

关于图值随机元序列的强极限定理

汪忠志, 李文喜

(安徽工业大学数理科学与工程学院, 安徽 马鞍山 243002)

摘 要: 本文研究在局部连通图中取值的随机元的 r -阶均值集、 r -阶广义样本均值集的基本性质及其极限性质. 利用关于随机元的分离引理以及随机游动的常返性, 得到了关于图值随机元序列广义强大数定理. 推广了已有的结果.

关键词: 强大数定律; 图; r -阶权函数; r -阶均值集; r -阶广义样本均值; 随机游动

MR(2010) 主题分类号: 60F15

中图分类号: O211.4

文献标识码: A

文章编号: 0255-7797(2017)01-0118-11

1 引言

概率极限理论是概率论的重要分支之一. 经典的极限理论曾经是概率论研究的中心课题, 近现代极限理论的研究至今方兴未艾. 自上世纪 30 年代以来, 许多学者致力于将概率论推广到各种数学结构中. 著名概率学家 Loève 在阐述概率论的基本特征时曾指出“到今天, 概率论在数学上已经发展的充分成熟, 于是就呈现出来这样一种预兆, 即要摆脱这些限制而考虑从测度空间到愈益抽象的空间的更一般的函数族……”. 关于抽象空间上的概率理论的研究, 可以上溯到 1935 年 Kolmogorov^[1] 关于 Banach 空间上的概率分布的特征泛函以及 1948 年 Fréchet^[2] 关于 Banach 空间上的 Gauss 分布的工作.

关于抽象空间上的随机元的定义, 有多种不同的方式. 在一般情况下, 它们还确实是彼此不同的概念. 不同的定义有各自的优缺点, 分别适应研究不同问题的需要. 对取值于抽象空间上的随机元的随机过程的合理解释与深刻的应用激发了许多学者对一般拓扑空间上的概率的研究, 而研究的关键是给出随机元“均值”(平均)的合理定义以及相应的收敛性概念.

Banach 空间上的随机元 $x_1, x_2, \dots, x_n$ 的均值可以自然地定义为 $n^{-1}(x_1 + x_2 + \dots + x_n)$, 利用 Galfand-Pettis 积分可以定义随机元的均值(期望)(参见文 [3]). 与线性空间不同, 在一般(非线性)拓扑空间中, 必须寻找合适的途径来定义随机元的“均值”以及相应的收敛性概念. Fréchet 在文 [2] 中讨论了一般度量空间上的概率, 并且给出了完备度量空间 (X, d) 上关于概率测度 μ 的均值(亦称 Fréchet 均值)的定义. 即设 $\xi: \Omega \rightarrow X$ 是定义在概率空间 $(\Omega, \mathcal{F}, P)$, 在 (X, d) 中取值的随机元. 令

$$\Lambda = \arg \inf_{x' \in X} \int d^2(x, x') d\mu(x),$$

称 Λ 为随机元 ξ 的均值集 (Frechet 均值).

*收稿日期: 2014-08-22

接收日期: 2015-03-19

基金项目: 国家自然科学基金 (11071104); 国家社会科学基金 (13BJY011); 安徽省自然科学基金 (1308085QF113; 1408085MA04); 安徽工业大学研究生创新基金 (2012090) 资助.

作者简介: 汪忠志, 男, 安徽安庆, 教授, 主要研究方向: 概率论及其应用.

可以看出这个定义显然是包含了最小二乘法的基本思想. 最早获得度量空间上随机元的极限定理的是 Ziezold, 他(她)在文 [4] 中讨论了可分拟度量空间上的随机元的强大数定律, 随后 Sverdrup-Yhygeson [5] 讨论了取值于连通紧空间上的随机元的强大数定律, Bhattacharya 和 Patrangenaru [6] 给出了有界子集均为紧子集的度量空间上的随机元的极限定理, 推广了 Ziezold [4] 的结果. 最近, Natalia Mosina [7,8] 等给出了在图与群上取值的随机元的一个新的概率框架, 讨论了随机元均值集(期望)的若干性质及大数定律, 并用在辫群(Braid group)上取值的随机元的均值集和大数定律, 破解了一个基于辫群上共轭元的难解问题的零知识证明协议, 这在密码学上具有十分重要的意义.

本文在文献 [7] 的基础上, 提出了在局部有限图上取值的随机元的 r -阶权函数、 r -阶均值集以及 r -阶广义样本均值集等概念, 讨论了其基本性质, 并且就随机元的均值集是单点集和两点集情形, 获得了关于图值随机元序列的广义强大数定律.

2 预备知识

设 $(\Omega, \mathcal{F}, P)$ 是固定的概率空间, $\Gamma = (V(\Gamma), E(\Gamma))$ 是局部有限图. 考虑定义在可测空间 $(\Omega, \mathcal{F})$ 上且在 Γ 的顶点集中取值的随机元 $\xi: \Omega \rightarrow V(\Gamma)$.

假设 μ 是由随机元 ξ 在 $V(\Gamma)$ 的原子上诱导出的概率测度

$$\mu(s) = P\{\omega \in \Omega | \xi(\omega) = s\}, \quad \forall s \in V(\Gamma), \quad (2.1)$$

记为 $\mu_\xi(\cdot)$.

现在在新的概率空间 $(V(\Gamma), \mathcal{S}, \mu)$ 上来研究随机元 $\xi: \Omega \rightarrow V(\Gamma)$.

