta=\emptyset$. By Lemma 3, $(1 / t) \log a_{t}^{+}(u, \omega) \rightarrow \operatorname{diag}\left\{\lambda_{1}, \ldots, \lambda_{\mathrm{d}}\right\}$ and $K_{\emptyset} k_{t}(u, \omega) \rightarrow K_{\emptyset} k_{\infty}(u, \omega)$ as $t \rightarrow$ $\infty$. Then $K_{\emptyset} k_{\infty}(u k, \omega)=K_{\emptyset} k_{\infty}(u, \omega) k$. Because the complement of $Q_{\emptyset}$ in $K$ has a lower dimension, it follows that for almost all $k \in K, k_{\infty}(u k, \omega) \in Q_{\emptyset}$. Now Lemma 4 with $\Theta=\emptyset$ can be applied to prove all the remaining claims. We note that $\tilde{P}_{\emptyset} n_{t} \rightarrow \tilde{P}_{\emptyset} k_{\infty}$ implies the convergence of $n_{t}$ because $N \cap \tilde{P}_{\emptyset}$ contains only the identity matrix, and $p_{t} K_{\emptyset} \rightarrow K_{\emptyset}$ is equivalent to $K_{\emptyset} p_{t} \rightarrow K_{\emptyset}$ because both mean that any limiting point of $p_{t}$ as $t \rightarrow \infty$ belongs to $K_{\emptyset}$.

Remark 2. Because $K_{\emptyset}$ is finite, we may choose the $k_{t}$ component properly so that $t \rightarrow k_{t}$ is continuous and $k_{t} \rightarrow k_{\infty}$ in Theorem 3 .

Remark 3. If the vector fields of the sde (23) satisfy the Hörmander type condition mentioned earlier, then $u_{t}$ has a smooth transition density. Using the Markov property of $u_{t}$, we can show that the conclusions of Theorem 3 hold for all $u \in O(M)$ almost surely.

Now let $\phi_{t}=\xi_{t} \psi_{t}$ and $D \psi_{t}(u)=u s_{t}$, with $u=\left(u_{1}, \ldots, u_{d}\right) \in \pi^{-1}(m)$ and $m \in M$, be the decompositions given by Theorem 1 . Then $D \psi_{t}(m)=u s_{t} u^{-1}=$ $u a_{t} n_{t} u^{-1}$ with $a_{t} \approx \operatorname{diag}\left(e^{\lambda_{1} t}, \ldots, e^{\lambda_{d} t}\right)$ and $n_{t} \rightarrow n_{\infty}$ as $t \rightarrow \infty$. Therefore, for large time $t>0$, the linear map $D \psi_{t}(m): T_{m} M \rightarrow T_{m} M$ may be regarded as a fixed random linear map $u n_{\infty} u^{-1}$, followed by $u a_{t} u^{-1}$ which is a dilation along each axis $u_{i}$ at an exponential rate $\lambda_{i}$.

## 5. Multiple exponents

We will prove in this section a version of Theorem 3 when the Lyapunov exponents are not simple. The main task is to prove the convergence of $\tilde{P}_{\Theta} n_{t}$ when $\Theta$ is not empty. Note that we cannot directly apply Lemma 4 when $\Theta \neq \emptyset$ because we do not know how to verify the condition that $\forall i \in \Theta,\left(a_{j}^{+}\right)_{i} /\left(a_{j}^{+}\right)_{i+1}$ is bounded. If such $i$ is excluded from $\Theta$, then the condition $K_{\Theta} k_{t} \rightarrow K_{\Theta} k_{\infty}$ can no longer be verified with a smaller $\Theta$. Although we may extract a sequence of $t$ going to infinity for this to hold as in the proof of Lemma 6 below, but it will not be good enough to prove the convergence of $\tilde{P}_{\Theta} n_{t}$, for which a more direct method will be used.

Let $\mathscr{N}$ be the Lie algebra of $N$. Then $\mathcal{N}$ is the space of the upper triangular matrices with zero diagonal elements. For $Y \in \mathscr{G}$, let $Y=Y_{\mathscr{K}}+Y_{\mathscr{A}}+Y_{\mathscr{N}}$ be the direct sum decomposition $\mathscr{G}=\mathscr{K} \oplus \mathscr{A} \oplus \mathscr{N}$. Since $d s_{t}=\left(\circ d a_{t}\right) n_{t}+a_{t}\left(\circ d n_{t}\right)$, we obtain the sde's satisfied by $a_{t}$ and $n_{t}$.

