ALGEBRAIC NOTES ON TESTING SETS FOR LOWER AND UPPER GRIDS

EDUARDO MARQUES DE SÁ

Abstract. For a given finite dimensional subspace $\mathcal{P}$ of $k[x_1,\ldots,x_n]$, where k is a field, a subset $\mathcal{N}\subseteq k^n$ is a *$\mathcal{P}$-testing set* if any member of $\mathcal{P}$ that vanishes at all points of $\mathcal{N}$, vanishes all over k^n; and we say $\mathcal{N}$ is *optimal* if it has the smallest cardinality among all $\mathcal{P}$-testing sets. This is related to Lagrangian interpolation of data on a set $\mathcal{N}$ of nodes using functions from $\mathcal{P}$. We consider a *generic version* of this interpolation problem, when $\mathcal{P}$ has a monomial basis $\mathcal{B}$ that we identify with a *grid* (i.e. a finite subset of $\mathbb{N}_0^n$), each node is an n-tuple of independent variables and the set of nodes is identified with a grid $\mathcal{C}\subseteq\mathbb{N}_0^n$. A corollary to our main result offers an explicit formula for the determinant of the linear system corresponding to the generic interpolation problem in case $\mathcal{B}=\mathcal{C}$ is a σ-lower (or σ-upper) grid, where we say $\mathcal{B}$ is a *σ-lower* (resp., *σ-upper*) *grid* if it is a union of intervals of $\mathbb{N}_0^n$ having σ as common origin (resp., endpoint). We give explicit (optimal) $\mathcal{P}$-testing sets for spaces having monomial bases determined by σ-lower (or σ-upper) grids. The corollaries at the end, for the finite field case, have potential use in Number Theory and Coding Theory.

1. Introduction

The starting point for this research was a result of R. Livné [19, Theorem 4.3, p. 256] giving a sufficient condition for the isomorphism of the semi-simplifications of two 2-adic Galois representations. That result is an extension of the so-called Serre-Faltings method [11, 22] that has been frequently used to prove modularity of particular elliptic curves. For details on those matters see, for example, [19, 9, 15] and the references therein. Here, we only retain from Livné's method [19, Theorem 4.3] the crucial role of non-cubic subsets S of a finite dimensional vector space V over the field $\mathbb{Z}/2\mathbb{Z}$, where *non-cubic* means that a cubic homogeneous polynomial function on V that is zero on S is necessarily zero on V. This concept also occurs, in various degrees of generality, under names like "zero-testing sets" or "test sets", related to problems of the following kind. A polynomial function f is given by an oracle that produces $f(a)$ for any argument a; we know that f belongs to a given class $\mathcal{P}$ of functions, and then ask for good strategies to determine whether or not f is the zero function. In particular we may ask for a set T of arguments such that $f=0$ whenever f is zero at all points of T. [16, 7, 1]

These matters fall into the realm of Lagrange interpolation. To describe the contents of the paper we need a few well-known concepts (e.g. [20, 21, 10, 12]). In a broad approach to Lagrange interpolation we may start with a finite dimensional vector subspace $\mathcal{P}$ of the functional space k^A, where k is a field and A is an arbitrary set. Also given is a set $\mathcal{N}$ of points of A called *nodes* and some data on each node, more precisely a mapping $y:\mathcal{N}\to k$; we are then asked to find a function $f\in\mathcal{P}$ that agrees with y on $\mathcal{N}$. In other words, we consider the *evaluation of $\mathcal{P}$ at $\mathcal{N}$*, which is the linear mapping

$$\mathrm{Ev}_{\mathcal{P},\mathcal{N}}:\mathcal{P}\to k^{\mathcal{N}}$$

2020 *Mathematics Subject Classification.* 15A23, 15A69, 11T06. Secondary: 11T71, 11F80.

Key words and phrases. Interpolation, lower grid, upper grid, testing set, tensor, Vandermonde determinant, finite field.

Partially supported by the Centre for Mathematics of the University of Coimbra UID/00324 (funded by the Portuguese Government through FCT/MCTES, DOI 10.54499/UIDB/00324/2020).

that transforms $f \in \mathcal{P}$ into the restriction $f|_{\mathcal{N}}$, and then ask whether the given data y lies in the image of such evaluation. We say that the pair $(\mathcal{P}, \mathcal{N})$ is *poised for interpolation* whenever any data $y \in k^{\mathcal{N}}$ can be interpolated by a unique function of $\mathcal{P}$ [12, § 1.2], in other words, if the above evaluation map is an isomorphism; in such case the cardinality of $\mathcal{N}$ obviously equals the dimension of $\mathcal{P}$. We say that $\mathcal{N}$ is a $\mathcal{P}$-*testing set*, if any member of $\mathcal{P}$ that vanishes at all points of $\mathcal{N}$, vanishes all over A. A $\mathcal{P}$-testing set of the smallest cardinal is said to be an *optimal* $\mathcal{P}$-*testing set*. Clearly the $\mathcal{P}$-testing set property is equivalent to $\ker \mathrm{Ev}_{\mathcal{P},\mathcal{N}} = 0$. Therefore $\mathcal{N}$ is an optimal $\mathcal{P}$-testing set if and only if $\mathcal{P}$ and $\mathcal{N}$ are poised for interpolation.

We now describe the concrete objects to be considered below. The role of A will be played by the affine space k^n, where n is a positive integer, and the members of $\mathcal{P}$ are polynomial functions generated by polynomials from $k[x]$, where $x = (x_1, \dots, x_n)$ is an n-tuple of independent variables. The mapping $\Phi : k[x] \to k^{k^n}$ that transforms a polynomial f into the functional $\xi \rightsquigarrow f(\xi)$ is a homomorphism of k-algebras. When k is finite, Φ has a nonzero kernel. Therefore, a subspace $\mathcal{W}$ of $k[x]$ may not be faithfully represented by its functional image $\Phi(\mathcal{W})$. Having this in mind we use the expression *"$\mathcal{W}$-testing set"* with the same meaning as "$\Phi(\mathcal{W})$-testing set". Thus the cardinality of any optimal $\mathcal{W}$-testing set equals $\dim \Phi(\mathcal{W})$.

For monomials we use the notation $x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$, where $\alpha \in \mathbb{N}_0^n$. If $\mathcal{B}$ is a finite set of monomials, $\mathcal{P}_\mathcal{B}$ denotes the subspace of $k[x]$ generated by $\mathcal{B}$. We say $\mathcal{P}_\mathcal{B}$ is a *monomial space* and restrict our scope to such spaces. The set of all monomials will be identified with $\mathbb{N}_0^n$, under the correspondence $\alpha \leftrightsquigarrow x^\alpha$, viewing α as a simplified notation for x^α.