定义 2.1 设 $\forall v \in V(\Gamma)$. 令

$$M_\xi^{(r)}(v) := \sum_{i \in V(\Gamma)} d^r(v, i) \mu(i), \quad r > 0, \quad (2.2)$$

称之为 v 关于测度 μ 的 r -阶权函数, 其中 $d(v, i)$ 表示 v 与 i 在 Γ 中的距离.

如果 $M_\xi^{(r)}(v) < \infty$, 则称权函数 $M_\xi^{(r)}(v): V(\Gamma) \rightarrow [0, \infty]$ 在点 v 有定义.

注 一般来说, 权函数并不总是有限的. 本文中如无特别说明, 总假设 $M^{(r)}(\cdot) < \infty$ ($r > 0$), 即 $M^{(r)}(\cdot)$ 在 $V(\Gamma)$ 的每一点都有定义.

定义 2.2 设 $(V(\Gamma), \mathcal{S}, \mu)$ 为所考虑的概率空间, $\xi: \Omega \rightarrow V(\Gamma)$ 是随机元, $r > 0$. 令

$$\mathbb{E}(\xi) := \{v \in V(\Gamma) | M_\xi^{(r)}(v) \leq M_\xi^{(r)}(u), \quad \forall u \in V(\Gamma)\}, \quad (2.3)$$

并称之为随机元 ξ 的 r -阶均值集.

注 值得注意的是, 如果在 (2.3) 式中分别令 $r = 2, r = 1, r \rightarrow 0$ 以及 $r \rightarrow \infty$, 上述定义的均值集(期望)可以导出对应于 Euclidean 空间中随机变量的均值、中位数、众数以及中列数.

设 $\{\xi_i\}_{i=1}^\infty$ 是一列定义在概率空间 $(\Omega, \mathcal{F}, P)$ 上, 在图 Γ 中取值的独立同分布(i.i.d)随机元 $\xi_i: \Omega \rightarrow V(\Gamma)$, $i = 1, 2, \dots$, $0, a_1, a_2, \dots$ 是一列固定的整数. $\forall \omega \in \Omega$, 令 $\mu_{a_n, n}(u; \omega)$ 是 u 在时间段 $a_n + 1 - a_n + n$ 内出现的相对频率, 即

$$\mu_{a_n, n}(u; \omega) := \frac{\#\{i | \xi_i(\omega) = u, \quad a_n + 1 \leq i \leq a_n + n\}}{n}. \quad (2.4)$$

令

$$M_{a_n, n}^{(r)}(v) := \sum_{s \in V(\Gamma)} d^r(v, s) \mu_{a_n, n}(s) = \frac{1}{n} \sum_{i=a_n+1}^{a_n+n} d^r(v, \xi_i), \quad (2.5)$$

称 $M_{a_n, n}^{(r)}(\cdot)$ 为 r -阶广义样本权函数, 其中 $\sharp(A)$ 表示集合 A 中元素的个数.

定义 2.3 集

$$S_{a_n, n} = S(\xi_{a_n+1}, \dots, \xi_{a_n+n}) := \{v \in V(\Gamma) | M_{a_n, n}^{(r)}(v) \leq M_{a_n, n}^{(r)}(u), \forall u \in V(\Gamma)\}, \quad (2.6)$$

称之为随机元 $\{\xi\}_{i=a_n+1}^{a_n+n}$ 的 r -阶广义样本均值集.

为了以下证明的需要, 给出几个基本引理.

引理 2.1 设 Γ 是连通图, $u, v \in V(\Gamma)$. 如果 $M^{(r)}(u) < \infty$, 则 $M^{(r)}(v) < \infty$.

证 令 $d(u, v) = d$, 由三角形不等式

$$d(v, i) \leq d(u, i) + d(u, v) = d(u, i) + d, \forall i \in V(\Gamma),$$

有

$$\begin{aligned} M^{(r)}(v) &= \sum_{i \in V(\Gamma)} d^r(v, i) \mu(i) \leq \sum_{i \in V(\Gamma)} [d(u, i) + d]^r \mu(i) \\ &\leq c_r \left\{ \sum_{i \in V(\Gamma)} d^r \mu(i) + \sum_{i \in V(\Gamma)} d^r(u, i) \mu(i) \right\} \quad (c_r - \text{不等式}) \\ &= c_r [d^r + M^{(r)}(u)] < \infty. \end{aligned}$$

推论 2.1 设 $(V(\Gamma), \mathcal{S}, \mu)$ 是所考虑的概率空间, Γ 是连通图, $\xi : \Omega \rightarrow V(\Gamma)$ 是 Γ 上的随机元, 则

$$\text{domain}(M) := \{s | M^{(r)}(s) < \infty, s \in V(\Gamma)\} = V(\Gamma)$$

或 $\text{domain}(M) = \phi$.

引理 2.2 设 $\xi : \Omega \rightarrow V(\Gamma)$ 是 Γ -值随机元, 其中 Γ 是局部有限的连通图且 r -阶权函数 $M_\xi^{(r)}(\cdot) < \infty$, 则均值集 $\mathbb{E}(\xi)$ 非空且有限.