$$
\begin{equation*}
d a_{t}=\sum_{j=0}^{r}\left[\tilde{X}_{j}\left(u_{t}\right)\right]_{\mathscr{A}} a_{t} \circ d w_{t}^{j} \tag{26}
\end{equation*}
$$

and

$$
\begin{equation*}
d n_{t}=\sum_{j=0}^{r} \operatorname{Ad}\left(a_{t}^{-1}\right)\left[\tilde{X}_{j}\left(u_{t}\right)\right]_{\mathscr{N}} n_{t} \circ d w_{t}^{j} \tag{27}
\end{equation*}
$$

where for $h \in G, \operatorname{Ad}(h): \mathscr{G} \rightarrow \mathscr{G}$ is the differential of the map $g \mapsto h g h^{-1}$ from $G$ to $G$ at the identity. In fact, for $Y \in \mathscr{G}, \operatorname{Ad}(h) Y=h Y h^{-1}$ may be regarded as a matrix product. Note that for $a \in A$ and $Y \in \mathscr{N}, \operatorname{Ad}(a) Y \in \mathscr{N}$.

From (26) and the fact that $A$ is abelian, we obtain an sde for $\log a_{t}$.

$$
d \log a_{t}=\sum_{j=1}^{r}\left[\tilde{X}_{j}\left(u_{t}\right)\right]_{\mathscr{A}} \circ d w_{t}^{j}+\left[\tilde{X}_{0}\left(u_{t}\right)\right]_{\mathscr{A}} d t
$$

Using the stochastic calculus, we may write down the Itô integral equation for the above Stratonovich sde as follows.

$$
\log a_{t}=\int_{0}^{t} \sum_{j=1}^{r}\left[\tilde{X}_{j}\left(u_{s}\right)\right]_{\mathscr{A}} d w_{t}^{j}+\int_{0}^{t} F\left(u_{s}\right) d s
$$

where $F(u) \in \mathscr{A}$ is bounded, whose explicit expression is given in [6] and is not needed here. Divide the above by $t$ and then let $t \rightarrow \infty$. The first term on the right will converge to 0 , whereas by the ergodic theory the second term will converge almost surely if $u_{0}$ has a stationary distribution. As before, we may write $a_{t}(u, \omega)$ for $a_{t}$ to indicate its dependence on $(u, \omega)$. Let $\bar{\rho}$ be a stationary measure for $u_{t}$. Note that $\rho=\bar{\rho} \circ \pi_{o}^{-1}$. We have proved the following result.
Lemma 5. For $\bar{\rho} \times P$-almost all $(u, \omega) \in O(M) \times \Omega, \quad \lim _{t \rightarrow \infty}(1 / t) a_{t}(u, \omega)$ exists.

Lemma 6. Let $\bar{\rho}$ be a stationary measure for $u_{t}$ which has a continuous density on $O(M)$. Then for $\bar{\rho} \times P$-almost all $(u, \omega) \in O(M) \times \Omega$, (25) holds.

Proof. In the proof of Theorem 3, it is shown that $K_{\Theta} k_{t}(u k, \omega)=K_{\Theta} k_{t}(u, \omega) k$, hence, for almost all $k \in K, k_{t}(u k, \omega)$ has a limiting point contained in $Q_{\emptyset}$ as $t \rightarrow \infty$. It follows that for $\bar{\rho} \times P$-almost all $(u, \omega), k_{t_{j}}(u, \omega)$ converges to some $k(u, \omega) \in Q_{\emptyset}$ along some sequence $t_{j} \rightarrow \infty$. Fix such $(u, \omega)$ and write $k_{j}, a_{j}^{+}$and $a_{j}$ respectively for $k_{t_{j}}(u, \omega), a_{t_{j}}^{+}(u, \omega)$ and $a_{t_{j}}(u, \omega)$. We may assume that for $i \in \Theta$, $\left(a_{j}^{+}\right)_{i} /\left(a_{j}^{+}\right)_{i+1}$ is bounded. Otherwise, by taking a subsequence if necessary, we may assume $\left(a_{j}^{+}\right) /\left(a_{j}^{+}\right)_{i+1} \rightarrow \infty$ and we may exclude such an $i$ from $\Theta$. The conditions of Lemma 4 will be satisfied and we can conclude that $a_{j}\left(a_{j}^{+}\right)^{-1}$ is contained in a bounded subset of $A$. This proves $\lim _{j}\left(1 / t_{j}\right) \log a_{j}=\lim _{j}\left(1 / t_{j}\right) \log a_{j}^{+}$. Since by Lemma 3 and Lemma 5, both $\lim _{t \rightarrow \infty}(1 / t) \log a_{t}^{+}$and $\lim _{t \rightarrow \infty}(1 / t) \log a_{t}$ exist, the lemma is proved.

