Ming Liao

Decomposition of stochastic flows and Lyapunov exponents

Received: 19 November 1998 / Revised version: 1 October 1999 / Published online: 14 June 2000 – © Springer-Verlag 2000

Abstract. Let ϕ_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 ξ_t is isometric, ψ_t fixes m and $D\psi_t(u) = us_t$, 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 ψ_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.

$$dx_t = \sum_{j=1}^r X_j(x_t) \circ dw_t^j + X_0(x_t)dt,$$
(1)

where X_0, X_1, \ldots, X_r are (smooth) vector fields on $M, w_t = (w_t^1, \ldots, w_t^r)$ is an r-dimensional standard Brownian motion defined on a probability space (Ω, \mathscr{F}, P) , and $\circ d$ denotes the Stratonovich stochastic differential. The sde (1) can also be written more concisely as $dx_t = \sum_{j=0}^r X_j(x_t) \circ dw_t^j$, where $w_t^0 = t$.

Let Diff(*M*) be the group of diffeomorphisms: $M \to M$. A stochastic flow of the sde (1) is a process ϕ_t in Diff(*M*) with $\phi_0 = id_M$, 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 ϕ_t and is a diffusion process on *M*.

Let $D\phi_t$ be the differential of the random map $\phi_t: M \to M$. For $x \in M$, $D\phi_t(x)$ is a linear map: $T_xM \to T_{\phi_t(x)}M$. If $u = (u_1, \ldots, u_d)$ is a linear frame at x, then $D\phi_t(x)(u) = (D\phi_t(x)(u_1), \ldots, D\phi_t(x)(u_d))$ 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 $g = \{g_{ij}\}$, let $ug = (\sum_i u_i g_{i1}, \ldots, \sum_i u_i g_{id})$. This is a linear frame at x if g is non-singular. Note that $D\phi_t(ug) = D\phi_t(u)g$.

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 DMS-9703693.

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 ϕ_t in the form $\phi_t = \xi_t \circ \psi_t$, where ξ_t is a process in I(M) and ψ_t is a process in Diff(M) such that $\xi_0 = \psi_0 = \operatorname{id}_M$, $\psi_t(m) = m$ and $D\psi_t(u) = us_t$ for some process s_t in the group S of upper triangular matrices with positive diagonal elements. Moreover, ξ_t is a diffusion process in I(M), and if the stochastic flow ϕ_t is invariant under I(M), ξ_t will be left invariant, so the normalized Haar measure on I(M) will be a stationary measure for ξ_t .

Let $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_d$ be the Lyapunov exponents of the stochastic flow ϕ_t . It turns out that the component ψ_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 λ_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 $G = GL(d, R)_+$ be the group of $d \times d$ real matrices of positive determinants and let K = SO(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, $\lim_{t\to\infty}(1/t)\log a_t = \lim_{t\to\infty}(1/t)\log a_t^+ = \text{diag}(e^{\lambda_1}, \ldots, e^{\lambda_d})$, and both k_t and n_t converge as $t \to \infty$. Some of these properties have been mentioned in [6], we provide more complete proofs here.

The component ψ_t in the decomposition $\phi_t = \xi_t \psi_t$, defined by a given orthonormal frame $u = (u_1, \ldots, u_d)$ at $m \in M$, fixes the point m, so $D\psi_t$ is a linear map: $T_m M \to T_m M$. 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 λ_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 η_t of *X* is a smooth family of diffeomorphisms on *M* indexed by $t \ge 0$ such that $\forall x \in M$, $y_t = \eta_t(x)$ is a solution of the ordinary differential equation $(d/dt)y_t = X(y_t)$ and $\eta_0 = id_M$. If η_t is an isometry for all $t \ge 0$, 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 (u_1, \ldots, u_d) in $T_x M$. We will let $\pi: L(M) \to M$ be the natural projection given by $\pi(u) = x$. Let $G = GL(d, R)_+$ 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] = AB - BA. For $u = (u_1, \dots, u_d) \in L(M)$ and $g \in G$, $ug = (\sum_i u_i g_{i1}, \dots, \sum_i u_i g_{id})$ is a frame at $\pi(u)$. Given $A \in \mathscr{G}$, let $uA = (d/dt)[ue^{tA}]_{t=0}$, the tangent vector to the curve $t \mapsto ue^{tA}$ 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 $(d/dt)z_t|_{t=0} = X$ and let u_t be the parallel displacement of u along z_t . Let $H(X)(u) = (d/dt)u_t|_{t=0}$, called the horizontal lift of X to L(M) at u. Then $T_u^h L(M) = \{H(X)(u); X \in T_x M\}$ 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 = SO(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 $\pi_o: O(M) \to M$ be the restriction of $\pi: L(M) \to M$. For $u \in O(M)$, $X \in T_x M$ and $A \in \mathscr{K}$, both H(X)(u) and uA are contained in $T_u O(M)$. In fact,

$$T_u O(M) = \{ H(X)(u); \ X \in T_x M \} \oplus \{ uA; \ A \in \mathscr{K} \}.$$

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 = ks 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 $A = A_{\mathscr{K}} + A_{\mathscr{G}}$ with $A_{\mathscr{K}} \in \mathscr{K}$ and $A_{\mathscr{G}} \in \mathscr{G}$.

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

$$T_u L(M) = T_u O(M) \oplus u \mathscr{S}.$$
 (2)

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 η_t , its natural lift to L(M) is a vector field on L(M) defined by $\delta X(u) = (d/dt) D\eta_t(u)|_{t=0}$. 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 $\nabla X(u) = (\nabla X(u_1), \dots, \nabla X(u_d))$. Then there is a unique matrix $\tilde{X}(u) \in \mathcal{G}$ such that $\nabla X(u) = u \tilde{X}(u)$. If $u \in O(M)$, then

$$[X(u)]_{jk} = \langle u_j, \nabla X(u_k) \rangle, \tag{3}$$

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

$$\delta X(u) = H(X)(u) + u\tilde{X}(u) = H(X)(u) + u[\tilde{X}(u)]_{\mathscr{H}} + u[\tilde{X}(u)]_{\mathscr{G}}.$$
 (4)