证 对任意固定的顶点 $v \in \Gamma$, 其权函数

$$M^{(r)}(v) = \sum_{i \in V(\Gamma)} d^r(v, i) \mu(i) = \sum_{n=0}^{\infty} [n^r \sum_{i \in V(\Gamma), d(v, i)=n} \mu(i)] < \infty.$$

选取 $R \in \mathbb{N}$, 使得

$$\frac{1}{(\sqrt{2})^r} M^{(r)}(v) \leq \sum_{n=0}^R [n^r \sum_{i \in V(\Gamma), d(v, i)=n} \mu(i)] = \sum_{i \in B_v(R)} d^r(v, i) \mu(i), \quad (2.7)$$

其中

$$B_v(R) := \{i \in V(\Gamma) | d(v, i) \leq R\} \quad (2.8)$$

是 Γ 中以 v 为中心 R 为半径的球.

选取 $u \in V(\Gamma)$, 使得 $d(u, v) \geq 3R$. 利用三角形不等式及 (2.7) 式, 有

$$\begin{aligned}
 M^{(r)}(u) &= \sum_{i \in V(\Gamma)} d^r(u, i) \mu(i) \\
 &= \sum_{i \in B_v(R)} d^r(u, i) \mu(i) + \sum_{i \notin B_v(R)} d^r(u, i) \mu(i) \\
 &\geq \sum_{i \in B_v(R)} (2R)^r \mu(i) + \sum_{i \notin B_v(R)} d^r(u, i) \mu(i) \\
 &\geq \sum_{i \in B_v(R)} (2R)^r \mu(i) \\
 &\geq 2^r \sum_{i \in B_v(R)} d^r(v, i) \mu(i) \quad (d(v, i) \leq R, i \in B_v(R)) \\
 &\geq (\sqrt{2})^r M^{(r)}(v) > M^{(r)}(v).
 \end{aligned}$$

由此可知, 如果 $d(v, u) \geq 3R$, 则 $u \notin \mathbb{E}(\xi)$, 从而有 $\mathbb{E}(\xi) \subseteq B_v(3R)$. 由于 Γ 是局部有限图, 因此, 集合 $B_v(3R)$ 以及 $\mathbb{E}(\xi)$ 都是有限的. 函数 $M^{(r)}(\cdot)$ 在 $B_v(3R)$ 中能取到最小值, 从而 $\mathbb{E}(\xi) \neq \phi$.

引理 2.3 ^[9] 设 $\{\xi_i\}_{i=1}^\infty$ 是 i.i.d. 随机序列, 且 $\mathbb{E}(\xi_1) < \infty$, $\{a_i\}_{i=1}^\infty$ 是一列正整数, 则

$$\lim_{n \rightarrow \infty} \frac{\xi_{a_n+1} + \cdots + \xi_{a_n+n}}{n} = \mathbb{E}(\xi_1) \quad \text{a.s.} \quad (2.9)$$

引理 2.4 设 Γ 是局部有限的连通图, $v \in V(\Gamma)$, $\{\xi_i\}_{i=1}^\infty$ 是一列 i.i.d. Γ 值随机元, 即 $\xi_i : \Omega \rightarrow V(\Gamma), i = 1, 2, \dots$, 并且 $M_{\xi_1}^{(r)}(v) < \infty$. 则

$$P\left\{\lim_{n \rightarrow \infty} M_{a_n, n}^{(r)}(v) = M^{(r)}(v)\right\} = 1. \quad (2.10)$$

证 对 $\forall v \in V(\Gamma)$, $M^{(r)}(v) = \sum_{s \in V(\Gamma)} d^r(v, s) \mu(s) = \mathbb{E}d^r(v, \xi_1)$. 注意到 $M_{a_n, n}^{(r)}(v) = \frac{d^r(v, \xi_{a_n+1}) + \cdots + d^r(v, \xi_{a_n+n})}{n}$, 由引理 2.3 即得结论成立.

值得注意的是引理 2.4 中的收敛并不是一致地成立, 即对局部有限 (或无限) 图上的分布 μ , 及某些 $\varepsilon > 0$, 可能有

$$P\{\exists N \in \mathbb{N} \text{ s.t. } \forall n > N, \forall v \in V(\Gamma), |M_{a_n, n}^{(r)}(v) - M^{(r)}(v)| < \varepsilon\} \neq 1.$$

引理 2.5 ^[10,11] 设 $\{\xi_i\}_{i=1}^\infty$ 是一列 i.i.d. 随机变量, 且 $\mathbb{E}\xi_1 = 0$, $\mathbb{E}|\xi_1| < \infty$. 令 $R(n) = \sum_{i=1}^n \xi_i$, $n = 1, 2, \dots$, 则随机游动 $\{R(n)\}_{n=1}^\infty$ 是常返的.

引理 2.6 (分离引理) 设 Γ 是局部有限的连通图, $v \in V(\Gamma)$, $\{\xi_i\}_{i=1}^\infty$ 是一列 i.i.d. Γ 值随机元, 即 $\xi_i : \Omega \rightarrow V(\Gamma), i = 1, 2, \dots$. 如果 $M_{\xi_1}^{(r)}(\cdot) < \infty$, 则

$$P\{\exists N \in \mathbb{N} \text{ s.t. } \forall n > N, \max_{v \in \mathbb{E}(\xi_1)} M_{a_n, n}^{(r)}(v) < \inf_{u \in V(\Gamma) \setminus \mathbb{E}(\xi_1)} M_{a_n, n}^{(r)}(u)\} = 1. \quad (2.11)$$

证 欲证 (2.11) 式, 只须证存在 $\delta > 0$, 使得

$$P\{\exists N \in \mathbb{N} \forall n > N, \forall v \in \mathbb{E}(\xi_1), \forall u \in V(\Gamma) \setminus \mathbb{E}(\xi_1), M_{a_n, n}^{(r)}(u) - M_{a_n, n}^{(r)}(v) \geq \delta\} = 1 \quad (2.12)$$

成立即可.

