Hindawi Publishing Corporation
Algebra
Volume 2014, Article ID 970157, 7 pages
http://dx.doi.org/10.1155/2014/970157

Research Article

On Determinantal Varieties of Hankel Matrices

Edoardo Ballico[1] and Michele Elia[2]

[1] *University of Trento, 38123 Povo, Trento, Italy*
[2] *Polytechnic of Turin, 10129 Torino, Italy*

Correspondence should be addressed to Michele Elia; michele.elia7@gmail.com

Received 23 January 2014; Accepted 9 April 2014; Published 28 April 2014

Academic Editor: Sorin Dascalescu

Let $\mathfrak{H}$ be a class of $n \times n$ Hankel matrices $\mathbf{H}_A$ whose entries, depending on a given matrix $\mathbf{A}$, are linear forms in n variables with coefficients in a finite field $\mathbb{F}_q$. For every matrix in $\mathfrak{H}$, it is shown that the varieties specified by the leading minors of orders from 1 to $n-1$ have the same number q^{n-1} of points in $\mathbb{F}_q^n$. Further properties are derived, which show that sets of varieties, tied to a given Hankel matrix, resemble a set of hyperplanes as regards the number of points of their intersections.

1. Introduction

The representation of hypersurfaces of small degree as determinants is a classical subject. For instance, Hesse [1] discussed the representation of the plane quartic by symmetric determinants, and many different problems have been tackled over the years; see, for example, [2, 3]. An important question, when hypersurfaces are defined over finite fields, is the computation of the number of points. In general this is very difficult, for example, [4], and most frequently only bounds are given. This paper considers hypersurfaces over finite fields, which are defined by determinants of Hankel matrices whose entries are linear forms in the variables. These Hankel matrices are encountered in the proof of certain properties of finite state automata whose state change is governed by tridiagonal matrices [5, 6]. They also occur in the study of some decoding algorithms for error-correcting codes [7, 8].

It is remarkable that, for these determinantal varieties, the exact number of points can in many instances be explicitly found, in terms of the size of the field and the number of variables.

Let $p(z) = z^n + a_1 z^{n-1} + a_2 z^{n-2} + \cdots + a_{n-1} z + a_n$ be an irreducible polynomial of degree n over $\mathbb{F}_q$ with root $\alpha \in \mathbb{F}_{q^n}$, which is thus an eigenvalue of the companion matrix $\mathbf{A}$ which is assumed to have the coefficients of $p(z)$ in the last column, all 1s in the first subdiagonal, and the remaining entries are 0s [9].

The definition of Hankel matrices that we are dealing with uses the Krylov matrices

$$\begin{aligned} \mathbf{K}(\mathbf{A}, \mathbf{x}) &= \left(\mathbf{x}, \mathbf{A}\mathbf{x}, \mathbf{A}^2\mathbf{x}, \ldots, \mathbf{A}^{n-1}\mathbf{x}\right), \\ \mathbf{K}\left(\mathbf{A}^T, \mathbf{y}^T\right) &= \left(\mathbf{y}^T, \mathbf{A}^T\mathbf{y}^T, \left(\mathbf{A}^T\right)^2\mathbf{y}^T, \ldots, \left(\mathbf{A}^T\right)^{n-1}\mathbf{y}^T\right), \end{aligned} \tag{1}$$

where $\mathbf{y} = (y_1, \ldots, y_n)$ is a row vector of n independent variables and $\mathbf{x}^T = (x_1, \ldots, x_n)$ is a column vector of n independent variables. Every Krylov matrix is nonsingular unless $\mathbf{x}$ and $\mathbf{y}$ are all-zero vectors, as will be proved later.

Definition 1. The class $\mathfrak{H}$ consists of $n \times n$ matrices defined as

$$\mathbf{H}_A = \mathbf{K}\left(\mathbf{A}^T, \mathbf{y}^T\right)^T \mathbf{K}(\mathbf{A}, \mathbf{x}). \tag{2}$$

These are Hankel matrices, because the entries

$$\left(\mathbf{H}_A\right)_{ij} = \mathbf{y}\mathbf{A}^i\mathbf{A}^j\mathbf{x} = \mathbf{y}\mathbf{A}^{i+j}\mathbf{x} \tag{3}$$

are clearly the same whenever the index sum $i + j = h$ is constant. When the vector $\mathbf{y}$ is a fixed element $\mathbf{y}_o$ of $\mathbb{F}_q^n$, the corresponding subclass of $\mathfrak{H}$ is denoted by $\mathfrak{H}(\mathbf{y}_o)$.

Given a polynomial f in the ring $\mathbb{F}_q[x_1,\ldots,x_n]$, the variety $\mathscr{V}(f)$ is defined as the set of points in the affine space $\mathbb{F}_q^n$ that annihilate f; that is,

$$\mathscr{V}(f)=\left\{(a_1,a_2,\ldots,a_n)\in\mathbb{F}_p^n \mid f(a_1,\ldots,a_n)=0\right\}\subseteq\mathbb{F}_p^n. \tag{4}$$

More generally, given s polynomials $f_1,\ldots,f_s \in \mathbb{F}_p[x_1,\ldots,x_n]$ the variety $\mathscr{V}(f_1,\ldots,f_s)$ is the set of solutions of the system

$$f_1=0,\ldots,f_s=0. \tag{5}$$

Note that $\mathscr{V}(f_1,\ldots,f_s)=\bigcap_{i=1}^{s}\mathscr{V}(f_i)$ is the intersection and $\mathscr{V}(f_1f_2,\ldots,f_s)=\bigcup_{i=1}^{s}\mathscr{V}(f_i)$ is the union of the varieties $\mathscr{V}(f_1),\ldots,\mathscr{V}(f_s)$.

The entries in $\mathbf{H}_A$ are bilinear forms of the entries in $\mathbf{y}$ and $\mathbf{x}$. Let $D_j(x_1,\ldots,x_n)$ denote the leading minor of order j of a given Hankel matrix $\mathbf{H}_A$ obtained fixing $\mathbf{y}=(b_1,\ldots,b_n)\in\mathbb{F}_q^n$, and define the determinantal varieties as $\mathscr{V}(D_j(x_1,\ldots,x_n)):=\{(a_1,\ldots,a_n)\in\mathbb{F}_q^n : D_j(a_1,\ldots,a_n)=0\}$. Then, we prove that every polynomial $D_j(x_1,\ldots,x_n)$ is irreducible over $\overline{\mathbb{F}}_q$ (Proposition 10), and obtain the following general result.

Theorem 2. *We have* $|\mathscr{V}(D_j(x_1,\ldots,x_n))|=q^{n-1}$ *if* $j=1,\ldots,n-1$ *and* $|\mathscr{V}(D_n(x_1,\ldots x_n))|=1$.

