第22卷第4期 华东交通大学学报 Vol.22 No.4
2005年08月 Journal of East China Jiaotong University Aug., 2005

文章编号:1005－0523(2005)04－0161－04

一个随机环境下的NLAR模型的极限行为

俞　政,肖欣玲

(中南大学 数学科学与计算技术学院,湖南 长沙 410075)

摘要:一个非线性门限自回归模型的变形 $X_{n+1}=\Phi(X_n)+\varepsilon_{n+1}(Z_{n+1})$ 被讨论.在这个新的模型中,$\{Z_n\}$ 是一个有限状态的马尔可夫链.对这个马尔可夫链的每一个状态 i,有一个独立同分布的随机变量的序列 $\{\varepsilon_n(i)\}$ 与之对应,而 $\varepsilon_n(Z_n)=\sum_i\varepsilon_n(i)I_{\{i\}}(Z_n)$.在这篇文章中,讨论了由这个模型确定的序列 $\{X_n\}$ 的极限行为.一个关于这个序列在某种意义下以几何速率收敛的充分条件被建立.

关 键 词:遍历性;非线性时间序列;随机环境.

中图分类号:TM392.3　　　　**文献标识码**:A

1 基本术语

设$(\Omega,\hbar,P_r)$是一个概率空间,在以下的行文中涉及到的随机变量,随机向量均假定是定义在该空间上的.设p为一正整数,R^p 记维实空间, B_p 为 R^p 上的Borel σ 代数.

令 $E=\{1,2,\cdots,e\}$ 是一个有限集合,F 记 E 的所有子集生成的 σ—代数,$\{Z(n),n\geq 0\}$ 表示一个定义在$(\Omega,\hbar,P_r)$上的不可约非周期的齐次马氏链,它的状态空间为(E,F);$\{\varepsilon_n(1)\},\cdots,\{\varepsilon_n(1)\},\cdots,\{\varepsilon_n(e)\}$ 是 e 个 $i.i.d$ 的随机变量序列,其中每一个都是定义在上$(\Omega,\hbar,P_r)$上,以(R^p,B_p)为状态空间的.

设 $Z_n=Z(n)$,$\forall$ n$\geq$0,且 $\varepsilon_n(Z_n)=:\sum_{i=1}^{e}\varepsilon_n(i)I_{\{i\}}(Z_n)$,

定义1.1 令 $\hat{x}_{n+1}=\Phi(\hat{x}_n)+\bar{\varepsilon}_{n+1}(Z_{n+1})$;　$\hat{x}_0=\in R^p$ (1)

其中 $\bar{\varepsilon}_{n+1}(Z_{n+1})=(\varepsilon_{n+1}(Z_{n+1}),0\cdots,0)'$,$\Phi$: $R^p\to R^p$ 是一个Borel可测映射,且有形式 $\Phi(\hat{x})=(\varphi(x_1,\cdots,x_p),x_1,\cdots,x_{p-1})'$,$\varphi$ 是一个 R^p 到 R^1 的Borel可测映射,$\hat{x}=(x_1,\cdots,x_p)'\in R^p$;

称由(1)式确定的模型为随机环境下的NLAR模型.

定义1.2 设 p 维向量随机序列 $\{X_n\}$ 由(1)定义,是一概率分布.

若当 $X_0\sim F$,则称 F 为模型(1)的不变概率分布;

定义1.3 设模型(1)有唯一的不变概率分布 F,且对任何的初始状态 $X_0=x$,由(1)迭代产生的 X_n 的概率分布记为 F_n^x.如果存在常数 ρ:$0<\rho<1$,使得 $\lim_{n\to\infty}\rho^{-n}\|F_n^x-F\|_r=0$,其中 $\|\cdot\|_r$ 为全变差范数,则称模型(1)为伴随几何遍历的.

定义1.4 对于模型(1),称序列$\{(X_n,Z_n)\}$为其导出序列.

收稿日期:2004－12－18

基金项目:国家自然科学基金(No.10171009),高校博士点基金(No.20010533001),"985行动计划"和"211工程"资助项目

作者简介:俞政(1957－),男,湖南长沙人,副教授.

此外,凡文中涉及的一般状态马氏链及非线性时间序列分析的知识,可参见[2],[3].

2 主要结果

这一节建立关于模型(1)的伴随几何遍历性的结果,若干将被引用的条件列举如下:

$C1$ $\forall$ i$\in E$, $E\varepsilon_n(i)=0$, $E|\varepsilon_n(i)|<\infty$;

$C2$ $\{Z_n\}$, $\{\varepsilon_n(1)\}$, $\cdots$, $\{\varepsilon_n(e)\}$相互独立且$\forall$ i$\in E$, $n\geq 0$, $\varepsilon_{n+1}(i)$与$\{X_k, k\leq n\}$独立, Z_{n+1}与X_0独立;

$C3$ $\forall$ i$\in E$, $\varepsilon_n(i)$有处处为正的下半连续的分布密度函数 $\gamma_i(\cdot)$.