The nodes for interpolation are selected from a cartesian product $\mathcal{X} = \mathcal{X}_1 \times \cdots \times \mathcal{X}_n$, where $\mathcal{X}_i = \{x_{i0}, x_{i1}, \dots, x_{ij}, \dots\}$ (cf. [20, 21, 10]). In this paper the x_{ij} are independent variables to be later on replaced with elements of k. The members of $\mathcal{X}$ are called *generic nodes*. A *grid* is any finite subset of $\mathbb{N}_0^n$. For any grid $\mathcal{C} \subset \mathbb{N}_0^n$, define $\mathcal{X}_\mathcal{C} \subset \mathcal{X}$ by

$$\mathcal{X}_\mathcal{C} = \{(x_{1\alpha_1}, \dots, x_{n\alpha_n}) : (\alpha_1, \dots, \alpha_n) \in \mathcal{C}\}.$$

Given two grids $\mathcal{B}, \mathcal{C} \subset \mathbb{N}_0^n$, evaluating a polynomial $f \in \mathcal{B}$ at a generic node $(x_{1\tau_1}, \dots, x_{n\tau_n}) \in \mathcal{C}$ produces an element of the field of fractions $\mathbb{K} = k(\{x_{ij}\})$. So in this extended setting the evaluation mapping has the form

$$\mathrm{Ev}_{\mathcal{B},\mathcal{C}} : \mathfrak{P}_\mathcal{B} \to \mathbb{K}^{\mathcal{X}_\mathcal{C}}, \tag{1}$$

where $\mathfrak{P}_\mathcal{B}$ is the $\mathbb{K}$-subspace of $\mathbb{K}[x]$ generated by $\mathcal{B}$. We shall consider the case $\mathcal{C} = \mathcal{B}$, and call $(\mathfrak{P}_\mathcal{B}, \mathcal{X}_\mathcal{B})$ a *twin pair*. In the non-generic case (i.e. when $\mathcal{X} \subseteq k^n$), if k has characteristic 0 and $\mathcal{B}$ is a lower set, T. Sauer [20] shows that the twin $\mathcal{P}_\mathcal{B}$ is, roughly speaking, the only reasonable subspace of $k[x]$ to interpolate on the node set $\mathcal{X}_\mathcal{B}$.

Contents. In Section 2 we show that all generic twin pairs are poised for interpolation, and prove some existential results on testing sets aiming at the finite field case. Section 3 contains our main results, on an arbitrary square matrix A of the form $A = A_1 \otimes \cdots \otimes A_n$, each A_i having an LU-(or a UL)-decomposition. We give an explicit formula for any principal minor of A indexed by a lower grid, in terms of principal minors of the tensor factors. Such formulas are indeed valid for translates of lower grids and *upper grids* (to be defined). In the course of proof we obtain characterizations of lower and upper grids. In Section 4 we get explicit formulas for the determinant — denoted $\det \mathbb{V}[\mathcal{B}]$ — of the evaluation map (1) of the twin pair $(\mathfrak{P}_\mathcal{B}, \mathcal{X}_\mathcal{B})$, in case $\mathcal{B}$ is a lower (or upper) grid. Then $\det \mathbb{V}[\mathcal{B}]$ is shown to be isotonic for lower grids, that is, if $\mathcal{B} \subseteq \mathcal{B}'$ are lower grids, then $\det \mathbb{V}[\mathcal{B}]$ divides $\det \mathbb{V}[\mathcal{B}']$. Section 5 is devoted to the case of finite fields, to obtain (optimal) testing sets for some relevant subspaces of $k[x]$ with concepts and language borrowed from Coding Theory, and to address the zero-testing problem for homogeneous polynomials derived from R. Livné's [19, p. 256].

Acknowledgement. I thank Ariel Pacetti for proposing the topic of this research, for long discussions on the subject matter and multiple suggestions that improved the presentation of this manuscript.

Basic conventions.
$[n]$ denotes $\{1,\dots,n\}$. $[\sigma,\tau]$ denotes an interval in a given poset, e.g. $\mathbb{N}_0^n$.
$\mathcal{X}_{\mathcal{C}}^{\mathrm{var}}$ is the set of variables x_{ij} occurring in $\mathcal{X}_{\mathcal{C}}$.
$\mathcal{H}_d$ is the space generated by the homogeneous polynomials of degree d.
$k[x]^{\leqslant d}$ is the subspace of polynomials of degrees $\leqslant d$; we let $\deg 0 = -\infty$.
A matrix like $M = \big(m_{i,j}\big)_{i\in R,\, j\in C}$ is said to be an *$R\times C$-matrix.*
$[M]_{i,j}$ and m_{ij} are alternative notations for $m_{i,j}$.
$M[I|J]$ is the $I\times J$-submatrix of M, for any $I\subseteq R$ and $J\subseteq C$.
$M[i_1\cdots i_r|j_1\cdots j_s]$ is the same as $M[I|J]$ in case $I=\{i_1,\dots,i_r\}$ and $J=\{j_1,\dots,j_s\}$.
$M(I|J)$ is the complementary submatrix of $M[I|J]$, namely $M[R\smallsetminus I|C\smallsetminus J]$.
When M is square: the *order* of M is the number of its rows (columns).
$M[I]$ is the (square) principal submatrix whose rows are indexed by I.
$M(I)$ is the (square) principal submatrix whose rows are indexed by $R\smallsetminus I$.

2. On Poised Generic Pairs

Let $\mathcal{M}$ denote the box $[0,m_1]\times[0,m_2]\times\cdots\times[0,m_n]\subseteq\mathbb{N}_0^n$, where $m_1,\dots,m_n$ are fixed natural numbers. For $i\in[n]$, let V_i be the matrix whose row $s\in[0,m_i]$ is $(1,x_{is},x_{is}^2,\dots,x_{is}^{m_i})$, that we call *generic Vandermonde matrix*. Let $\mathbb{V}=V_1\otimes\cdots\otimes V_n$ be the tensor (or Kronecker) product of the V_i. Recall [14, §1.4] that $\mathbb{V}=V_1\otimes\cdots\otimes V_n$ is recursively given by $\mathbb{V}=V_1\otimes\mathbb{V}'$, where $\mathbb{V}':=V_2\otimes\cdots\otimes V_n$, and the two-fold tensor product $V_1\otimes\mathbb{V}'$ is expanded as

$$\mathbb{V}=\begin{bmatrix} \mathbb{V}' & x_{10}\,\mathbb{V}' & x_{10}^2\,\mathbb{V}' & \dots & x_{10}^{m_1}\,\mathbb{V}' \\ \mathbb{V}' & x_{11}\,\mathbb{V}' & x_{11}^2\,\mathbb{V}' & \dots & x_{11}^{m_1}\,\mathbb{V}' \\ \mathbb{V}' & x_{12}\,\mathbb{V}' & x_{12}^2\,\mathbb{V}' & \dots & x_{12}^{m_1}\,\mathbb{V}' \\ \vdots & \vdots & \vdots & & \vdots \\ \mathbb{V}' & x_{1m_1}\,\mathbb{V}' & x_{1m_1}^2\,\mathbb{V}' & \dots & x_{1m_1}^{m_1}\,\mathbb{V}' \end{bmatrix}. \tag{2}$$

