МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2017 Т. 8 № 1 С. 81–94

УДК 519.212.2+519.115

Число разложений случайной подстановки в композицию двух инволюций с заданным циклом в одном из сомножителей

В. Г. Михайлов

Математический институт им. В. А. Стеклова Российской академии наук, Москва

Получено 30.V.2016

Аннотация. Исследуется число разложений случайной равновероятной подстановки порядка n в композицию двух инволюций при фиксации цикла в одном из сомножителей. Доказаны теоремы об асимптотической нормальности логарифма числа таких разложений при $n \to \infty$.

Ключевые слова: случайные подстановки, разложение подстановки, произведение инволюций, асимптотическая логарифмическая нормальность

The number of decomposition of random permutation into the product of two involutions with given cycle in one of multipliers

V. G. Mikhailov

Steklov Mathematical Institute of the Russian Academy of Sciences, Moscow

Abstract. We investigate the number of decompositions of random permutation of the n-th order into the product of two involutions with given cycle in one of multipliers. Theorems on the asymptotical logarithmic normality of this number as $n \to \infty$ are proved.

Key words: random permutations, decomposition of permutation, product of involutions, asymptotic logarithmic normality

Citation: *Mathematical Aspects of Cryptography*, 2017, v. 8, № 1, pp. 81–94 (Russian)

Список литературы

[1] Flajolet P., Sedgewick W., *Analytic Combinatorics*, Cambridge: Cambridge Univ. Press, 200, 824 pp.

[2] Chovla S., Herstein I. N, Moore W. K., "On recursions connected with symmetric groups. I", *Canad. J. Math.*, **3** (1951), 328–334.

[3] Lugo M., "The cycle structure of compositions of random involutions", arXiv:0911.3604v1 [math.CO] 18 Nov 2009.

[4] Lugo M., *Profiles of large combinatorial structures*, PhD Thesis, Univ. Pensylvania, 2010.

[5] Burnette Ch., Schmutz E., "Representing random permutations as the product of two involutions", arXiv: 1507.05701v1 [math.CO] 21 Jul 2015.

[6] Сачков В. Н., *Вероятностные методы в комбинаторном анализе*, М.: Наука, 1978, 288 с.

[7] Erdös P., Turán P., "On some problems of a statistical group-theory. III", *Acta. Math. Acad. Sci. Hungar.*, **18** (1967), 309–320.

[8] Колчин В. Ф., *Случайные отображения*, М.: Наука, 1984, 208 с.

[9] Arratia R., Barbour A. D., Tavaré S., "Limit theorems for combinatorial structures", *Ann. Probab.*, **28**:4 (2000), 1620–1644.

[10] Arratia R., Tavaré S., "Limit theorems for combinatorial structures via discrete process approximations", *Rand. Struct. & Algor.*, **3**:3 (1992), 321–345.

[11] DeLaurentis J. M., Pittel B. G., "Random permutations and Brownian motion", *Pacific J. Math.*, **119**:2 (1985), 287–301.

[12] Manstavicius E., "The Berry – Esseen bound in the theory of random permutations", *Ramanujan J.*, **2**:1-2 (1998), 185–199.