Drelikhov, V. O.; **Kruglov, I. A.**

Local characteristics of smoothing properties of endomorphisms of finite abelian groups.

(Russian. English summary) Zbl 1476.94027
Mat. Vopr. Kriptografii 6, No. 3, 33-45 (2015).

Summary: Let G be a finite Abelian group, G^n be its n-fold Cartesian product, and $\vec{\xi} = (\xi_1, \xi_2, \ldots, \xi_n)$ be a random element of G^n. We investigate the local characteristics of closeness of distribution of random element $H(\vec{\xi})$, where $H\colon G^n \to G^m$, to the uniform distribution on G^m. Main results are connected with the case of independent identically distributed elements $\xi_1, \xi_2, \ldots, \xi_n$ and endomorphism H of group G^n onto the group G^m.

MSC:

94A60 Cryptography
20K30 Automorphisms, homomorphisms, endomorphisms, etc. for abelian groups
42A16 Fourier coefficients, Fourier series of functions with special properties, special Fourier series

Keywords:

smoothing of distributions; endomorphism; Fourier coefficients

Full Text: DOI MNR

References:

[1] Egorov B. A., Maksimov Yu. I., "Ob odnoi posledovatelnosti sluchainykh velichin, prinimayuschikh znacheniya iz kompaktnoi kommutativnoi gruppy", Teoriya veroyatn. i ee primen., 13:4 (1968), 621-630 · Zbl 0196.18403

[2] Kapitonov V. M., "O skorosti skhodimosti posledovatelnosti raspredelenii, opredelyaemykh skhemoi avtoregressii na kompaktnoi gruppe", Teoriya veroyatn. i ee primen., 18:3 (1973), 608-615 · Zbl 0324.60006

[3] Maksimov Yu. I., "O tsepyakh Markova, svyazannykh s dvoichnymi registrami sdviga so sluchainymi elementami", Trudy po diskretnoi matematike, 1, 1997, 203-220 · Zbl 1022.94007

[4] Chung F., Diaconis P., Gracham R. L., "A random walk problem arising in random number generation", Ann. Probab., 15:3 (1987), 1148-1165 · Zbl 0622.60016 · doi:10.1214/aop/1176992088

[5] Hildebrand M., "Random processes of the form \(X_{n+1}=a_n\cdot X_n+b_n(\operatorname{mod}\,p)\)", Ann. Probab., 21:2 (1993), 710-720 · Zbl 0776.60012 · doi:10.1214/aop/1176989264

[6] Grenander U., Veroyatnosti na algebraicheskikh strukturakh, Mir, M., 1965, 274 pp.

[7] Solodovnikov Vik. I., "Bent-funktsii iz konechnoi abelevoi gruppy v konechnuyu abelevu gruppu", Diskretnaya matematika, 14:1 (2004), 99-113 · Zbl 1047.94011 · doi:10.4213/dm234