本文分两步来完成. 首先证对固定的 $v_0 \in \mathbb{E}(\xi_1)$ 以及充分大的 $m > 0$, 有

$$P\{\exists N \in \mathbb{N} \text{ s.t. } \forall n > N, \forall v \in \mathbb{E}(\xi_1), \forall u \in V(\Gamma) \setminus B_{v_0}(m), M_{a_n, n}^{(r)}(u) - M_{a_n, n}^{(r)}(v) \geq \delta\} = 1 \quad (2.13)$$

成立. 其次证明

$$P\{\exists N \in \mathbb{N} \text{ s.t. } \forall n > N, \forall v \in \mathbb{E}(\xi_1), \forall u \in B_{v_0}(m) \setminus \mathbb{E}(\xi_1), M_{a_n, n}^{(r)}(u) - M_{a_n, n}^{(r)}(v) \geq \delta\} = 1. \quad (2.14)$$

由测度的 σ -可加性即得 (2.11) 式成立.

设 $v_0 \in \mathbb{E}(\xi_1)$. 因 $M^{(r)}(v_0) < \infty$, 如引理 2.2 中的做法选取 $R \in \mathbb{R}$, 使得 $\frac{1}{(\sqrt{2})^r} M^{(r)}(v_0) \leq \sum_{i \in B_{v_0}(R)} d^r(v_0, i) \mu(i)$. 令 $m = 3R$. 由引理 2.2 的证明过程可知, 如果 u 满足 $d(u, v_0) \geq 3R$, 则

$$M^{(r)}(u) = \sum_{i \in V(\Gamma)} d^r(u, i) \mu(i) \geq 2^r \sum_{i \in B_{v_0}(R)} d^r(u, i) \mu(i) \geq (\sqrt{2})^r M^{(r)}(v_0), \quad (2.15)$$

由此可知 $\mathbb{E}(\xi_1) \subseteq B_{v_0}(3R)$.

因为 Γ 是局部有限的, 所以 $B_{v_0}(R)$ 是有限的. $\forall \varepsilon > 0$, 令

$$C_\varepsilon := \{\exists N = N(\varepsilon), \forall n > N, \forall u \in B_{v_0}(R), |\mu_{a_n, n}(u) - \mu(u)| < \varepsilon\}, \quad (2.16)$$

由关于随机变量 $\mu_{a_n, n}(u) = \frac{1}{n} \sum_{i=a_n+1}^{a_n+n} \mathbf{1}_{\{u\}}(\xi_i)$ 的强极限定理可知, 当 $n \rightarrow \infty$ 时, $\mu_{a_n, n}(u) \rightarrow \mu(u)$ a.s., 因而 $P(C_\varepsilon) = 1$. 特别的, 取

$$\varepsilon = \varepsilon^* := \frac{1}{2} \left(1 - \frac{1}{(\sqrt{2})^r} \right) \min\{\mu(u) | u \in B_{v_0}(R), \mu(u) \neq 0\},$$

而且事件 C_{ε^*} 是集

$$\{\exists N = N(\varepsilon^*), \forall n > N, \forall u \in V(\Gamma) \setminus B_{v_0}(3R), M_{a_n, n}^{(r)}(u) \geq \frac{1}{2}[(\sqrt{2})^r + 1]M^{(r)}(v_0)\} \quad (2.17)$$

的子集. 事实上, 在 (2.16) 式定义的集合 C_{ε^*} 上有 $\mu_{a_n, n}(i) \geq \frac{1}{2}(1 + \frac{1}{(\sqrt{2})^r})\mu(i), i \in B_{v_0}(R)$. 利用上述结论以及 (2.15) 式, 有

$$\begin{aligned} M_{a_n, n}^{(r)}(u) &= \sum_{i \in V(\Gamma)} d^r(u, i) \mu_{a_n, n}(i) \geq 2^r \sum_{i \in B_{v_0}(R)} d^r(u, i) \mu_{a_n, n}(i) \\ &\geq \frac{1}{2} \left(1 + \frac{1}{(\sqrt{2})^r} \right) \cdot 2^r \sum_{i \in B_{v_0}(R)} d^r(u, i) \mu(i) \geq \frac{1}{2} ((\sqrt{2})^r + 1) M^{(r)}(v_0). \end{aligned}$$

于是

$$P\{\exists N \in \mathbb{N} \text{ s.t. } \forall n > N, \forall u \in V(\Gamma) \setminus B_{v_0}(3R), M_{a_n, n}^{(r)}(u) \geq \frac{1}{2}((\sqrt{2})^r + 1)M^{(r)}(v_0)\} = 1. \quad (2.18)$$

由引理 2.4, $\forall v \in V(\Gamma)$ 以及 $\forall \varepsilon > 0$, 有

$$P\{\exists N = N(\varepsilon), \forall n > N, |M_{a_n, n}^{(r)}(v) - M^{(r)}(v)| < \varepsilon\} = 1.$$

因为 $B_{v_0}(3R)$ 是有限集, 可知上述收敛在 $B_{v_0}(3R)$ 上一致成立, 即

$$P\{\exists N = N(\varepsilon), \forall n > N, \forall v \in B_{v_0}(3R), |M_{a_n, n}^{(r)}(v) - M^{(r)}(v)| < \varepsilon\} = 1. \quad (2.19)$$