Lemma 7. Let $z_{t}=\left(z_{t}^{1}, \ldots, z_{t}^{d}\right)$ be a process in $R^{d}$ satisfying the Itô sde

$$
d z_{t}^{i}=\sum_{j=1}^{r} \sum_{k=1}^{d} a_{i j k}(t, \cdot) z_{t}^{k} d w_{t}^{j}+\sum_{k=1}^{d} b_{i k}(t, \cdot) z_{t}^{k} d t
$$

where the coefficients $a_{i j k}(t, \omega)$ and $b_{i k}(t, \omega)$ are continuous processes adapted to the filtration generated by the Browian motion $w_{t}$. Assume almost surely $a_{i j k}(t, \omega)$ and $b_{i k}(t, \omega)$ converge to 0 exponentially as $t \rightarrow \infty$, that is, $\exists \delta>0$ such that almost surely, $\left|a_{i j k}(t, \cdot)\right| \leq e^{-\delta t}$ and $\left|b_{i k}(t, \cdot)\right| \leq e^{-\delta t}$ for sufficiently large $t>0$. Then almost surely, $z_{t}$ converges in $R^{d}$ as $t \rightarrow \infty$.

Proof. Let $A_{n}=\left\{(t, \omega) ; \forall s \leq t,\left|a_{i j k}(s, \omega)\right| \leq n e^{-\delta s}\right.$ and $\left.\left|b_{i k}(s, \omega)\right| \leq n e^{-\delta s}\right\}$ and let $\tau_{n}(\omega)=\inf \left\{t ;(t, \omega) \notin A_{n}\right\}$. It is clear that $\tau_{n}$ form an increasing sequence of stopping times and by the assumption, for almost all $\omega, \tau_{n}(\omega)=\infty$ for sufficiently large $n$. By stopping the process at $\tau_{n}$, we may assume the coefficients $a_{i j k}(t, \cdot)$ and $b_{i k}(t, \cdot)$ are uniformly bounded by $C e^{-\delta t}$ for some constant $C>0$. In this proof, $C$ will be a positive constant which may change from formula to formula.

The Itô sde is equivalent to the following Itô integral equation.

$$
z_{t}^{i}=z_{0}^{i}+\int_{0}^{t} \sum_{j, k} a_{i j k}(s, \cdot) z_{s}^{k} d w_{s}^{j}+\int_{0}^{t} \sum_{k} b_{i k}(s, \cdot) z_{s}^{k} d s
$$

Let $\left|z_{t}\right|$ be the Euclidean norm of $z_{t}$ and let $z_{t}^{*}=\sup _{0 \leq s \leq t}\left|z_{t}\right|$. Then

$$
E\left[\left(z_{t}^{*}\right)^{2}\right] \leq C\left\{\left|z_{0}\right|^{2}+\int_{0}^{t} e^{-2 \delta s} E\left[\left(z_{s}^{*}\right)^{2}\right] d s\right\} .
$$

By Gronwall's inequality, $E\left[\left(z_{t}^{*}\right)^{2}\right] \leq C \exp \left(\int_{0}^{t} e^{-2 \delta s} d s\right)$, hence, $E\left[\left(z_{\infty}^{*}\right)^{2}\right] \leq C$. Let $y_{n}=\sup _{n \leq s \leq n+1}\left|z_{s}-z_{n}\right|$. It suffices to show $\sum_{n} y_{n}<\infty$ almost surely. From

$$
z_{s}^{i}-z_{n}^{i}=\int_{n}^{s} \sum_{j, k} a_{i j k}(u, \cdot) z_{u}^{k} d w_{u}^{j}+\int_{n}^{s} \sum_{k} b_{i k}(u, \cdot) z_{u}^{k} d u,
$$

we obtain

$$
P\left(y_{n} \geq e^{-\delta n / 2}\right) \leq e^{\delta n} E\left(y_{n}^{2}\right) \leq C e^{\delta n} \int_{n}^{n+1} e^{-2 \delta u} E\left[\left(z_{\infty}^{*}\right)^{2}\right] d u \leq C e^{-\delta n}
$$

It follows that $\sum_{n} P\left(y_{n} \geq e^{-\delta n / 2}\right)<\infty$, and by Borel-Cantelli lemma, $\sum_{n} y_{n}<$ $\infty$ almost surely.

$$
\text { For any matrix } g \in G \text {, let }|g|=\sqrt{\sum_{i, j} g_{i j}^{2}} \text {. }
$$

Lemma 8. For $\bar{\rho} \times P$-almost all $(u, \omega) \in O(M) \times \Omega$ and any $\varepsilon>0,\left|n_{t}(u, \omega)\right| \leq$ $e^{\varepsilon t}$ for sufficiently large $t$.