While proving this theorem, the cardinality of certain subsets $S(i,j,n)\subset\mathbb{F}_q^n$ is also computed. The sets $S(i,j,n)$ are the zero-loci of all $D_h(x_1,\ldots,x_n)$'s with $i\le h\le j$ (Theorem 18). That is, every $S(i,j,n)$ is specified by $j+1-i$ equations of degree higher than 1; nevertheless its cardinality $q^{n+i-1-j}$ is the same as in the case of the intersections in $\mathbb{F}_q^n$ of $j+1-i$ distinct hyperplanes. In the next section, preliminary notions, properties, and useful lemmas are collected, while the main results are proved in Section 3.

2. Preliminaries

It is direct to check that $\mathbf{v}_\alpha=(1,\alpha,\ldots,\alpha^{n-1})$ is a row eigenvector of $\mathbf{A}$, associated with the eigenvalue α; that is, $\mathbf{v}_\alpha\mathbf{A}=\alpha\mathbf{v}_\alpha$.

Let $\sigma:\overline{\mathbb{F}}_q\to\overline{\mathbb{F}}_q$ denote the q-Frobenius; that is, set $\sigma(x):=x^q$ for all x. The action of σ is extended to vectors and matrices component-wise. Since $\sigma(\mathbf{A})=\mathbf{A}$, because the entries of this matrix are in $\mathbb{F}_q$, we have

$$\sigma(\mathbf{v}_\alpha\mathbf{A})=\sigma(\alpha\mathbf{v}_\alpha)\Longrightarrow\sigma(\mathbf{v}_\alpha)\mathbf{A}=\sigma(\alpha)\sigma(\mathbf{v}_\alpha); \tag{6}$$

that is, all eigenvectors of $\mathbf{A}$ are conjugate vectors under σ. Hence the matrix

$$\mathbf{B}=\begin{bmatrix}\mathbf{v}_\alpha\\ \sigma(\mathbf{v}_\alpha)\\ \sigma^2(\mathbf{v}_\alpha)\\ \vdots\\ \sigma^{n-1}(\mathbf{v}_\alpha)\end{bmatrix} \tag{7}$$

reduces $\mathbf{A}$ to diagonal form over $\mathbb{F}_{q^n}$; that is,

$$\mathbf{D}=\mathbf{BAB}^{-1}=\operatorname{diag}\left(\alpha,\ldots,\sigma^{n-1}(\alpha)\right), \tag{8}$$

$\mathbf{D}$ being the diagonal matrix of the eigenvalues of $\mathbf{A}$.

Observe that, writing (8) as $\mathbf{AB}^{-1}=\mathbf{B}^{-1}\mathbf{D}$, the columns of $\mathbf{B}^{-1}$ are column eigenvectors of $\mathbf{A}$. Thus there is a column vector $\mathbf{u}$ that allows us to write $\mathbf{B}^{-1}$ in the form

$$\mathbf{B}^{-1}=\left(\mathbf{u}_\alpha,\sigma(\mathbf{u}_\alpha),\ldots,\sigma^{n-1}(\mathbf{u}_\alpha)\right). \tag{9}$$

The following lemma is useful to show that every matrix similar to $\mathbf{A}$ gives the same class $\mathfrak{H}$. Let $\mathrm{GL}(n,\mathbb{F}_q)$ denote the general linear group of $n\times n$ nonsingular matrices with entries in $\mathbb{F}_q$.

Lemma 3. *Matrices of* $GL(n,\mathbb{F}_q)$ *that have the same characteristic irreducible polynomial* $p(z)$ *are* $\mathbb{F}_q$*-similar.*

Proof. Let α be a root of $p(z)$. To prove the lemma it is sufficient to show that any two matrices $\mathbf{A}$ and $\mathbf{E}$ of $\mathrm{GL}(n,\mathbb{F}_q)$, having the same characteristic polynomial $p(z)$, are similar. The previous arguments indicate that there are two $\mathbb{F}_{q^n}$-matrices $\mathbf{B}$ and $\mathbf{S}$ of form (7) such that

$$\mathbf{BAB}^{-1}=\mathbf{D},\qquad \mathbf{SES}^{-1}=\mathbf{D}. \tag{10}$$

Multiplying the first equation by $\mathbf{S}^{-1}$ on the left, and by $\mathbf{S}$ on the right, we have $(\mathbf{S}^{-1}\mathbf{B})\mathbf{A}(\mathbf{S}^{-1}\mathbf{B})^{-1}=\mathbf{E}$. Thus, the lemma is proved by showing that $\mathbf{S}^{-1}\mathbf{B}$ is a $\mathbb{F}_q$-matrix. Since we may always assume that

$$\mathbf{S}^{-1}=\left(\mathbf{s}_\alpha,\sigma(\mathbf{s}_\alpha),\ldots,\sigma^{n-1}(\mathbf{s}_\alpha)\right), \tag{11}$$

where $\mathbf{s}_\alpha$ is a convenient column eigenvector of $\mathbf{E}$ and $\mathbf{B}$ is of form (7), we have

$$\begin{aligned}\mathbf{S}^{-1}\mathbf{B}&=\mathbf{s}_\alpha\mathbf{v}_\alpha+\sigma(\mathbf{s}_\alpha)\sigma(\mathbf{v}_\alpha)+\cdots+\sigma^{n-1}(\mathbf{s}_\alpha)\sigma^{n-1}(\mathbf{v}_\alpha)\\&=\mathbf{s}_\alpha\mathbf{v}_\alpha+\sigma(\mathbf{s}_\alpha\mathbf{v}_\alpha)+\cdots+\sigma^{n-1}(\mathbf{s}_\alpha\mathbf{v}_\alpha),\end{aligned} \tag{12}$$

which is patently invariant under the action of the automorphism σ; thus $\mathbf{S}^{-1}\mathbf{B}$ is a $\mathbb{F}_q$-matrix. □

Corollary 4. $\mathbf{A}$ *and* $\mathbf{A}^T$ *are* $\mathbb{F}_q$*-similar.*

2.1. B and z. The equation $\mathbf{w}=\mathbf{yB}^{-1}$ defines an $\mathbb{F}_q$-linear mapping ψ from $\mathbb{F}_q^n$ into $\mathbb{F}_{q^n}^n$. Taking the vector $\mathbf{y}$ to be the element of $\mathbb{F}_{q^n}$

$$\mathbf{y}_o=\left(\mathrm{Tr}(1),\mathrm{Tr}(\alpha),\mathrm{Tr}\left(\alpha^2\right),\ldots,\mathrm{Tr}\left(\alpha^{n-1}\right)\right)\in\mathbb{F}_q^n, \tag{13}$$

we have $\mathbf{w}_o=(1,1,\ldots,1)=\psi(\mathbf{y}_o)$. The image $\mathrm{Im}(\psi)$ is the $\mathbb{F}_{q^n}$-linear span of $(1,1\ldots,1)$; hence it is a one-dimensional $\mathbb{F}_{q^n}$-linear subspace of $\mathbb{F}_{q^n}^n$.

