Journal of Number Theory 161 (2016) 311–342

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

A family of measures on symmetric groups and the field with one element

Jeffrey C. Lagarias [1]

Dept. of Mathematics, University of Michigan, Ann Arbor, MI 48109-1043, United States

ARTICLE INFO

Article history:
Received 9 July 2015
Accepted 18 September 2015
Available online 12 November 2015
Communicated by Jerome Hoffman, Robert Perlis, Ling Long, Karl Mahlburg, Jorge Morales, Holly Swisher

MSC:
primary 11R09
secondary 11R32, 12E20, 12E25

Keywords:
Finite field
Polynomial factorization
Symmetric group

ABSTRACT

For each $n \geq 1$ this paper considers a one-parameter family of complex-valued measures on the symmetric group S_n, depending on a complex parameter z. For parameter values $z = q = p^f$ this measure describes splitting probabilities of monic degree n polynomials over $\mathbb{F}_q[X]$, conditioned on being square-free. It studies these measures in the case $z = 1$, and shows that they have an interesting internal structure having a representation theoretic interpretation. These measures may encode data relevant to the hypothetical "field with one element $\mathbb{F}_1$". It additionally studies the case $z = -1$, which also has a representation theoretic interpretation.

1. Introduction

This paper considers a one-parameter family of complex-valued measures on the symmetric group S_n, called *z-splitting measures*, introduced by the author and B.L. Weiss in [15]. The parameter z may take complex values. These measures were constructed to interpolate at parameter values $z = q = p^f$, a prime power, probability

E-mail address: lagarias@umich.edu.

[1] The author's work was partially supported by NSF grant DMS-1401224.

http://dx.doi.org/10.1016/j.jnt.2015.09.003

measures that give the probabilities of given factorization type of monic degree n polynomials over finite fields $\mathbb{F}_q$, conditioned to have a square-free factorization. In [15] these measures at $z = p$ arose as limiting distributions on how the prime ideal (p) in $\mathbb{Z}$ splits in the number field generated by a root of a random degree n polynomial $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{Z}[X]$ with coefficients drawn from a box $|a_i| \leq B$, as $B \to \infty$, after conditioning on the polynomial discriminant D_f being relatively prime to p. With limiting probability 1 as $B \to \infty$ such a polynomial $f(X)$ is irreducible and has splitting field having Galois group S_n, in which case adjoining a single root of it yields an S_n-*extension*, meaning a non-Galois degree n extension of $\mathbb{Q}$ whose Galois closure has Galois group S_n. The resulting splitting distributions were compared to those in a conjecture of Bhargava [1] for the distribution of splitting types of a fixed prime ideal (p) in those S_n-extensions k of $\mathbb{Q}$ having field discriminant $|D_k|$ at most D, in the limit $D \to \infty$. The Bhargava distribution matches the $z \to \infty$ limit of the z-splitting measures, which is the uniform distribution on S_n. The z-splitting measures for $z = p$ are also relevant to the distribution to splitting types of monic polynomials with p-adic integer coefficients studied by Weiss [35].

To define the z-splitting measures, we first specify them to be constant on conjugacy classes C_λ of S_n, which we label by partitions λ specifying the (common) cycle structure of all elements $g \in C_\lambda$. For each $m \geq 1$ we define the m-th *necklace polynomial* $M_m(X)$ by

$$M_m(X) := \frac{1}{m} \sum_{d|m} \mu(d) X^{m/d},$$

where $\mu(d)$ is the Möbius function. We next introduce the *cycle polynomial* $N_\lambda(X)$ attached to a partition λ, by

$$N_\lambda(X) := \prod_{j=1}^{n} \binom{M_j(z)}{m_j(\lambda)},$$

in which $m_j = m_j(\lambda)$ counts the number of cycles in $g \in S_n$ of length j, and for a complex number z we interpret $\binom{z}{k} := \frac{(z)_k}{k!} = \frac{z(z-1)\cdots(z-k+1)}{k!}$. The *$z$-splitting measure* $\nu^*_{n,z}$ is then defined on conjugacy classes C_λ of S_n by

$$\nu^*_{n,z}(C_\lambda) := \frac{1}{z^{n-1}(z-1)} N_\lambda(X). \tag{1.1}$$

The value of the measure on a single element $g \in S_n$ with $g \in C_\lambda$ is $\nu^*_{n,z}(g) := \frac{1}{|C_\lambda|}\nu^*_{n,z}(C_\lambda)$. In [15] it was shown that for all integers $k \neq 0, 1$ the measures $\nu^*_{n,k}$ are nonnegative, so are probability measures. In addition a limit measure as $z \to \infty$ exists and is the uniform measure on S_n.

This paper studies these measures at the parameter value $z = 1$, which is the sole remaining integer value where the z-splitting measure is well-defined, cf. Lemma 2.5.