# RELATIVELY PRIME POLYNOMIALS AND NONSINGULAR HANKEL MATRICES OVER FINITE FIELDS

MARIO GARCÍA-ARMAS, SUDHIR R. GHORPADE, AND SAMRITH RAM

ABSTRACT. The probability for two monic polynomials of a positive degree $n$ with coefficients in the finite field $\mathbb{F}_q$ to be relatively prime turns out to be identical with the probability for an $n \times n$ Hankel matrix over $\mathbb{F}_q$ to be nonsingular. Motivated by this, we give an explicit map from pairs of coprime polynomials to nonsingular Hankel matrices that explains this connection. A basic tool used here is the classical notion of Bezoutian of two polynomials. Moreover, we give simpler and direct proofs of the general formulae for the number of $m$-tuples of relatively prime polynomials over $\mathbb{F}_q$ of given degrees and for the number of $n \times n$ Hankel matrices over $\mathbb{F}_q$ of a given rank.

## 1. INTRODUCTION

It is a remarkable fact that the probability for two randomly chosen monic polynomials of the same positive degree with coefficients in the binary field $\mathbb{F}_2$ to be coprime is exactly 1/2. This observation appears to go back at least to an exercise in the treatise, first published in 1969, of Knuth [9, §4.6.1, Ex. 5] (see also Remark 4.2). More recently, it was made by Corteel, Savage, Wilf, and Zeilberger [2] in 1998 in the course of their work on Euler's pentagonal sieve in the theory of partitions, and it led them to ask for a "nice simple bijection" between the coprime and the non-coprime ordered pairs of monic polynomials of degree $n$ over $\mathbb{F}_2$. This was answered first by Reifegerste [12] in 2000 and by Benjamin and Bennett [1] in 2007. The latter deals with the more general case of polynomials over any finite field $\mathbb{F}_q$ where the probability turns out to be $1 - (1/q)$ instead of $1/2$. Since there are $q^{2n}$ ordered pairs of monic polynomials over $\mathbb{F}_q$ of degree $n$, this means that

$$|\mathrm{CPP}_n(\mathbb{F}_q)| = q^{2n} - q^{2n-1} = q^{2n-1}(q-1), \tag{1}$$

where $\mathrm{CPP}_n(\mathbb{F}_q)$ denotes the set of ordered pairs of coprime monic polynomials over $\mathbb{F}_q$ of degree $n$. In effect, Benjamin and Bennett gave an explicit surjective map from $\mathrm{CPP}_n(\mathbb{F}_q)$ onto the set of ordered pairs of non-coprime monic polynomials over $\mathbb{F}_q$ of degree $n$ in such a way that the cardinality of each fiber is $q - 1$.

A couple of years prior to [2] and working on a seemingly unrelated topic, Kaltofen and Lobo [8] observed that the probability for a $n \times n$ Toeplitz matrix with entries in $\mathbb{F}_q$ to be nonsingular is exactly $1 - (1/q)$. In fact, this observation can be traced back to Daykin [3] who had essentially proved the same result (and also a more general one) in 1960 with Hankel matrices in place of Toeplitz matrices. Since there are $q^{2n-1}$ Toeplitz matrices (or equivalently, Hankel matrices) of size

*Date*: November 5, 2010.
2000 *Mathematics Subject Classification.* 11T06, 11T35, 15B05.
*Key words and phrases.* Finite field, relatively prime polynomials, Toeplitz matrix, Hankel matrix, Bezoutian.

$n \times n$ with entries in $\mathbb{F}_q$, this means that

$$|\mathrm{TGL}_n(\mathbb{F}_q)| = |\mathrm{HGL}_n(\mathbb{F}_q)| = q^{2n-1} - q^{2n-2} = q^{2n-2}(q-1), \tag{2}$$

where $\mathrm{TGL}_n(\mathbb{F}_q)$ (resp: $\mathrm{HGL}_n(\mathbb{F}_q)$) denotes the set of all $n \times n$ nonsingular Toeplitz (resp: Hankel) matrices with entries in $\mathbb{F}_q$.

One of the main aims of this paper is to explain the uncanny coincidence that the probability in both of the above situations turns out to be the same or, more precisely, the fact that the formulae (1) and (2) differ just by a factor of $q$. We do this by giving an explicit surjective map from $\mathrm{CPP}_n(\mathbb{F}_q)$ onto $\mathrm{HGL}_n(\mathbb{F}_q)$ such that each fiber has cardinality $q$. This readily yields a similar map with $\mathrm{HGL}_n(\mathbb{F}_q)$ replaced by $\mathrm{TGL}_n(\mathbb{F}_q)$. As a consequence, we obtain new proofs of (1) and (2) by combining any one of the known proofs with this surjective map. We further add to this collection of proofs by giving alternative, short and completely self-contained proofs of more general versions of (1) and (2).

## 2. Preliminaries

Let $F$ be a field. Recall that a matrix $M = (m_{ij})$ with entries in $F$ is said to be a *Toeplitz matrix* (resp: *Hankel matrix*) if $m_{ij} = m_{rs}$ whenever $i - j = r - s$ (resp: $i + j = r + s$). Thus every $n \times n$ Toeplitz (resp: Hankel) matrix over $F$ looks like $(a_{n+i-j})$ (resp: $(a_{i+j-1})$) for a unique $(2n-1)$-tuple $(a_1, \dots, a_{2n-1}) \in F^{2n-1}$.

We denote by $\mathrm{T}_n(F)$ (resp: $\mathrm{H}_n(F)$) the set of all Toeplitz (resp: Hankel) matrices with entries in $F$ and, as in the Introduction, set

$$\mathrm{TGL}_n(F) = \mathrm{T}_n(F) \cap \mathrm{GL}_n(F) \quad \text{and} \quad \mathrm{HGL}_n(F) = \mathrm{H}_n(F) \cap \mathrm{GL}_n(F).$$

The following simple observation shows that at least as far as enumerative and bijective combinatorics is concerned, Toeplitz and Hankel matrices are the same.