Equation (8) implies that $\mathbf{BA}=\mathbf{DB}$; then, introducing the vector

$$\mathbf{z}^T=\mathbf{B}(x_1,x_2,\ldots,x_n)^T=(z_1,z_2,\ldots,z_n), \tag{14}$$

it is immediate to see that $z_i = \sigma^{i-1}(z_1)$ for every i, whenever $\mathbf{x}^T \in \mathbb{F}_q^n$. The linear forms $\mathbf{y}_o\mathbf{A}^j\mathbf{x}^T$ are transformed into linear forms $\mathbf{w}_o\mathbf{D}^j\mathbf{z}^T$, and matrix $\mathbf{H}_A$ can be written as

$$\mathbf{H}_A = \begin{bmatrix} \mathbf{w}_o^T\mathbf{z} & \mathbf{w}_o^T\mathbf{D}\mathbf{z} & \mathbf{w}_o^T\mathbf{D}^2\mathbf{z} & \cdots & \mathbf{w}_o^T\mathbf{D}^{n-1}\mathbf{z} \\ \mathbf{w}_o^T\mathbf{D}\mathbf{z} & \mathbf{w}_o^T\mathbf{D}^2\mathbf{z} & \mathbf{w}_o^T\mathbf{D}^3\mathbf{z} & \cdots & \mathbf{w}_o^T\mathbf{D}^n\mathbf{z} \\ \mathbf{w}_o^T\mathbf{D}^2\mathbf{z} & \mathbf{w}_o^T\mathbf{D}^3\mathbf{z} & \mathbf{w}_o^T\mathbf{D}^4\mathbf{z} & \cdots & \mathbf{w}_o^T\mathbf{D}^{n+1}\mathbf{z} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ \mathbf{w}_o^T\mathbf{D}^{n-1}\mathbf{z} & \mathbf{w}_o^T\mathbf{D}^n\mathbf{z} & & \cdots & \mathbf{w}_o^T\mathbf{D}^{2n-2}\mathbf{z} \end{bmatrix}. \quad (15)$$

Definition 5. Let $D_j(x_1, \ldots, x_n)$ denote the leading minor of order j of a given Hankel matrix $\mathbf{H}_A$ in $\mathfrak{H}$. When there is no ambiguity surrounding the variables, this minor is in brief denoted by $D_j(1)$. The determinant of $\mathbf{H}_A$ is $D_n(x_1, \ldots, x_n)$, or $D_n(1)$.

Lemma 6. *Let* $\mathbf{x}$ *be a vector of* n *variables, and let* $\mathbf{y}$ *be a constant vector in* $\mathbb{F}_q^n$*; then we have the following.*

(1) *The determinant* $D_n(x_1, \ldots, x_n)$ *of* $\mathbf{H}_A$ *is zero if and only if all variables are set equal to zero.*

(2) *The matrix* $\mathbf{H}_A$ *is a linear combination of* n *nonsingular matrices, the coefficients of the linear combination being the entries of* $\mathbf{x}$*.*

(3) *Any linear combination of the rows of* $\mathbf{H}_A$ *is a set of* n *linearly independent linear forms.*

Proof. $D_n(x_1, \ldots, x_n)$ is not zero, because it is the product of two determinants that are different from zero

$$\begin{aligned} D_n(x_1, \ldots, x_n) &= \det\left(\mathbf{K}\left(\mathbf{A}^T, \mathbf{y}^T\right)^T \mathbf{K}(\mathbf{A}, \mathbf{x})\right) \\ &= \det\left(\mathbf{K}\left(\mathbf{A}^T, \mathbf{y}^T\right)^T\right) \det(\mathbf{K}(\mathbf{A}, \mathbf{x})). \end{aligned} \quad (16)$$

In particular, $\det(\mathbf{K}(\mathbf{A}, \mathbf{x})) = 0$ if and only if $\mathbf{x}$ is the all-zero vector; the same observation holds for $\mathbf{y}$. This proves point (1).

Point (2) is proved by writing

$$\mathbf{K}\left(\mathbf{A}^T, \mathbf{y}^T\right)^T \mathbf{K}(\mathbf{A}, \mathbf{x}) = \sum_{i=1}^{n} x_i \mathbf{M}_i, \quad (17)$$

where the matrices $\mathbf{M}_i$ have constant entries that depend on $\mathbf{y}$, and taking $x_j = 1$ and $x_i = 0$ for every $i \neq j$, that is, $\mathbf{x} = \mathbf{e}_j$. When $\mathbf{x} = \mathbf{e}_j$, we have

$$\begin{aligned} D_n(0, \ldots, 1, \ldots, 0) &= \det\left(\mathbf{K}\left(\mathbf{A}^T, \mathbf{y}^T\right)^T\right) \det\left(\mathbf{K}\left(\mathbf{A}, \mathbf{e}_j\right)\right) \\ &= \det\left(\mathbf{M}_j\right). \end{aligned} \quad (18)$$

This implies that $\det(\mathbf{M}_j) \neq 0$.

Point (3) is proved by noting that $D_n(x_1, \ldots, x_n) = 0$ has only one solution, namely, $x_1 = \cdots = x_n = 0$, and $D_n(x_1, \ldots, x_n) = 0$ identifies linear combinations of the rows of $\mathbf{H}_A$. It follows that every linear combination of the rows should have only the all-zero solution; therefore the n entries in every row must be linearly independent, by a theorem of Rouché-Capelli. □

By correspondence (14), every $D_j(x_1, x_2, \ldots, x_n)$ is transformed into a polynomial $Q_j(z_1, \ldots, z_n)$ in the variables z_is with the coefficients in $\mathbb{F}_{q^n}$.

2.2. Auxiliary Results. Let $V(a_1, a_2, \ldots, a_j)$ be a Vandermonde determinant of order j identified by the j-tuple $(a_1, a_2, \ldots, a_j)$.

Definition 7. For every triple of integers j, i, and t such that $t \geq 2i - 1 \geq 2j - 1 > 0$, the subset $S(j, i, t)$ of $\mathbb{F}_q^t$ is defined as

$$S(j, i, t) := \left\{(a_1, \ldots, a_t) \in \mathbb{F}_q^t : D_h(a_1, \ldots, a_t) = 0 \quad \forall h \in \{j, \ldots, i\}\right\}. \quad (19)$$

Definition 8. The set $\mathfrak{C}_j^n$ is defined to be the collection of $\binom{n}{j}$ subsets, where each subset consists of the unordered collection of j distinct integers from the set $\{1, 2, \ldots, n\}$.

