文章编号:1000-2367(2022)03-0073-06 DOI:10.16366/j.cnki.1000-2367.2022.03.009

有限域上随机多项式的统计渐近性质

李萌[1],苗雨[2],杨广宇[1]

(1.郑州大学 数学与统计学院,郑州 450001;2.河南师范大学 数学与信息科学学院,河南 新乡 453007)

摘 要:主要研究有限域上随机多项式的统计渐近性质.具体地,应用相依图和 Stein 方法证明了关于互素多项式经验密度的中心极限定理和中偏差原理,从而将已有文献中关于整数环上的部分结果推广到了多项式环.

关键词:大偏差原理;多项式环;随机多项式;有限域;中心极限定理.

中图分类号:O211.4 **文献标志码**:A

文献[1]在 1849 年研究整数性质时发现了一个有趣的密度定理:任取两个自然数其恰好互素的可能性为 $6/\pi^2$,也即

$$\lim_{N\to\infty}\frac{\#\{(m,n)\in\mathbf{N}^2:1\le m,n\le N,\gcd(m,n)=1\}}{N^2}=\frac{1}{\zeta(2)}=\frac{6}{\pi^2},\tag{1}$$

其中 $\#A$ 表示集合 A 中元素个数,$\gcd(m,n)$ 表示自然数 m,n 的最大公因子,$\zeta(\cdot)$ 是 Riemann-zeta 函数.文献[2-4]进一步证明了任取 n 个自然数,其恰好互素的可能性为 $\zeta^{-1}(n)$.文献[5]给出了 Dirichlet 密度定理的严格概率证明.在此基础上,文献[6]考虑了涨落问题,证明了中心极限定理.文献[7]将概率方法与数论函数估计相结合研究了有关整数互素的一些有趣统计量的中心极限定理.最近,文献[8]应用纯概率方法给出了中心极限定理的收敛速度并证明了中偏差与大偏差原理.若对 Dirichlet 定理的历史感兴趣,请参阅文献[9]中的历史注记.关于数论中的概率方法方面更深入的讨论可参阅文献[10-12].

自然地,可考虑有限域上多项式环中元素的类似问题.给定素数 q,令 $F_q=Z/qZ$ 是含 q 个元素的有限域,$F_q[x]$ 是 F_q 上的多项式环.记 $\mathscr{M}$ 为 $F_q[x]$ 中首 1 多项式之全体,$\mathscr{P}$ 为 $F_q[x]$ 中首 1 不可约(素)多项式全体;任给 $f\in\mathscr{M}$,若 f 为非零多项式,则令 $|f|:=q^{\deg(f)}$;否则,令 $|f|=0$.注意到 $|f|$ 可度量 f 的大小.任给 $t\in\mathscr{D}_q:=\{q^z:z=0,1,2,\cdots.\}$,分别用 $\mathscr{M}_t$ 与 $\mathscr{P}_t$ 表示不超过 t 的首 1 多项式和首 1 不可约多项式全体.关于有限域上多项式环的更多介绍可参阅文献[13-14].事实上,可将 $F_q[x]$ 中元素做如下排列:

$$f_n(x)=\sum_{i=1}^{\infty}b_i^{(q)}(n)x^{i-1},n=0,1,2,\cdots,$$

其中 $b_i^{(q)}(n)\in\{0,1,\cdots,q-1\}$ 表示 n 的 q 进制展开中第 i 个位置上的值,即 $n=\sum_{i=1}^{\infty}b_i^{(q)}(n)q^{i-1}$,注意到此处牵涉到的级数都只是有限项.文献[15-17]研究了函数域上的 Dirichlet 定理,证明了任取两个多项式其恰好互素的可能性为 $1-q^{-1}$,即

$$\lim_{N\to\infty}\frac{\#\{(m,n)\in\mathbf{N}^2:0\le m,n\le N-1,\gcd(f_m,f_n)=1\}}{N^2}=\frac{1}{\zeta_q(2)}=1-\frac{1}{q},\tag{2}$$

其中 $\zeta_q(\cdot)$ 是 Dedekind q-zeta 函数:

收稿日期:2021-03-10;**修回日期**:2021-05-21.