**Proposition 2.1.** *There is a bijection between* $\mathrm{T}_n(F)$ *and* $\mathrm{H}_n(F)$*, which induces a bijection between* $\mathrm{TGL}_n(F)$ *and* $\mathrm{HGL}_n(F)$.

*Proof.* Let $E$ be the $n \times n$ matrix with 1 on the antidiagonal and 0 elsewhere, i.e., $E = (\delta_{i,n-j+1})$ where $\delta$ is the Kronecker delta. Then $E$ is nonsingular and the map given by $A \mapsto AE$ sets up the desired bijection. $\square$

As usual, $F[X]$ will denote the set of polynomials in one variable $X$ with coefficients in $F$. Recall that for any $u, v \in F[X]$ of degree $\le n$, the $n$th order *Bezoutian* (matrix) of $u$ and $v$ is the $n \times n$ matrix $B_n(u, v) = (b_{ij})$ determined by the equation

$$\frac{u(X)v(Y) - v(X)u(Y)}{X - Y} = \sum_{i,j=1}^{n} b_{ij} X^{i-1} Y^{j-1}.$$

The coefficients $b_{ij}$ are not hard to determine explicitly; in fact, if $u = \sum_{i=0}^{n} u_i X^i$ and $v = \sum_{i=0}^{n} v_i X^i$, then upon letting $u_k = v_k := 0$ for $k > n$, we have

$$b_{ij} = \sum_{s=1}^{\min\{i,j\}} (v_{s-1} u_{i+j-s} - u_{s-1} v_{i+j-s}) \quad \text{for } 1 \le i, j \le n.$$

It is clear from the definition that if $u$ and $v$ have a nonconstant common factor then the system of homogeneous linear equations corresponding to $B_n(u, v)$ has a nontrivial solution, and hence $B_n(u, v)$ is singular. It is a classical fact that the converse is also true; we record this below for convenience and refer to the survey article [5] of Helmke and Fuhrmann for a proof.

**Proposition 2.2.** *Let $u, v \in F[X]$. Assume that $\deg u = n$ and $\deg v \le n$. Then $B_n(u, v)$ is nonsingular if and only if $u$ and $v$ are coprime.*

As an illustration, consider $u, v \in F[X]$ such that $v$ is the constant polynomial 1 and $u(X) = u_0 + u_1 X + \cdots + u_n X^n$ with $u_0, u_1, \ldots, u_n \in F$. Then

$$\frac{u(X) - u(Y)}{X - Y} = \sum_{k=1}^{n} u_k \frac{X^k - Y^k}{X - Y} = \sum_{k=1}^{n} u_k \sum_{i=1}^{k} X^{i-1} Y^{k-i} = \sum_{i,j=1}^{n} u_{i+j-1} X^{i-1} Y^{j-1},$$

where, by convention, $u_k := 0$ for $k > n$. Thus the $n$th order Bezoutian $B_n(u, 1)$ has $u_n$ on its antidiagonal and 0 below that. In particular, if $\deg u = n$, i.e., if $u_n \neq 0$, then $u$ and $v$ are coprime, and moreover $B_n(u, v)$ is nonsingular.

## 3. An Explicit Surjection

Fix a positive integer $n$ and a field $F$. As in the Introduction, let

$$\mathrm{CPP}_n(F) := \left\{(f, g) \in F[X]^2 : f, g \text{ are coprime and both are monic of degree } n\right\}.$$

Moreover, let us consider

$$\mathrm{P}_n(F) := \left\{(u, v) \in F[X]^2 : u \text{ is monic, } \deg u = n, \text{ and } \deg v < n\right\}, \text{ and}$$
$$\mathrm{HP}_n(F) := \{(u, v) \in \mathrm{P}_n(F) : u \text{ and } v \text{ are coprime}\}.$$

We may refer to an element of $\mathrm{P}_n(F)$ as a *Padé pair* and an element of $\mathrm{HP}_n(F)$ as a *Hermite pair*.

**Lemma 3.1.** $\mathrm{CPP}_n(F)$ *is in bijection with* $\mathrm{HP}_n(F)$.

*Proof.* The map given by $(f, g) \mapsto (f, g - f)$ does the job. □

**Lemma 3.2.** *Let $(u, v) \in \mathrm{P}_n(F)$. Then there are unique $a_i \in F$, $i \ge 1$, such that*

$$\frac{v(X)}{u(X)} = \sum_{i=1}^{\infty} \frac{a_i}{X^i}. \tag{3}$$

*Proof.* Write $u(X) = X^n\,[1 - u^*(1/X)]$ for a unique $u^* \in F[X]$ with no constant term. Expanding as a formal power series, we obtain

$$\frac{v(X)}{u(X)} = X^{-n} v(X) \sum_{j=0}^{\infty} u^*(1/X)^j.$$

This yields the desired $a_i \in F$. □

**Definition 3.3.** For $(u, v) \in \mathrm{P}_n(F)$, we define $H_n(u, v)$ to be the $n \times n$ Hankel matrix whose $(i, j)$th entry is $a_{i+j-1}$ for $1 \le i, j \le n$, where $a_1, a_2, \ldots$ are as in (3).

The following result which relates $H_n(u, v)$ to the $n$th order Bezoutian $B_n(u, v)$ is classical and is sometimes referred to as Barnett's factorization. We include a proof for the sake of completeness, especially since the proofs found in the literature are often a bit involved and tend have an additional assumption that the polynomials $u$ and $v$ are coprime, i.e., $(u, v)$ is a Hermite pair rather than a Padé pair.