Every subset $\mathfrak{h}_i = \{h_1, \ldots, h_j\}$ defines a mapping $\tau_i(\ell) = h_\ell$ from the set $\{1, 2, \ldots, j\}$ into $\{1, 2, \ldots, n\}$.

Lemma 9. *Consider a Hankel matrix* $\mathbf{H}_A$*, as defined in* (2) *with* $\mathbf{y} = \mathbf{y}_o \in \mathbb{F}_q^n$*; the leading minors* $D_j(x_1, \ldots, x_n)$*,* $j = 1, \ldots, n$ *are multivariate homogeneous polynomials of degree* j*, which may be written over* $\mathbb{F}_{q^n}$*, in the form*

$$\begin{aligned} &D_j(x_1, \ldots, x_n) \\ &\quad = Q_j(z_1, \ldots, z_n) \\ &\quad = \sum_{\{h_1, h_2, \ldots, h_j\} \in C_j^n} V\left(\sigma^{h_1-1}(\alpha), \ldots, \sigma^{h_j-1}(\alpha)\right)^2 z_{h_2} \cdots z_{h_j}, \end{aligned} \quad (20)$$

where the summation is extended to all combinations of the n *integers* $\{1, 2, \ldots, n\}$*, taking* j *at a time, and the coefficients of the monomials* $z_{h_1} \cdots z_{h_j}$ *are squares of Vandermonde determinants.*

Proof. In matrix (15), the bilinear forms $\mathbf{w}\mathbf{D}^{i+j-2}\mathbf{z}$ have the explicit expression

$$\sum_{h=1}^{n} z_h \sigma^{h-1}\left(\alpha^{i+j-2}\right) = \sum_{h=1}^{n} z_h \sigma^{h-1}\left(\alpha^{i-1}\right) \sigma^{h-1}\left(\alpha^{j-1}\right), \quad (21)$$

where i is the row index and j is the column index. Each column is a linear combination of columns with coefficients z_h such that all columns with the same coefficient z_h are proportional. Matrix (15) can be written as a sum of the form

$$\mathbf{H}_A = \sum_{h=1}^{n} z_h \sigma^{h-1}(\Gamma), \quad (22)$$

where Γ is the $n \times n$ matrix

$$\begin{bmatrix} 1 & \alpha & \cdots & \alpha^{n-1} \\ \alpha & \alpha^2 & \cdots & \alpha^n \\ \vdots & \vdots & \vdots & \vdots \\ \alpha^{n-1} & \alpha^n & \cdots & \alpha^{2n-1} \end{bmatrix}, \tag{23}$$

which has rank 1, since every row is proportional to the first row, and the same holds for the columns. The leading minor $D_j(x_1, \ldots, x_n)$ is computed by writing the determinant as a sum of n^j determinants, which contain a single variable z_k in every column, determinants with repeated variables are 0, because of the previous observation that their corresponding columns are proportional, and in the remaining determinants the corresponding variable is collected from each column.

The coefficient of the monomial $z_{h_1} z_{h_2} \cdots z_{h_j}$ is obtained as follows. Let $u_i = \sigma^{h_i - 1}(\alpha)$. Then the coefficient of $z_{h_1}, \ldots, z_{h_j}$ is equal to

$$\begin{aligned} &\sum_{\tau \in S_j} \begin{vmatrix} 1 & u_{\tau(2)} & \cdots & u_{\tau(j)} \\ u_{\tau(1)} & u_{\tau(2)}^2 & \cdots & u_{\tau(j)}^j \\ \vdots & \vdots & \vdots & \vdots \\ u_{\tau(1)}^{j-1} & u_{\tau(2)}^j & \cdots & u_{\tau(j)}^{2j-1} \end{vmatrix} \\ &\quad = \sum_{\tau \in S_j} \operatorname{sgn}(\tau) \prod_{\ell=1}^{j} u_{\tau(\ell)}^{\ell-1} \begin{vmatrix} 1 & 1 & \cdots & 1 \\ u_1 & u_2^2 & \cdots & u_j^j \\ \vdots & \vdots & \vdots & \vdots \\ u_1^{j-1} & u_2^j & \cdots & u_j^{2j-1} \end{vmatrix}. \end{aligned} \tag{24}$$

Collecting the common factor, the remaining summation is exactly the same determinant; thus we have

$$\begin{vmatrix} 1 & 1 & \cdots & 1 \\ u_1 & u_2^2 & \cdots & u_j^j \\ \vdots & \vdots & \vdots & \vdots \\ u_1^{j-1} & u_2^j & \cdots & u_j^{2j-1} \end{vmatrix}^2 = V\left(\sigma^{h_1-1}(\alpha), \ldots, \sigma^{h_j-1}(\alpha)\right)^2, \tag{25}$$

which gives

$$\begin{aligned} &Q_j(z_1, \ldots, z_n) \\ &\quad = \sum_{\mathfrak{h} \in \mathfrak{C}_j^n} V\left(\sigma^{h_1-1}(\alpha), \ldots, \sigma^{h_j-1}(\alpha)\right)^2 z_{h_1} z_{h_2} \cdots z_{h_j}, \end{aligned} \tag{26}$$

with the summation extended to every subset $\mathfrak{h} = \{h_1, \ldots, h_j\}$ of $\mathfrak{C}_j^n$, and this concludes the proof. □

Proposition 10. *The product $\prod_{i=1}^{n-1} Q_i(z_1, \ldots, z_n)$ is not identically zero over $\mathbb{F}_{q^n}$.*

Furthermore, the leading minors $D_j(x_1, \ldots, x_n)$, $j = 1, \ldots n$, are irreducible degree-j polynomials over $\overline{\mathbb{F}}_q$.

Proof. As a consequence of (26), every $Q_j(z_1, \ldots, z_n)$ is irreducible over $\mathbb{F}_{q^n}$. Further, observing that each variable z_i occurs at degree 1 in any $Q_j(z_1, \ldots, z_n)$, it has maximum degree $n - 1$ in the product polynomial $\mathfrak{D} = \prod_{j=1}^{n-1} Q_j(z_1, \ldots, z_n)$. Therefore $\mathfrak{D}$ is not identically zero in $\mathbb{F}_{q^n}^n$, because $n - 1$ is certainly less than q^n for any q.