基金项目:国家自然科学基金(11971154);河南省高等学校青年骨干教师项目(2019GGJS012).

作者简介:李萌(1995-),女,山西晋城人,郑州大学硕士研究生,研究方向为概率极限理论,E-mail:lm18435204685@163.com.

通信作者:杨广宇(1979-),男,河南许昌人,郑州大学副教授,博士,研究方向为概率极限理论、渐近统计,E-mail:guangyu@zzu.edu.cn.

$$\zeta_q(s):=\sum_{f\in\mathscr{M}}\frac{1}{|f|^s}=\frac{1}{1-q^{1-s}},s>1.$$

文献[18]证明了任取 n 个多项式,其恰好互素的可能性为 $\zeta_q^{-1}(n)$. 关于有限域上随机多项式的其他有趣的统计渐近性质可参阅文献[19－20].

本文主要目的是考虑有限域上随机多项式的涨落问题及精细渐近行为,即要证明函数域上随机多项式的中心极限定理与中偏差原理;其一方面将文献[7－8]中关于整数环上的部分结果推广到了多项式环,另一方面也可用于构造投影 $F_q[x]$-模的自由模表示及有限域上多项式因子分解的概率算法,并进一步研究算法的有效性及效率等问题,具体可参见文献[16,18].为方便起见,在这里简单介绍一下关于大偏差理论的术语.设 I 是非负的下半连续函数(即水平集 $\{x:I(x)\leq\alpha\}$ 对任意的 $\alpha>0$ 都是闭集),说实值随机序列 $\{\xi_n\}$ 满足速度为 $\{b_n\}$,速率函数为 I 的大偏差原理,若对任意 Borel 可测集 A,有下式成立

$$-\inf_{x\in A^\circ}I(x)\leq\liminf_{n\to\infty}\frac{1}{b_n}\lg P(\xi_n\in A)\leq\limsup_{n\to\infty}\frac{1}{b_n}\lg P(\xi_n\in A)\leq-\inf_{x\in\bar{A}}I(x),$$

其中 $A^\circ,\bar{A}$ 分别表示集合 A 的内部与闭包. 关于大偏差理论及其应用的更详尽介绍可参阅文献[21－22].

1 主要结果

设 $(\Omega,\mathscr{A},P)$ 是完备概率空间.给定 $t\in\mathscr{D}_q$,令 $X^{(t)}$ 是取值于 $\mathscr{M}_t$ 的均匀随机变量.设 $X_1^{(t)},X_2^{(t)},\cdots,X_n^{(t)}$ 是取自总体 $X^{(t)}$ 的简单随机样本,即它们相互独立且公共分布为 $\mathscr{M}_t$ 上的均匀分布. 考虑如下的 U-统计量

$$U_n^{(t)}:=\frac{1}{\binom{n}{2}}\sum_{1\leq i<j\leq n}1_{\{\gcd(X_i^{(t)},X_j^{(t)})=1\}},t\in\mathscr{D}_q,n\geq2. \tag{3}$$

为叙述主要结果,需要回忆随机变量之间的 Wasserstein 度量.任给随机变量 U,V,称

$$d_W(U,V):=\sup\{|E[h(U)]-E[h(V)]|:h\in\mathscr{H}\},$$

为 U,V 的 Wasserstein 度量,其中 $\mathscr{H}$ 表示 $\mathbf{R}$ 上的 1-Lipschitz 函数之全体.

