Linear Algebra and its Applications 539 (2018) 134–159

Contents lists available at ScienceDirect

Linear Algebra and its Applications

www.elsevier.com/locate/laa

Uniform probability and natural density of mutually left coprime polynomial matrices over finite fields

Julia Lieb

Department of Mathematics, University of Wuerzburg, Emil-Fischer-Str. 40, 97074 Wuerzburg, Germany

A R T I C L E I N F O

Article history:
Received 22 February 2017
Accepted 5 November 2017
Available online 9 November 2017
Submitted by R. Brualdi

MSC:
15A031
15B33
15B52
11T06

Keywords:
Polynomial matrices
Mutual left coprimeness
Natural density
Uniform probability
Finite fields

A B S T R A C T

We compute the uniform probability that finitely many polynomials over a finite field are pairwise coprime and compare the result with the formula one gets using the natural density as probability measure. It will turn out that the formulas for the two considered probability measures asymptotically coincide but differ in the exact values. Moreover, we calculate the natural density of mutually left coprime polynomial matrices and compare the result with the formula one gets using the uniform probability distribution. The achieved estimations are not as precise as in the scalar case but again we can show asymptotic coincidence.

1. Introduction

Polynomial matrices over finite fields play an important role in various mathematical areas, e.g. for the investigation of discrete-time linear systems [16], [3] or in the theory

E-mail address: julia.lieb@mathematik.uni-wuerzburg.de.

https://doi.org/10.1016/j.laa.2017.11.006

of convolutional codes [17]. For many of these applications, coprimeness conditions for the considered matrices are essential, [3].

A polynomial matrix $D \in \mathbb{F}[z]^{n\times m}$ is called left prime if there exists $X \in \mathbb{F}[z]^{m\times n}$ with $DX = I$, where I denotes the identity matrix. It is easily shown that this is equivalent to the condition that the fullsize minors of D are coprime; see e.g. [21]. In this paper, we will need another characterization of left primeness, namely that D has to be of full row rank for every $z \in \overline{\mathbb{F}}$, which clearly is equivalent to the fact that it can be completed to a unimodular matrix, i.e. to a matrix with nonzero constant determinant. That it is possible to characterize left primeness by this last condition is part of the famous Quillen–Suslin theorem, also known as Serre conjecture [8], which was formulated in 1957 for polynomial matrices in several variables $z_1, \ldots, z_k$. Already in 1958, Seshadri [19] proved its correctness in principal ideal domains and therefore, in the cases $k = 1$ and $k = 2$. The final proof for the general case followed in 1976 [15], [20].

We use the one-dimensional version of this theorem to compute the probability of left primeness for specially structured polynomial matrices using two different probability measures, namely uniform probability and natural density. For the case $n = 1$, i.e. for matrices consisting only of one row, the probability of left primeness coincides with the probability of coprimeness for polynomials, which was computed in [4] to be equal to $1 - t^{m-1}$, where $t := |\mathbb{F}|^{-1}$. For matrices of arbitrary sizes, Guo and Yang [5] computed the natural density of left primeness to be equal to $\prod_{j=m-n}^{m-1}(1 - t^j)$, using techniques from [11], where this computation was done for integer matrices. Unfortunately, their proof contains a mistake. This has already been noticed by Micheli and Schnyder [13], [12]. In [12, Problem 4.2, Theorem 4.4], this problem is solved in a far more general context. The author computes densities over integrally closed subrings of global function fields using the definition of density given in [14]. The used strategy could also be found in [2] where the density of coprime algebraic integers of a number field is calculated.

In Theorem 9 of [9], the probability that a matrix of the form $[D_1\ D_2] \in \mathbb{F}[z]^{m\times 2m}$ with $\deg(\det(D_i)) = n_i \in \mathbb{N}$ is left prime, i.e. that $D_1 \in \mathbb{F}[z]^{m\times m}$ and $D_2 \in \mathbb{F}[z]^{m\times m}$ are left coprime, was calculated. It turns out that the obtained formula, namely $1 - t^m + O(t^{m+1})$ for $t \to 0$, asymptotically coincides with the formula for the natural density of left primeness for an arbitrary polynomial matrix from $\mathbb{F}[z]^{m\times 2m}$, computed in [5] – respectively [12] – to be equal to $\prod_{j=m}^{2m-1}(1 - t^j)$.

According to Proposition 10.3 of [3], the property of N matrices from $\mathbb{F}[z]^{m\times m}$ to be mutually left coprime is equivalent to the left primeness of a specially structured matrix from $\mathbb{F}^{(N-1)m\times mN}$. In [7], the uniform probability of mutual left coprimeness was calculated for polynomials with fixed degrees, i.e. for $m = 1$, where mutual left coprimeness and pairwise coprimeness coincide. This result was generalized in [9], obtaining a probability of $1 - \sum_{y=2}^{m+1}\binom{N}{y}t^m + O(t^{m+1})$ for the probability of mutual left coprimeness for N matrices from $\mathbb{F}[z]^{m\times m}$ whose degrees of the determinant are fixed. In this article, we firstly improve the estimation for the case $m = 1$ and secondly, compute the natural density of mutual left coprimeness in the cases $m = 1$ and $m \in \mathbb{N}$. It will turn out