引理 2.1 设$\{(X_n, Z_n)\}$是模型(1)的导出序列,在条件 $C1$, $C2$ 之下,$\{(X_n, Z_n)\}$是定义在$(\Omega, \hbar, P_r)$上,以$(R^p\times E, B_p\times F)$为状态空间的齐次马氏链

证明 显然.

以下,令

$$p_{ij}=P_r(Z_{n+1}=j|Z_n=i), n\geq 0, i, j\in E,$$
$$P((\hat{x}, i), \Lambda\times\{j\}=P_r(X_{n+1}\in\Lambda, Z_{n+1}=j|X_n=\hat{x}, Z_n=i),$$
$$n\geq 0, i, j\in e, (\hat{x}, i)\in R^p\times E, \Lambda\times\{j\}\in B_p\times F$$

并且, $\forall$ l≥ 2,

$$P^{(l)}((\hat{x}, i), \Lambda\times\{j\})=P_r(X_{n+1}\in\Lambda, Z_{n+1}=j|Y_n=\hat{x}, Z_n=i);$$
$$n\geq 0, i, j\in E, (\hat{x}, i)\in R^p\times E, \Lambda\times\{j\}\in B_p\times F.$$

由条件概率的性质,得 $P^{(1)}((\hat{x}, i), \Lambda\times\{j\})=\sum_{k\in E}\int_{R^p}P((\hat{x}, i), d\hat{\omega}\times\{k\})P^{(l-1)}((\hat{\omega}, k), \Lambda\times\{j\})$ (2)

注意到关于模型(1)的假设之一是:$\{Z_n\}$是不可约的,从而可知,对(E, F)上的任一测度 λ, $\{Z_n\}$是 λ一不可约的.适当地选取一个测度,仍以 λ 记之,满足$\forall$ i$\in E$, $\lambda\{i\}>0$ 于是可以导出一个定义在$(R^p\times E, B_p\times F)$上的测度 $\mu_m\times\lambda$,这里 μ_p 为(R^p, B_p)上的 Lebesgue 测度,使得 $\mu_p(A)>0$ 蕴含 $\mu_p\times\lambda(A\times\{j\})>0$, $A\in B_p$, $i\in E$.

引理 2.2 设模型(1)满足 $C1$ 和 $C2$,$\{(X_n, Z_n)\}$是模型(1)的导出序列,令 $\Lambda=\Lambda_1\times\Lambda_2\times\cdots\times\Lambda_p$, $\Lambda_k\in B_k$, $k=1, 2, \cdots, p$; $I_{\Lambda k}(\cdot)$表示 Λ_k 的示性函数; 则它的转移函数为

$$P((\hat{x}, i), \Lambda\times\{j\})=p_{ij}\prod_{q=1}^{p-1}I_{\Lambda_{q+1}}(x_q)\int_{\Lambda 1}r_j(y_1-h(\hat{x}))dy_1;$$

对 l: $2\leq l\leq p-1$,

$$P^{(1)}((\hat{x}, i), \Lambda\times\{j\})=\prod_{q=1}^{p-l}I_{\Lambda_{q+1}}(x_q)\sum_{k_1, \cdots, k_{l-1}\in E}p_{ik_1}\cdots p_{k_{l-1}j}\int_{\Lambda_1\times\cdots\times\Lambda_1}rk_1(y_l-h(\hat{x}))\cdot r_{k_2}(y_{l-1}-h(y_l, x_1, \cdots, x_{p-1}))\cdots$$

$$\cdot r_{k_{l-1}}(y_2-h(y_3, \cdots, y_1, x_1, \cdots, x_{p-l+2}))\cdot r_j(y_1-h(y_2, \cdots, y_l, x_1, \cdots, x_{p-l+1}))dy_l\cdots dy_1;$$

$$P^{(p)}((\hat{x}, i), \Lambda\times\{j\})=\sum_{k_1, \cdots k_{p-1}\in E}p_{ik_1}\cdots p_{k_{p-1}j}\int_{\Lambda}r_{k_1}(y_p-h(\hat{x}))\cdot r_{k_2}(y_{p-1}-h(y_p, x_1, \cdots, x_{p-1}))\cdots$$

$$\cdot r_{k_{p-1}}(y_2-g(y_3, \cdots, y_p, x_1, x_2))\cdot r_j(y_1-h(y_2, \cdots, y_p, x_1))dy_p\cdots dy_1;$$