Proof. Let $n_{i j}(t)$ be the element of $n_{t}=n_{t}(u, \omega)$ at row $i$ and column $j$. We want to show that for $\bar{\rho} \times P$-almost all $(u, \omega)$ and any $\varepsilon>0$,

$$
\begin{equation*}
\left|n_{i j}(t)\right| \leq e^{\varepsilon t} \text { for sufficiently large } t>0 \tag{28}
\end{equation*}
$$

For $x=\left(x_{1}, \ldots, x_{d}\right) \in R^{d}$. Consider the quadratic form

$$
q_{t}(x)=x s_{t}^{*} s_{t} x^{*}=\sum_{i=1}^{d}\left(a_{t}\right)_{i}^{2}\left[\sum_{j=1}^{d} n_{i j}(t) x_{j}\right]^{2}=\sum_{i=1}^{d}\left(a_{t}\right)_{i}^{2}\left\langle n_{i} .(t), x\right\rangle_{0}^{2},
$$

where $n_{i} .(t)$ is the $i$-th row vector of $n_{t}$ and $\langle\cdot, \cdot\rangle_{0}$ is the Euclidean inner product on $R^{d}$. Since $q_{t}(x)=x k_{t}^{*}\left(a_{t}^{+}\right)^{2} k_{t} x^{*}$, the eigenvalues of $q_{t}$ are $\left(a_{t}^{+}\right)_{1}^{2} \geq\left(a_{t}^{+}\right)_{2}^{2} \geq$ $\cdots \geq\left(a_{t}^{+}\right)_{d}^{2}$. Let $x^{1}(t), x^{2}(t), \ldots, x^{d}(t)$ be the associated orthonormal eigenvectors and let $0<i_{1}<i_{2}<\cdots<i_{l}=d$ be the indices given by (19). Assume $i \leq i_{1}$. Since for $1 \leq j \leq d$,

$$
\left(a_{t}\right)_{i}^{2}\left\langle n_{i} \cdot(t), x^{j}(t)\right\rangle_{0}^{2} \leq q_{t}\left(x^{j}(t)\right) \leq\left(a_{t}^{+}\right)_{1}^{2} \approx\left(a_{t}^{+}\right)_{i}^{2} \approx\left(a_{t}\right)_{i}^{2} \approx e^{2 \lambda_{i} t}
$$

for large $t$, it follows that $\forall \varepsilon>0,\left\langle n_{i} \cdot(t), x^{j}(t)\right\rangle_{0}^{2} \leq e^{\varepsilon t}$ for sufficiently large $t$, hence, $\left\langle n_{i} .(t), n_{i} .(t)\right\rangle_{0}=\sum_{j=1}^{d}\left\langle n_{i} .(t), x^{j}(t)\right\rangle_{0}^{2} \leq d e^{\varepsilon t}$. This proves (28) for $i \leq i_{1}$ and any $j$.

Suppose that we have proved (28) for $i \leq i_{k}$. Let $D_{k}(t)=$ det $\left[\left\{x_{q}^{p}(t)\right\}_{i_{k}<p \leq d, i_{k}<q \leq d}\right]$. We will show that for any $\varepsilon>0$,

$$
\begin{equation*}
\left|D_{k}(t)\right| \geq e^{-\varepsilon t} \text { for suficiently large } t>0 . \tag{29}
\end{equation*}
$$

If this is not true, we can extract a sequence of $t$ going to infinity such that for some $\varepsilon>0,\left|D_{k}(t)\right| \leq e^{-\varepsilon t}$ along this sequence. We can then find a vector $v(t)$ of unit length such that $v(t)$ is a linear combination of $x^{i_{k}+1}(t), x^{i_{k}+2}(t), \ldots, x^{d}(t)$ and $\forall j>i_{k},\left|v_{j}(t)\right| \leq e^{-\varepsilon t}$ along that sequence of $t$. Since for $p \leq i_{k}, \lambda_{p}>\lambda_{i_{k}+1}$ and

$$
e^{2 \lambda_{p} t}\left\langle n_{p \cdot}(t), v(t)\right\rangle_{0}^{2} \approx\left(a_{t}\right)_{p}^{2}\left\langle n_{p .}(t), v(t)\right\rangle_{0}^{2} \leq q_{t}(v(t)) \leq\left(a_{t}^{+}\right)_{i_{k}+1}^{2} \approx e^{2 \lambda_{i_{k}+1} t},
$$