定理 1[中心极限定理] 定义

$$\mathscr{U}_n^{(t)}=\frac{U_n^{(t)}-E(U_n^{(t)})}{\sqrt{\mathrm{Var}(U_n^{(t)})}}, \tag{4}$$

则对任意固定的 $t\in\mathscr{D}_q$,

$$d_W(\mathscr{U}_n^{(t)},\mathscr{N}(0,1))\leq\frac{c}{\sqrt{n}}, \tag{5}$$

这里,$\mathscr{N}(0,1)$ 为标准正态随机变量,c 为非负的普适性常数.特别当 $n\to\infty$ 时,

$$\mathscr{U}_n^{(t)}\to_d\mathscr{N}(0,1), \tag{6}$$

其中"$\to_d$"表示依分布收敛.

进一步,记

$$\sigma_{q,t}^2:=P(\gcd(X_1^{(t)},X_2^{(t)})=1=\gcd(X_1^{(t)},X_3^{(t)}))-P^2(\gcd(X_1^{(t)},X_2^{(t)})=1), \tag{7}$$

则由 2.1 节中计算可知,当 $t\to\infty$ 时有

$$\sigma_{q,t}^2\to\sigma_q^2:=\prod_{\phi\in\mathscr{P}}(1-2q^{-2\deg(\phi)}+q^{-3\deg(\phi)})-(1-q^{-1})^2. \tag{8}$$

则有下述大偏差结果:

定理 2[中偏差] 设正实数列 $\{a_n\}$ 满足:当 $n\to\infty$ 时,$\sqrt{n}/a_n\to0$ 且 $a_n/n\to0$.则对任意固定的 $t\in\mathscr{D}_q$,随机变量序列 $\{na_n^{-1}(U_n^{(t)}-E(U_n^{(t)}))\}$ 满足速度为 $\{a_n^2/n\}$、速率函数为 $I_{q,t}(x)=x^2/(8\sigma_{q,t}^2)(x\in\mathbf{R})$ 的大偏差原理.

注记 1 事实上,从定理 1 与定理 2 的证明中可知:当 $t=t_n\in\mathscr{D}_q$ 随 n 变化趋于无穷时,定理 1 仍然成立;定理 2 也成立,但此时的速率函数变为 $I_q(x)=x^2/(8\sigma_q^2),x\in\mathbf{R}$.

2　定理证明

本节中,将采用相依图的方法证明主要结果(定理 1 与定理 2).

2.1　辅助性引理

本小结主要介绍证明中需要的相依图概念以及两个关键性定理,更详尽的信息请参阅文献[23－26].

给定图 $G=(V,E)$,其中 V 是顶点集,E 是边集,以及随机变量族$\{X_\lambda,\lambda\in\Lambda\}$.说图 G 是该随机变量族的相依图,若(i) 顶点集 V 与该随机变量族是一一对应的,(ii) 若 $V_1,V_2\subseteq V$ 且 $V_1\cap V_2=\varnothing$,则 V_1 中顶点对应的随机变量与 V_2 中顶点对应的随机变量相互独立.具有相依图结构的随机变量族有某种相依性质,该性质也可用相依邻居的概念刻画.说随机变量族$\{X_1,X_2,\cdots,X_n\}$有相依邻居 $N_i\subseteq\{1,2,\cdots,n\}$,$i=1,2,\cdots,n$,若 $i\in N_i$ 并且 X_i 与$\{X_j,j\notin N_i\}$ 相互独立.

引理 1[23]　给定随机变量族 $\{X_1,X_2,\cdots,X_n\}$,$E(X_i)=0$,$E(X_i^4)<\infty$,记 $\sigma_n^2=\mathrm{Var}(\sum_{i=1}^n X_i)$,$W_n=\sum_{i=1}^n X_i/\sigma_n$.设$\{X_1,X_2,\cdots,X_n\}$ 有相依邻居 N_i,$i=1,2,\cdots,n$,令 $D_n:=\max\limits_{1\le i\le n}\sharp N_i$,则

$$d_W(W_n,\mathcal{N}(0,1))\le\frac{D_n^2}{\sigma_n^3}\sum_{i=1}^n E(|X_i|^3)+\frac{\sqrt{28}D_n^{3/2}}{\sqrt{\pi}\sigma_n^2}\sqrt{\sum_{i=1}^n E(X_i^4)}.$$