It follows that the rows and columns of $\mathbb{V}$ are arranged in lexicographic order. Moreover, $\mathbb{V}$ is an $\mathcal{M}\times\mathcal{M}$-matrix, whose entry in row (indexed by) $(\sigma_1,\dots,\sigma_n)$ and column (indexed by) $(\alpha_1,\dots,\alpha_n)$ is $x_{1\sigma_1}^{\alpha_1}\cdots x_{n\sigma_n}^{\alpha_n}$. This is precisely the evaluation of the monomial $x_1^{\alpha_1}\cdots x_n^{\alpha_n}$ at the generic point $(x_{1\sigma_1},\dots,x_{n\sigma_n})$. So for any finite $\mathcal{B},\mathcal{C}\subseteq\mathbb{N}_0^n$ (and choosing a large enough $\mathcal{M}$), we have the following fact, which is well-known for a longtime [12, §2.1]

> *The matrix of the evaluation mapping* (1) *with respect to the basis $\mathcal{B}$ and the canonical basis of $\mathbb{K}^{\mathcal{X}_{\mathcal{C}}}$ is the submatrix $\mathbb{V}[\mathcal{C}|\mathcal{B}]$.* □

Definition 1. Given a grid $\mathcal{B}$ and $i\in[n]$, let $\theta_{ij}(\mathcal{B})$ be the number of those $\alpha\in\mathcal{B}$ such that $\alpha_i=j$. Denote by $\mathcal{B}_i$ the projection of $\mathcal{B}$ on the i-th coordinate, i.e. $\mathcal{B}_i:=\{\alpha_i:\alpha\in\mathcal{B}\}$.

Let $S_i(\mathcal{B})$ be the following tuple $(m_i,m_i,\dots,m_i,\dots,j,j,\dots,j,\dots,1,1,\dots,1,0,0,\dots,0)$, where each j occurs $\theta_{ij}(\mathcal{B})$ times. Note that $S_i(\mathcal{B})$ is a permutation of the sequence $(\alpha_i:\alpha\in\mathcal{B})$.

Given $\mathcal{C}\subseteq\mathbb{N}_0^n$, such that $|\mathcal{C}|=|\mathcal{B}|$, define $\delta_{ij}(\mathcal{C},\mathcal{B})=\sum_{s=1}^{\theta_{ij}(\mathcal{C})}\big[S_i(\mathcal{B})\big]_s$. □

Proposition 2. *For any grids $\mathcal{B},\mathcal{C}\subseteq\mathbb{N}_0^n$ such that $|\mathcal{C}|=|\mathcal{B}|$, we have:*
(a) The determinant of $\mathbb{V}[\mathcal{C}|\mathcal{B}]$ is either zero, or a homogeneous polynomial of degree equal to the degree of the product of all members of $\mathcal{B}$. Moreover
(b) The degree of $\det(\mathbb{V}[\mathcal{C}|\mathcal{B}])$ *in the variable x_{ij} is not greater than $\delta_{ij}(\mathcal{C},\mathcal{B})$.*

Proof. (a) For $x^\alpha\in\mathcal{B}$, all entries in the column α of $\mathbb{V}$ are monomials of degree $|\alpha|$. So all $|\mathcal{B}|!$ terms of $\det\mathbb{V}[\mathcal{C}|\mathcal{B}]$ are monomials of degree $\sum_{\alpha\in\mathcal{B}}|\alpha|=\deg\prod\mathcal{B}$.

(b) Each row of $\mathbb{V}[\mathcal{C}|\mathcal{B}]$ is indexed by an n-tuple $g=(g_1,\dots,g_n)$, which determines the generic point $(x_{1g_1},\dots,x_{ng_n})$, for $g\in\mathcal{C}$; among these points, the variable x_{ij} occurs exactly $\theta_{ij}(\mathcal{C})$ times; each such occurrence corresponds to a row of $\mathbb{V}[\mathcal{C}|\mathcal{B}]$ of the form $(\mu_{\alpha g}x_{ij}^{\alpha_i}:\alpha\in\mathcal{B})$,

where each $\mu_{\alpha g}$ is a monomial prime with x_{ij}. Therefore, each term of $\det \mathbb{V}[\mathcal{C}|\mathcal{B}]$ has the form μx_{ij}^{e}, where μ is prime with x_{ij} and the exponent e is a sum of $\theta_{ij}(\mathcal{C})$ entries of $S_i(\mathcal{B})$ in *distinct* positions of $S_i(\mathcal{B})$. The maximum of such exponents is thus the sum of the greatest $\theta_{ij}(\mathcal{C})$ entries of $(\alpha_i : \alpha \in \mathcal{B})$, which is $\sum_{s=1}^{\theta_{ij}(\mathcal{C})} \big[S_i(\mathcal{B})\big]_s$, as required. □

Definition 3. A *k-replacement of $\mathcal{X}_{\mathcal{C}}^{\mathrm{var}}$* is a map $\mathcal{X}_{\mathcal{C}}^{\mathrm{var}} \to k$, that transforms x_{ij} into $\overline{x}_{ij} \in k$. The k-replacement is called *proper* if, for each $i \in [n]$, the elements $\overline{x}_{iw}$ for $w \in \mathcal{C}_i$ are pairwise distinct. A k-replacement induces a mapping $\mathcal{X}_{\mathcal{C}} \to k^n$, $(x_{1\alpha_1}, \ldots, x_{n\alpha_n}) \rightsquigarrow (\overline{x}_{1\alpha_1}, \ldots, \overline{x}_{n\alpha_n})$. If the induced map is injective we call it a *k-embedding (of $\mathcal{X}_{\mathcal{C}}$ into k^n)*. Clearly, a proper k-replacement induces a k-embedding, which is then said to be a *proper k-embedding*.

The image of $\mathcal{X}_{\mathcal{C}}$ (resp., $\mathcal{X}_{\mathcal{C}}^{\mathrm{var}}$) is denoted by $\overline{\mathcal{X}}_{\mathcal{C}}$ (resp., $\overline{\mathcal{X}}_{\mathcal{C}}^{\mathrm{var}}$).

Theorem 4. *Suppose that the generic pair $(\mathfrak{P}_{\mathcal{B}}, \mathcal{X}_{\mathcal{C}})$ is poised for interpolation. Then:*

(a) If $|k| > \max\{\delta_{ij}(\mathcal{C}, \mathcal{B})\}_{i\in[n], j\in\mathcal{C}_i}$ there exists a k-embedding of $\mathcal{X}_{\mathcal{C}}$ whose image is an optimal $\mathcal{P}_{\mathcal{B}}$-testing set.