we see that for $p \leq i_{k},\left\langle n_{p} \cdot(t), v(t)\right\rangle_{0}=\sum_{j=1}^{d} n_{p j}(t) v_{j}(t)$ must converge to 0 exponentially along that sequence of $t$. Set $p=i_{k}$. Recall (28) is assumed to hold for $i \leq i_{k}$ and $v_{j}(t) \rightarrow 0$ exponentially for $j>i_{k}$. It follows that for $j>i_{k}=p, n_{p j}(t) v_{j}(t)$ must converge to 0 exponentially. Since $n_{i_{k} i_{k}}=1$ and $n_{i_{k} j}=0$ for $j<i_{k}$, we see that $v_{i_{k}}(t)$ must converge to 0 exponentially. Setting $p=i_{k}-1, i_{k}-2, \ldots, 1$, we can successively prove that $v_{i_{k}-1}(t), v_{i_{k}-2}(t)$, $\cdots, v_{1}(t)$ all converge to 0 exponentially. This is impossible because $v(t)$ has unit length. The contradiction proves (29).

Now assume $i_{k}<i \leq i_{k+1}$ for $1 \leq k<l$. Define

$$
\begin{equation*}
h_{p}(t)=\sum_{j=1}^{d} n_{i j}(t) x_{j}^{p}(t), \text { for } p=i_{k}+1, i_{k}+2, \ldots, d \tag{30}
\end{equation*}
$$

Then $\left(a_{t}\right)_{i}^{2}\left[h_{p}(t)\right]^{2} \leq q_{t}\left(x^{p}(t)\right) \leq\left(a_{t}^{+}\right)_{i_{k}+1}^{2} \approx\left(a_{t}\right)_{i}^{2} \approx e^{2 \lambda_{i} t}$, hence, $\forall \varepsilon>0$, $\left|h_{j}(t)\right| \leq e^{\varepsilon t}$ for sufficiently large $t>0$. Since $n_{i j}(t)=0$ for $j \leq i_{k}$, we may solve for $n_{i j}(t), i_{k}<j \leq d$, from the linear system of equations (30). The determinant in Cramer's solution formula is just $D_{k}$. By (29), we see that $n_{i j}(t)$ must have the desired bounds.

Recall that the Lie algebra $\mathcal{N}$ of $N$ is the space of upper triangular matrices with zero diagonal elements. It is known that exp: $\mathcal{N} \rightarrow N$ is a diffeomorphism (see Ch. VI in [5]). Let $0=i_{0}<i_{1}<\cdots<i_{l}=d$ be the indices given by (19). Define

$$
\begin{equation*}
\mathcal{N}_{\Theta}=\left\{Y \in \mathscr{N} ; Y_{i j}=0 \text { for } i \leq i_{k}<j, 1 \leq k<l\right\} \tag{31}
\end{equation*}
$$

and

$$
\begin{equation*}
\mathcal{N}_{\Theta}^{\prime}=\left\{Y \in \mathscr{N} ; Y_{i j}=0 \text { for } i_{k-1}<i \leq i_{k} \text { and } j \leq i_{k}, 1 \leq k \leq l\right\} . \tag{32}
\end{equation*}
$$

The non-zero elements of a matrix in $\mathcal{N}_{\Theta}$ are confined in several triangular regions lying above and along the diagonal, whereas the non-zero elements of a matrix in $\mathcal{N}_{\Theta}^{\prime}$ are confined in the region above these triangles. Consult the figure for $\tilde{P}_{\Theta}$ given in the last section.

Note that $\mathscr{N}=\mathscr{N}_{\Theta} \oplus \mathscr{N}_{\Theta}^{\prime}$ and $\mathscr{N}_{\emptyset}=\{0\}$. Moreover, both $\mathscr{N}_{\Theta}$ and $\mathscr{N}_{\Theta}^{\prime}$ are sub Lie algebras of $\mathscr{N}$. In fact, $\mathscr{N}_{\Theta}^{\prime}$ is an ideal of $\mathscr{N}$, that is, $\forall Y \in \mathscr{N}$ and $Z \in \mathcal{N}_{\Theta}^{\prime},[Y, Z] \in \mathscr{N}_{\Theta}^{\prime}$. Let $N_{\Theta}=\exp \left(\mathscr{N}_{\Theta}\right)$ and $N_{\Theta}^{\prime}=\exp \left(\mathscr{N}_{\Theta}^{\prime}\right)$. Then both $N_{\Theta}$ and $N_{\Theta}^{\prime}$ are Lie subgroups of $N$ with $N_{\Theta}^{\prime}$ normal. We have the decomposition $N=N_{\Theta} N_{\Theta}^{\prime}$ in the sense that the map $\left(n_{1}, n_{2}\right) \mapsto n_{1} n_{2}$ is a diffeomorphism: $N_{\Theta} \times N_{\Theta}^{\prime} \rightarrow N$. We also note that $N_{\Theta} \subset \tilde{P}_{\Theta}$.