当 $1\leq l\leq p-1$ 时,

$$P^{(p+l)}((\hat{x}, i), \Lambda\times\{j\})$$
$$=\sum_{k_1, \cdots, k_{l-1}\in E}P_{ik_1}\cdots P_{k_{l-1}k_1}\int_{R^l}r_{k1}(y_{p+l}-h(\hat{x}))\cdots r_{k_l}(y_{p+1}-h(y_{p+2}, \cdots, y_{p+l}, x_1, \cdots, x_{p-l+1}))dy_{p+l}\cdots dy_{p+1}$$
$$\sum_{k_l, \cdots, k_{p+l-1}\in E}P_{k_lk_{l+1}}\cdots P_{k_{p+l-1}j}\int_{\Lambda}r_{l+1}(y_p-h(y_{p+1}, \cdots, y_{p+1}, x_1, \cdots, x_{p-1}))\cdots r_j(y_1-h(y_2, \cdots, y_{p+1}))dy_p\cdots dy_1;$$

$$P^{(2p)}((\hat{x}, i), \Lambda\times\{j\})=\sum_{k_1, \cdots, k_{p-1}\in E}P_{ik_1}\cdots P_{k_{p-1}k_p}\int_{R^p}r_{k1}(y_{2p}-h(\hat{x}))\cdots r_{k_p}(y_{p+1}-h(y_{p+2}, \cdots, y_{p+l, x_1}))dy_{2p}\cdots$$
$$dy_{p+1}$$

$$\sum_{k_1, \cdots, k_{2}p-1\in E}P_pk_{p+1}\cdots P_{k_2p-1}j\int_{\Lambda}r_{k_{p+1}}(y_p-h(y_{p+1}, \cdots, y_{2p}))\cdots r_j(y_1-h(y_2, \cdots, y_{p+1}))dy_p\cdots dy_1;$$

对 $1\leq l\leq m-1$, $n\geq 2$,

$$P^{(np+l)}((\hat{x},i),\Lambda\times\{j\})=\sum_{k_1,\cdots,k_{l-1}\in E}P_{ik_1}\cdots P_{k_{l-1}k_l}\int_{R^l}r_{k1}(y_{np+1}-h(\hat{x}))\cdot r_{k_2}(y_{np+l-1}-h(y_{np+l},x_1,\cdots,x_{p-1}))\cdots$$

$$\cdot r_{k_l}(r_{np+1}-h(y_{np+2},\cdots,y_{np+l},x_1,\cdots,x_{p+l-1}))dy_{np+l}\cdots dy_{np+1}$$

$$\cdot\sum_{k_l,\cdots,k_{p+l-1}\in E}P_{k_lk_{l+1}}\cdots P_{k_{p+l-1}k_{p+l}}\int_{R^p}r_{k_{l+1}}(y_{np}-h(y_{np+1},\cdots,y_{np+l},x_1,\cdots,x_{p-l}))\cdots$$

$$\cdot r_{k_{p+l}}(y_{(n-1)p+1}-h(y_{(n-1)p+2},\cdots,y_{np+1}))dy_{np}\cdots dy_{(n-1)p+1}\cdots\cdot$$

$$\cdot\sum_{k(n-1)p+l,\cdots k_{np+l-1}\in E}P_{k_{(n-1)p+l}k_{(n-1)p+l+1}}\cdots P_{k_{np+l-1}j}\int_{\Lambda}r_{k_{(n-1)p+l-1}}(y_p-h(y_{p+1},\cdots,y_{2p}))\cdots r_j(y_1-h(y_2,\cdots,y_{p+1}))dy_p\cdots dy_1$$

证明　由归纳法并反复应用(2)即可.

引理2.3　设模型(1)满足 $C1$, $C2$ 和 $C3$,则(1)的导出序列 $\{(X_n,Z_n)\}$ 是 $\mu_p\times\lambda$ 不可约和非周期的.

证明　类似于[2]中命题2.1.1的证明,利用引理2.2的结果证之,即可.

引理2.4　设模型(1)满足 $C1$, $C2$ 和 $C3$,并且 Φ 在 R^p 中的任何有界集上有界.则 $\forall$ $J\subset E$ 及 R^p 中的任一有界可测集合 K, $K\times J$ 是一个关于(1)的导出序列 $\{(X_n,Z_n)\}$ 的小集.

证明　类似于[2]中命题2.1.1的证明,利用引理2.2的结果即可证之.