To prove the second statement, fix $j \in \{1, \ldots, n-1\}$. In this step it is checked that $g := D_j(x_1, \ldots, x_n) \in \mathbb{F}_q[x_1, \ldots, x_n]$ is irreducible over $\overline{\mathbb{F}}_q$. It is only necessary to use the fact that $g \in \mathbb{F}_q[x_1, \ldots, x_n]$ is a homogeneous polynomial of degree $j < n$ which is irreducible over $\mathbb{F}_{q^n}$. Assume that g is reducible over $\overline{\mathbb{F}}_q$ and call $h \in \overline{\mathbb{F}}_q$ an irreducible factor of minimal degree $x < j$. Let $\mathbb{F}_{q^e}$ be the minimal extension of $\mathbb{F}_q$ in which h is defined. Since g is irreducible, the polynomials $\sigma^i(h)$, $1 \le i < e$, obtained by applying the Frobenius σ^i to h are nonproportional irreducible factors of g. Hence $\deg(g) \ge (e-1)x \ge nx \ge n$, which is a contradiction. □

Remark 11. The determinant $D_n(x_1, \ldots, x_n)$ is found to be

$$D_n(x_1, \ldots, x_n) = \Delta^2 \prod_{u=1}^{n} z_u = p(1)^2 \delta^2 \prod_{u=1}^{n} \left[\sigma^{u-1}(\mathbf{v}_\alpha)\, \mathbf{x}\right], \tag{27}$$

where δ is the discriminant of $p(z)$, and the product involving $\mathbf{x}$ can be seen as a norm in the field $\mathbb{F}_{q^n}$; therefore $D_n(x_1, \ldots, x_n)$ is irreducible over $\mathbb{F}_q$.

Lemma 12. *The variety $\mathcal{V}(D_1(1)) \cap \mathcal{V}(D_2(1)) \cap \cdots \cap \mathcal{V}(D_{n-1}(1))$ has cardinality q over $\mathbb{F}_q$.*

Proof. Equation (17) shows that any $D_j(1)$ is a polynomial of degree j with coefficients in $\mathbb{F}_q$; furthermore, every entry is a linear form with coefficients in $\mathbb{F}_q$. Hence $D_1(1) = 0$ implies $u_1 = 0$; in turn $D_2(1) = 0$ implies $u_2 = 0$, given that $u_1 = 0$ and arguing recursively; finally, $D_{n-1}(1) = 0$ implies $u_{n-1} = 0$, while the variable u_n is free and may assume q values. The conclusion follows. □

Lemma 13. *Let $b_i \neq 0$, $1 \le i \le j$, and assume $n \ge 2j - 1$. Then $|\mathcal{V}(D_1(1) - b_1) \cap \cdots \cap \mathcal{V}(D_j(1) - b_j)| = q^{n-j}$.*

Proof. We use induction on j, the case $j = 1$ being obvious. The inductive assumption in $\mathbb{F}_q^{2j-3}$ gives $|\mathcal{V}(D_1(1) - b_1) \cap \cdots \cap \mathcal{V}(D_{j-1}(1) - b_{j-1})| = q^{j-2}$. Fix $(a_1, \ldots, a_{2j-3}) \in \mathbb{F}_q^{2j-3}$ with $D_i(1) = b_i$ for all $1 \le i \le j-1$. Since $D_{j-1}(a_1, a_2, \ldots, a_{2j-3}) \neq 0$, for all $a_{2j-2}, c \in \mathbb{F}_q$ there is a unique $a_{2j-1} \in \mathbb{F}_q$ such that $D_j(a_1, \ldots, a_{2j-1}) = c$. Take $c = b_j$. This completes the proof. □

3. Main Results

Proposition 14. *The equality $|V(D_j(1))| = |V(D_{n-j}(1))|$ holds for every $1 \le j \le n - 1$.*

Proof. In the proof of Lemma 9, it was shown that

$$D_j(1) = D_j(x_1, \ldots, x_n) = Q_j(z_1, \ldots, z_n), \tag{28}$$

with $z_i = \sum_{j=1}^{n} \sigma^{j-1}(\alpha) x_j$. Further, it was noted in that lemma that $z_i = \sigma^{i-1}(z_1)$ for every i, whenever every $x_j \in \mathbb{F}_q$.

The relation $\mathbf{z} = \mathbf{B}^{-1}\mathbf{x}$ establishes a one-to-one correspondence between $\mathbb{F}_q^n$ and a subspace of dimension 1 of $\mathbb{F}_{q^n}^n$, and further $\mathbf{x} = \mathbf{Bz}$. There thus exists a one-to-one correspondence between the zeros of $D_j(1)$ in $\mathbb{F}_q^n$ and the zeros of $Q_j(z_1, \ldots, z_n)$ in the one-dimensional subspace of $\mathbb{F}_{q^n}^n$, which is the image of $\mathbb{F}_q^n$. Referring to (26), which yields the representation $Q_j(z_1, \ldots, z_n)$ of $D_j(1)$, assuming $z_1 \neq 0$, considering the change of variables

$$z_i = \frac{1}{t_i \prod_{\ell \neq i-1}^{n-1} \left(\sigma^{i-1}(\alpha) - \sigma^{\ell}(\alpha)\right)^2} = \frac{1}{\mathfrak{d}_i\, t_i}, \tag{29}$$

and recalling that the coefficients of the monomials are squares of Vandermonde determinants $V(\sigma^{h_1-1}(\alpha), \sigma^{h_2-1}(\alpha), \ldots, \sigma^{h_j-1}(\alpha))^2$, we obtain

$$Q_j(z_1, \ldots, z_n) = \frac{1}{\delta^2 \prod_{i=1}^{n} t_i} Q_{n-j}(t_1, \ldots, t_n), \tag{30}$$

where δ is the discriminant of the polynomial with root α. The variety $\mathscr{V}(D_j(1))$ is obtained by considering $t_1 = \mathbf{v}(\alpha)\mathbf{x}^T$ and the other variables as $t_i = \sigma^{i-1}(t_1)$, $i = 2, \ldots, n$; thus $\prod t_i = 0$ only when every $t_i = 0$, $\forall i$; further $\delta \neq 0$. Finally, we have the chain of bijections

$$\begin{aligned} \mathbf{x} \longleftrightarrow \mathbf{z}^T = \mathbf{B}^{-1}\mathbf{x}^T \longleftrightarrow z_1 \longleftrightarrow t_1 \\ = \begin{cases} \dfrac{1}{\mathfrak{d}_1\, z_1} & \text{if } z_1 \neq 0 \\ 0 & \text{if } z_1 = 0 \end{cases} \longleftrightarrow \mathbf{y}^T \longleftrightarrow \tilde{\mathbf{x}}^T = \mathbf{B}\mathbf{t}^T. \end{aligned} \tag{31}$$

In conclusion, this equation shows an explicit one-to-one mapping between the zeros $(a_1, \ldots, a_n)$ of $D_j(1)$ and the zeros $(\tilde{a}_1, \ldots, \tilde{a}_n)$ of $D_{n-j}(1)$, which implies $|\mathscr{V}(D_j(1))| = |\mathscr{V}(D_{n-j}(1))|$. □

In the following example, the procedure for obtaining a point of $\mathscr{V}(D_{n-j}(1))$ from a point of $\mathscr{V}(D_j(1))$ is explicitly illustrated.