Theorem 4. For $u \in O(M)$, let $D \phi_{t}(u)=u_{t} s_{t}$, where $u_{t} \in O(M)$ with $u_{0}=u$ and $s_{t} \in S$. Let $s_{t}=p_{t} a_{t}^{+} k_{t}$ and $s_{t}=a_{t} n_{t}$ be respectively a polar and the Iwasawa decompositions of $s_{t}$, and let $n_{t}=n_{t}^{\Theta} n_{t}^{\prime}$ with $n_{t}^{\Theta} \in N_{\Theta}$ and $n_{t}^{\prime} \in N_{\Theta}^{\prime}$. Let $\bar{\rho}$ be a stationary measure of $u_{t}$ which has a continuous density on $O(M)$. Then for $\bar{\rho} \times P$-almost all $(u, \omega) \in O(M) \times \Omega$,
(a) $K_{\Theta} k_{t} \rightarrow K_{\Theta} k_{\infty}$ as $t \rightarrow \infty$ for some $k_{\infty} \in K$;
(b) $\lim _{t \rightarrow \infty}(1 / t) \log a_{t}=\lim _{t \rightarrow \infty}(1 / t) \log a_{t}^{+}=\operatorname{diag}\left(e^{\lambda_{1}}, \ldots, e^{\lambda_{d}}\right)$;
(c) $\forall \varepsilon>0,\left|n_{t}^{\Theta}\right| \leq e^{\varepsilon t}$ for sufficiently large $t>0$;
(d) $n_{t}^{\prime} \rightarrow n_{\infty}^{\prime}$ as $t \rightarrow \infty$ for some $n_{\infty}^{\prime} \in \tilde{P}_{\Theta} k_{\infty}$, consequently, $\tilde{P}_{\Theta} n_{t} \rightarrow \tilde{P}_{\Theta} k_{\infty}$;
(e) $p_{t} K_{\Theta} \rightarrow K_{\Theta}$ as $t \rightarrow \infty$.

Proof. (a) and (b) are proved in Lemma 3 and Lemma 6. Because the map $\left(n^{\Theta}, n^{\prime}\right) \mapsto$ $n=n^{\Theta} n^{\prime}$ is a diffeomorphism: $N_{\Theta} \times N_{\Theta}^{\prime} \rightarrow N$, (c) follows from Lemma 8.

The main task is to prove (d). From (27) and $d n_{t}=d\left(n_{t}^{\Theta} n_{t}^{\prime}\right)=\left(\circ d n_{t}^{\Theta}\right) n_{t}^{\prime}+$ $n_{t}^{\Theta}\left(\circ d n_{t}^{\prime}\right)$, we may obtain the sde's for $n_{t}^{\Theta}$ and $n_{t}^{\prime}$. For $Y \in \mathscr{G}$, let $Y_{\mathcal{N}}=Y_{\Theta}+Y^{\prime}$ be the decomposition $\mathscr{N}=\mathscr{N}_{\Theta} \oplus \mathscr{N}_{\Theta}^{\prime}$. Note that for $a \in A$, the linear map $\operatorname{Ad}(a)$ : $\mathscr{N} \rightarrow \mathscr{N}$ leaves this decomposition invariant. We have

$$
\begin{equation*}
d n_{t}^{\Theta}=\sum_{j=0}^{r}\left\{\operatorname{Ad}\left(a_{t}^{-1}\right)\left[\tilde{X}_{j}\left(u_{t}\right)\right]_{\Theta}\right\} n_{t}^{\Theta} \circ d w_{t}^{j} \tag{33}
\end{equation*}
$$

and

$$
\begin{equation*}
d n_{t}^{\prime}=\sum_{j=0}^{r}\left\{\operatorname{Ad}\left(\left(n_{t}^{\Theta}\right)^{-1}\right) \operatorname{Ad}\left(a_{t}^{-1}\right)\left[\tilde{X}_{j}\left(u_{t}\right)\right]^{\prime}\right\} n_{t}^{\prime} \circ d w_{t}^{j} \tag{34}
\end{equation*}
$$