**Proposition 3.4.** $B_n(u, v) = B_n(u, 1) H_n(u, v) B_n(u, 1)$ *for any* $(u, v) \in \mathrm{P}_n(F)$.

*Proof.* Let $R(T) := v(T)/u(T)$ and let $a_i$, $i \geq 1$, be as in (3). Then

$$\frac{R(Y)-R(X)}{X-Y} = \sum_{i=1}^{\infty} a_i \sum_{j=1}^{i} \frac{X^{i-j}\,Y^{j-1}}{X^i Y^i} = \sum_{k,\ell=1}^{\infty} a_{k+\ell-1} X^{-k}\,Y^{-\ell}.$$

Now if $u(X) = u_0 + \cdots + u_{n-1}X^{n-1} + X^n$ with $u_0, \ldots, u_{n-1} \in F$ and $u_n := 1$, then

$$\begin{aligned}\frac{u(X)v(Y)-v(X)u(Y)}{X-Y} &= u(X)\frac{R(Y)-R(X)}{X-Y}u(Y)\\ &= \left(\sum_{r=0}^{n} u_r X^r\right)\left(\sum_{k,\ell=1}^{\infty} a_{k+\ell-1}X^{-k}Y^{-\ell}\right)\left(\sum_{s=0}^{n} u_s Y^s\right)\\ &= \sum_{i,j\leq n}\left(\sum_{k,\ell\geq 1} u_{i+k-1}\, a_{k+\ell-1}\, u_{\ell+j-1}\right)X^{i-1}Y^{j-1},\end{aligned}$$

where, by convention, $u_t = 0$ for $t > n$ and $a_t = 0$ for $t \leq 0$. Comparing the coefficients of $X^{i-1}Y^{j-1}$ for $1 \leq i, j \leq n$, we obtain the desired result. □

**Theorem 3.5.** *There is a surjective map* $\sigma : \mathrm{CPP}_n(F) \to \mathrm{TGL}_n(F)$ *such that for any* $A \in \mathrm{TGL}_n(F)$*, the fiber* $\sigma^{-1}(\{A\})$ *is in one-to-one correspondence with* $F$*. In particular,* $|\mathrm{CPP}_n(\mathbb{F}_q)| = q\,|\mathrm{TGL}_n(\mathbb{F}_q)|$.

*Proof.* From Propositions 2.2 and 3.4, we see that $H_n(u,v)$ is nonsingular for any $(u,v) \in \mathrm{HP}_n(F)$. Thus, we obtain a well-defined map $\eta : \mathrm{HP}_n(F) \to \mathrm{HGL}_n(F)$ given by $(u,v) \mapsto H_n(u,v)$. Now let $B \in \mathrm{HGL}_n(F)$. Then there are unique $b_1, \ldots, b_{2n-1} \in F$ such that the $(i,j)$th entry of $B$ is $b_{i+j-1}$ for $1 \leq i, j \leq n$. Let $\lambda$ be an arbitrary element of $F$ and set $b_{2n} := \lambda$. Since $B$ is nonsingular, there are unique $u_0, \ldots, u_{n-1} \in F$ such that

$$B\begin{pmatrix} u_0\\ u_1\\ \vdots\\ u_{n-1}\end{pmatrix} = -\begin{pmatrix} b_{n+1}\\ b_{n+2}\\ \vdots\\ b_{2n}\end{pmatrix}. \tag{4}$$

Next, define $u_n := 1$ and $v_0, v_1, \ldots, v_{n-1}$ to be the unique elements of $F$ given by the following triangular system of equations:

$$\begin{pmatrix} v_0\\ v_1\\ \vdots\\ v_{n-1}\end{pmatrix} = \begin{pmatrix} b_1 & b_2 & \ldots & b_n\\ 0 & b_1 & \ldots & b_{n-1}\\ \vdots & & \ddots & \vdots\\ 0 & 0 & \ldots & b_1\end{pmatrix}\begin{pmatrix} u_1\\ u_2\\ \vdots\\ u_n\end{pmatrix}. \tag{5}$$

Finally, define $u, v \in F[X]$ by

$$u = \sum_{i=0}^{n} u_i X^i \quad \text{and} \quad v = \sum_{i=0}^{n-1} v_i X^i.$$

Then $(u,v) \in \mathrm{P}_n(F)$ and if we let $a_k \in F$, $k \geq 1$, as in (3), then we have

$$\sum_{i=1}^{n} v_{i-1}X^{i-1} = \left(\sum_{j=0}^{n} u_j X^j\right)\left(\sum_{k\geq 1} a_k X^{-k}\right) = \sum_{i\leq n}\left(\sum_{j=0}^{n} a_{j-i+1}u_j\right)X^{i-1},$$

where, by convention, $a_k := 0$ for $k \leq 0$. Comparing the coefficients of $X^{i-1}$ for $-n < i \leq n$, we find that (5) and (4) are satisfied with $b_1, \ldots, b_{2n}$ replaced by