Example 15. Consider the irreducible polynomial $p_7(z) = z^7 + z^4 + z^3 + z^2 + 1$ of degree $n = 7$ over $\mathbb{F}_3$ with the transpose companion matrix

$$\mathbf{A}_7 = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ -1 & 0 & -1 & -1 & -1 & 0 & 0 \end{bmatrix}. \tag{32}$$

Taking $\mathbf{y} = [1, 0, 0, 0, 0, 0, 0]$, and $\mathbf{x}^T = [x_1, x_2, x_3, x_4, x_5, x_6, x_7]$, the Hankel matrix (17) becomes

$$\mathbf{H}_{A_7} = \begin{bmatrix} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 \\ x_2 & x_3 & x_4 & x_5 & x_6 & x_7 & \xi_8 \\ x_3 & x_4 & x_5 & x_6 & x_7 & \xi_8 & \xi_9 \\ x_4 & x_5 & x_6 & x_7 & \xi_8 & \xi_9 & \xi_{10} \\ x_5 & x_6 & x_7 & \xi_8 & \xi_9 & \xi_{10} & \xi_{11} \\ x_6 & x_7 & \xi_8 & \xi_9 & \xi_{10} & \xi_{11} & \xi_{12} \\ x_7 & \xi_8 & \xi_9 & \xi_{10} & \xi_{11} & \xi_{12} & \xi_{13} \end{bmatrix}, \tag{33}$$

where

$$\begin{aligned} \xi_8 &= -x_1 - x_3 - x_4 - x_5, \\ \xi_9 &= -x_2 - x_4 - x_5 - x_6, \\ \xi_{10} &= -x_3 - x_5 - x_6 - x_7, \\ \xi_{11} &= x_1 + x_3 + x_5 - x_6 - x_7, \\ \xi_{12} &= x_1 + x_2 + x_3 - x_4 + x_5 + x_6 - x_7, \\ \xi_{13} &= x_1 + x_2 - x_3 - x_4 + x_5 + x_6 - x_7. \end{aligned} \tag{34}$$

The forms $D_3(1)$ and $D_4(1)$ of degrees 3 and 4, respectively, are

$$\begin{aligned} D_3(1) &= x_1x_3x_5 - x_1x_4^2 - x_2^2x_5 - x_2x_3x_4 - x_3^3, \\ D_4(1) &= x_1x_3x_5x_7 - x_1x_3x_6^2 - x_1x_4^2x_7 - x_1x_4x_5x_6 - x_1x_5^3 \\ &\quad - x_2^2x_5x_7 + x_2^2x_6^2 - x_2x_4x_3x_7 + x_2x_4^2x_6 + x_2x_5x_3x_6 \\ &\quad - x_2x_4x_5^2 - x_3^3x_7 - x_3^2x_4x_6 + x_3^2x_5^2 + x_4^4. \end{aligned} \tag{35}$$

Given a point $\mathbf{x}^T = [0, 1, -1, -1, 0, 0, 1] \in \mathbb{F}_3^7$ which is a zero of $D_3(1)$, a zero of $D_4(1)$ is obtained as follows.

Compute the vector $\mathbf{z} = \mathbf{B}_7^{-1}\mathbf{x}^T$ whose first component is $z_1 = 1 + \alpha^2 + \alpha^3 + \alpha^6 \in \mathbb{F}_{3^7}^7$, and the remaining entries are obtained as $\sigma^{\ell}(z_1) = 1 + \alpha^{3^{\ell-1}2} + \alpha^{3^{\ell-1}3} + \alpha^{3^{\ell-1}6}$, $\ell = 1, \ldots, 6$; then compute

$$\begin{aligned} \mathfrak{d}^2 &= \prod_{i=1}^{6} \left(\alpha - \alpha^{3^i}\right)^2 = \alpha + \alpha^3 + \alpha^4 - \alpha^5, \\ t_1 &= \frac{1}{z_1 \mathfrak{d}^2} = -1 - \alpha + \alpha^2 + \alpha^4 - \alpha^5, \end{aligned} \tag{36}$$

and construct the vector $\mathbf{t} = [t_1, \sigma(t_1), \ldots, \sigma^6(t_1)] \in \mathbb{F}_{3^7}^7$. Finally, a zero of $D_4(1)$ is obtained as

$$\mathbf{B}_7\mathbf{t}^T = [1, -1, 0, 1, 1, -1, -1]^T \in \mathbb{F}_3^7, \tag{37}$$

where $\mathbf{B}_7$ is the matrix whose columns are the eigenvectors of $\mathbf{A}_7$ in $\mathbb{F}_{3^7}^7$

$$\mathbf{B}_7 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \alpha & \alpha^3 & \alpha^{3^2} & \alpha^{3^3} & \alpha^{3^4} & \alpha^{3^5} & \alpha^{3^6} \\ \alpha^2 & \alpha^{2\cdot 3} & \alpha^{2\cdot 3^2} & \alpha^{2\cdot 3^3} & \alpha^{2\cdot 3^4} & \alpha^{2\cdot 3^5} & \alpha^{2\cdot 3^6} \\ \alpha^3 & \alpha^{3\cdot 3} & \alpha^{3\cdot 3^2} & \alpha^{3\cdot 3^3} & \alpha^{3\cdot 3^4} & \alpha^{3\cdot 3^5} & \alpha^{3\cdot 3^6} \\ \alpha^4 & \alpha^{4\cdot 3} & \alpha^{4\cdot 3^2} & \alpha^{4\cdot 3^3} & \alpha^{4\cdot 3^4} & \alpha^{4\cdot 3^5} & \alpha^{4\cdot 3^6} \\ \alpha^5 & \alpha^{5\cdot 3} & \alpha^{5\cdot 3^2} & \alpha^{5\cdot 3^3} & \alpha^{5\cdot 3^4} & \alpha^{5\cdot 3^5} & \alpha^{5\cdot 3^6} \\ \alpha^6 & \alpha^{6\cdot 3} & \alpha^{6\cdot 3^2} & \alpha^{6\cdot 3^3} & \alpha^{6\cdot 3^4} & \alpha^{6\cdot 3^5} & \alpha^{6\cdot 3^6} \end{bmatrix}. \tag{38}$$

Remark 16. Since the n forms in the first row of (17) are linearly independent, by Lemma 6, a change of variables from $x_1, \ldots, x_n$ to $u_1, \ldots, u_n$ takes a matrix $\mathbf{H}_A$ to the form

$$\mathbf{H}_A = \begin{bmatrix} u_1 & u_2 & u_3 & \cdots & u_n \\ u_2 & u_3 & \cdots & u_n & \ell_1 \\ u_3 & \cdots & u_n & \ell_1 & \ell_2 \\ & \vdots & & & \\ u_n & \ell_1 & \ell_2 & \cdots & \ell_{n-1} \end{bmatrix}, \tag{39}$$

where the n variables u_is are free, and every ℓ_h is a linear form in the u_is.