特别地, 注意到 $\mathbb{E}(\xi_1) \subseteq B_{v_0}(3R)$, 取 $\varepsilon = \frac{(\sqrt{2})^r - 1}{4} M^{(r)}(v_0)$,

$$P\{\exists N = N(\varepsilon), \forall n > N, \forall v \in \mathbb{E}(\xi_1), \frac{5 - (\sqrt{2})^r}{4} M^{(r)}(v) < M_{a_n, n}^{(r)}(v) < \frac{(\sqrt{2})^r + 3}{4} M^{(r)}(v)\} = 1. \quad (2.20)$$

最后, 在 (2.18) 和 (2.20) 式给出的集合的交集上, 由 $M^{(r)}(v_0) = M^{(r)}(v)$ (因 $v_0, v \in \mathbb{E}(\xi_1)$) 以及 (2.13) 式, 对满足条件 $\delta \leq \frac{1}{4} M^{(r)}(v_0)$ 的 δ 有

$$\begin{aligned} M_{a_n, n}^{(r)}(u) - M_{a_n, n}^{(r)}(v) &\geq \frac{(\sqrt{2})^r + 1}{2} M^{(r)}(v) - \frac{(\sqrt{2})^r + 3}{4} M^{(r)}(v) \\ &= \frac{(\sqrt{2})^r - 1}{4} M^{(r)}(v) = \frac{(\sqrt{2})^r - 1}{4} M^{(r)}(v_0). \end{aligned}$$

第二步, 利用 (2.15) 式, 取

$$\varepsilon = \varepsilon' := \frac{1}{4} \min\{M^{(r)}(u) - M^{(r)}(v_0) | u \in B_{v_0}(3R), M^{(r)}(u) - M^{(r)}(v_0) > 0\},$$

即以概率 1, 存在 $N = N(\varepsilon')$ 使得对 $\forall n > N$ 和 $u \in B_{v_0}(3R)$, 有 $|M_{a_n, n}^{(r)}(u) - M^{(r)}(u)| < \varepsilon'$. 由于 $\mathbb{E}(\xi_1) \subseteq B_{v_0}(3R)$, 因此, 当 $v \in \mathbb{E}(\xi_1)$ 时, 有 $|M_{a_n, n}^{(r)}(v) - M^{(r)}(v)| < \varepsilon$. 注意到 $M^{(r)}(u) - M^{(r)}(v_0) > 0$, 知存在 $N = N(\varepsilon')$, 使得当 $n > N$ 时, $\forall u \in B_{v_0}(3R) \setminus \mathbb{E}(\xi_1)$, 有

$$\begin{aligned} M_{a_n, n}^{(r)}(v_0) &< M^{(r)}(v_0) + \varepsilon' \leq M^{(r)}(v_0) + \frac{1}{4} [M^{(r)}(u) - M^{(r)}(v_0)], \\ M^{(r)}(u) - \frac{1}{4} [M^{(r)}(u) - M^{(r)}(v_0)] &\leq M^{(r)}(u) - \varepsilon' < M_{a_n, n}^{(r)}(u), \end{aligned}$$

且有

$$\begin{aligned} &M_{a_n, n}^{(r)}(u) - M_{a_n, n}^{(r)}(v_0) \\ &\geq M^{(r)}(u) - \frac{1}{4} [M^{(r)}(u) - M^{(r)}(v_0)] - M^{(r)}(v_0) - \frac{1}{4} [M^{(r)}(u) - M^{(r)}(v_0)] \\ &= \frac{1}{2} [M^{(r)}(u) - M^{(r)}(v_0)] \geq 2\varepsilon'. \end{aligned}$$

即

$$P\{\exists N = N(\varepsilon), \forall n > N, \forall u \in B_{v_0}(3R) \setminus \mathbb{E}(\xi_1) : M_{a_n, n}^{(r)}(u) - M_{a_n, n}^{(r)}(v_0) \geq 2\varepsilon'\} = 1.$$

因此 (2.14) 式对 $\delta \leq 2\varepsilon'$ 成立. 取 $\delta = \min(\frac{(\sqrt{2})^r - 1}{4} M^{(r)}(v_0), 2\varepsilon')$ 即可得引理成立.

3 强极限定理

经典的强大数定律表明, 如果独立同分布随机变量的期望存在, 则样本均值几乎处处收敛到随机变量的数学期望. 然而, 下面的例子可以看出, 对在图上取值的随机元的广义样本均值在普通意义下并不一定收敛.

例 3.1 考虑图 $\Gamma = (V, E)$, 其中 $V = \{v_1, v_2\}$, $E = \{(v_1, v_2)\}$. μ 是由随机元 $\xi_1 : \Omega \rightarrow V$ 诱导的 $V(\Gamma)$ 上的概率测度, 且 $\mu(v_1) = \mu(v_2) = \frac{1}{2}$. 此时有 $M^{(r)}(v_1) = M^{(r)}(v_2) = 1/2$, $\mathbb{E}(\xi) = \{v_1, v_2\}$.