引理 2[24]　设 $(\Omega,\mathscr{A})=\bigotimes_{i=1}^{k(n)}(\mathscr{X}_i,\mathscr{B}_i)$ 是乘积可测空间,其上概率为乘积测度 $P=\bigotimes_{i=1}^{k(n)}\mu_i$.设 $X_{k(n)}=(X_1,X_2,\cdots,X_{k(n)})$ 是$(\Omega,\mathscr{A},P)$ 上典则过程,令 $Y_{k(n)}=(Y_1,Y_2,\cdots,Y_{k(n)})$ 是 $X_{k(n)}$ 的独立版本,即 $Y_{k(n)}$ 与 $X_{k(n)}$ 相互独立且同分布.给定有界可测函数 $f:\Omega\to R$,其一阶、二阶差分如(14) 式所定义.又设$\{d_n\}$ 如(17) 式所定义.若存在正实数列$\{\beta_n\}$,$\{\lambda_n\}$ 及正常数 δ 使得当 $n\to\infty$ 时有下列条件成立:

(i) $\lambda_n^{-3}\beta_n^2 d_n\to 0$,

(ii) $\lambda_n^{-2}\beta_n\mathrm{Var}(f(X_{k(n)}))\to\delta$,

则随机变量序列 $\{\lambda_n^{-1}(f(X_{k(n)})-E[f(X_{k(n)})])\}$ 满足速度为$\{\beta_n\}$、速率函数为 $I(x)=x^2/(2\delta)$($x\in\mathbf{R}$) 的大偏差原理.

2.2　定理 1 的证明

为方便起见,记 $a_{ij}^{(t)}=1_{\{\gcd(X_i^{(t)},X_j^{(t)})=1\}}$,$1\le i<j\le n$,则 $\{a_{ij}^{(t)},1\le i<j\le n\}$ 同分布.由文献[15]知

$$\tau_{q,t}:=E(a_{ij}^{(t)})=P(\gcd(X_i^{(t)},X_j^{(t)})=1)=1-q^{-1}+q^{-1}(1-q^{-1})t^{-2}\to 1-q^{-1},t\to\infty. \tag{9}$$

考虑 $a_{ij}^{(t)}$ 的中心化 $\tilde a_{ij}^{(t)}=a_{ij}^{(t)}-E(a_{ij}^{(t)})$,从而有 $U_n^{(t)}-E(U_n^{(t)})=\dfrac{2}{n(n-1)}\sum\limits_{1\le i<j\le n}\tilde a_{ij}^{(t)}$.下面,来计算 $\sum\limits_{1\le i<j\le m}\tilde a_{ij}^{(t)}$ 的方差.注意到,

$$\mathrm{Var}\Big(\sum_{1\le i<j\le n}\tilde a_{ij}^{(t)}\Big)=E\Big[\Big(\sum_{1\le i<j\le n}\tilde a_{ij}^{(t)}\Big)^2\Big]=E\Big(\sum_{1\le i<j\le n}\tilde a_{ij}^{(t)}\cdot\sum_{1\le k<l\le n}\tilde a_{kl}^{(t)}\Big)=\sum_{(i,j),(k,l)}E(\tilde a_{ij}^{(t)}\tilde a_{kl}^{(t)}), \tag{10}$$

其中,最后一个求和式的指标满足 $1\le i<j\le n$,$1\le k<l\le n$.分 3 种情况来讨论(10)式中最后一个求和式的计算.

情形 1　$\{i,j\}\cap\{k,l\}=\varnothing$.此时显然有 $E(\tilde a_{ij}^{(t)}\tilde a_{kl}^{(t)})=E(\tilde a_{ij}^{(t)})E(\tilde a_{kl}^{(t)})=0$.