$a_1, \dots, a_{2n}$, respectively. Since $u_n = 1$, the triangular nature of (5) implies that $a_i = b_i$ for $1 \le i \le n$. Further, successive comparison of (4) with its counterpart where $b_i$'s are replaced by $a_i$'s yields $a_i = b_i$ for $1 \le i \le 2n$. In particular, $B = H_n(u, v)$. Now since $B$ is nonsingular, Propositions 3.4 and 2.2 show that $u$ and $v$ are coprime. Thus $(u, v) \in \mathrm{HP}_n(F)$ and $\eta(u, v) = B$. It is clear from the construction above that a Hermite pair $(u, v)$ satisfying $\eta(u, v) = B$ is uniquely determined by the matrix $B$ and the element $b_{2n} = \lambda$. Also, in view of (4), distinct values of $\lambda$ in $F$ give rise to distinct monic polynomials $u$ in $F[X]$ of degree $n$. This shows that for each $B \in \mathrm{HGL}_n(F)$, the fiber $\eta^{-1}(\{B\})$ is in one-to-one correspondence with $F$. Finally, combining $\eta$ with the bijections given by Proposition 2.1 and Lemma 3.1, we obtain the desired surjective map $\sigma : \mathrm{CPP}_n(F) \to \mathrm{TGL}_n(F)$. □

## 4. Relatively Prime Polynomials

The general version of (1) alluded to in the Introduction is the theorem stated below. It may be noted that this generalizes [2, Prop. 3], [11, Thm. 9] and [10, Prop. 2.4], and also that it is a more precise form of [1, Cor. 5] and [6, Thm. 1.1]. We remark at the outset that in this theorem, considering arbitrary polynomials (not necessarily monic) in $\mathbb{F}_q[X]$ does not affect the probability.

**Theorem 4.1.** *Let $m$ be a positive integer and $n_1, \dots, n_m$ be nonnegative integers. The probability that $m$ monic polynomials in $\mathbb{F}_q[X]$ of degrees $n_1, \dots, n_m$, chosen independently and uniformly at random, are relatively prime is $1 - q^{1-m}$ if $\min\{n_1, \dots, n_m\} \ge 1$ and $1$ otherwise.*

*Proof.* Let $N(n_1, \dots, n_m)$ denote the number of ordered $m$-tuples $(f_1, \dots, f_m)$ of coprime monic polynomials in $\mathbb{F}_q[X]$ such that $\deg f_i = n_i$ for $i = 1, \dots, m$. Evidently, it suffices to show that

$$(6) \qquad N(n_1, \dots, n_m) = \begin{cases} q^{n_1 + \cdots + n_m}\left(1 - q^{1-m}\right) & \text{if } \min\{n_1, n_2, \dots, n_m\} \ge 1, \\ q^{n_1 + \cdots + n_m} & \text{if } \min\{n_1, n_2, \dots, n_m\} = 0. \end{cases}$$

To this end, we shall assume, without loss of generality, that $n_1 \ge \cdots \ge n_m$. We can partition the set of ordered $m$-tuples $(f_1, \dots, f_m)$ of monic polynomials in $\mathbb{F}_q[X]$ with $\deg f_i = n_i$ for $i \le i \le m$, into disjoint subsets $S_0, S_1, \dots, S_{n_m}$, where for $0 \le d \le n_m$, the set $S_d$ consists of $m$-tuples whose GCD is of degree $d$. Given any monic polynomial $h \in \mathbb{F}_q[X]$ of degree $d$ and any coprime $m$-tuple $\big(g_1, \dots, g_m\big)$ of monic polynomials such that $\deg g_i = n_i - d$ for $i = 1, \dots, m$, it is easy to see that $(hg_1, \dots, hg_m) \in S_d$. Conversely, if $\big(f_1, \dots, f_m\big) \in S_d$, then the polynomial $h = \mathrm{GCD}\big(f_1, \dots, f_m\big)$ is monic of degree $d$ and $(f_1/h, \dots, f_m/h)$ is an ordered $m$-tuple of coprime monic polynomials of degrees $n_1 - d, \dots, n_m - d$, respectively. This shows that $|S_d| = q^d N(n_1 - d, \dots, n_m - d)$ for $0 \le d \le n_m$, and consequently,

$$(7) \qquad q^{n_1 + \cdots + n_m} = \sum_{d=0}^{n_m} |S_d| = \sum_{d=0}^{n_m} q^d N(n_1 - d, n_2 - d, \dots, n_m - d).$$

If $n_m = 0$, we immediately obtain $N(n_1, \dots, n_m) = q^{n_1 + \cdots + n_m}$. On the other hand, if $n_m \ge 1$, substituting $n_i$ by $n_i - 1$ $(i = 1, \dots, m)$ in the above relation yields

$$(8) \qquad q^{n_1 + \cdots + n_m - m} = \sum_{d=1}^{n_m} q^{d-1} N(n_1 - d, n_2 - d, \dots, n_m - d).$$

Multiplying equation (8) by $q$ and subtracting the result from (7), we obtain $N(n_1, n_2, \dots, n_m) = q^{n_1 + \cdots + n_m}\left(1 - q^{1-m}\right)$, as desired. □

**Remark 4.2.** As indicated in the Introduction, the case $m = 2$ (and $q$ prime) of the above result appears as an exercise (# 5 of §4.6.1) in Knuth [9]. The solution outlined by Knuth uses the result obtained in the previous exercise and in turn, a deep analysis of the euclidean algorithm. The general result with arbitrary $m$ and $q$ (but with $n_1 = \cdots = n_m = n$) given in Corteel, Savage, Wilf and Zeilberger [2] seems to have been arrived at independently by completely different means. Also, it is indicated in a footnote in [2, p.188] that the degrees $n_1, \ldots, n_m$ could well be different (i.e., one has a result such as Theorem 4.1 above), and this observation is ascribed to D. Zagier. Many of the subsequent works (e.g. [1, 6, 4, 12]) cite [2] as an earliest reference for this result (and in fact, the authors of this paper did the same before it was pointed out by a referee that the result is classical). In retrospect, the key ideas in the answer by Benjamin and Bennett [1] to the question in [2] about a nice bijective proof can be traced back to [9, §4.6] and a more detailed analysis by Norton [11] as well as by Ma and van zur Gathen [10]. In the same vein, the short proof given above of Theorem 4.1, even though it was discovered independently, can be viewed as an extension of the "alternative proof" that appears in the solution of Exercise 5 of §4.6.1 in the first edition of Knuth [9], but for some mysterious reason, is missing in the subsequent editions. Thus, the contents of this section may help resurrect an original and perhaps the simplest proof. Finally, we remark that nontrivial generalizations of Theorem 4.1 are studied by Gao and Panario [4] and by Hou and Mullen [6], while an application to a conjecture about the enumeration of certain Singer cycles is discussed in [7].