(b) If $|k| \geqslant \max_{i\in[n]} \sum_{j\in\mathcal{C}_i}(\delta_{ij}(\mathcal{C}, \mathcal{B}) + 1)$, there exists a proper k-embedding of $\mathcal{X}_{\mathcal{C}}$ whose image is an optimal $\mathcal{P}_{\mathcal{B}}$-testing set.

Proof. We know that $(\mathfrak{P}_{\mathcal{B}}, \mathcal{X}_{\mathcal{C}})$ is poised if and only if $\det \mathbb{V}[\mathcal{C}|\mathcal{B}] \neq 0$. We shall use the following result (check [3, Lemma 2.1] and [2, Lemma 2.1]):

(3) *Let $f(\xi_1, \ldots, \xi_N)$ be a nonzero polynomial over k. For each $w \in [N]$, let T_w be a subset of k such that $|T_w|$ is greater than the degree of f in the variable ξ_w. Then f is not zero in at least one point of $T_1 \times \cdots \times T_N$.*

(a) We apply (3), with $\{\xi_1, \ldots, \xi_N\} = \mathcal{X}_{\mathcal{C}}^{\mathrm{var}}$, to the polynomial $f = \det \mathbb{V}[\mathcal{C}|\mathcal{B}] \in k[\mathcal{X}_{\mathcal{C}}^{\mathrm{var}}]$. By Proposition 2(*b*), the assumption $|k| > \max\{\delta_{ij}(\mathcal{C}, \mathcal{B})\}_{i\in[n], j\in\mathcal{C}_i}$ implies that $|k|$ is greater than the degree of f in each variable $x_{ij} \in \mathcal{X}_{\mathcal{C}}^{\mathrm{var}}$. So there exists a replacement of $\mathcal{X}_{\mathcal{C}}^{\mathrm{var}}$ that produces a nonzero point of $\det \mathbb{V}[\mathcal{C}|\mathcal{B}]$. The image $\overline{\mathcal{X}}_{\mathcal{C}}$ is the set of the replaced columns of $\mathbb{V}[\mathcal{C}|\mathcal{B}]$. These are linear independent and therefore distinct. So from our replacement we get a k-embedding of $\mathcal{X}_{\mathcal{C}}$.

(b) The method of proof is the same as that of *(a)*. For each variable $x_{ij} \in \mathcal{X}_{\mathcal{C}}^{\mathrm{var}}$ we consider a subset $T_{ij} \subseteq k$, satisfying the following conditions:

$$|T_{ij}| = \delta_{ij}(\mathcal{C}, \mathcal{B}) + 1, \text{ for } \quad i \in [n],\ j \in \mathcal{C}_i, \tag{4}$$

(5) For each fixed $i \in [n]$, the sets T_{ij}, for $j \in \mathcal{C}_i$, are pairwise disjoint.

These conditions imply, for each $i \in [n]$, that $\sum_{j\in\mathcal{C}_i} T_{ij} = \sum_{j\in\mathcal{C}_i}(\delta_{ij}(\mathcal{C}, \mathcal{B})+1)$. Our assumption on the cardinality of k implies the existence of subsets T_{ij} satisfying (4)-(5). According to (3), there exists a replacement $\mathcal{X}_{\mathcal{C}}^{\mathrm{var}} \to k$, $x_{ij} \rightsquigarrow \overline{x}_{ij}$, that produces a nonzero point of $\det \mathbb{V}[\mathcal{C}|\mathcal{B}]$, and satisfies $\overline{x}_{ij} \in T_{ij}$. Such replacement obviously determines a proper k-embedding of $\mathcal{X}_{\mathcal{C}}$. □

Remark. We may add to the above the following well-known facts of Algebraic Geometry. If k is infinite, the set $\mathcal{E}$ of all (proper) k-embeddings of $\mathcal{X}_{\mathcal{C}}$ whose image is an optimal $\mathcal{P}_{\mathcal{B}}$-testing set has cardinality $|k|$. If k is the real or the complex field, $\mathcal{E}$ is an open dense set in the Euclidean topology of $k^{n|\mathcal{B}|}$. □

Theorem 5. *For any grid $\mathcal{B}$ the generic twin pair $(\mathfrak{P}_{\mathcal{B}}, \mathcal{X}_{\mathcal{B}})$ is poised for interpolation.*

Proof. We have to show that $\mathbb{V}[\mathcal{B}]$ is nonsingular. Let $\mathbb{V}_0$ be the matrix obtaining from $\mathbb{V}$ after zeroing out x_{10}, and let $\mathbb{V}' = V_2 \otimes \cdots \otimes V_n$. In view of (2) it is clear that $\mathbb{V}_0$ may be written as

$$\mathbb{V}_0 = \begin{bmatrix} \mathbb{V}' & 0 \\ * & U \end{bmatrix}, \quad \text{where} \quad U := \begin{bmatrix} x_{11}\mathbb{V}' & x_{11}^2\mathbb{V}' & \ldots & x_{11}^{m_1}\mathbb{V}' \\ x_{12}\mathbb{V}' & x_{12}^2\mathbb{V}' & \ldots & x_{12}^{m_1}\mathbb{V}' \\ \vdots & \vdots & & \vdots \\ x_{1m_1}\mathbb{V}' & x_{1m_1}^2\mathbb{V}' & \ldots & x_{1m_1}^{m_1}\mathbb{V}' \end{bmatrix}, \tag{6}$$

and $*$ denotes an unspecified block. Clearly the columns/rows of $\mathbb{V}'$ (resp., U) are indexed by the nodes α such that $\alpha_1 = 0$ (resp., $\alpha_1 > 0$). We now factor x_{1j} out of the j-th row of blocks of U, for all $j \in [m_1]$. So U may be represented as

$$U = \big(\operatorname{Diag}(x_{11}, x_{12}, \ldots, x_{1m}) \otimes I_h\big) \cdot \big(V_1' \otimes \mathbb{V}'\big), \tag{7}$$

where V_1' is the $[m_1] \times [m_1]$ Vandermonde matrix whose row s is $(1, x_{1s}, x_{1s}^2, \ldots, x_{1s}^{m_1-1})$, and I_h is the h-order identity matrix, where h is the order of $\mathbb{V}'$. Therefore

$$\det \mathbb{V}_0 = (x_{11}x_{12}\cdots x_{1m_1})^h \det \mathbb{V}' \det(\mathbb{V}_1' \otimes \mathbb{V}'). \tag{8}$$

We consider the set of all tensor products of generic Vandermonde matrices and prove, by induction on the order of such tensors, that all principal minors of all of those tensors are nonzero.