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

Proof. Let η_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 $D\eta_t(U(x)) = U(\eta_t(x))$. Then the Lie bracket $[X, U](x) = (d/dt)D\eta_t^{-1}[U(\eta_t(x))]|_{t=0} = (d/dt)U(x)|_{t=0} = 0$ and $\nabla_X U = \nabla_U X + [X, U] = \nabla_U X$ at *x*. Let Π_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

$$\delta X(u) = \frac{d}{dt} [\Pi_t(u)g_t]_{t=0} = \frac{d}{dt} [\Pi_t(u)]_{t=0} + \frac{d}{dt} (ug_t)|_{t=0}.$$

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

$$\frac{d}{dt}[\Pi_t^{-1}(D\eta_t(u))]_{t=0} = \frac{d}{dt}[\Pi_t^{-1}(U(\eta_t(x)))]_{t=0} = \nabla_X U(x) = \nabla_U X(x) = \nabla_u X.$$

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: $\mathscr{I} \to T_u O(M)$ defined by $X \mapsto \delta X(u)$ is injective. Moreover, if M is a sphere, then it is also surjective.

Proof. If $X, Y \in \mathcal{I}$ and $\delta X(u) = \delta Y(u)$, then X - Y is an infinitesimal isometry which fixes u, so its flow η_t will leave all the geodesics starting at $\pi_o(u)$ invariant. By the connectedness of M, $\eta_t = id_M$ 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 $T_u O(M) = \{\delta X(u); X \in \mathcal{I}\}$.

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 ϕ_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 $\eta \in \text{Diff}(M)$, then $D\eta(X)$ is a vector field on M given by $D\eta(X)(x) = D\eta(X(\eta^{-1}(x)))$ for $x \in M$. We will assume

$$\forall i = 0, 1, \dots, r \text{ and } \forall \xi \in \mathscr{I}(M), \quad [\delta D\xi(X_i)(u)]_O \in \delta \mathscr{I}(u).$$
(5)

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 ϕ_t of the sde (1) has a unique decomposition $\phi_t = \xi_t \psi_t$, where ξ_t is a process in I(M) and ψ_t is a process in Diff(M) such that $\xi_0 = \psi_0 = id_M$, $\psi_t(m) = m$ and $D\psi_t(u) = us_t$ for some process $s_t \in S$. Moreover, ξ_t is a diffusion process in I(M) and ψ_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 $D\xi(X_j)$ for j = 0, 1, ..., r and $\xi \in I(M)$. By Lemma 2, for any $X \in \mathcal{J}$, there is a unique $J(X) \in \mathcal{I}$ such that

$$\delta J(X)(u) = [\delta X(u)]_O. \tag{6}$$

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

$$\delta X(u) = \delta J(X)(u) + u[\tilde{X}(u)]_{\mathscr{G}}.$$
(7)

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

$$dD\phi_t(u) = \sum_{j=0}^r \delta X_j(D\phi_t(u)) \circ dw_t^j.$$
(8)

Note that the term $\delta X_0(D\phi_t(u))dt$ 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 $Y \in \mathcal{I}$, let ξY 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 ξ_t be the solution of the following sde on I(M)

with $\xi_0 = \mathrm{id}_M$.

$$d\xi_t = \sum_{j=0}^r \xi_t [D\xi_t^{-1}(X_j)]^J \circ dw_t^j.$$
(9)

is a diffusion process on I(M). Since $\xi_t^{-1}\xi_t = \mathrm{id}_M$, $(\circ d\xi_t^{-1})\xi_t + \xi_t^{-1}(\circ d\xi_t) = 0$. By (9), we obtain an sde for ξ_t^{-1} .

$$d\xi_t^{-1} = -\sum_{j=0}^{\prime} [D\xi_t^{-1}(X_j)]^J \xi_t^{-1} \circ dw_t^j.$$
(10)

For $x \in M$, let $x_t = \phi_t(x)$ and $y_t = \xi_t^{-1}(x_t)$. By (1) and (10), we have

$$dy_{t} = D\xi_{t}^{-1}(\circ dx_{t}) + (\circ d\xi_{t}^{-1})(x_{t})$$

= $\sum_{j=0}^{r} \{D\xi_{t}^{-1}(X_{j}(x_{t})) - [D\xi_{t}^{-1}(X_{j})]^{J}(\xi_{t}^{-1}(x_{t}))\} \circ dw_{t}^{j}$
= $\sum_{j=0}^{r} \{D\xi_{t}^{-1}(X_{j}) - [D\xi_{t}^{-1}(X_{j})]^{J}\}(y_{t}) \circ dw_{t}^{j}.$

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

$$\delta X^H(u) = u[\tilde{X}(u)]_{\mathscr{G}}.$$
(11)

We have proved that y_t is a solution of the the following sde on M.

$$dy_t = \sum_{j=0}^r [D\xi_t^{-1}(X_j)]^H(y_t) \circ dw_t^j.$$
(12)

The vector fields $[D\xi_t^{-1}(X_j)]^H$ of the above sde are random and time dependent, whose natural lifts $\delta[D\xi_t^{-1}(X_j)]^H$ can still be defined by fixing *t* and ω . Since $X^H(m) = 0$ for any $X \in \mathscr{I}$, it follows that $[D\xi_t^{-1}(X_j)]^H(m) = 0$, hence, if $y_0 = m$, then $y_t = m$ for all t > 0.

Let $\psi_t = \xi_t^{-1} \phi_t$. Then ψ_t is a process in 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

$$dD\psi_t(u) = \sum_{j=0}^r \delta[D\xi_t^{-1}(X_j)]^H (D\psi_t(u)) \circ dw_t^j.$$
(13)

This can be proved by the same method used to prove (8).