对模型(1)中的变换 φ,引入下面的记号:

$$y_1=\varphi=(y_0,y_{-1},\cdots,y_{-p+1})\triangleq\varphi_1(y_0,y_{-1},\cdots,y_{-p+1})$$

$$y_2=\varphi(y_1,y_0,\cdots,y_{-p+2})=\varphi(\varphi_1(y_0,\cdots,y_{-p+1}),y_0,\cdots,y_{-p+2})\triangleq\varphi_2(y_0,\cdots,y_{-p+1})$$

一般地

$$y_k=\varphi(y_{k-1},\cdots,y_{k-p})=\cdots=\varphi_k(y_0,y_{-1},\cdots,y_{-p+1}),\qquad K\geq 1\tag{2.1}$$

定理2.1　该模型(1)满足 $C1$, $C2$ 和 $C3$,变换 φ 满足下列条件:

(1) 存在正数 C_k,使得对任何 y_0', y_0, y_{-1}, $\cdots$, y_{-p+1} 和 $k\geq 1$,有

$$|\varphi_k(y_0,y_{-1},\cdots,y_{-p+1})-\varphi_k(y_0',y_{-1},\cdots,y_{-p+1})|\leq C_k|y_0-y_0'|;\tag{2.2}$$

(2)存在正常数 e 和 M 及 C,使得对任何 $y_0,y_{-1},\cdots,y_{-p+1}$ 和 $k\geq 1$,有

$$|\varphi_k(y_0,y_{-1},\cdots,y_{-p+1})|\leq M\rho^k(|y_0|+\cdots+y_{-p+1})+C;\tag{2.3}$$

则(1)是伴随几何遍历的.

证明　由(2.1)和(2.3)易知,在定理给定的条件下 $\forall=(x_1,\cdots,x_p)'\in R^p$,有

$$|\varphi(\hat{x})|\leq M\rho(|y_0|+\cdots+y_{-p+1})+C;$$

即 $\varphi(\hat{x})$ 在 R^p 中任一有界集上有界,从而由 Φ 的定义可知, Φ 在 R^p 中任一有界集上有界,于是由引理2.1,引理2.3和引理2.4知 $\{(X_n,Z_n)\}$ 是一个 $\mu_p\times\lambda$ 不可约和非周期的马氏链,且对 R^p 中任何正 μ_p 测度的有界集 D, $D\times E$ 都是 $\{(X_n,Z_n)\}$ 的小集.

取准则函数 $g(\hat{x},i)=|x_1|+\cdots+|x_p|\triangleq\|\hat{x}\|_1$, $\forall=(x_1,x_2,\cdots x_p)'\in R^p$ 及 $i\in E$;

以下,与[1]中定理4.2.15的证明类似,可证 $\{(X_n,Z_n)\}$ 是几何遍历的,由此立即可得(1)是伴随几何遍历的.

参考文献:

[1] 安鸿志,陈敏.非线性时间序列分析[M].上海:上海科学技术出版社,1998.
[2] 盛昭瀚,王涛,刘德林.非线性时间序列模型的稳定性分析—遍历性理论与应用[M].北京:科学出版社,1993.
[3] S. P. Meyn and R. L. Tweedie. Markov Chains and Stochastic Stability, Beijing World Publishing Corporation, 1999.
[4] K.S. Chan and H. Tong. On use of the Deterministic Lyapunov Function for the Ergodicity of Stochastic Difference Equations. J. Adv. Appl. Probab. 17, 666-678, 1985.
[5] Hongzhi An, Min Chen and Fuchun Huang. The geometric ergodicity and existence of moments for a class of non-linear time series model. J. Statistics & Probability Letters. 31, 213-224, 1997.

The Limit Behavior of a NLAR Model under the Random Environment

YU Zheng, XIAO Xin-ling

(School of Math. Sciences & Computing Technology, Changsha 410075, China)

Abstract: We study the problem of a variety of nonlinear threshold autoregressive model $X_{n+1} = \Phi(X_n) + \varepsilon_{n+1}(Z_{n+1})$ in which $\{Z_n\}$ is a Markov chain with finite state space, and for every state of the Markov chain, $\{\varepsilon_n(i)\}$ is a sequence of independent and identically distributed random variables, and $\varepsilon_n(Z_n) =: \sum_i \varepsilon_n I_{\{i\}}(Z_n)$. Also, in this paper, the limit behavior of the sequence $\{X_n\}$ defined by the above model is investigated and a sufficient condition for the convergence of sequence $\{X_n\}$ with a geometric convergence rate is provided.

Key words: ergodic; nonlinear time series; random environment.

(上接第157页)

A New Dynamic Threshold Secret Sharing Scheme to Identify Cheaters

HAN Jin-guang, KANG Bao-yuan, WANG Qing-ju

(College of Mathematics Science and Computing Technology, Central South University, Changsha, Hunan 410075, China)

Abstract: A threshold sheme is a method whereby pieces of the secret , called shares are distributed to participants so that : the secret can be reconstructed from the knowledge of any or more shares, and the secret cannot be reconstructed from the knowledge of any or less shares. A dynamic secret sharing sheme is an especial threshold sheme. Its character is that the secret can be renewed without modifying and rebaking any share. This paper proposes a new dynamic threshold secrete sharing sheme to identify cheaters by integrating the discrete logarithm problem and the integer factorization problem with higher roots problem. This paper also discusses the security of the sheme.

Key words: crptography; secret sharing; dynamic threshold scheme