So let $\mathcal{B} \subseteq \mathcal{M}$. Split $\mathcal{B}$ into two disjoint sets, $\mathcal{B}'$ and $\mathcal{B}''$, where $\mathcal{B}' = \{\alpha \in \mathcal{B} : \alpha_1 = 0\}$ and $\mathcal{B}'' = \{\alpha \in \mathcal{B} : \alpha_1 > 0\}$. Then

$$\mathbb{V}[\mathcal{B}] = \begin{bmatrix} \mathbb{V}'[\mathcal{B}'] & Z \\ * & U[\mathcal{B}''] \end{bmatrix}.$$

From (7) we clearly have

$$U[\mathcal{B}''] = \big(\operatorname{Diag}(x_{11}, \ldots, x_{1m}) \otimes I_h\big)[\mathcal{B}''] \cdot \big(\mathbb{V}_1' \otimes \mathbb{V}'\big)[\mathcal{B}''].$$

Put $x_{10} = 0$; as this kills Z, we get $\det \mathbb{V}_0[\mathcal{B}] = \det \mathbb{V}'[\mathcal{B}'] \cdot \det U[\mathcal{B}'']$. The method used to prove (8) produces

$$\det \mathbb{V}_0[\mathcal{B}] = x_{11}^{h_1} \cdots x_{1m_1}^{h_{m_1}} \det \mathbb{V}'[\mathcal{B}'] \cdot \det(\mathbb{V}_1' \otimes \mathbb{V}')[\mathcal{B}''],$$

where h_j is the number of rows of $\mathcal{B}$ that cross the square block $x_{1j}\mathbb{V}'$ of U in the partition (6). As $\mathbb{V}'$ and $\mathbb{V}''$ are tensor products of generic Vandermonde matrices of lower order than that of $\mathbb{V}$, the induction hypothesis entails $\det \mathbb{V}'[\mathcal{B}'] \cdot \det \mathbb{V}''[\mathcal{B}''] \neq 0$. So $\det \mathbb{V}_0[\mathcal{B}] \neq 0$ and, therefore, $\det \mathbb{V}[\mathcal{B}] \neq 0$. □

3. Triangular Tensor product patterns

Let $\mathcal{J} := J_1 \times \cdots \times J_n$, where $J_1, \ldots, J_n$ are arbitrary finite sets, each one endowed with a total order $\leqslant$ (the same symbol for all these sets). The members of $\mathcal{J}$ are n-tuples $\alpha = (\alpha_1, \ldots, \alpha_n)$, $\beta = (\beta_1, \ldots, \beta_n)$, etc., and $\mathcal{J}$ is partially ordered by the entrywise order, denoted by $\leqslant$ as well. Let $\top = (\top_1, \ldots, \top_n)$ and $\bot = (\bot_1, \ldots, \bot_n)$ be, respectively, the top and bottom elements of $\mathcal{J}$. Thus $\mathcal{J} = [\bot, \top]$, and $J_i = [\bot_i, \top_i]$.

Let R be a commutative ring with identity 1. For each $i \in [n]$ let A_i be an arbitrary square matrix over R, whose rows and columns are indexed by J_i. We let A be the tensor product $A_1 \otimes \cdots \otimes A_n$. Thus A is a $\mathcal{J} \times \mathcal{J}$ matrix.

Definition 6. Intervals of $\mathcal{J}$, denoted as $[\alpha, \beta]$, are tacitly referred to the partial order $\leqslant$. A union of intervals of $\mathcal{J}$ with common origin σ (resp., common endpoint τ) is called a *σ-lower set* (resp., *τ-upper set).* A *lower set of* $\mathcal{J}$ is a σ-lower set of $\mathcal{J}$ where σ is $\bot$, the bottom element of $\mathcal{J}$. An *upper set of* $\mathcal{J}$ is a τ-upper set of $\mathcal{J}$ where τ is $\top$, the top element of $\mathcal{J}$. For $\mathcal{B} \subseteq \mathcal{J}$ we let $\theta_{ij}(\mathcal{B})$ (or just θ_{ij} if no confusion arises) and $\mathcal{B}_i$ be as in Definition 1. □

Clearly $\theta_{ij}(\mathcal{B}) = 0$ if and only if $j \notin \mathcal{B}_i$. If $\mathcal{B}$ is a σ-lower set of $\mathcal{J}$ then $\mathcal{B}_i$ is a J_i-interval, $\mathcal{B}_i = [\sigma_i, \max \mathcal{B}_i]$; moreover, $\theta_{ig}(\mathcal{B})$ is weakly decreasing with respect to $g \in \mathcal{B}_i$. If $\mathcal{B}$ is a τ-upper set then $\mathcal{B}_i = [\min \mathcal{B}_i, \tau_i]$, and $\theta_{ig}(\mathcal{B})$ is weakly increasing with respect to $g \in \mathcal{B}_i$.

Theorem 7. *Let $A = A_1 \otimes \cdots \otimes A_n$ be a $\mathcal{J} \times \mathcal{J}$ matrix, over the ring R.*

(*a*) *Suppose that each* A_i *has an* LU *factorization* $A_i = L_i U_i$*, where* L_i *and* U_i *are, respectively, lower and upper triangular matrices over some extension of* R*. If* $\mathcal{B}$ *is a lower set of* $\mathcal{J}$*,*

$$\det A[\mathcal{B}] = \prod_{i=1}^{n} \prod_{h \in \mathcal{B}_i} \det A_i\big[[\bot_i, h]\big]^{\theta_{i,h} - \theta_{i,h_+}}, \tag{9}$$

where h_+ *denotes the successor of* h *in* J_i*, with the convention* $\theta_{i,h_+} = 0$ *when* h *is* $\max \mathcal{B}_i$*.*

(*b*) *Suppose that each* A_i *has a* UL *factorization* $A_i = U_i' L_i'$*, where* U_i' *and* L_i' *are, respectively, upper and lower triangular matrices over some extension of* R*. If* $\mathcal{B}$ *is an upper set of* $\mathcal{J}$*,*

$$\det A[\mathcal{B}] = \prod_{i=1}^{n} \prod_{h \in \mathcal{B}_i} \det A_i\big[[h, \top_i]\big]^{\theta_{i,h} - \theta_{i,h_-}} \tag{10}$$

where h_- *denotes the predecessor of* h *in* $\mathcal{B}_i$*, with the convention* $\theta_{i,h_-} = 0$ *when* h *is* $\min \mathcal{B}_i$*.*

Corollary 8. *Let* $A = A_1 \otimes \cdots \otimes A_n$ *be a* $\mathcal{J} \times \mathcal{J}$ *matrix, over an integral domain* R*.*

(*a*) *If* $\mathcal{B}$ *is a lower set of* $\mathcal{J}$ *and all leading minors of all* A_i *are nonzero, then* (9) *holds.*

(*b*) *If* $\mathcal{B}$ *is an upper set of* $\mathcal{J}$ *and all trailing minors of all* A_i *are nonzero, then* (10) *holds.*

The proofs of the previous theorem and corollary are based on the following lemma.