## 5. Hankel Matrices over $\mathbb{F}_q$

The general version of (2) alluded to in the Introduction is the following.

**Theorem 5.1.** *The number $N(n, r; q)$ of $n \times n$ Hankel matrices of rank $r$ with entries in the finite field $\mathbb{F}_q$ is given by*

$$N(n,r;q) = \begin{cases} 1 & \text{if } r = 0, \\ q^{2r-2}(q^2-1) & \text{if } 1 \le r \le n-1, \\ q^{2n-2}(q-1) & \text{if } r = n. \end{cases} \tag{9}$$

Before giving a proof of the above theorem, we introduce some notation and prove a few auxiliary results. Let $F$ be a field and, as before, $n$ a positive integer. Given any $n \times n$ matrix $A$ with entries in $F$ and any positive integers $d$, $i_1, \ldots, i_d, j_1, \ldots, j_d$ such that $i_1 < \cdots < i_d \le n$ and $j_1 < \cdots < j_d \le n$, we denote by $A[i_1, \ldots, i_d | j_1, \ldots, j_d]$ the $d \times d$ submatrix of $A$ formed by the rows indexed by $i_1, \ldots, i_d$ and the columns indexed by $j_1, \ldots, j_d$. Note that the $d^{\text{th}}$ leading principal submatrix of $A$ is $A[1, \ldots, d | 1, \ldots, d]$ and this will be denoted simply by $A_d$. Define

$$\delta(A) := \begin{cases} 0 & \text{if } A_d \text{ is singular for each } d = 1, \ldots, n, \\ \max\{d : A_d \text{ is nonsingular}\} & \text{otherwise.} \end{cases}$$

For $r, k \in \{0, 1, \ldots, n\}$, let $\mathrm{H}_n(r, F) := \{A \in \mathrm{H}_n(F) : \mathrm{rank}(A) \le r\}$, and moreover,

$$\mathrm{H}_n^{(k)}(F) := \{A \in \mathrm{H}_n(F) : \delta(A) = k\} \quad \text{and} \quad \mathrm{H}_n^{(k)}(r, F) := \mathrm{H}_n(r, F) \cap \mathrm{H}_n^{(k)}(F).$$

Note that $\mathrm{HGL}_n(F) = \mathrm{H}_n^{(n)}(F) = \mathrm{H}_n^{(n)}(n, F)$ and also that

$$\mathrm{H}_n(F) = \coprod_{k=0}^{n} \mathrm{H}_n^{(k)}(F) \quad \text{and} \quad \mathrm{H}_n(r, F) = \coprod_{k=0}^{r} \mathrm{H}_n^{(k)}(r, F), \tag{10}$$

where $\coprod$ denotes disjoint union. The main idea in the proof of Theorem 5.1 is to use the above decompositions and to characterize $\mathrm{H}_n^{(k)}(\mathbb{F}_q)$ and $\mathrm{H}_n^{(k)}(r,\mathbb{F}_q)$ suitably so as to be able to determine their cardinalities recursively. Here is the first step.

**Lemma 5.2.** *Let $A = (a_{i+j-1}) \in \mathrm{H}_n(F)$. Then*

$$A \in \mathrm{H}_n^{(0)}(F) \Longleftrightarrow a_1 = \cdots = a_n = 0. \tag{11}$$

*Moreover, for $0 \le r \le n-1$,*

$$A \in \mathrm{H}_n^{(0)}(r,F) \Longleftrightarrow a_1 = \cdots = a_{2n-r-1} = 0. \tag{12}$$

*In particular, $|\mathrm{H}_n^{(0)}(\mathbb{F}_q)| = q^{n-1}$ and $|\mathrm{H}_n^{(0)}(r,\mathbb{F}_q)| = q^r$.*

*Proof.* If $A \in \mathrm{H}_n^{(0)}(F)$, then $\det(A_k) = 0$ for $k = 1,\ldots,n$. Using this successively, we obtain $a_1 = \cdots = a_n = 0$. Conversely, if $a_1 = \cdots = a_n = 0$, then it is clear that $\det(A_k) = 0$ for $k = 1,\ldots,n$, i.e., $A \in \mathrm{H}_n^{(0)}(F)$. Next, let $0 \le r \le n-1$ and suppose $A \in \mathrm{H}_n^{(0)}(r,F)$. Then $a_1 = \cdots = a_n = 0$, as before. Moreover, by successively using the vanishing of the $(r+1)\times(r+1)$ minor $\det A[n-r, n-r+1,\ldots,n | j, j+1,\ldots,j+r]$ for $j = 2,\ldots,n-r$, we obtain $a_{n+1} = \cdots = a_{2n-r-1} = 0$ as well. Conversely, suppose $a_1 = \cdots = a_{2n-r-1} = 0$, then $A \in \mathrm{H}_n^{(0)}(F)$ and it is easily seen that every $(r+1)\times(r+1)$ submatrix of $A$ has a column of zeros, and so $A \in \mathrm{H}_n^{(0)}(r,F)$. $\square$

The following result is an analogue of (11) for $\mathrm{H}_n^{(k)}(F)$ where $k \ge 1$.