Since $\psi_t(m) = m$, $D\psi_t(u) = us_t$ for some process $s_t \in G$. By (13) and (11), we obtain an sde for s_t .

$$ds_{t} = \sum_{j=0}^{r} \{ [D\xi_{t}^{-1}(X_{j})]^{\tilde{}}(u) \}_{\mathscr{S}} s_{t} \circ dw_{t}^{j}.$$
(14)

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 $D\phi_t(u) = D\xi_t(D\psi_t(u)) = D\xi_t(u)s_t$ and $s_t \in S$, we see that the orthonormal frame $D\xi_t(u) = (D\xi_t(u_1), \ldots, D\xi_t(u_d))$ can be obtained by performing a standard Gram-Schmidt orthogonalization procedure to $D\phi_t(u) = (D\phi_t(u_1), \ldots, D\phi_t(u_d))$. 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 $\xi_0 = \psi_0 = id_M$. Conversely, given any $\xi_0 \in I(M)$ and $\psi_0 \in \text{Diff}(M)$ with $\psi_0(m) = m$ and $D\psi_0(u) = us$ 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 $\xi_0 = \psi_0 = id_M$, just by solving (9) with ξ_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 \mathbb{R}^n and let (x_1, x_2, \ldots, x_n) be the standard coordinates of \mathbb{R}^n . Let $\partial_i = (\partial/\partial x_i)$. Fix the point $m = (0, \ldots, 0, 1)$ on S^{n-1} . Let $u = (\partial_1, \ldots, \partial_{n-1})$. This is an orthonormal frame at m for S^{n-1} . We may express X as

$$X(x) = \sum_{j=1}^{n} a_j(x)\partial_j \tag{15}$$

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

$$J(X) = -\sum_{i=1}^{n-1} a_i(m) Z_{in} + \sum_{1 \le i < j \le (n-1)} \partial_i a_j(m) Z_{ij}.$$
 (16)

Note that for $1 \le i \le (n-1)$, $\partial_i \in T_m S^{n-1}$, so $\partial_i a_j(m)$ is well defined. We extend X to a neighborhood of S^{n-1} in \mathbb{R}^n by setting X(x) = X(x/|x|).

We extend X to a neighborhood of S^{n-1} in \mathbb{R}^n by setting X(x) = X(x/|x|). Then $\sum_{i=1}^n x_i a_i(x) = 0$ for x in this neighborhood, hence,

$$a_n(m) = 0$$
 and $a_i(m) + \partial_i a_n(m) = 0$ for $1 \le i \le (n-1)$. (17)

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

$$D\eta(u) = (D\eta(\partial_1), \dots, D\eta(\partial_{n-1})) = (\sum_{i=1}^n \partial_1 \eta_i \, \partial_i, \dots, \sum_{i=1}^n \partial_{n-1} \eta_i \, \partial_i)$$

Since $(d/dt)\eta_i = a_i(\eta), (d/dt)\partial_j\eta_i = \sum_{k=1}^n \partial_k a_i(\eta)\partial_j\eta_k$ and $(d/dt)\partial_j\eta_i(0, m) = \partial_j a_i(m)$. By (17), $\partial_j a_n(m) = -a_j(m) = 0$ for $1 \le j \le (n-1)$, we have

$$\delta X(u) = \frac{d}{dt} D\eta(u)|_{t=0} = \left(\sum_{i=1}^{n-1} \partial_1 a_i(m) \partial_i, \ldots, \sum_{i=1}^{n-1} \partial_{n-1} a_i(m) \partial_i\right) = uA,$$

where *A* is the $(n-1) \times (n-1)$ matrix given by $A_{ij} = \partial_j a_i(m)$. It follows that if $X = x_j \partial_i$ for $i \le j$, 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 $x' = (x_1, \dots, x_{n-1})$ and will find its Taylor expansion at *m* up to the second order. Let $O(|x'|^2)$ denote any function on S^{n-1} which converges to 0 as $x' \to 0$ (that is, as $x \to m$) in the order of $|x'|^2 = \sum_{i=1}^{(n-1)} x_i^2$. We will also use $O(|x'|^2)$ to denote any vector field on S^{n-1} whose components are such functions. Note that if $X = O(|x'|^2)$, then $\delta X(u) = 0$. Moreover, $x_n = 1 + O(|x'|^2)$, $\partial_i x_n = -x_i/x_n$, and

$$\partial_i [a_j(x_1,\ldots,x_{n-1},\sqrt{1-|x'|^2})]_{x=m} = \partial_i a_j(m)$$

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

$$X(x) = \sum_{j=1}^{n} a_j(x)\partial_j$$

= $\sum_{j=1}^{n-1} a_j(m)\partial_j + \sum_{i=1}^{n-1} \sum_{j=1}^{n-1} \partial_i a_j(m)x_i\partial_j + \sum_{j=1}^{n-1} \partial_j a_n(m)x_j\partial_n + O(|x'|^2)$

$$= \sum_{j=1}^{n-1} a_j(m) [x_n \partial_j - x_j \partial_n] + \sum_{1 \le i < j \le (n-1)} \partial_i a_j(m) [x_i \partial_j - x_j \partial_i] + \sum_{j=1}^{n-1} \partial_j a_j(m) x_j \partial_j + \sum_{1 \le i < j \le (n-1)} [\partial_j a_i(m) + \partial_i a_j(m)] x_j \partial_i + O(|x'|^2) = -\sum_{j=1}^{n-1} a_j(m) Z_{jn} + \sum_{1 \le i < j \le (n-1)} \partial_i a_j(m) Z_{ij} + \sum_{j=1}^{n-1} \partial_j a_j(m) x_j \partial_j + \sum_{1 \le i < j \le (n-1)} [\partial_j a_i(m) + \partial_i a_j(m)] x_j \partial_i + O(|x'|^2).$$

Now (16) follows from the above and the fact that $\delta(x_i \partial_i)(u) \in u \mathscr{S}$ for $i \leq j$.

The diffusion process ξ_t on I(M) is called left invariant if for any $\xi \in I(M)$, $\xi\xi_t$ is equal in distribution to the same diffusion process starting at $\xi\xi_0$. It is well known that if ξ_t is left invariant, then the normalized Haar measure on I(M) is a stationary measure of ξ_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 ϕ_t will be called invariant under I(*M*) if for any $\xi \in I(M)$, $\xi \phi_t \xi^{-1} \cong \phi_t$ (equal in distribution as processes in Diff(*M*)). Note that $\xi \phi_t \xi^{-1}$ is the stochastic flow of the sde $dx_t = \sum_{j=0}^r D\xi(X_j)(x_t) \circ dw_t^j$. If $X_0 = 0$ and if for any $\xi \in I(M)$, $D\xi(X_j) = \sum_{i=1}^r \alpha_i^j(\xi)X_i$, where $\alpha(\xi) = \{\alpha_i^j(\xi)\}$ is an $r \times r$ orthogonal matrix, then this sde can be written as $dx_t = \sum_{j=1}^r X_j(x_t) \circ d\beta_t^j$, where $\beta_t = \alpha(\xi)w_t$ is an *r*-dimensional Brownian motion. Therefore, in this case, ϕ_t is invariant under I(*M*).