情形 2　$\{i,j\}\cap\{k,l\}=\{i,j\}=\{k,l\}$,即 $i=k$,$j=l$.此时有

$$E(\tilde a_{ij}^{(t)}\tilde a_{kl}^{(t)})=E[(\tilde a_{ij}^{(t)})^2]=E[(a_{ij}^{(t)})^2]-(E(a_{ij}^{(t)}))^2=E(a_{ij}^{(t)})(1-E(a_{ij}^{(t)}))=\tau_{q,t}(1-\tau_{q,t})\to q^{-1}(1-q^{-1}),t\to\infty.$$

情形 3　$\sharp(\{i,j\}\cap\{k,l\})=1$.不失一般性,设 $i=k$,$j\ne l$.注意到,

$$E(\tilde a_{ij}^{(t)}\tilde a_{kl}^{(t)})=E(\tilde a_{ij}^{(t)}\tilde a_{il}^{(t)})=E[(a_{ij}^{(t)}-Ea_{ij}^{(t)})(a_{il}^{(t)}-Ea_{il}^{(t)})]=E(a_{ij}^{(t)}a_{il}^{(t)})-[E(a_{ij}^{(t)})]^2.$$

注意到上式中第 2 项之前已有处理,因而只需估计第 1 项.显然,

$$E(a_{ij}^{(t)}a_{il}^{(t)})=P(\gcd(X_i^{(t)},X_j^{(t)})=\gcd(X_i^{(t)},X_l^{(t)})=1)=P(\gcd(X_1^{(t)},X_2^{(t)})=\gcd(X_1^{(t)},X_3^{(t)})=1).$$

为估计这个概率,需要引入辅助随机变量.设 Y,Y_1,Y_2,Y_3 是取值于多项式环 $F_q[x]$ 上的独立同分布随机变量,且满足 $P(\phi \mid Y)=|\phi|^{-1}=q^{-\deg(\phi)},\phi\in\mathscr{P}$, 其中 $g \mid f$ 表示 g 整除 f. 不难算得

$$P(\gcd(Y_1,Y_2)=\gcd(Y_1,Y_3)=1)=\prod_{\phi\in\mathscr{P}}(1-2q^{-2\deg(\phi)}+q^{-3\deg(\phi)}). \tag{11}$$

又注意到,当 $t\to\infty$ 时,$P\circ(X^{(t)})^{-1}\to_d P\circ Y^{-1}$, 因而可得,$t\to\infty$时 $P(\gcd(X_1^{(t)},X_2^{(t)})=\gcd(X_1^{(t)},X_3^{(t)})=1)\to\prod_{\phi\in\mathscr{P}}(1-2q^{-2\deg(\phi)}+q^{-3\deg(\phi)})$.

也即,$t\to\infty$时有

$$E(\tilde{a}_{ij}^{(t)}\tilde{a}_{kl}^{(t)})\to\prod_{\phi\in\mathscr{P}}(1-2q^{-2\deg(\phi)}+q^{-3\deg(\phi)})-(1-q^{-1})^2. \tag{12}$$

总结上述 3 种情况的分析可知

$$\begin{aligned}\mathrm{Var}\Big(\sum_{1\le i<j\le n}\tilde{a}_{ij}^{(t)}\Big)&=\sum_{(i,j),(k,l)}E(\tilde{a}_{ij}^{(t)}\tilde{a}_{kl}^{(t)})=\sum_{i=k,j=l}E(\tilde{a}_{ij}^{(t)})^2+\sum_{\#(\{i,j\}\cap\{k,l\})=1}(E(a_{ij}^{(t)}a_{il}^{(t)})-[E(a_{ij}^{(t)})]^2)=\\&\frac{n(n-1)}{2}E(a_{12}^{(t)})(1-E(a_{12}^{(t)}))+n(n-1)(n-2)(E(a_{12}^{(t)}a_{13}^{(t)})-[E(a_{12}^{(t)})]^2)=\\&\frac{n(n-1)}{2}\tau_{q,t}(1-\tau_{q,t})+n(n-1)(n-2)\sigma_{q,t}^2\to\frac{n(n-1)}{2}q^{-1}(1-q^{-1})+\\&n(n-1)(n-2)\sigma_q^2,t\to\infty,\end{aligned} \tag{13}$$

其中 $\tau_{q,t},\sigma_{q,t}^2,\sigma_q^2$ 分别如(9)、(7) 及(8) 式中所定义.