**Lemma 5.3.** *Let $k \in \{1,\ldots,n-1\}$ and $A = (a_{i+j-1}) \in \mathrm{H}_n(F)$ be such that $A_k$ is nonsingular. Suppose $\mathbf{x} = (x_1,\ldots,x_k) \in F^k$ is the unique solution of the system $A_k\mathbf{x}^T = (a_{k+1},\ldots,a_{2k})^T$, i.e., for $t = 1,\ldots,k$, the following relation holds:*

$$a_{k+t} = x_1 a_t + \cdots + x_k a_{t+k-1}. \tag{13}$$

*Then*

$$A \in \mathrm{H}_n^{(k)}(F) \Longleftrightarrow \text{ the relation (13) holds for } t = 1,\ldots,n. \tag{14}$$

*Proof.* Suppose $A \in \mathrm{H}_n^{(k)}(F)$. We will use induction on $t$ to show that (13) holds for $t = 1,\ldots,n$. The case when $1 \le t \le k$ is known by the hypothesis. So let us assume that $t \ge k+1$ and that (13) holds for all values of $t$ smaller than given one. Consider the $t \times t$ matrix $A_t$ and successively make the following $t-k$ elementary column transformations:

$$C_t - (x_1 C_{t-k} + \cdots + x_k C_{t-1}),\ \ldots,\ C_{k+1} - (x_1 C_1 + \cdots + x_k C_k)$$

where $C_j$ indicates the $j^{\text{th}}$ column. This transforms $A_t$ to the $t \times t$ matrix

$$A' = \left(\begin{array}{ccc|ccc} a_1 & \cdots & a_k & h_1 & \cdots & h_{t-k} \\ \vdots & \iddots & \vdots & \vdots & & \vdots \\ a_k & \cdots & a_{2k-1} & h_k & \cdots & h_{t-1} \\ \hline a_{k+1} & \cdots & a_{2k} & h_{k+1} & \cdots & h_t \\ \vdots & & \vdots & \vdots & \iddots & \vdots \\ a_t & \cdots & a_{k+t-1} & h_t & \cdots & h_{2t-k-1} \end{array}\right),$$

where $h_m = a_{k+m} - (x_1 a_m + \cdots + x_k a_{m+k-1})$ for $m = 1,\ldots 2t-k-1$. By induction hypothesis, $h_m = 0$ for $m = 1,\ldots,t-1$, and therefore

$$\det(A_t) = \det(A') = (-1)^{(t-k)(t-k+1)/2}\det(A_k) h_t^{t-k}.$$

Since $\det(A_t) = 0$ and $\det(A_k) \neq 0$, it follows that $h_t = 0$, i.e., the relation (13) holds for the given value of $t$.

Conversely, suppose the relation (13) holds for $t = 1, \dots, n$. Then we can write $\mathbf{v}_{k+1} = x_1\mathbf{v}_1 + \cdots + x_k\mathbf{v}_k$, where $\mathbf{v}_j$ denotes the $j^{\text{th}}$ column vector of $A$. In particular, $\operatorname{rank}(A_{k+1}) \leq k$, which implies that $A \in \mathrm{H}_n^{(k)}(F)$. □

Let us pause to observe that the formula (2) for the number of nonsingular Hankel matrices can already be derived as a consequence of the above results.

**Corollary 5.4.** *$|\mathrm{H}_n^{(0)}(\mathbb{F}_q)| = q^{n-1}$ and $\left|\mathrm{H}_n^{(k)}(\mathbb{F}_q)\right| = q^{n+k-2}(q-1)$ for $1 \leq k \leq n$. In particular, $|\mathrm{HGL}_n(\mathbb{F}_q)| = q^{2n-2}(q-1)$.*

*Proof.* Induct on $n$. If $n = 1$, then $k$ is 0 or 1, and the desired formulae are obvious. Suppose $n > 1$ and the result holds for positive values of $n$ smaller than the given one. By Lemma 5.2, $|\mathrm{H}_n^{(0)}(\mathbb{F}_q)| = q^{n-1}$. Now suppose $1 \leq k < n$. Then by Lemma 5.3, we see that the map $A = (a_{i+j-1}) \mapsto (A_k,\ a_{2k}, a_{n+k+1}, \dots, a_{2n-1})$ gives a bijection of $\mathrm{H}_n^{(k)}(F)$ onto $\mathrm{H}_k^{(k)}(F) \times F^{n-k}$. Hence using the induction hypothesis, $\left|\mathrm{H}_n^{(k)}(\mathbb{F}_q)\right| = q^{2k-2}(q-1)q^{n-k} = q^{n+k-2}(q-1)$. Finally, in view of (10), the induction hypothesis, and an easy evaluation of a telescopic sum, we conclude that $|\mathrm{HGL}_n(\mathbb{F}_q)| = \left|\mathrm{H}_n^{(n)}(\mathbb{F}_q)\right| = \left|\mathrm{H}_n(\mathbb{F}_q)\right| - \sum_{k=0}^{n-1}\left|\mathrm{H}_n^{(k)}(\mathbb{F}_q)\right| = q^{2n-1} - q^{2n-2}$. □

If a Hankel matrix in $\mathrm{H}_n^{(k)}(F)$ satisfies a rank condition, the validity of (13) can be pushed a little further. More precisely, one has the following analogue of (12).