Fix the integers $k \geq 1$ and $j \geq 1$, and let $D_j(k)$ denote the $j \times j$ determinant of a Hankel matrix with free variable entries u_i, $i = k, \ldots, 2j - 2 + k$

$$\begin{vmatrix} u_k & u_{k+1} & \cdots & u_{k+j-2} & u_{k+j-1} \\ u_{k+1} & u_{k+2} & \cdots & u_{k+j-1} & u_{k+j} \\ & \vdots & \vdots & \vdots & \\ u_{k+j-1} & u_{k+j} & \cdots & u_{k+2j-3} & u_{k+2j-2} \end{vmatrix}. \tag{40}$$

And set $D_0(1) = 1$ by definition.

Proposition 17. *Let m, k be natural integers. Let $\mathbf{H}^{(2k+2m-1)}$ be a $(2k + 2m - 1) \times (2k + 2m - 1)$ Hankel matrix with first row $(u_1, \ldots, u_{2k+2m-1})$. Let $E(k, m)$ be the set of points $(b_1, \ldots, b_{2k+2m-1}) \in \mathbb{F}_q^{2k+2m-1}$ with the same first $2k - 1$ coordinates $b_i = a_i$, $i = 1, \ldots, 2k - 1$ such that the minor $D_k(b_1, \ldots, b_{2k+2m-1}) \neq 0$, and the minors $D_i(b_1, \ldots, b_{2k+2m-1}) = 0$ for all $i \in \{k+1, \ldots, k+m\}$. Then $E(k, m)$ has cardinality q^m.*

Proof. Observe that the first row $(u_1, \ldots, u_{2k+2m-1})$ of the Hankel matrix $\mathbf{H}^{(2k+2m-1)}$ completely specifies the leading $(k+m) \times (k+m)$ Hankel submatrix $\mathbf{H}^{(k+m)}$, and consequently also every minor $D_i(1)$ for $i = 1, \ldots, k + m$.

Let $R_j(u_1, \ldots, u_{2k+2m-1})$ denote the jth row of $\mathbf{H}^{(k+m)}$. Let $A(k + 1, m)$ be the subset of $\mathbb{F}_q^{2m}$ consisting of all $(b_{2k}, \ldots, b_{2k+2m-1}) \in \mathbb{F}_q^{2m}$ such that $R_{k+1}(a_1, \ldots, a_{2k-1}, b_{2k}, \ldots, b_{2k+2m-1})$ is linearly dependent on $R_1(b_1, \ldots, a_{2k-1}, b_{2k}, \ldots, b_{2k+2m-1}), \ldots, R_k(b_1, \ldots, a_{2k-1}, b_{2k}, \ldots, b_{2k+2m-1})$.

The case $m = 1$ is easily settled. Consider the identity

$$\begin{aligned} &D_{k+1}(a_1, \ldots, a_{2k-1}, u_{2k}, u_{2k+1}, \ldots, u_{2k+2m-1}) \\ &\quad = u_{2k+1} D_k(a_1, \ldots, a_{2k-1}, u_{2k}, u_{2k+1}, \ldots, u_{2k+2m-1}) \\ &\qquad + B(a_1, \ldots, a_{2k-1}, u_{2k}), \end{aligned} \tag{41}$$

for some $B(u_1, \ldots, u_{2k}) \in \mathbb{F}_q[u_1, \ldots, u_{2k}]$, and take $u_{2k} = a_{2k} \in \mathbb{F}_q$; it follows that

$$D_{k+1}(a_1, \ldots, a_{2k-1}, a_{2k}, a_{2k+1}, u_{2k+2}, \ldots, u_{2k+2m-1}) = 0, \tag{42}$$

for a unique $a_{2k+1} \in \mathbb{F}_q$ because $D_k(1) \neq 0$ by hypothesis. Since u_{2k} is any element $a_{2k} \in \mathbb{F}_q$ (i.e., it may assume q values in $\mathbb{F}_q$, while u_{2k+1} is uniquely specified), the assertion $|E(k, 1)| = q$ is proved.

Now, assume $m \geq 2$, and note that row $k + 1$ is uniquely determined up to position $k+1$ as a linear combination of the above rows up to the same position $k + 1$. Extend this linear combination to uniquely determine the remaining elements of the $\mathbf{H}^{(k+m)}$ Hankel matrix.

The assertion $|E(k, m)| = q^m$ is a consequence of the following claims.

Claim 1. One has $|A(k + 1, m)| = q^m$.

Consider a vector $(b_{2k}, \ldots, b_{2k+2m-1}) \in \mathbb{F}_q^{2m}$, which belongs to $A(k+1, m)$ if and only if there are $c_i \in \mathbb{F}_q$, $1 \leq i \leq k$, such that

$$\begin{aligned} &R_{k+1}(a_1, \ldots, a_{2k-1}, b_{2k}, \ldots, b_{2k+2m-1}) \\ &\quad = \sum_{i=1}^{k} c_i R_i(a_1, \ldots, a_{2k-1}, b_{2k}, \ldots, b_{2k+2m-1}), \end{aligned} \tag{43}$$

since $D_k(a_1, \ldots, a_{2k-1}, b_{2k}, \ldots, b_{2k+2m-1}) \neq 0$, and this same condition implies that the coefficients $c_1, \ldots, c_k$ are uniquely determined by the entries of the vector $(a_1, \ldots, a_{2k-1})$ and by the entry $b_{2k} = a_{2k}$ in row $R_{k+1}(a_1, \ldots, a_{2k-1}, b_{2k}, \ldots, b_{2k+2m-1})$.

We know that for each $a_{2k} \in \mathbb{F}_q$ there is a unique a_{2k+1} such that $D_{k+1}(a_1, \ldots, a_{2k-1}, a_{2k}, a_{2k+1}) = 0$.

Fix $u_{2k} = a_{2k}$ and hence fix $c_1, \ldots, c_k$, and $u_{2k+1} = a_{2k+1}$. The values of $u_{2k+i} = a_{2k+i}$, $i = 2, \ldots, m$ are uniquely specified by the linear combination condition, jointly with the Hankel matrix properties. Since the remaining u_{2k+m+i}, $i = 1, \ldots, m-1$ are free, the cardinality of $A(k + 1, m)$ is precisely q^m.

Claim 2. Since the first $k + 1$ rows of the Hankel matrix $\mathbf{H}^{(k+m)}$ are linearly dependent, it follows that $D_j(a_1, \ldots, a_{2k+m}, b_{2k+m+1}, \ldots, b_{2k+2m-1}) = 0$ for every $j \in \{k + 2, \ldots, k + m\}$.

To conclude the proof, it remains to show that the $(k+1)$th row, constructed as above, is the only possible $(k + 1)$th row that leads to a Hankel matrix satisfying the hypotheses of the proposition. This property is the third claim.