Let $F_{j}^{\Theta}(t)=\operatorname{Ad}\left(a_{t}^{-1}\right)\left[\tilde{X}_{j}\left(u_{t}\right)\right]_{\Theta}$ and $F_{j}^{\prime}(t)=\operatorname{Ad}\left(a_{t}^{-1}\right)\left[\tilde{X}_{j}\left(u_{t}\right)\right]^{\prime}$. Then $F_{j}^{\Theta}(t) \in$ $\mathscr{N}_{\Theta}$ and $F_{j}^{\prime}(t) \in \mathcal{N}_{\Theta}^{\prime}$. Note that for $a \in A$ and $Y \in \mathscr{G},\left[\operatorname{Ad}\left(a^{-1}\right) Y\right]_{i j}=$ $a_{i}^{-1} a_{j} Y_{i j}$. By Lemma 6, $\left(a_{t}\right)_{i} \approx e^{\lambda_{i} t}$ for large $t>0$. It follows that for $Y \in \mathcal{N}$, $\left[\operatorname{Ad}\left(a_{t}^{-1}\right) Y\right]_{i j} \approx e^{-\left(\lambda_{i}-\lambda_{j}\right) t} Y_{i j}$. If $Y \in \mathcal{N}_{\Theta}^{\prime}$, then either $\left(\lambda_{i}-\lambda_{j}\right)>0$ or $Y_{i j}=0$, hence, $\operatorname{Ad}\left(a_{t}^{-1}\right) Y$ converges to 0 exponentially as $t \rightarrow \infty$ for $Y \in \mathcal{N}_{\Theta}^{\prime}$. This implies that almost surely $F_{j}(t)^{\prime}$ converges to 0 exponentially as $t \rightarrow \infty$. The same thing can be said for the coefficients $\operatorname{Ad}\left(\left(n_{t}^{\Theta}\right)^{-1}\right) F_{j}^{\prime}(t)$ of the Stratonovich sde (34) because of (c). Before we can apply Lemma 7, we need to make sure that the coefficients of the corresponding Itô equation also have this property.

Note that the vector fields in the sde (34) may be considered as matrix products. Using stochastic calculus, we may write down the Itô form of (34) as follows.

$$
\begin{aligned}
d n_{t}^{\prime}= & \sum_{j=1}^{r}\left\{\operatorname{Ad}\left(\left(n_{t}^{\Theta}\right)^{-1}\right) F_{j}^{\prime}(t)\right\} n_{t}^{\prime} d w_{t}^{j} \\
& +\left\{\frac{1}{2} \sum_{j=1}^{r} \operatorname{Ad}\left(\left(n_{t}^{\Theta}\right)^{-1}\right) F_{j}^{\prime}(t) \operatorname{Ad}\left(\left(n_{t}^{\Theta}\right)^{-1}\right) F_{j}^{\prime}(t)\right. \\
& +\frac{1}{2} \sum_{j=1}^{r} \operatorname{Ad}\left(\left(n_{t}^{\Theta}\right)^{-1}\right)\left[F_{j}^{\prime}(t), F_{j}^{\Theta}(t)\right]
\end{aligned}
$$

$$
\begin{aligned}
& +\frac{1}{2} \sum_{j=1}^{r} \operatorname{Ad}\left(\left(n_{t}^{\Theta}\right)^{-1}\right) \operatorname{Ad}\left(a_{t}^{-1}\right)\left[\left[\tilde{X}_{j}\left(u_{t}\right)\right]^{\prime},\left[\tilde{X}_{j}\left(u_{t}\right)\right]_{\mathscr{A}}\right] \\
& \left.+\frac{1}{2} \sum_{j=1}^{r} \operatorname{Ad}\left(\left(n_{t}^{\Theta}\right)^{-1}\right) \operatorname{Ad}\left(a_{t}^{-1}\right)\left[Y_{j} \tilde{X}_{j}\left(u_{t}\right)\right]^{\prime}+\operatorname{Ad}\left(\left(n_{t}^{\Theta}\right)^{-1}\right) F_{0}^{\prime}(t)\right\} n_{t}^{\prime} d t
\end{aligned}
$$

where $Y_{j}(u)=H\left(X_{j}\right)(u)+u\left[\tilde{X}_{j}(u)\right]_{\mathscr{K}}$ are the vector fields in the sde (23) for $u_{t}$ on $O(M)$. It is easy to check that the coefficients of the above Itô sde converge to 0 exponentially. By Lemma $7, n_{t}^{\prime} \rightarrow n_{\infty}^{\prime}$ as $t \rightarrow \infty$ for some $n_{\infty}^{\prime} \in \mathcal{N}_{\Theta}^{\prime}$.