**Lemma 5.5.** *Let $k, r$ be integers with $1 \leq k \leq r < n$ and $A = (a_{i+j-1}) \in \mathrm{H}_n(F)$ be such that $A_k$ is nonsingular. Suppose $\mathbf{x} = (x_1, \dots, x_k) \in F^k$ is the unique solution of the system $A_k\mathbf{x}^T = (a_{k+1}, \dots, a_{2k})^T$. Then*

$$A \in \mathrm{H}_n^{(k)}(r, F) \iff \text{the relation (13) holds for } t = 1, \dots, 2n-r-1. \tag{15}$$

*Proof.* Suppose $A \in \mathrm{H}_n^{(k)}(r, F)$. Again, we use induction on $t$. By Lemma 5.3, the relation (13) holds if $1 \leq t \leq n$. Assume that $n+1 \leq t \leq 2n-r-1$ and that (13) holds for all values of $t$ smaller than the given one. Define $\mathbf{x}^{(0)}, \mathbf{x}^{(1)}, \dots, \mathbf{x}^{(t-1)}$ in $F^k$ recursively as follows. First, $\mathbf{x}^{(0)} := \mathbf{x} = (x_1, \dots, x_k)$. Next, if $\ell \geq 1$ and if $\mathbf{x}^{(\ell-1)} = \left(x_1^{(\ell-1)}, \dots, x_k^{(\ell-1)}\right)$ is known, then we let $x_0^{(\ell-1)} := 0$ and let $\mathbf{x}^{(\ell)} = \left(x_1^{(\ell)}, \dots, x_k^{(\ell)}\right) \in F^k$ be given by

$$x_s^{(\ell)} = x_s x_k^{(\ell-1)} + x_{s-1}^{(\ell-1)} \quad \text{for } s = 1, \dots, k.$$

Observe that for $1 \leq \ell < t$ and $1 \leq m < t$, we have

$$\sum_{s=1}^{k} x_s^{(\ell)} a_{m+s-1} = x_k^{(\ell-1)} \sum_{s=1}^{k} x_s a_{m+s-1} + \sum_{s=1}^{k-1} x_s^{(\ell-1)} a_{m+s} = \sum_{s=1}^{k} x_s^{(\ell-1)} a_{m+s}, \tag{16}$$

where the last equality follows from (13) with $t$ replaced by $m$. Successive application of (16) shows that

$$\sum_{s=1}^{k} x_s^{(\ell)} a_{m+s-1} = \sum_{s=1}^{k} x_s a_{m+s+\ell-1} \quad \text{for } 0 \leq \ell < t \text{ and } 1 \leq m \leq t-\ell. \tag{17}$$

Now consider the $(2n-t) \times (2n-t)$ principal submatrix $B$ of $A$ given by

$$B := A[1, 2, \dots, k, t+k-n+1, \dots, n-1, n | 1, 2, \dots, k, t+k-n+1, \dots, n-1, n]$$

and make the following $2n-t-k$ elementary column transformations:

$$C_{2n-t}-\sum_{s=1}^{k} x_s^{(n-k-1)}C_s,\ C_{2n-t-1}-\sum_{s=1}^{k} x_s^{(n-k-2)}C_s,\dots,\ C_{k+1}-\sum_{s=1}^{k} x_s^{(t-n)}C_s,$$

where $C_j$ indicates the $j^{\text{th}}$ column. This transforms $B$ to the $(2n-t)\times(2n-t)$ matrix

$$B'=\left(\begin{array}{ccc|ccc} a_1 & \cdots & a_k & u_{1,1} & \cdots & u_{1,2n-t-k}\\ \vdots & ⋰ & \vdots & \vdots & & \vdots\\ a_k & \cdots & a_{2k-1} & u_{k,1} & \cdots & u_{k,2n-t-k}\\ \hline a_{t+k-n+1} & \cdots & a_{t+2k-1} & v_{1,1} & \cdots & v_{1,2n-t-k}\\ \vdots & & \vdots & \vdots & ⋰ & \vdots\\ a_n & \cdots & a_{n+k-1} & v_{2n-t-k,1} & \cdots & v_{2n-t-k,2n-t-k}\end{array}\right),$$

for some $u_{i,j},\ v_{i,j}\in F$. In fact, for $1\le i\le k$ and $1\le j\le 2n-t-k$,

$$\begin{aligned} u_{i,j}&=a_{i+t+k-n+j-1}-\sum_{s=1}^{k} x_s^{(t-n+j-1)}a_{i+s-1}\\ &=a_{i+j+t-n-1+k}-\sum_{s=1}^{k} x_s a_{i+j+t-n-1+s-1}=0,\end{aligned}$$

where the penultimate equality follows from (17) and the last equality follows from (13) since $t\ge n+1$. Moreover, for $1\le i,j\le 2n-t-k$,

$$v_{i,j}=a_{2t+2k-2n+i+j-1}-\sum_{s=1}^{k} x_s^{(t-n+j-1)}a_{t+k-n+i+s-1};$$

also, since $t\ge n+1$, using (17), we have

$$(18)\quad v_{i,j}=a_{2t+2k-2n+i+j-1}-\sum_{s=1}^{k} x_s a_{2t+k-2n+i+j+s-2}\quad \text{if } i+j\le 2n-t-k+1.$$

In particular, $v_{i,j}$ depends only on $i+j$ whenever $i+j\le 2n-t-k+1$. Furthermore, if $i+j\le 2n-t-k$, then from (13) we deduce that $v_{i,j}=0$ . Consequently, upon letting $v=v_{1,2n-t-k}=\cdots=v_{2n-t-k,1}$, we obtain

$$\det(B)=\det(B')=(-1)^{(2n-t-k)(2n-t-k+1)/2}\det(A_k)v^{2n-t-k}.$$

But since $A\in \mathrm{H}_n^{(k)}(r,F)$ and $2n-t\ge r+1$, we have $\det(A_k)\ne 0$ and $\det(B)=0$. Hence $v=0$, and from (18), we conclude that (13) holds for the given value of $t$.