Lemma 9. *Let* $\mathcal{L} := \mathcal{L}_1 \otimes \cdots \otimes \mathcal{L}_n$*, where* $\mathcal{L}_i$ *is the* $J_i \times J_i$ *lower triangular* 01*-matrix having entries* 1 *on and below the main diagonal. The following conditions are equivalent:*

(*a*) $\mathcal{B}$ *is a lower set (resp., upper set) of* $\mathcal{J}$*;*

(*b*) *Any* $\mathcal{J} \times \mathcal{J}$*-matrices* L *and* U *over* R*, such that* $\mathcal{L}_{\sigma\tau} = 0 \Rightarrow L_{\sigma\tau} = U_{\tau\sigma} = 0$ *(for all* $\sigma, \tau \in \mathcal{J}$*), satisfy the identity* $(LU)[\mathcal{B}] = L[\mathcal{B}]\, U[\mathcal{B}]$ *(resp.,* $(UL)[\mathcal{B}] = U[\mathcal{B}]\, L[\mathcal{B}]$*).*

Proof. We first prove the following claim

$$\text{For any } \alpha, \beta \in \mathcal{J} \text{ we have: } \beta \leqslant \alpha \text{ if and only if } \mathcal{L}_{\alpha\beta} = 1. \tag{11}$$

The case $n = 1$ is obvious. So take $n > 1$ and let $\mathcal{L}' := \mathcal{L}_1 \otimes \cdots \otimes \mathcal{L}_{n-1}$. Passing from $\mathcal{L}'$ to $\mathcal{L}$ consists in replacing, in $\mathcal{L}'$, each 1 with a triangle $\mathcal{L}_n$, and each 0 with a $J_n \times J_n$ zero matrix. Define $\alpha' := (\alpha_1, \ldots \alpha_{n-1})$ and $\beta' := (\beta_1, \ldots \beta_{n-1})$.

Suppose $\alpha' = \beta'$. Then $\beta \leqslant \alpha$ is equivalent to $\beta_n \leqslant \alpha_n$. Moreover, the positions (α, α) and (β, β) lie in the diagonal of *the same* block $\mathcal{L}_n$, resulting from the replacement of the entry (α', α') of $\mathcal{L}'$ with $\mathcal{L}_n$. Relative to the latter block, α and β occupy the α_n-th and the β_n-th diagonal positions. So $\beta_n \leqslant \alpha_n$ if and only if $\big[\mathcal{L}_n\big]_{\alpha_n \beta_n} = 1$, and (11) follows.

Now suppose $\alpha' \neq \beta'$. By the inductive hypothesis, $\beta' \leqslant \alpha'$ is equivalent to $[\mathcal{L}']_{\alpha'\beta'} = 1$; so $\beta \leqslant \alpha$ holds if and only if: (*i*) $[\mathcal{L}']_{\alpha'\beta'} = 1$ and (*ii*) $\beta_n \leqslant \alpha_n$. The condition (*i*) means that $\mathcal{L}'[\{\alpha', \beta'\}] = \left[\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right]$, i.e. the following configuration of blocks

$$\begin{bmatrix} B & 0 \\ C & A \end{bmatrix}, \quad \text{with } A = B = C = \mathcal{L}_n,$$

occurs as a principal submatrix of $\mathcal{L}$, where the (α, α)-entry of $\mathcal{L}$ is the (α_n, α_n)-entry of A, and the (β, β)-entry of $\mathcal{L}$ is the (β_n, β_n)-entry of B. Thus (*ii*) holds iff (α, β) lies on, or below the diagonal of $C = \mathcal{L}_n$, i.e. $\mathcal{L}_{\alpha\beta} = 1$. So (11) follows easily in this case. Therefore (11) is proved.

We only prove our lemma in the "lower set case". The "upper set case" is left to the reader.

(*a*) $\Rightarrow$ (*b*). For $\alpha, \beta \in \mathcal{B}$ we have $[LU]_{\alpha\beta} = \sum_{\gamma \in \mathcal{J}} L_{\alpha\gamma} U_{\gamma\beta}$. Suppose $L_{\alpha\gamma} U_{\gamma\beta} \neq 0$; then, combining (11) with the assumptions of (*b*) on L and U, it is clear that $\gamma \in \mathcal{B}$. Therefore

$$[LU]_{\alpha\beta} = \sum_{\gamma \in \mathcal{B}} L_{\alpha\gamma} U_{\gamma\beta} = \big[L[\mathcal{B}] \cdot U[\mathcal{B}]\big]_{\alpha\beta}.$$

(*b*) $\Rightarrow$ (*a*). Applying (*b*) to the R-matrices $L := \mathcal{L}$ and $U := \mathcal{L}^T$ we obtain $(\mathcal{L}\mathcal{L}^T)[\mathcal{B}] = \mathcal{L}[\mathcal{B}]\mathcal{L}^T[\mathcal{B}]$. In particular, for any $\sigma \in \mathcal{B}$, we have $(\mathcal{L}\mathcal{L}^T)[\sigma] = (\mathcal{L}[\mathcal{B}]\mathcal{L}[\mathcal{B}]^T)[\sigma]$. This may be

written as $\sum_{\tau\in\mathcal{J}}\mathcal{L}_{\sigma\tau}\mathcal{L}_{\sigma\tau}=\sum_{\beta\in\mathcal{B}}\mathcal{L}_{\sigma\beta}\mathcal{L}_{\sigma\beta}$. Taking (11) into account, we get

$$\sum_{\tau\in[\bot,\sigma]}\mathcal{L}_{\sigma\tau}=\sum_{\beta\in\mathcal{B},\ \beta\leqslant\sigma}\mathcal{L}_{\sigma\beta}. \tag{12}$$

Note that all entries of $\mathcal{L}$ occurring is these sums are equal to $1\in R$. Suppose that some $\overline{\tau}\leqslant\sigma$ does not lie in $\mathcal{B}$; so $\overline{\tau}$ does not occur in the right hand side of (12). Let us zero out in $\mathcal{L}$ the entry $\mathcal{L}_{\sigma\overline{\tau}}$; the modified matrix still satisfies the condition imposed by (b) on L. So the equation (12) remains valid after zeroing out $\mathcal{L}_{\sigma\overline{\tau}}$. This contradiction shows that all $\tau\leqslant\sigma$ lie in $\mathcal{B}$. Therefore $\mathcal{B}$ is a lower set. □