Theorem 2. Assume ϕ_t is invariant under I(M). Then ξ_t is left invariant.

Proof. It suffices to show that for any $\xi \in I(M)$, if ξ'_t is the solution of (9) (replacing ξ_t by ξ'_t) with $\xi'_0 = \xi$, then $\xi'_t \cong \xi\xi_t$ (equal in distribution as processes in I(M)). By Remark 1, we have the unique decomposition $\phi_t \xi = \xi'_t \psi'_t$, where ψ'_t is a process in Diff(*M*) such that $\psi'_t(m) = m$ and $D\psi'_t(u) = us'_t$ for some $s'_t \in S$. On the other hand, $\xi\xi_t\psi_t = \xi\phi_t = \xi\phi_t\xi^{-1}\xi \cong \phi_t\xi$. This proves $\xi\xi_t \cong \xi'_t$ and $\psi_t \cong \psi'_t$.

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 ϕ_t be the stochastic flow of the sde (1). We will assume that its one point motion has an ergodic stationary measure ρ . This assumption is implied by the following Hörmander type condition: the Lie algebra Lie(X_1, \ldots, 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, ω) ,

$$[D\phi_t(x)^* D\phi_t(x)]^{1/2t} \to \Lambda(x,\omega) \text{ as } t \to \infty,$$
(18)

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

$$e^{\lambda_1} \ge e^{\lambda_2} \ge \cdots \ge e^{\lambda_d}$$

independent of (x, ω) . 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 λ_i jumps at i_k for $1 \le k \le (l-1)$, that is,

$$\lambda_1 = \dots = \lambda_{i_1} > \lambda_{i_1+1} = \dots = \lambda_{i_2} > \lambda_{i_2+1} \cdots \lambda_{i_{l-1}} > \lambda_{i_{l-1}+1} = \dots = \lambda_d.$$
(19)

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 $1 \le k \le l$,

$$\forall Y \in [V_k(x,\omega) - V_{k+1}(x,\omega)], \quad \lim_{t \to \infty} \frac{1}{t} \log \|D\phi_t(x)(Y)\| = \lambda_{i_k}, \quad (20)$$

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 ϕ_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 $G = GL(d, R)_+$. 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 SL(d, R) and the multiplication group $R_+ = (0, \infty)$, where SL(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 = SO(d), the subgroup of *G* consisting of orthogonal matrices of determinant 1. Any $g \in G$ has a polar decomposition $g = pa^+k$ with $a^+ \in \exp(\overline{\mathscr{A}_+})$ 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 $(pm, m^{-1}k)$ with *m* ranging over the centralizer of a^+ in *K*, that is, $m \in K$ with $ma^+m^{-1} = a^+$.

Let Θ be a subset of $\{1, 2, ..., (d-1)\}$ and let $i_1 < i_2 < \cdots < i_l$ be the integers in $\{1, 2, ..., d\}$ which are not contained in Θ . Then $i_l = d$. Let K_{Θ} be the subgroup of K which leaves the following subspaces of R^d invariant.

$$E_1 = \operatorname{span}(e_1, \dots, e_{i_1}), \quad E_2 = \operatorname{span}(e_{i_1+1}, \dots, e_{i_2}), \dots,$$

$$E_l = \operatorname{span}(e_{i_{l-1}+1}, \dots, e_d), \quad (21)$$

where $\{e_1, e_2, \ldots, e_d\}$ is the standard basis of \mathbb{R}^d . The non-zero elements of a matrix in K_{Θ} are contained in l sub-matrices arranged along the diagonal. Note that if $\Theta \subset \Theta'$, then $K_{\Theta} \subset K_{\Theta'}$, and K_{\emptyset} is the subgroup of K formed by the diagonal matrices with diagonal elements equal to ± 1 , where \emptyset is the empty set.

From now on, unless explicitly stated otherwise, we will let Θ be the set of integers *i* with $1 \le i \le (d-1)$ such that $\lambda_i = \lambda_{i+1}$. Then K_{Θ} is the centralizer of diag $(e^{\lambda_1}, \ldots, e^{\lambda_d})$ 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: $\mathbb{R}^d \to T_x M$ defined by $\eta = (\eta_1, \dots, \eta_d) \mapsto u\eta = \sum_i u_i \eta_i$. The adjoint map $u^*: T_x M \to \mathbb{R}^d$ is defined by $\langle u^*Y, \eta \rangle_0 = \langle Y, u\eta \rangle$ for $Y \in T_x M$ and $\eta \in \mathbb{R}^d$, 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: $\mathbb{R}^d \to \mathbb{R}^d$ 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 ω . 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_{Θ} contains the centralizer of a_t^+ in K.

Lemma 3. For almost all $(x, \omega) \in M \times \Omega$ and all $u \in \pi_0^{-1}(x)$,

$$\lim_{t \to \infty} \frac{1}{t} \log a_t^+(u, \omega) = \operatorname{diag}\{\lambda_1, \lambda_2, \dots, \lambda_d\},\tag{22}$$

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

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

Proof. Since $D\phi_t(x) = u_t s_t u^{-1}$, $D\phi_t(x)^* = (u^*)^{-1} s_t^* u_t^*$, where s_t^* is the matrix transpose of s_t . It follows that $D\phi_t(x)^* D\phi_t(x) = u(s_t^* s_t)u^{-1}$. By (18), for $\rho \times P$ -almost all (x, ω) and all $u \in \pi_o^{-1}(x)$, $[s_t(u, \omega)^* s_t(u, \omega)]^{1/2t}$ converges to some symmetric matrix with eigenvalues $\{e^{\lambda_1}, e^{\lambda_2}, \ldots, e^{\lambda_d}\}$. This symmetric matrix may

be diagonalized with an orthogonal matrix, we have, $[s_t(u, \omega)^* s_t(u, \omega)]^{1/2t} \rightarrow k_{\infty}^* \operatorname{diag}(e^{\lambda_1}, \ldots, e^{\lambda_d}) k_{\infty} \text{ as } t \rightarrow \infty$, for some $k_{\infty} \in K$.