Conversely, suppose the relation (13) holds for $t=1,\dots,2n-r-1$. Then we can write $\mathbf{v}_j=x_1\mathbf{v}_{j-k}+\cdots+x_k\mathbf{v}_{j-1}$ for $j=k+1,\dots,k+n-r$, where $\mathbf{v}_j$ denotes the $j^{\text{th}}$ column vector of $A$. Hence the column space of $A$ is spanned by $\mathbf{v}_1,\dots,\mathbf{v}_k,\mathbf{v}_{k+n-r+1},\dots,\mathbf{v}_n$. In particular, $\mathrm{rank}(A)\le k+n-(k+n-r+1)+1=r$. This together with Lemma 5.3 shows that $A\in\mathrm{H}_n^{(k)}(r,F)$. □

**Corollary 5.6.** $|\mathrm{H}_n^{(0)}(r,\mathbb{F}_q)|=q^r$ *for* $0\le r<n$ *and* $\left|\mathrm{H}_n^{(k)}(r,\mathbb{F}_q)\right|=q^{r+k-1}(q-1)$ *for* $1\le k\le r<n$. *Consequently,* $|\mathrm{H}_n(r,\mathbb{F}_q)|=q^{2r}$ *for* $0\le r<n$.

*Proof.* The first assertion follows from Lemma 5.2. Now suppose $1\le k\le r<n$. By Lemma 5.5, we see that the map $A=(a_{i+j-1})\mapsto(A_k,\ a_{2k},a_{2n-r+k},\dots,a_{2n-1})$ gives a bijection of $\mathrm{H}_n^{(k)}(r,F)$ onto $\mathrm{HGL}_k(F)\times F^{r-k+1}$. Hence by Corollary 5.4, $\left|\mathrm{H}_n^{(k)}(\mathbb{F}_q)\right|=q^{2k-2}(q-1)q^{r-k+1}=q^{r+k-1}(q-1)$. Finally, $|\mathrm{H}_n(r,\mathbb{F}_q)|=q^{2r}$ is

obvious when $r = 0$, whereas if $1 \le r < n$, then using (10) and an easy evaluation of a telescopic sum, we conclude that $\left|\mathrm{H}_n(r, \mathbb{F}_q)\right| = \sum_{k=0}^{r} \left|\mathrm{H}_n^{(k)}(r, \mathbb{F}_q)\right| = q^{2r}$. □

We are now ready to prove the main result of this section.

*Proof of Theorem 5.1:* The case $r = 0$ is trivial and for $r = n$, Corollary 5.4 applies. Finally, if $1 \le r < n$, then $N(n, r; q) = |\mathrm{H}_n(r, \mathbb{F}_q)| - |\mathrm{H}_n(r-1, \mathbb{F}_q)| = q^{2r} - q^{2r-2}$, thanks to Corollary 5.6. □

A noteworthy consequence of Theorem 5.1 is that for a fixed positive integer $r$, the number of $n \times n$ Hankel matrices of rank $r$ remains constant for every $n \ge r+1$.

## Acknowledgments

We are grateful to Bharath Sethuraman for his help in bringing together the two sets of authors from two different continents. We also thank an anonymous referee for bringing [9, §4.6] and [4] to our attention.

## References

[1] A.T. Benjamin and C.D. Bennett, *The probability of relatively prime polynomials*, Math. Mag. **80** (2007), 196-202.

[2] S. Corteel, C. Savage, H. Wilf, and D. Zeilberger, *A Pentagonal Number Sieve*, J. Combin. Theory Ser. A **82** (1998), 186-192.

[3] D. E. Daykin, *Distribution of bordered persymmetric matrices in a finite field*, J. Reine Angew. Math. **203** (1960), 47–54.

[4] Z. Gao and D. Panario, *Degree distribution of the greatest common divisor of polynomials over* $\mathbb{F}_q$, Random Structures Algorithms **29** (2006), 26–37.

[5] U. Helmke and P. A. Fuhrmann, *Bezoutians*, Linear Algebra Appl. **122/123/124** (1989), 1039–1097.

[6] X. Hou and G.L. Mullen, *Number of irreducible polynomials and pairs of relatively prime polynomials in several variables over finite fields*, Finite Fields Appl. **15** (2009), 304–331.

[7] S. R. Ghorpade and S. Ram, *Block companion Singer cycles, primitive recursive vector sequences, and coprime polynomial pairs over finite fields*, preprint, 2010.

[8] E. Kaltofen and A. Lobo, *On rank properties of Toeplitz matrices over finite fields*, pp. 241–249, Proc. 1996 Internat. Symp. Symbolic Algebraic Comput. (*ISSAC '96*), ACM Press, New York, 1996.

[9] D. E. Knuth, *The Art of Computer Programming*, Vol. 2, *Seminumerical Algorithms*, First, Second, and Third edition, Addison Wesley, Reading, MA, 1969, 1981, and 1997.

[10] K. Ma and J. von zur Gathen, *Analysis of euclidean algorithms for polynomials over finite fields*, J. Symbolic Computation **9** (2003), 429–455.

[11] G. H. Norton, *Precise analysis of the right- and left-shift greatest common divisor algorithms for* $GF(q)[x]$, SIAM J. Comput. **18** (1989), 605–624.

[12] A. Reifegerste, *On an involution concerning pairs of polynomials in* $\mathbb{F}_2$, J. Combin. Theory Ser. A **90** (2000), 216-220.

Department of Mathematics, University of British Columbia,
Vancouver, BC V6T 1Z2, Canada.
*E-mail address*: marioga@math.ubc.ca

Department of Mathematics, Indian Institute of Technology Bombay,
Powai, Mumbai 400076, India.
*E-mail address*: srg@math.iitb.ac.in

Department of Mathematics, Indian Institute of Technology Bombay,
Powai, Mumbai 400076, India.
*E-mail address*: samrithram@gmail.com