Claim 3. If $b_{2k+i} \neq a_{2k+i}$, for every $i = 2, \ldots, m$, then $D_{x+k}(a_1, \ldots, a_{2k-1}, a_{2k}, a_{2k+1}, b_{2k+2}, \ldots, b_{2k+2m-1}) \neq 0$ for every $x \in \{2, \ldots, m\}$.

Let $x \geq 2$ be the smallest integer such that the $(k+x) \times (k+x)$ Hankel matrix $\mathbf{H}^{(k+x)}$, with leading minor $D_k(1) \neq 0$, has the whole $(k+1)$th row that is not a linear combination of the above rows: this means that the entry b_{k+x} is different from a_{k+x}.

Let $c_1, \ldots, c_k$ be the coefficients of the linear combination of the first k rows of $\mathbf{H}^{(k+1+x)}$ yielding the row $(a_k, \ldots, a_{k+1+x})$.

From every hth row of the matrix $\mathbf{H}^{(k+x)}$, with $h \geq k+1$, the linear combination of the first k rows may be subtracted to get a row whose entries with index y are zero for every $y = 1, \ldots, h+k+1$. The counter-diagonal entries between row $k+1$ and the bottom row are $b_{2k+x} - a_{2k+x}$. The determinant of $\mathbf{H}^{(k+x)}$ and that of the modified matrix are the same; using the generalized Laplace formula for the expansion of a determinant with respect to the last $x+1$ rows, we get $D_{k+1+x}(1) = D_k(1)(a_{2k+x} - b_{2k+x})^x \neq 0$.

The contradiction forces $b_{2k+x} = a_{2k+x}$, which concludes the proof. □

Theorem 18. *For all integers n, j, and i such that $n \geq 2j-1 \geq 2i-1 > 0$ we have*

$$\left|S\left(j,i,n\right)\right| = q^{n-1-j+i}. \tag{44}$$

Proof. For all integers $n \geq t \geq 2j-1$ we have $|S(j,i,n)| = |S(j,i,t)| \cdot q^{n-t}$, because in each determinant $D_h(1)$, $h \leq j$, the variables x_e, $e \geq 2j$, do not occur; hence Lemma 12 gives the case $i = 1$ for all j. We may thus assume $i \geq 2$. Induction will be applied to j, the case $j = 2$ being obvious. The inductive assumption gives

$$\left|S\left(h,h,2h-1\right) \setminus S\left(h,h-1,2h-1\right)\right| = \left(q-1\right)q^{2h-3}, \tag{45}$$

for all $h < j$. Notice that $S(j,i,n) = S(j,1,n) \sqcup \{\sqcup_{h=2}^{i}(S(j,h,n) \setminus S(j,h-1,n))\}$. Lemma 9 gives $|S(j,h,n) \setminus S(j,h-1,n)| = (q-1)q^{2h-3}q^{n-2j+1+j-h}$. Hence

$$\left|S\left(j,i,n\right)\right| = q^{n-j} + \left(q-1\right)\sum_{h=2}^{i} q^{n-j+h-2} = q^{n-j-1+i}. \tag{46}$$

□

Remark 19. Take integers n, j, and i such that $n \geq 2j-1 \geq 2i-1 \geq 3$. Applying Theorem 18, first for (n,j,i) and then for $(n,j,i-1)$, gives $|S(j,i,n) \setminus S(j,i+1,n)| = q^{n-j-2+i}(q-1)$.

Proof of Theorem 2. We know by Lemma 6 that $|\mathscr{V}(D_j(1))| = |\mathscr{V}(D_{n-j}(1))|$, for every $1 \leq j \leq n-1$; the proof is completed by showing that $|\mathscr{V}(D_j(1))| = q^{n-1}$ for every $1 \leq j \leq \lfloor n/2 \rfloor$. This is true by the case $i = j$ of Theorem 18. $\mathscr{V}(D_n(1))$ has only one point, because $D_n(1)$ is an irreducible polynomial over $\mathbb{F}_q$. □

Corollary 20. *Given $j < n$, if $\gcd\{j, q-1\} = 1$, the varieties $\mathscr{V}(D_j(1) - b)$, $\forall b \in \mathbb{F}_q$ have cardinality q^{n-1}.*

Proof. Performing the substitution $x_i = tx_i'$ gives the equation $t^j D_j(x_1', \ldots, x_n') - b = 0$. By hypothesis $\gcd\{j, q-1\} = 1$, the equation $t^j = b$ always has a solution in $\mathbb{F}_q$, since we have $t = b^\mu$ with $\mu j = 1 \bmod q-1$. Thus all varieties with $b \neq 0$ have the same cardinality, say $n_b = |\mathscr{V}(D_j(1) - 1)|$, and the equation

$$q^{n-1} + \left(q-1\right)n_b = q^n \tag{47}$$

implies $n_b = q^{n-1}$. □

Note that, when j has some factor in common with $q-1$, the cardinalities of $\mathscr{V}(D_j(1) - b)$ are close to q^{n-1} but depend on b. It is an interesting problem to determine how close these cardinalities are to $q^{(n-1)}$.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

References

[1] O. Hesse, "Ueber determinanten und ihre anwendung in der geometrie, insbesondere auf Curven vieter ordung," *Journal für die Reine und Angewandte Mathematik*, vol. 49, pp. 243–264, 1855.

[2] A. Beauville, "Determinantal hypersurfaces," *The Michigan Mathematical Journal*, vol. 48, pp. 39–64, 2000.

[3] R. Zaare-Nahandi and H. Usefi, "A note on minors of a generalized Hankel matrix," *International Mathematical Journal*, vol. 3, no. 11, pp. 1197–1201, 2003.

[4] A. Weil, *Courbes Algébriques et Variétés Abéliennes*, Hermann, Paris, France, 1971.

[5] K. Cattell and J. C. Muzio, "Analysis of one-dimensional linear hybrid cellular automata over $\mathbb{F}_q$," *IEEE Transactions on Computers*, vol. 45, no. 7, pp. 782–792, 1996.

[6] K. Cattell and J. C. Muzio, "Synthesis of one-dimensional linear hybrid cellular automata," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 15, no. 3, pp. 325–335, 1996.

[7] M. T. Comer and E. L. Kaltofen, "On the Berlekamp/Massey algorithm and counting singular Hankel matrices over a finite field," *Journal of Symbolic Computation*, vol. 47, no. 4, pp. 480–491, 2012.

[8] K. Imamura and W. Yoshida, "A simple derivation of the Berlekamp-Massey algorithm and some applications," *IEEE Transactions on Information Theory*, vol. 33, no. 1, pp. 146–150, 1987.

[9] R. A. Horn and C. R. Johnson, *Matrix Analysis*, Dover, New York, NY, USA, 1980.