In order to finish the proof of (d), it remains to show that $n_{\infty}^{\prime} \in \tilde{P}_{\Theta} k_{\infty}$. As in the proofs of Theorem 3 and Lemma 6 , for $\bar{\rho} \times P$-almost all $(u, \omega)$, we may extract a sequence $t_{j} \rightarrow \infty$ such that the conditions of Lemma 4 are satisfied for $g_{j}=g_{t_{j}}$ possibly with a smaller $\Theta$. Apply this lemma one obtains $\tilde{P}_{\Theta} n_{t_{j}} \rightarrow \tilde{P}_{\Theta} k_{\infty}$. This is also true for the original $\Theta$. Therefore, $\tilde{P}_{\Theta} n_{\infty}^{\prime}=\lim _{j} \tilde{P}_{\Theta} n_{t_{j}}^{\prime}=\lim _{j} \tilde{P}_{\Theta} n_{t_{j}}=\tilde{P}_{\Theta} k_{\infty}$. This proves (d).

To prove (e), it suffices to show that any limiting point of $p(t)=p_{t}$ is contained in $K_{\Theta}$. If this is not true, then along some sequence of $t \rightarrow \infty, p(t)$ converges to some $p \in\left(K-K_{\Theta}\right)$. Then there exist indices $i>j$ such that $\lambda_{i}<\lambda_{j}$ and $p_{i j} \neq 0$. By (b) and Lemma 8, $\left[s_{t} k_{t}^{*}\right]_{i j}=\left[a_{t} n_{t} k_{t}^{*}\right]_{i j}=a_{i}(t) \sum_{b=1}^{d} n_{i b}(t) k_{j b}(t)$ grows at the exponential rate $\lambda_{i}$. On the other hand, this is also equal to $\left[p_{t} a_{t}^{+} k_{t} k_{t}^{*}\right]_{i j}=$ $\left[p_{t} a_{t}^{+}\right]_{i j}=p_{i j}(t) a_{j}^{+}(t)$, which grows at the exponential rate $\lambda_{j}>\lambda_{i}$. This is impossible.

Remark 4. As in Remark 2, if the vector fields of the sde (23) satisfy the Hörmander type condition, then the conclusions of Theorem 4 hold for all $u \in O(M)$ almost surely.

Now let $\phi_{t}=\xi_{t} \psi_{t}$ and $D \psi_{t}(u)=u s_{t}$, with $u=\left(u_{1}, \ldots, u_{d}\right) \in \pi^{-1}(m)$ and $m \in M$, be the decompositions given by Theorem 1. Then $D \psi_{t}(m)=u s_{t} u^{-1}=$ $u a_{t} n_{t}^{\Theta} n_{t}^{\prime} u^{-1}$ with $n_{t}^{\prime} \rightarrow n_{\infty}^{\prime}$. Therefore, for large time $t>0$, the linear map $D \psi_{t}(m): T_{m} M \rightarrow T_{m} M$ may be regarded as a fixed random linear map $u n_{\infty}^{\prime} u^{-1}$, followed by another linear map $u a_{t} n_{t}^{\Theta} u^{-1}$ which leaves the subspaces

$$
\begin{aligned}
& U_{1}=\operatorname{span}\left(u_{1}, \ldots, u_{i_{1}}\right), \quad U_{2}=\operatorname{span}\left(u_{i_{1}+1}, \cdots, u_{i_{2}}\right), \ldots, \\
& U_{l}=\operatorname{span}\left(u_{i_{l-1}+1}, \ldots, u_{d}\right)
\end{aligned}
$$

of $T_{m} M$ invariant and changes the length of vectors in each $U_{k}$ at the exponential rate $\lambda_{i_{k}}$ for $1 \leq k \leq l$.

Acknowledgements. The author wishes to thank the anonymous referee for pointing out an error concerning Theorem 2.

## References

1. Arnold, L.: Random dynamical systems, Springer (1998)
2. Carverhill, A.P.: Flows of stochastic dynamical systems: ergodic theory, Stochastics 14, 273-317 (1985)
3. Elworthy, K.D.: Geometric aspects of diffusions on manifolds, (Ecole d'Eté de Probabilités de Saint Flour XVII, July 1987), Lect Notes in Math 1362, 276-425 (1989)
4. Guivarc'h, Y. et Raugi, A.: Frontière de Furstenberg, propriétés de contraction et convergence, Z. Wahr verw Gebiete 68, 187-242 (1985)
5. Helgason, S.: Differential geometry, Lie groups, and symmetric spaces, Academic Press (1978)
6. Liao, M.: Lyapunov exponents of stochastic flows, Ann Probab 25, 1241-1256 (1997)

[^0]:    M. Liao: Department of Mathematics, Auburn University, 208 Parker Hall, Auburn, AL 36849, USA. e-mail: liaomin@mail. auburn.edu. Supported in part by NSF DMS9703693.