Since $s_t^* s_t = k_t^* (a_t^+)^2 k_t$, we have $[s_t^* s_t]^{1/2t} = k_t^* \exp[(1/t) \log a_t^+] k_t$. Let b and k'_{∞} be respectively limiting points of $(1/t) \log a_t^+$ and k_t as $t \to \infty$. Then

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

By the uniqueness of the polar decomposition, $b = \text{diag}(\lambda_1, \dots, \lambda_d)$ and $k'_{\infty} \in K_{\Theta}k_{\infty}$.

Corollary 1. For $\rho \times P$ -almost all (x, ω) and all $u \in \pi_o^{-1}(x)$, the eigenspace of $\Lambda(x, \omega)$ corresponding to the eigenvalue $\exp(\lambda_{i_k})$ is given by $E_k(x, \omega) = u k_\infty^{-1}(u, \omega) E_k$ for $1 \le k \le l$, where E_k are subspaces of \mathbb{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 ,

$$du_{t} = \sum_{j=0}^{r} \{H(X_{j})(u_{t}) + u_{t}[\tilde{X}_{j}(u_{t})]_{\mathscr{H}}\} \circ dw_{t}^{j}$$
(23)

and

$$ds_t = \sum_{j=0}^r [\tilde{X}_j(u_t)] \mathscr{G}s_t \circ dw_t^j.$$
(24)

Note that $[\tilde{X}_i(u_t)] g_{s_t}$ 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 = KAN in the sense that the map $(h, a, n) \mapsto g = han$ is a diffeomorphism: $K \times A \times N \to G$. Note that S = AN, so if $s \in S$, then its Iwasawa decomposition s = an does not have a *K*-component. We will let $s_t = a_t n_t$ be the Iwasawa decomposition of the process s_t .

Let 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 $\tilde{P}_{\Theta} = \tilde{N}AK_{\Theta}$ 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}_{Θ} 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, $Q_{\Theta} = \{k \in K; k \in \tilde{P}_{\Theta}N\}$ 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 = NAK, 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 $K_{\Theta} k_j \to K_{\Theta} k_{\infty}$ in $(K_{\Theta} \setminus K)$ for some $k_{\infty} \in Q_{\Theta}$, $\forall i \in \Theta, (a_j^+)_i/(a_j^+)_{i+1} \leq C$ for some constant C > 0, and $\forall i \notin \Theta$ with $1 \leq i \leq (d-1), (a_j^+)_i/(a_j^+)_{i+1} \to \infty$ as $j \to \infty$, where $(a_j^+)_i$ is the *i*-th diagonal element of a_j^+ . Then $\tilde{P}_{\Theta} n_j \to \tilde{P}_{\Theta} k_{\infty}$ in $(\tilde{P}_{\Theta} \setminus G), a_j (a_j^+)^{-1}$ is contained in a compact subset of A, and $h_j = p_j p'_j$ with $p'_j \in K$ satisfying $p'_i K_{\Theta} \to K_{\Theta}$ in K/K_{Θ} .

For $x \in M$, the fiber $\pi_0^{-1}(x)$ may be identified with *K* via the map $k \mapsto uk$ 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 $u \in \pi_o^{-1}(x)$,

$$\lim_{t \to \infty} \frac{1}{t} \log a_t^+(u, \omega) = \lim_{t \to \infty} \frac{1}{t} \log a_t(u, \omega) = \operatorname{diag}(e^{\lambda_1}, \dots, e^{\lambda_d}).$$
(25)

Moreover, as $t \to \infty$, $K_{\emptyset}k_t(u, \omega) \to K_{\emptyset}k_{\infty}(u, \omega)$ for some $k_{\infty}(u, \omega) \in Q_{\emptyset}$, $n_t(u, \omega) \to n_{\infty}(u, \omega)$ for some $n_{\infty}(u, \omega) \in \tilde{P}_{\emptyset}k_{\infty}(u, \omega)$, and $p_t(u, \omega)K_{\emptyset} \to K_{\emptyset}$.

Proof. For any $k \in K$, $s_t k = k'_t s'_t$ for $k'_t \in K$ and $s'_t \in S$. On the other hand, $s_t k = p_t a_t^+ k_t k$, hence, $s'_t = (k'_t^{-1} p_t) a_t^+ (k_t k)$ is a polar decomposition of s'_t . Since $D\phi_t(uk) = u_t s_t k = (u_t k'_t) s'_t$ and $u_t k'_t \in O(M)$, it follows that $k_t(uk, \omega) = k_t(u, \omega)k$. Because all the Lyapunov exponents are simple, $\Theta = \emptyset$. By Lemma 3, $(1/t) \log a_t^+(u, \omega) \to \operatorname{diag}\{\lambda_1, \ldots, \lambda_d\}$ and $K_{\emptyset}k_t(u, \omega) \to K_{\emptyset}k_{\infty}(u, \omega)$ as $t \to \infty$. Then $K_{\emptyset}k_{\infty}(uk, \omega) = K_{\emptyset}k_{\infty}(u, \omega)k$. Because the complement of Q_{\emptyset} in K has a lower dimension, it follows that for almost all $k \in K$, $k_{\infty}(uk, \omega) \in Q_{\emptyset}$. Now Lemma 4 with $\Theta = \emptyset$ can be applied to prove all the remaining claims. We note that $\tilde{P}_{\emptyset}n_t \to \tilde{P}_{\emptyset}k_{\infty}$ implies the convergence of n_t because $N \cap \tilde{P}_{\emptyset}$ contains only the identity matrix, and $p_t K_{\emptyset} \to K_{\emptyset}$ is equivalent to $K_{\emptyset}p_t \to K_{\emptyset}$ because both mean that any limiting point of p_t as $t \to \infty$ belongs to K_{\emptyset} .