下面,采用相依图与 Stein 方法来完成定理 1 的证明.给定 $t\in\mathscr{D}_q$, 令

$$\mathscr{U}_n^{(t)}:=\frac{U_n^{(t)}-E(U_n^{(t)})}{\sqrt{\mathrm{Var}(U_n^{(t)})}}=\frac{\sum_{1\le i<j\le n}\tilde{a}_{ij}^{(t)}}{\sqrt{\mathrm{Var}\big(\sum_{1\le i<j\le n}\tilde{a}_{ij}^{(t)}\big)}}.$$

注意到,$\{\tilde{a}_{ij}^{(t)},1\le i<j\le n\}$ 具有相依图结构. 因此,由引理 1 可知

$$d_W(\mathscr{U}_n^{(t)},\mathscr{N}(0,1))\le\frac{D_n^2}{(\sigma_n^{(t)})^3}\sum_{1\le i<j\le n}E(|\tilde{a}_{ij}^{(t)}|^3)+\frac{\sqrt{28}D_n^{3/2}}{\sqrt{\pi}(\sigma_n^{(t)})^2}\sqrt{\sum_{1\le i<j\le n}E[(\tilde{a}_{ij}^{(t)})^4]},$$

其中 $D_n=2n-5$(n 充分大),$\sigma_n^{(t)}:=\sqrt{\mathrm{Var}\big(\sum_{1\le i<j\le n}\tilde{a}_{ij}^{(t)}\big)}$. 此外,又注意到

$$|\tilde{a}_{ij}^{(t)}|=|1_{\{\gcd(X_i^{(t)},X_j^{(t)})=1\}}-P(\gcd(X_i^{(t)},X_j^{(t)})=1)|\le 1.$$

因此,结合前面关于方差的渐近分析可得,对任意的 $t\in\mathscr{D}_q$ 都有

$$d_W(\mathscr{U}_n^{(t)},\mathscr{N}(0,1))\le\frac{2n^4}{(\sigma_n^{(t)})^3}+4\sqrt{\frac{7}{\pi}}\frac{n^{5/2}}{(\sigma_n^{(t)})^2}\le\frac{c}{\sqrt{n}},$$

其中 c 是不依赖于 n,t 的正普适性常数. 定理 1 证毕.

2.3 定理 2 的证明

证明主要基于文献[24]中的想法.

记 $X_n^{(t)}=(X_1^{(t)},X_2^{(t)},\cdots,X_n^{(t)})$,令 $Y_n^{(t)}=(Y_1^{(t)},Y_2^{(t)},\cdots,Y_n^{(t)})$ 是 $X_n^{(t)}$ 的独立版本,即 $Y_n^{(t)}$ 与 $X_n^{(t)}$ 相互独立且同分布.任给 $1\le i\le n$,令 $\mathscr{M}_t^i=\mathscr{M}_t$,设 f 是从 $\prod_{i=1}^n\mathscr{M}_t^i$ 到 $\mathbf{R}$ 的有界可测函数,如下定义其一阶与二阶差分($j<i$):

$$\begin{aligned}\Delta_i f(X_n^{(t)};y_i)&:=f(x_1^{(t)},\cdots,x_n^{(t)})-f(x_1^{(t)},\cdots,x_{i-1}^{(t)},y_i,x_{i+1}^{(t)},\cdots,x_n^{(t)}),\\\Delta_i\Delta_j f(X_n^{(t)};y_j,y_i)&:=\Delta_i f(X_n^{(t)};y_i)-f(x_1^{(t)},\cdots,x_{j-1}^{(t)},y_j,x_{j+1}^{(t)},\cdots,x_n^{(t)})+\\&\quad f(x_1^{(t)},\cdots,x_{j-1}^{(t)},y_j,x_{j+1}^{(t)},\cdots,x_{i-1}^{(t)},y_i,x_{i+1}^{(t)},\cdots,x_n^{(t)}).\end{aligned} \tag{14}$$