Proof of Theorem 7. Suppose $\mathcal{B}$ is a lower set of $\mathcal{J}$. Clearly the matrices $L:=L_1\otimes\cdots\otimes L_n$ and $U:=U_1\otimes\cdots\otimes U_n$ are, respectively, lower and upper triangular, and we have $A=LU$. Applying Lemma 9, we get $A[\mathcal{B}]=L[\mathcal{B}]U[\mathcal{B}]$. Therefore

$$\det A[\mathcal{B}]=\det L[\mathcal{B}]\cdot\det U[\mathcal{B}].$$

Define D_i as the $J_i\times J_i$ diagonal matrix whose diagonal entry in the position $\alpha_i\in J_i$ is $D_i[\alpha_i]=L_i[\alpha_i]U_i[\alpha_i]$. Define $D:=D_1\otimes\cdots\otimes D_n$. Thus $D[\alpha]=D_1[\alpha_1]\cdots D_n[\alpha_n]$ for any $\alpha\in\mathcal{J}$. Therefore

$$\det A[\mathcal{B}]=\det D[\mathcal{B}]=\prod_{i=1}^{n}\prod_{\alpha\in\mathcal{B}}D_i[\alpha_i]. \tag{13}$$

Let $\mathcal{B}_i=\{h_{i1},h_{i2},\dots,h_{iw_i}\}$, where $\sigma_i=h_{i1}<h_{i2}<\cdots<h_{iw_i}$. Apply formula (13), in the case $n=1$, replacing A with A_i and $\mathcal{B}$ with $\mathcal{B}_i$; as the lower sets of J_i are the leading intervals $[h_{i1},h_{ij}]=\{h_{i1},h_{i2},\dots,h_{ij}\}$, we get

$$\det A_i\big[[h_{i1},h_{ij}]\big]=\prod_{s=1}^{j}D_i[h_{is}]. \tag{14}$$

By the definition of the $\theta_{ij}=\theta_{ij}(\mathcal{B})$ we have

$$\prod_{\alpha\in\mathcal{B}}D_i[\alpha_i]=\prod_{s=1}^{w_i}D_i[h_{is}]^{\theta_{i,h_{is}}}.$$

We now prove, by induction on $t=1,\dots,w_i$, that, for any integers $\theta_{i,h_{i1}}\geqslant\cdots\geqslant\theta_{i,h_{it}}\geqslant 0$,

$$\prod_{s=1}^{t}D_i[h_{is}]^{\theta_{i,h_{is}}}=\left(\prod_{s=1}^{t-1}\det A_i\big[[h_{i1},h_{is}]\big]^{\theta_{i,h_{is}}-\theta_{i,h_{i,s+1}}}\right)\det A_i\big[[h_{i1},h_{it}]\big]^{\theta_{i,h_{it}}}. \tag{15}$$

For $t=1$, (15) reduces to $D_i[h_{i1}]^{\theta_{i,h_{i1}}}=\det A_i\big[h_{i1}\big]^{\theta_{i,h_{i1}}}$ which follows from (14). Our induction hypothesis is (15) when t is replaced with $t-1$. First we transform the left hand side of (15) using (14):

$$\begin{aligned}\prod_{s=1}^{t}D_i[h_{is}]^{\theta_{i,h_{is}}}&=\left(\prod_{s=1}^{t-1}D_i[h_{is}]^{\theta_{i,h_{is}}-\theta_{i,h_{it}}}\right)\left(\prod_{s=1}^{t}D_i[h_{is}]\right)^{\theta_{i,h_{it}}}\\&=\left(\prod_{s=1}^{t-1}D_i[h_{is}]^{\overline{\theta}_{i,h_{is}}}\right)\det A_i\big[[h_{i1},h_{it}]\big]^{\theta_{i,h_{it}}},\end{aligned} \tag{16}$$

where $\overline{\theta}_{i,h_{is}}$ denotes $\theta_{i,h_{is}}-\theta_{i,h_{it}}$. Clearly $\overline{\theta}_{i,h_{i1}}\geqslant\cdots\geqslant\overline{\theta}_{i,h_{it}}=0$ and $\overline{\theta}_{i,h_{is}}-\overline{\theta}_{i,h_{iu}}=\theta_{i,h_{is}}-\theta_{i,h_{iu}}$. The induction hypothesis applied to the integers $\overline{\theta}_{i,h_{i1}}\geqslant\cdots\geqslant\overline{\theta}_{i,h_{i,t-1}}\geqslant 0$ implies

$$\left(\prod_{s=1}^{t-1}D_i[h_{is}]^{\overline{\theta}_{i,h_{is}}}\right)=\left(\prod_{s=1}^{t-2}\det A_i\big[[h_{i1},h_{is}]\big]^{\theta_{i,h_{is}}-\theta_{i,h_{i,s+1}}}\right)\det A_i\big[[h_{i1},h_{i,t-1}]\big]^{\overline{\theta}_{i,h_{i,t-1}}}. \tag{17}$$

Our claim (15) follows from (16) and (17). Join (13) with the case $t = w_i$ of (15) to obtain

$$\det A[\mathcal{B}] = \prod_{i=1}^{n}\prod_{s=1}^{w_i} \det A_i\big[[h_{i1}, h_{is}]\big]^{\theta_{i,h_{is}} - \theta_{i,h_{i,s+1}}},$$

with the convention $\theta_{i,h_{i,w_i+1}} = 0$. Up to notation this is nothing but (9).

The proof of (10), for an upper set, is omitted as it mirrors the proof we have just done. □

Proof of Corollary 8. We shall assume, as we may, that R is a field, otherwise we may extend it to its field of fractions. Now recall the following known facts:

(18) *A nonsingular square matrix M has an* LU *factorization (resp.,* UL *factorization) if and only if all leading (resp., trailing) minors of M are nonzero.*

The LU case of this result is well-known in the theory of linear systems (check, e.g. [13, §3.2], whose proof extends trivially to an arbitrary field); as a matter of fact, the non vanishing of the leading minors is equivalent to the possibility of performing the Gauss elimination procedure on the rows of M *without pivoting*. For the UL case, note that an LU factorization of M^{-1}, say $M^{-1} = \underline{L}\,\underline{U}$ implies a UL factorization of M, namely $M = \underline{U}^{-1}\underline{L}^{-1}$; moreover, C. Jacobi's identity [5, Lemma A.1(e)] entails that a minor of M is nonzero iff the minor of M^{-1} in complementary position is nonzero.

In view of these facts, Corollary 8 follows from Theorem 7. □

4. The case of Vandermonde Minors

4.1. **Determinantal formulas.** We now go back to the box $\mathcal{M} = [0, m_1] \times [0, m_2] \times \cdots \times [0, m_n]$ and the Vandermonde tensor product $\mathbb{V} = V_1 \otimes \cdots \otimes V_n$ of Section 2.