Remark 2. Because K_{\emptyset} is finite, we may choose the k_t component properly so that $t \to k_t$ is continuous and $k_t \to k_{\infty}$ 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 $D\psi_t(u) = us_t$, with $u = (u_1, \ldots, u_d) \in \pi^{-1}(m)$ and $m \in M$, be the decompositions given by Theorem 1. Then $D\psi_t(m) = us_t u^{-1} = ua_t n_t u^{-1}$ with $a_t \approx \text{diag}(e^{\lambda_1 t}, \ldots, e^{\lambda_d t})$ and $n_t \to n_\infty$ as $t \to \infty$. Therefore, for large time t > 0, the linear map $D\psi_t(m)$: $T_m M \to T_m M$ may be regarded as a fixed random linear map $un_\infty u^{-1}$, followed by $ua_t u^{-1}$ which is a dilation along each axis u_i at an exponential rate λ_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 Θ 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 $\forall i \in \Theta, (a_j^+)_i/(a_j^+)_{i+1}$ is bounded. If such *i* is excluded from Θ , then the condition $K_{\Theta}k_t \to K_{\Theta}k_{\infty}$ can no longer be verified with a smaller Θ . 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 \mathcal{N} be the Lie algebra of N. Then \mathcal{N} is the space of the upper triangular matrices with zero diagonal elements. For $Y \in \mathcal{G}$, let $Y = Y_{\mathcal{K}} + Y_{\mathcal{A}} + Y_{\mathcal{N}}$ be the direct sum decomposition $\mathcal{G} = \mathcal{K} \oplus \mathcal{A} \oplus \mathcal{N}$. Since $ds_t = (\circ da_t)n_t + a_t(\circ dn_t)$, we obtain the sde's satisfied by a_t and n_t .

$$da_t = \sum_{j=0}^r [\tilde{X}_j(u_t)]_{\mathscr{A}} a_t \circ dw_t^j$$
(26)

and

$$dn_{t} = \sum_{j=0}^{r} \operatorname{Ad}(a_{t}^{-1})[\tilde{X}_{j}(u_{t})]_{\mathscr{N}} n_{t} \circ dw_{t}^{j}, \qquad (27)$$

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

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

$$d\log a_t = \sum_{j=1}^r [\tilde{X}_j(u_t)]_{\mathscr{A}} \circ dw_t^j + [\tilde{X}_0(u_t)]_{\mathscr{A}} dt.$$

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

$$\log a_t = \int_0^t \sum_{j=1}^r [\tilde{X}_j(u_s)]_{\mathscr{A}} dw_t^j + \int_0^t F(u_s) ds,$$

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 $t \to \infty$. 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, ω) . 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 $(u, \omega) \in O(M) \times \Omega$, $\lim_{t\to\infty} (1/t)a_t(u, \omega)$ 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 $K_{\Theta}k_t(uk, \omega) = K_{\Theta}k_t(u, \omega)k$, hence, for almost all $k \in K$, $k_t(uk, \omega)$ has a limiting point contained in Q_{\emptyset} as $t \to \infty$. It follows that for $\bar{\rho} \times P$ -almost all (u, ω) , $k_{t_j}(u, \omega)$ converges to some $k(u, \omega) \in Q_{\emptyset}$ along some sequence $t_j \to \infty$. Fix such (u, ω) 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 $i \in \Theta$, $(a_j^+)_i/(a_j^+)_{i+1}$ is bounded. Otherwise, by taking a subsequence if necessary, we may assume $(a_j^+)/(a_j^+)_{i+1} \to \infty$ and we may exclude such an i from Θ . The conditions of Lemma 4 will be satisfied and we can conclude that $a_j(a_j^+)^{-1}$ is contained in a bounded subset of A. This proves $\lim_j (1/t_j) \log a_j = \lim_j (1/t_j) \log a_j^+$. Since by Lemma 3 and Lemma 5, both $\lim_{t\to\infty} (1/t) \log a_t^+$ and $\lim_{t\to\infty} (1/t) \log a_t$ exist, the lemma is proved.

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

$$dz_t^i = \sum_{j=1}^r \sum_{k=1}^d a_{ijk}(t, \cdot) z_t^k \, dw_t^j + \sum_{k=1}^d b_{ik}(t, \cdot) z_t^k \, dt,$$

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

Proof. Let $A_n = \{(t, \omega); \forall s \leq t, |a_{ijk}(s, \omega)| \leq ne^{-\delta s} \text{ and } |b_{ik}(s, \omega)| \leq ne^{-\delta s} \}$ and let $\tau_n(\omega) = \inf\{t; (t, \omega) \notin A_n\}$. It is clear that τ_n form an increasing sequence of stopping times and by the assumption, for almost all ω , $\tau_n(\omega) = \infty$ for sufficiently large *n*. By stopping the process at τ_n , we may assume the coefficients $a_{ijk}(t, \cdot)$ and $b_{ik}(t, \cdot)$ are uniformly bounded by $Ce^{-\delta t}$ 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.

$$z_t^i = z_0^i + \int_0^t \sum_{j,k} a_{ijk}(s, \cdot) z_s^k dw_s^j + \int_0^t \sum_k b_{ik}(s, \cdot) z_s^k ds.$$

Let $|z_t|$ be the Euclidean norm of z_t and let $z_t^* = \sup_{0 \le s \le t} |z_t|$. Then

$$E[(z_t^*)^2] \le C\{|z_0|^2 + \int_0^t e^{-2\delta s} E[(z_s^*)^2] \, ds\}.$$

By Gronwall's inequality, $E[(z_t^*)^2] \le C \exp(\int_0^t e^{-2\delta s} ds)$, hence, $E[(z_{\infty}^*)^2] \le C$. Let $y_n = \sup_{n \le s \le n+1} |z_s - z_n|$. It suffices to show $\sum_n y_n < \infty$ almost surely. From

$$z_s^i - z_n^i = \int_n^s \sum_{j,k} a_{ijk}(u, \cdot) z_u^k dw_u^j + \int_n^s \sum_k b_{ik}(u, \cdot) z_u^k du,$$

we obtain

$$P(y_n \ge e^{-\delta n/2}) \le e^{\delta n} E(y_n^2) \le C e^{\delta n} \int_n^{n+1} e^{-2\delta u} E[(z_{\infty}^*)^2] du \le C e^{-\delta n}.$$

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

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

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

Proof. Let $n_{ij}(t)$ 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, ω) and any $\varepsilon > 0$,

$$|n_{ij}(t)| \le e^{\varepsilon t} \text{ for sufficiently large } t > 0.$$
(28)

For $x = (x_1, \ldots, x_d) \in \mathbb{R}^d$. Consider the quadratic form

$$q_t(x) = x s_t^* s_t x^* = \sum_{i=1}^d (a_t)_i^2 [\sum_{j=1}^d n_{ij}(t) x_j]^2 = \sum_{i=1}^d (a_t)_i^2 \langle n_i(t), x \rangle_0^2,$$