对任意固定的 $t\in\mathscr{D}_q$, 令

$$f(X_n^{(t)})=\sqrt{n}U_n^{(t)}=\frac{2}{\sqrt{n}(n-1)}\sum_{1\le i<j\le n}1_{\{\gcd(X_i^{(t)},X_j^{(t)})=1\}}, \tag{15}$$

则对任意的 $t \in \mathscr{D}_q$, $x_n^{(t)}, y_n^{(t)} \in \prod_{i=1}^{n} \mathscr{M}_t^i$, 有

$$\Delta_i f(x_n^{(t)}; y_i) \leq \frac{4}{\sqrt{n}}, \Delta_i \Delta_j f(x_n^{(t)}; y_j, y_i) \leq \frac{8}{\sqrt{n}(n-1)}. \tag{16}$$

进一步的,若记 $\beta_n = a_n^2/n$, $\lambda_n = a_n/\sqrt{n}$,

$$d_n^{(t)} := \sum_{i=1}^{n} (\sup_{\omega \in \Omega} \Delta_i f(X_n^{(t)}; Y_i^t))^2 (\frac{1}{3} \sup_{\omega \in \Omega} \Delta_i f(X_n^{(t)}; Y_i^t) + \frac{1}{4} \sum_{j=1}^{i-1} \sup_{\omega \in \Omega} \Delta_i \Delta_j f(X_n^{(t)}; Y_j^{(t)}, Y_i^{(t)})), \tag{17}$$

则利用(16)估计式,通过简单计算可得

$$\frac{\beta_n^2}{\lambda_n^3} \cdot d_n^{(t)} \leq \frac{a_n^4}{n^2} \cdot \frac{n^{3/2}}{a_n^3} \cdot \frac{112}{3\sqrt{n}} \leq \frac{40 a_n}{n}.$$

进一步有 $\frac{\beta_n}{\lambda_n^2} \cdot \mathrm{Var}(f(X_n^{(t)})) = \mathrm{Var}(\sqrt{n} U_n^{(t)}) = \frac{4}{n(n-1)^2} \cdot \mathrm{Var}\left(\sum_{1 \leq i < j \leq n} a_{ij}^{(t)}\right) \to 4\sigma_{q,t}^2$, $n \to \infty$, 此处取极限时用到了方差的渐近估计(13)式且 $\sigma_{q,t}^2$ 如(7)式中所定义.因而,由引理 2 可知,随机序列 $\{n a_n^{-1}(U_n^{(t)} - E(U_n^{(t)}))\}$ 满足速度为 $\{a_n^2/n\}$、速率函数为 $I_{q,t}(x) = x^2/(8\sigma_{q,t}^2)$ 的大偏差原理.定理 2 证毕.

参 考 文 献

[1] DIRICHLET G L. Über die Bestimmung der mittleren Werthe in der Zahlentheorie, Abhandlungen Königlich Preuss Akad[J]. Wiss, 1849(1): 69-83.

[2] CESÀRO E. Sur le plus grand commun diviseur de plusieurs nombres[J]. Annali di Matematica Pura ed Applicata, 1885, 13: 291-294.

[3] LEHMER D N. Asymptotic evaluation of certain totient-sums[J]. Amer J Math, 1900, 22: 293-335.

[4] NYMANN J E. On the probability that k positive integers are relatively prime[J]. J Number Theory, 1972(4): 469-473.

[5] KUBOTA H, SUGITA H. Probabilistic proof of limit theorems in number theory by means of adeles[J]. Kyushu J Math, 2002, 56: 391-404.