设 $\{\xi_i\}_{i=1}^\infty$ 是独立同分布随机元序列, 换句话说就是考虑从图 Γ 的顶点 v_1, v_2 中随机地选一系列点. 由定义知

$$\begin{aligned} M_{a_n, n}^{(r)}(v_1) &= \frac{1}{n} \# \{i | \xi_i = v_2, a_n + 1 \leq i \leq a_n + n\}, \\ M_{a_n, n}^{(r)}(v_2) &= \frac{1}{n} \# \{i | \xi_i = v_1, a_n + 1 \leq i \leq a_n + n\}. \end{aligned}$$

由定义 2.3, 有

$$\begin{aligned} v_1 \in S_{a_n, n} &\iff M_{a_n, n}^{(r)}(v_1) \leq M_{a_n, n}^{(r)}(v_2) \\ &\iff \# \{i | \xi_i = v_2, a_n + 1 \leq i \leq a_n + n\} \leq \# \{i | \xi_i = v_1, a_n + 1 \leq i \leq a_n + n\}. \end{aligned}$$

同理

$$\begin{aligned} v_2 \in S_{a_n, n} &\iff M_{a_n, n}^{(r)}(v_2) \leq M_{a_n, n}^{(r)}(v_1) \\ &\iff \# \{i | \xi_i = v_1, a_n + 1 \leq i \leq a_n + n\} \leq \# \{i | \xi_i = v_2, a_n + 1 \leq i \leq a_n + n\}. \end{aligned}$$

令

$$R(n) := \# \{i | \xi_i = v_2, 1 \leq i \leq n\} - \# \{i | \xi_i = v_1, 1 \leq i \leq n\}, \quad n = 1, 2, \dots$$

和

$$\begin{aligned} W(n) &:= n[M_{a_n, n}^{(r)}(v_1) - M_{a_n, n}^{(r)}(v_2)] \\ &= \# \{i | \xi_i = v_2, a_n + 1 \leq i \leq a_n + n\} - \# \{i | \xi_i = v_1, a_n + 1 \leq i \leq a_n + n\}, \quad n = 1, 2, \dots, \end{aligned}$$

$\{R(n)\}_{n=1}^\infty$ 可看成是 $\mathbb{Z}$ 上的对称随机游动, 且

$$W(n) = R(a_n + n) - R(a_n),$$

于是有

$$\{v_1 \in S_{a_n, n}\} = \{M_{a_n, n}^{(r)}(v_1) \leq M_{a_n, n}^{(r)}(v_2)\} = \{W(n) \leq 0\}$$

及

$$\{v_2 \in S_{a_n, n}\} = \{M_{a_n, n}^{(r)}(v_1) \geq M_{a_n, n}^{(r)}(v_2)\} = \{W(n) \geq 0\}.$$

显然, $W(n)$ 与 $R(n)$ 同分布. 由于 $\mathbb{Z}$ 上的对称随机游动是常返的, 从而有 $P\{v_i \in S_{a_n, n}, \text{ i.o.}\} = 1, i = 1, 2$. 因此

$$\begin{aligned} \limsup_{n \rightarrow \infty} S_{a_n, n} &= \{v_1, v_2\} = \mathbb{E}(\xi_1), \\ \liminf_{n \rightarrow \infty} S_{a_n, n} &= \phi, \end{aligned}$$

由此可知 $\lim_{n \rightarrow \infty} S_{a_n, n}$ 不存在.

定理 3.1 设 Γ 是局部有限图, $\{\xi_i\}_{i=1}^\infty$ 是定义在概率空间 $(\Omega, \mathcal{F}, P)$ 上在 $V(\Gamma)$ 中取值的一列 i.i.d. 随机元, μ 是定义在 Γ 上由 ξ_1 诱导出的概率测度. 假设 $M^{(r)}(u) < \infty, \forall u \in V(\Gamma)$. 则

$$P\{\limsup_{n \rightarrow \infty} S_{a_n, n} \subseteq \mathbb{E}(\xi_1)\} = 1. \quad (3.1)$$

证 由引理 2.6, 有

$$P\{\exists N \in \mathbb{N} \text{ s.t. } \forall n > N, \max_{v \in \mathbb{E}(\xi_1)} M_{a_n, n}^{(r)}(v) < \inf_{u \in V(\Gamma) \setminus \mathbb{E}(\xi_1)} M_{a_n, n}^{(r)}(u)\} = 1,$$

若 $u \in \mathbb{E}(\xi_1)$, 有

$$P\{\exists N \in \mathbb{N} \text{ s.t. } \forall n > N, u \in S_{a_n, n}\} = P(u \in \limsup_{n \rightarrow \infty} S_{a_n, n}) = 1,$$

由测度的 σ -可加性, 有

$$P\{u \in \limsup_{n \rightarrow \infty} S_{a_n, n}, \forall u \in V(\Gamma) \setminus \mathbb{E}(\xi_1)\} = 1.$$

前面分别就 $\mathbb{E}\xi_1$ 是单点与两点集这两种情况来证明强大数定理, 关于 $\mathbb{E}\xi_1$ 是多点集情形的证明比较复杂, 将在另文中讨论.

1. $\mathbb{E}\xi_1$ 是单点集情形.