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 \mathbb{R}^d . Since $q_t(x) = xk_t^*(a_t^+)^2k_tx^*$, the eigenvalues of q_t are $(a_t^+)_1^2 \ge (a_t^+)_2^2 \ge$ $\cdots \ge (a_t^+)_d^2$. 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 $i \le i_1$. Since for $1 \le j \le d$,

$$(a_t)_i^2 \langle n_i.(t), x^j(t) \rangle_0^2 \le q_t(x^j(t)) \le (a_t^+)_1^2 \approx (a_t^+)_i^2 \approx (a_t)_i^2 \approx e^{2\lambda_i t}$$

for large t, it follows that $\forall \varepsilon > 0$, $\langle n_i.(t), x^j(t) \rangle_0^2 \le e^{\varepsilon t}$ for sufficiently large t, hence, $\langle n_i.(t), n_i.(t) \rangle_0 = \sum_{j=1}^d \langle n_i.(t), x^j(t) \rangle_0^2 \le de^{\varepsilon t}$. This proves (28) for $i \le i_1$ and any j.

Suppose that we have proved (28) for $i \leq i_k$. Let $D_k(t) = \det [\{x_q^p(t)\}_{i_k . We will show that for any <math>\varepsilon > 0$,

$$|D_k(t)| \ge e^{-\varepsilon t}$$
 for suficiently large $t > 0.$ (29)

If this is not true, we can extract a sequence of t going to infinity such that for some $\varepsilon > 0$, $|D_k(t)| \le e^{-\varepsilon t}$ 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 $\forall j > i_k, |v_j(t)| \le e^{-\varepsilon t}$ along that sequence of t. Since for $p \le i_k, \lambda_p > \lambda_{i_k+1}$ and

$$e^{2\lambda_p t} \langle n_p.(t), v(t) \rangle_0^2 \approx (a_t)_p^2 \langle n_p.(t), v(t) \rangle_0^2 \le q_t(v(t)) \le (a_t^+)_{i_k+1}^2 \approx e^{2\lambda_{i_k+1} t},$$

we see that for $p \leq i_k$, $\langle n_{p}(t), v(t) \rangle_0 = \sum_{j=1}^d n_{pj}(t)v_j(t)$ 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 $j > i_k = p$, $n_{pj}(t)v_j(t)$ 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 $p = i_k - 1, i_k - 2, ..., 1$, 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 $i_k < i \le i_{k+1}$ for $1 \le k < l$. Define

$$h_p(t) = \sum_{j=1}^d n_{ij}(t) x_j^p(t), \text{ for } p = i_k + 1, i_k + 2, \dots, d.$$
 (30)

Then $(a_t)_i^2 [h_p(t)]^2 \leq q_t(x^p(t)) \leq (a_t^+)_{i_k+1}^2 \approx (a_t)_i^2 \approx e^{2\lambda_i t}$, hence, $\forall \varepsilon > 0$, $|h_j(t)| \leq e^{\varepsilon t}$ for sufficiently large t > 0. Since $n_{ij}(t) = 0$ for $j \leq i_k$, we may solve for $n_{ij}(t)$, $i_k < j \leq d$, from the linear system of equations (30). The determinant in Cramer's solution formula is just D_k . By (29), we see that $n_{ij}(t)$ 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: $\mathcal{N} \to N$ 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

$$\mathcal{N}_{\Theta} = \{ Y \in \mathcal{N}; \ Y_{ij} = 0 \text{ for } i \le i_k < j, \ 1 \le k < l \}$$

$$(31)$$

and

$$\mathcal{N}'_{\Theta} = \{ Y \in \mathcal{N}; \ Y_{ij} = 0 \text{ for } i_{k-1} < i \le i_k \text{ and } j \le i_k, \ 1 \le k \le l \}.$$
(32)

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

Note that $\mathcal{N} = \mathcal{N}_{\Theta} \oplus \mathcal{N}'_{\Theta}$ and $\mathcal{N}_{\emptyset} = \{0\}$. Moreover, both \mathcal{N}_{Θ} and \mathcal{N}'_{Θ} are sub Lie algebras of \mathcal{N} . In fact, \mathcal{N}'_{Θ} is an ideal of \mathcal{N} , that is, $\forall Y \in \mathcal{N}$ and $Z \in \mathcal{N}'_{\Theta}$, $[Y, Z] \in \mathcal{N}'_{\Theta}$. Let $N_{\Theta} = \exp(\mathcal{N}_{\Theta})$ and $N'_{\Theta} = \exp(\mathcal{N}'_{\Theta})$. Then both N_{Θ} and N'_{Θ} are Lie subgroups of N with N'_{Θ} normal. We have the decomposition $N = N_{\Theta}N'_{\Theta}$ in the sense that the map $(n_1, n_2) \mapsto n_1n_2$ is a diffeomorphism: $N_{\Theta} \times N'_{\Theta} \to N$. 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 $n_t = n_t^{\Theta} n_t'$ with $n_t^{\Theta} \in N_{\Theta}$ and $n_t' \in N_{\Theta}'$. 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) $K_{\Theta}k_t \to K_{\Theta}k_{\infty}$ as $t \to \infty$ for some $k_{\infty} \in K$; (b) $\lim_{t\to\infty} (1/t) \log a_t = \lim_{t\to\infty} (1/t) \log a_t^+ = \operatorname{diag}(e^{\lambda_1}, \dots, e^{\lambda_d});$ (c) $\forall \varepsilon > 0, |n_t^{\Theta}| \le e^{\varepsilon t}$ for sufficiently large t > 0; (d) $n'_t \to n'_{\infty}$ as $t \to \infty$ for some $n'_{\infty} \in \tilde{P}_{\Theta}k_{\infty}$, consequently, $\tilde{P}_{\Theta}n_t \to \tilde{P}_{\Theta}k_{\infty}$; (e) $p_t K_{\Theta} \to K_{\Theta} \text{ as } t \to \infty$.