[6] SUGITA H, TAKANOBU S. The probability of two integers to be co-prime, revisited-on the behavior of CLT-scaling limit[J]. Osaka J Math, 2003, 40: 945-976.

[7] FERNÁNDEZ J L, FERNÁNDEZ P. Asymptotic normality and greatest common divisors[J]. Int J Number Theory, 2015, 11: 89-126.

[8] MEHRDAD B, ZHU L. Limit theorems for empirical density of greatest common divisors[J]. Math Proc Camb Phil Soc, 2016, 161: 517-533.

[9] MAZE G, ROSENTHAL J, WANGER U. Natural density of rectangular unimodular integer matrices[J]. Linear Algebra Appl, 2011, 434: 1319-1324.

[10] KAC M. Statistical independence in probability, analysis and number theory[M]. New York: John Wiley & Sons Inc, 1959.

[11] KUBILIUS J. Probabilistic methods in the theory of numbers[M]. Translations of Mathematical Monographs: American Mathematical Society, 1964.

[12] TENENBAUM G. Introduction to analytic and probabilistic number theory[M]. Cambridge: Cambridge University Press, 1995.

[13] LIDL R, NIEDERREITER H. Finite fields, Encyclopedia of Mathematics and its Applications[M]. Cambridge: Cambridge University Press, 1997.

[14] ROSEN M. Number theory in function fields[M]. New York: Springer-Verlag, 2002.

[15] MORRISON K E. Random polynomials over finite fields[EB/OL]. [2021-02-11]. http://www.calpoly.edu/~kmorriso/Research/RPFF.pdf.

[16] BENJAMIN A T, BENNETT C D. The probability of relatively prime polynomials[J]. Math Magaz, 2007, 80: 196-202.

[17] SUGITA H, TAKANOBU S. The probability of two F_q-polynomials to be coprime[J]. Adv Stud Pure Math, 2007, 49: 455-478.

[18] GUO X, YANG G Y. The probability of rectangular unimodular matrices over $F_q[x]$[J]. Linear Algebra Appl, 2013, 438: 2675-2682.

[19] ARRATIA R, BARBOUR A D, TAVARÉ S. On random polynomials over finite fields[J]. Math Proc Camb Phil Soc, 1993, 114: 347-368.

[20] HANSEN J. Factorization in $F_q[x]$ and Brownian motion[J]. Combin Probab Comput, 1993(2): 285-299.

[21] DEMBO A, ZEITOUNI O. Large deviations techniques and applications[M]. 2nd. New York: Springer, 1998.

[22] VARADHAN S R S. Large deviations and applications[M]. Philadelphia: SIAM, 1984.

[23] ROSS N. Fundamentals of Stein's method[J]. Probab Surv, 2011(8): 210-293.

[24] DÖRING H, EICHELSBACHER P. Moderate deviations in a random graph and for the spectrum of Bernoulli random matrices[J]. Elec-

tron J Probab,2009,14:2636-2656.
[25] JANSON S.Normal convergence by higher semiinvariants with applications to sums of dependent random variables and random graphs [J].Ann Probab,1988,16:305-312.
[26] BALDI P,RINOTT Y.Asymptotic normality of some graph-related statistics[J].J Appl Probab,1989,26:171-175.

Asymptotic statistics of random polynomials over finite fields

Li Meng, Miao Yu, Yang Guangyu

(1. School of Mathematics and Statistics, Zhengzhou University, Zhengzhou 450001, China;
2. College of Mathematics and Information Science, Henan Normal University, Xinxiang 453007, China)

Abstract: In this paper, we mainly study the asymptotic statistical properties of random polynomials over finite fields. To be explicit, we establish, by the dependency graphs and Stein's methods, the central limit theorems and moderate deviations for the empirical density of the co-prime random polynomials, which extends the partial results on the integer rings in the literature to the polynomial rings.

Keywords: large deviation principles; polynomial rings; random polynomials; finite fields; central limit theorems

[责任编校 陈留院 赵晓华]