定理 3.2 设 Γ 是局部有限连通图, $\{\xi_i\}_{i=1}^\infty$ 是一列 i.i.d. Γ -值随机元序列, $\xi_i: \Omega \rightarrow V(\Gamma)$. 如果 $M_{\xi_1}^{(r)}(\cdot) < \infty$ 且 $\mathbb{E}(\xi_1) = \{v\}, v \in V(\Gamma)$, 即 $\mathbb{E}(\xi_1)$ 是单点集, 则

$$\lim_{n \rightarrow \infty} S(\xi_{a_n+1}, \dots, \xi_{a_n+n}) = \mathbb{E}(\xi_1) \text{ a.s.} \quad (3.2)$$

证 (3.2) 式可以表述为

$$P(\exists N \in \mathbb{N} \text{ s.t. } \forall n > N, S(\xi_{a_n+1}, \dots, \xi_{a_n+n}) = \{v\}) = 1$$

或等价地

$$P\{\exists N \in \mathbb{N} \text{ s.t. } \forall n > N, \forall u \in V(\Gamma) \setminus \{v\}, M_{a_n, n}^{(r)}(v) < M_{a_n, n}^{(r)}(u)\} = 1. \quad (3.3)$$

由引理 2.6, 有

$$P\{\exists N \in \mathbb{N} \text{ s.t. } \forall n > N, M_{a_n, n}^{(r)}(v) < \inf_{u \in V(\Gamma) \setminus \{v\}} M_{a_n, n}^{(r)}(u)\} = 1,$$

于是

$$P\{\exists N \text{ s.t. } \forall n > N, \{v\} = S(\xi_{a_n+1}, \dots, \xi_{a_n+n})\} = 1.$$

2. $\mathbb{E}\xi_1$ 是两点集的情形.

定理 3.3 设 Γ 是局部有限连通图, $\{\xi_i\}_{i=1}^\infty$ 是一列 i.i.d. Γ -值随机元, $\xi_i: \Omega \rightarrow V(\Gamma)$. 如果 $M_{\xi_1}^{(r)}(\cdot) < \infty$ 且 $\mathbb{E}(\xi_1) = \{v_1, v_2\}, v_i \in V(\Gamma), i = 1, 2$, 即 $\sharp \mathbb{E}(\xi_1) = 2$, 则

$$\limsup_{n \rightarrow \infty} S(\xi_{a_n+1}, \dots, \xi_{a_n+n}) = \mathbb{E}(\xi_1) \text{ a.s.} \quad (3.4)$$

证 由定理 3.1 知 $\limsup_{n \rightarrow \infty} S_{a_n, n} \subseteq \mathbb{E}(\xi_1)$. 欲证 (3.4) 式, 只须证明相反的包含关系. 注意到 $\mathbb{E}(\xi_1) = \{v_1, v_2\}$, 即 $M_{\xi}^{(r)}(\cdot)$ 只在点 v_1 和 v_2 上取到最小值, 即

$$M^{(r)}(v_1) = M^{(r)}(v_2) < M^{(r)}(u), \quad \forall u \in \Gamma \setminus \{v_1, v_2\}.$$

由权函数的定义, 有

$$\begin{aligned} M^{(r)}(v_1) &= \sum_{s \in \Gamma} d^r(v_1, s) \mu(s), \quad M^{(r)}(v_2) = \sum_{s \in \Gamma} d^r(v_2, s) \mu(s), \\ M_{a_n, n}^{(r)}(v_1) &= \sum_{s \in \Gamma} d^r(v_1, s) \frac{\#\{i | \xi_i = s, a_n + 1 \leq i \leq a_n + n\}}{n}, \\ M_{a_n, n}^{(r)}(v_2) &= \sum_{s \in \Gamma} d^r(v_2, s) \frac{\#\{i | \xi_i = s, a_n + 1 \leq i \leq a_n + n\}}{n}. \end{aligned}$$

由引理 2.4, 有

$$M_{a_n, n}^{(r)}(v_1) \rightarrow M^{(r)}(v_1) \quad \text{a.s. 以及} \quad M_{a_n, n}^{(r)}(v_2) \rightarrow M^{(r)}(v_2) \quad \text{a.s..}$$

由引理 2.6 知, 存在数 $N \in \mathbb{N}$, 当 $n > N$, 几乎处处有

$$\max\{M_{a_n, n}^{(r)}(v_1), M_{a_n, n}^{(r)}(v_2)\} < \inf_{u \in \Gamma \setminus \{v_1, v_2\}} M_{a_n, n}^{(r)}(u).$$

因此当 $n > N$,

$$v_1 \in S_{a_n, n} \quad \text{当且仅当} \quad M_{a_n, n}^{(r)}(v_1) \leq M_{a_n, n}^{(r)}(v_2)$$

当且仅当

$$\sum_{s \in V(\Gamma)} (d^r(v_1, s) - d^r(v_2, s)) \#\{i | \xi_i = s, a_n + 1 \leq i \leq a_n + n\} \leq 0.$$

同理

$$v_2 \in S_{a_n, n} \quad \text{当且仅当} \quad M_{a_n, n}^{(r)}(v_2) \leq M_{a_n, n}^{(r)}(v_1)$$

当且仅当

$$\sum_{s \in V(\Gamma)} (d^r(v_2, s) - d^r(v_1, s)) \#\{i | \xi_i = s, a_n + 1 \leq i \leq a_n + n\} \leq 0.$$

欲证 $\{v_1, v_2\} \subseteq \limsup_{n \rightarrow \infty} S_{a_n, n}$, 只须证明 $M_{a_n, n}^{(r)}(v_1) - M_{a_n, n}^{(r)}(v_2)$ 无穷多次取正值和负值. 令

$$\begin{aligned} W(n) &:= n[M_{a_n, n}^{(r)}(v_2) - M_{a_n, n}^{(r)}(v_1)] \\ &= \sum_{s \in V(\Gamma)} [d^r(v_2, s) - d^r(v_1, s)] \cdot \#\{i | \xi_i = s, a_n + 1 \leq i \leq a_n + n\}, \quad n = 1, 2, \dots \end{aligned}$$