Proof. (a) and (b) are proved in Lemma 3 and Lemma 6. Because the map $(n^{\Theta}, n') \mapsto$

 $n = n^{\Theta} n'$ is a diffeomorphism: $N_{\Theta} \times N'_{\Theta} \to N$, (c) follows from Lemma 8. The main task is to prove (d). From (27) and $dn_t = d(n_t^{\Theta} n'_t) = (\circ dn_t^{\Theta})n'_t + n_t^{\Theta}(\circ dn'_t)$, we may obtain the sde's for n_t^{Θ} and n'_t . For $Y \in \mathcal{G}$, let $Y_{\mathcal{N}} = Y_{\Theta} + Y'$ be the decomposition $\mathcal{N} = \mathcal{N}_{\Theta} \oplus \mathcal{N}'_{\Theta}$. Note that for $a \in A$, the linear map $\mathrm{Ad}(a)$: $\mathcal{N} \to \mathcal{N}$ leaves this decomposition invariant. We have

$$dn_t^{\Theta} = \sum_{j=0}^r \{ \operatorname{Ad}(a_t^{-1}) [\tilde{X}_j(u_t)]_{\Theta} \} n_t^{\Theta} \circ dw_t^j$$
(33)

and

$$dn'_{t} = \sum_{j=0}^{\prime} \{ \mathrm{Ad}((n_{t}^{\Theta})^{-1}) \mathrm{Ad}(a_{t}^{-1}) [\tilde{X}_{j}(u_{t})]' \} n'_{t} \circ dw_{t}^{j}.$$
(34)

Let $F_i^{\Theta}(t) = \operatorname{Ad}(a_t^{-1})[\tilde{X}_j(u_t)]_{\Theta}$ and $F'_i(t) = \operatorname{Ad}(a_t^{-1})[\tilde{X}_j(u_t)]'$. Then $F_i^{\Theta}(t) \in$ \mathcal{N}_{Θ} and $F'_{i}(t) \in \mathcal{N}'_{\Theta}$. Note that for $a \in A$ and $Y \in \mathcal{G}$, $[\mathrm{Ad}(a^{-1})Y]_{ij} =$ $a_i^{-1}a_jY_{ij}$. By Lemma 6, $(a_t)_i \approx e^{\lambda_i t}$ for large t > 0. It follows that for $Y \in \mathcal{N}$, $[\operatorname{Ad}(a_t^{-1})Y]_{ij} \approx e^{-(\lambda_i - \lambda_j)t} Y_{ij}$. If $Y \in \mathcal{N}'_{\Theta}$, then either $(\lambda_i - \lambda_j) > 0$ or $Y_{ij} = 0$, hence, $\operatorname{Ad}(a_t^{-1})Y$ converges to 0 exponentially as $t \to \infty$ for $Y \in \mathcal{N}'_{\Theta}$. This implies that almost surely $F_i(t)'$ converges to 0 exponentially as $t \to \infty$. The same thing can be said for the coefficients $Ad((n_t^{\Theta})^{-1})F'_i(t)$ 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.

$$dn'_{t} = \sum_{j=1}^{r} \{ \operatorname{Ad}((n_{t}^{\Theta})^{-1})F'_{j}(t)\}n'_{t} dw_{t}^{j}$$

+
$$\{ \frac{1}{2} \sum_{j=1}^{r} \operatorname{Ad}((n_{t}^{\Theta})^{-1})F'_{j}(t)\operatorname{Ad}((n_{t}^{\Theta})^{-1})F'_{j}(t)$$

+
$$\frac{1}{2} \sum_{j=1}^{r} \operatorname{Ad}((n_{t}^{\Theta})^{-1})[F'_{j}(t), F_{j}^{\Theta}(t)]$$

$$+\frac{1}{2}\sum_{j=1}^{r} \operatorname{Ad}((n_{t}^{\Theta})^{-1})\operatorname{Ad}(a_{t}^{-1})[[\tilde{X}_{j}(u_{t})]', [\tilde{X}_{j}(u_{t})]_{\mathscr{A}}] \\ +\frac{1}{2}\sum_{j=1}^{r} \operatorname{Ad}((n_{t}^{\Theta})^{-1})\operatorname{Ad}(a_{t}^{-1})[Y_{j}\tilde{X}_{j}(u_{t})]' + \operatorname{Ad}((n_{t}^{\Theta})^{-1})F_{0}'(t)]n_{t}' dt,$$

where $Y_j(u) = H(X_j)(u) + u[\tilde{X}_j(u)]_{\mathscr{X}}$ 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, $n'_t \to n'_\infty$ as $t \to \infty$ for some $n'_\infty \in \mathscr{N}'_{\Theta}$.

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

To prove (e), it suffices to show that any limiting point of $p(t) = p_t$ is contained in K_{Θ} . If this is not true, then along some sequence of $t \to \infty$, p(t) converges to some $p \in (K - K_{\Theta})$. Then there exist indices i > j such that $\lambda_i < \lambda_j$ and $p_{ij} \neq 0$. By (b) and Lemma 8, $[s_t k_t^*]_{ij} = [a_t n_t k_t^*]_{ij} = a_i(t) \sum_{b=1}^d n_{ib}(t)k_{jb}(t)$ grows at the exponential rate λ_i . On the other hand, this is also equal to $[p_t a_t^+ k_t k_t^*]_{ij} =$ $[p_t a_t^+]_{ij} = p_{ij}(t)a_j^+(t)$, 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 $D\psi_t(u) = us_t$, with $u = (u_1, \ldots, u_d) \in \pi^{-1}(m)$ and $m \in M$, be the decompositions given by Theorem 1. Then $D\psi_t(m) = us_t u^{-1} = ua_t n_t^{\Theta} n'_t u^{-1}$ with $n'_t \to n'_{\infty}$. Therefore, for large time t > 0, the linear map $D\psi_t(m)$: $T_m M \to T_m M$ may be regarded as a fixed random linear map $un'_{\infty} u^{-1}$, followed by another linear map $ua_t n_t^{\Theta} u^{-1}$ which leaves the subspaces

$$U_1 = \text{span}(u_1, \dots, u_{i_1}), \quad U_2 = \text{span}(u_{i_1+1}, \dots, u_{i_2}), \dots,$$

 $U_l = \text{span}(u_{i_{l-1}+1}, \dots, u_d)$

of $T_m M$ invariant and changes the length of vectors in each U_k at the exponential rate λ_{i_k} for $1 \le k \le l$.

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)
- 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)