МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2017 Т. 8 № 1 С. 31–50

УДК 519.217.2

Сходимость матриц переходных вероятностей некоторых цепей Маркова на конечной абелевой группе к равномерной матрице

И. А. Круглов

Академия криптографии Российской Федерации, Москва

Получено 20.IV.2015

Аннотация. Изучается класс конечных однородных цепей Маркова, связанных со схемой авторегрессии на конечных абелевых группах. В терминах параметров схемы авторегрессии найдены условия полной регулярности и точные формулы для среднеквадратического уклонения матриц переходных вероятностей за N шагов от предельной равномерной матрицы.

Ключевые слова: цепи Маркова, схема авторегрессии на конечных группах, среднеквадратическое уклонение от равномерной матрицы подстановки

Convergence of transition matrices of some Markov chains on finite Abelian group to the uniform matrix

I. A. Kruglov

Academy of Cryptography of the Russian Federation, Moscow

Abstract. A class of finite homogeneous Markov chains connected with the autoregression scheme on finite Abelian groups is studied. In terms of the autoregression scheme parameters some conditions of complete regularity are given and exact formulas for the mean square deviation of N-step transition matrices from the limiting uniform matrix are derived.

Keywords: Markov chains, autoregression scheme on finite groups, mean square deviation from the uniform matrix

Citation: *Mathematical Aspects of Cryptography*, 2017, v. 8, № 1, pp. 31–50 (Russian)

Список литературы

[1] Глухов М. М., “О числовых параметрах, связанных с заданием конечных групп системами образующих элементов”, *Труды по дискретной математике*, **1**, М.: Научное изд-во ТВП, 1997, 43–66.

[2] Горчинский Ю. Н., Круглов И. А., Капитонов В. М., “Вопросы теории распределений на конечных группах”, *Труды по дискретной математике*, **1**, М.: Научное изд-во ТВП, 1997, 85–112.

[3] Круглов И. А., “Условия предельной равновероятности распределений в схеме линейной авторегрессии со случайным управлением на конечной группе”, *Дискретн. матем.*, **17**:3 (2005), 12–18.

[4] Круглов И. А., “О слоях в системе образующих элементов подпрямого произведения подгрупп конечной группы”, *Дискретн. матем.*, **21**:1 (2009), 52–65.

[5] Круглов И. А., “Случайные последовательности вида $X_{t+1} = a_t \cdot X_t + b_t \pmod n$ с зависимыми коэффициентами a_t, b_t ”, *Дискретн. матем.*, **17**:2 (2005), 49–55.

[6] Diaconis P., *Group Representations in Probability and Statistics*, Lecture Notes – Monograph Series, **11**, Hayward, CA: Inst. of Math. Statist., 1988, 198 pp.

[7] Hildebrand M., “Random processes of the form $X_{n=1} = a_n X_n + b_n (\mathrm{mod} p)$ ”, *Ann. Probab.*, **21**:2 (1993), 710–720.

[8] Hildebrand M., “Random processes of the form $X_{n=1} = a_n \cdot X_n + b_n \pmod p$, where b_n takes on a single value”. In: “*Random Discrete Structures*”, IMA Vol. Math. Appl., **76**, Heidelberg etc.: Springer, 1996, 153–174.

[9] Asci C., “Generating uniform random vectors”, *J. Theoret. Probab.*, **14**:2 (2001), 333–356.

[10] Helleloid G., *Automorphism Groups of Finite p-groups: Structure and Applications*, Ph.D., The Univ. of Texas at Austin, 2007, 107 pp., http://arxiv.org/math.GR/07112816 math.GR/07112816

[11] Bianko S., *Random processes of the form $X_{n=1} = A_n \cdot X_n + B_n \pmod p$ in two dimensions*, Ph.D., State Univ. of New York at Albany, 2012, 37 pp.

[12] Hildebrand M., “A lower bound for the Chung – Diaconis – Graham random process”, *Proc. Amer. Math. Soc.*, **137**:4 (2009), 1479–1487.

[13] Hildebrand M., McCollum J., “Generating random vectors in $\left(Z/pZ\right)^d$ via an affine random process”, *J. Theor. Probab.*, **21**:4 (2008), 802–811.