和

$$R(n) = \sum_{s \in V(\Gamma)} [d^r(v_2, s) - d^r(v_1, s)] \cdot \#\{i | \xi_i = s, 1 \leq i \leq n\}, \quad n = 1, 2, \dots,$$

$\{R(n)\}_{n=1}^{\infty}$ 可以看成是 $\mathbb{Z}$ 上从 0 点出发的随机游动. 即 $R(0) = 0, R(n) = \sum_{i=1}^n \zeta_i$, 其中 $\zeta_i = \zeta_i(s) : V(\Gamma) \rightarrow \mathbb{Z}, i = 1, 2, \dots$ 是 i.i.d. 随机序列且 $\mathbb{E}(\zeta_1) = 0$ (因 $M^{(r)}(v_1) = M^{(r)}(v_2)$) 且 $P\{\zeta_i(s) = d^r(v_2, s) - d^r(v_1, s)\} = \mu(s), s \in V(\Gamma)$.

注意到, $W(n) = R(a_n + n) - R(a_n)$ 且 $W(n)$ 与 $R(n)$ 同分布,

$$v_1 \in S_n \iff W(n) \geq 0 \text{ 及 } v_2 \in S_n \iff W(n) \leq 0.$$

因为

$$\mathbb{E}(\zeta_1) = \sum_{s \in V(\Gamma)} (d^r(v_2, s) - d^r(v_1, s))\mu(s) = M^{(r)}(v_1) - M^{(r)}(v_2) = 0,$$

且

$$\begin{aligned} \sum_{s \in V(\Gamma)} |\zeta_1(s)|\mu(s) &= \sum_{s \in V(\Gamma)} |d^r(v_2, s) - d^r(v_1, s)|\mu(s) \\ &\leq \sum_{s \in V(\Gamma)} [d^r(v_2, s) + d^r(v_1, s)]\mu(s) = M^{(r)}(v_1) + M^{(r)}(v_2) < \infty. \end{aligned}$$

由引理 2.5, $\mathbb{Z}$ 上的随机游动 $\{R(n)\}_{n=1}^{\infty}$ 是常返的, 即 $\{R(n)\}_{n=1}^{\infty}$ 有无穷多次取正值和负值. 故

$$\limsup_{n \rightarrow \infty} S_{a_n, n} = \{v_1, v_2\} = \mathbb{E}(\xi).$$

参 考 文 献

- [1] Kolmogorov A N. La transformation de Laplace dans les espaces lineaires[J]. CD. Acad. Sci. Paris, 1935, 200: 1717–1718.
- [2] Fréchet M. Les éléments aléatoires de nature quelconque dans un espace distancié[J]. Ann. Inst. H. Poincaré Prob. Stat., 1948, 10: 215–310.
- [3] 吴智泉, 王向忱. 巴氏空间上的概率论 [M]. 吉林: 吉林大学出版社, 1990.
- [4] Ziezold H. Expected figures and a strong law of large numbers for random elements in quasi-metric spaces[J]. Trans. 7th Prague Conf. Inf. Theory, Stat. Dec. Func., Random Processes A, 1977, 591–602.
- [5] Sverdrup H, Thygeson. Strong law of large numbers for measures of central tendency and dispersion of random variables in compact metric spaces[J]. Ann. Stat., 1981, 9: 141–145.
- [6] Bhattacharya R N, Patrangenaru V. Large sample theory of intrinsic and extrinsic sample means on manifolds-I[J]. Ann. Stat., 2003, 31: 1–29.
- [7] Mosina N, Ushakov A. Strong law of large numbers on graphs and groups[J]. arXiv: 0904.1005v2 [Math. PR] 29 Jun 2010.
- [8] Mosina N, Ushakov A. Mean set attack: cryptanalysis of Sibert et al. authentication protocol[J]. J. Math. Crypt., 2010: 4(2): 149–174.
- [9] Gaposhkin V F. The law of large numbers for moving averages of independent random variables[J]. Math. Zametki, 1987, 42(1): 124–131.
- [10] Spitzer F. Principles of random walk (2nd ed.)[M]. New York, Berlin, Heidelberg: Springer-Verlag, 2001.

- [11] Feller W. An Introduction to probability theory and its applications, Vol.II (2nd ed.)[M]. New York: John Wiley, 1971.
- [12] 张丽娜. 任意 B 值随机变量的强收敛性 [J]. 数学杂志, 2002, 22(3): 297–300.

ON SOME LIMIT THEOREMS FOR GRAPH-VALUED RANDOM ELEMENTS

WANG Zhong-zhi, LI Wen-xi

(*School of Mathematics & Physics Science and Engineering, Anhui University of Technology,
Maanshan 243002, China*)

Abstract: In this paper, the authors discuss the basic properties of the general r th order mean set and r th order sample mean set of random elements, which take values on a locally connected graph, and the limit properties of them. By applying the separation lemma of random elements and the recurrence of random walk, we obtain the general strong law of large numbers for graph-valued random elements. Moreover, we generalize the existing results.

Keywords: general strong law of large numbers; graph; r -th order weight function; r -th order mean set; r -th order sample mean set; random walk

2010 MR Subject Classification: 60F15