Theorem 10. *If $\mathcal{B}$ is a σ-lower grid of $\mathcal{M}$, then*

$$\det \mathbb{V}[\mathcal{B}] = \prod_{i=1}^{n} \left(\prod_{t\in\mathcal{B}_i} x_{it}^{\sigma_i\,\theta_{it}} \right) \left(\prod_{u<w\in\mathcal{B}_i} (x_{iw} - x_{iu})^{\theta_{iw}} \right). \tag{19}$$

If $\mathcal{B}$ is a τ-upper grid of $\mathcal{M}$, then

$$\det \mathbb{V}[\mathcal{B}] = \prod_{i=1}^{n} \left(\prod_{t\in\mathcal{B}_i} x_{it}^{\sum_{0\leqslant s<t}(\theta_{it}-\theta_{is})} \right) \left(\prod_{u<w\in\mathcal{B}_i} (x_{iw} - x_{iu})^{\theta_{iu}} \right). \tag{20}$$

Proof. For $[r, s] \subseteq [0, m_i]$ the well-known expansion of a Vandermonde determinant entails

$$\det V_i\big[[r, s]\big] = \prod_{t=r}^{s} x_{it}^{r} \prod_{r\leqslant u<w\leqslant s} (x_{iw} - x_{iu}). \tag{21}$$

All minors of all V_i are nonzero. So we get from Corollary 8:

$$\begin{aligned}
\det \mathbb{V}[\mathcal{B}] &= \prod_{i=1}^{n} \prod_{s\in\mathcal{B}_i} \det V_i\big[[\sigma_i, s]\big]^{\theta_{i,s}-\theta_{i,s+1}} \\
&= \prod_{i=1}^{n} \prod_{s=\sigma_i}^{\max\mathcal{B}_i} \left(\prod_{t=\sigma_i}^{s} x_{it}^{\sigma_i} \prod_{\sigma_i\leqslant u<w\leqslant s} (x_{iw} - x_{iu}) \right)^{\theta_{i,s}-\theta_{i,s+1}} \\
&= \prod_{i=1}^{n} \left[\prod_{s=\sigma_i}^{\max\mathcal{B}_i} \prod_{t=\sigma_i}^{s} x_{it}^{\sigma_i(\theta_{i,s}-\theta_{i,s+1})} \right] \left[\prod_{s=\sigma_i}^{\max\mathcal{B}_i} \prod_{\sigma_i\leqslant u<w\leqslant s} (x_{iw} - x_{iu})^{\theta_{i,s}-\theta_{i,s+1}} \right]. \qquad (22)
\end{aligned}$$

For fixed $i \in [n]$ and $t \in \mathcal{B}_i$, the expressions $x_{it}^{\sigma_i(\theta_{i,s}-\theta_{i,s+1})}$ in the first bracket of (22) occur for all s in $[t, \max\mathcal{B}_i]$; the product of all such expressions is thus $x_{it}^{\sigma_i\,\theta_{it}}$. For fixed $u, w \in \mathcal{B}_i$,

$u < w$, the expressions $(x_{i,w} - x_{i,u})^{\theta_{i,s}-\theta_{i,s+1}}$ in the second bracket of (22) occur for all s in $[w, \max \mathcal{B}_i]$; the product of all such expressions is $(x_{iw} - x_{iu})^{\theta_{iw}}$. Therefore (19) holds.

When $\mathcal{B}$ is a τ-upper set of $\mathcal{M}$ we follow a similar path to get

$$\det \mathbb{V}[\mathcal{B}] = \prod_{i=1}^{n} \left[\prod_{s=\min \mathcal{B}_i}^{\tau_i} \prod_{t=s}^{\tau_i} x_{it}^{s(\theta_{i,s}-\theta_{i,s-1})} \right] \left[\prod_{s=\min \mathcal{B}_i}^{\tau_i} \prod_{s \leqslant u < w \leqslant \tau_i} (x_{iw} - x_{iu})^{\theta_{i,s}-\theta_{i,s-1}} \right]. \tag{23}$$

For fixed $i \in [n]$ and $t \in \mathcal{B}_i$, the terms $x_{it}^{s(\theta_{i,s}-\theta_{i,s-1})}$ in the first bracket of (23) occur for all s in $[\min \mathcal{B}_i, t]$; as $\theta_{is} = 0$ for $s < \min \mathcal{B}_i$, the product of all such expressions is

$$\prod_{0 \leqslant s \leqslant t} x_{it}^{s(\theta_{i,s}-\theta_{i,s-1})} = x_{it}^{\sum_{0 \leqslant s < t}(\theta_{it}-\theta_{is})}.$$

For fixed $i \in [n]$ and fixed $u < w \in \mathcal{B}_i$, the expressions $(x_{i,w} - x_{i,u})^{\theta_{i,s}-\theta_{i,s+1}}$ in the second bracket of (23) occur for all s in $[\min \mathcal{B}_i, u]$; the product of all such terms is thus $(x_{iw} - x_{iu})^{\theta_{iu}}$. Taking these expressions into account in (23) we easily get (20). □

Corollary 11. *If $\mathcal{B}$ and $\mathcal{B}'$ are σ-lower grids such that $\mathcal{B} \subseteq \mathcal{B}'$, then* $\det \mathbb{V}[\mathcal{B}]$ *divides* $\det \mathbb{V}[\mathcal{B}']$.

Proof. As $\mathcal{B} \subseteq \mathcal{B}'$, we have $\theta_{ij}(\mathcal{B}) \leqslant \theta_{ij}(\mathcal{B}')$ for $i \in [n]$ and $j \in \mathcal{B}'_i$. So the corollary is an easy consequence of formula (19). □

Example. Let us check formulas (19)-(20) in case $\mathcal{B}$ is the box $[\sigma, \tau] \subseteq \mathcal{M}$. Then $\mathcal{B}$ is a σ-lower grid and a τ-upper grid. Clearly $\mathcal{B}_i = [\sigma_i, \tau_i]$ and $\theta_{ij} = \theta_{ij}(\mathcal{B})$ is given by

$$\theta_{ij} = \begin{cases} |\mathcal{B}|/|\mathcal{B}_i|, & \text{if } j \in [\sigma_i, \tau_i] \\ 0 & \text{if } j \notin [\sigma_i, \tau_i] \end{cases}.$$

The exponent of x_{it} in (20) is the same as in (19) because

$$\sum_{s=0}^{t-1} (\theta_{it} - \theta_{is}) = \sum_{s=0}^{\sigma_i - 1} \theta_{it} + \sum_{s=\sigma_i}^{t-1} (\theta_{it} - \theta_{is}) = \sigma_i \theta_{it}.$$

So, as expected, (19) and (20) produce the same expression which, after rearrangements, is

$$\det \mathbb{V}\big[[\sigma, \tau]\big] = \prod_{i=1}^{n} \left[\prod_{t \in \mathcal{B}_i} x_{it}^{\sigma_i} \prod_{u < w \in \mathcal{B}_i} (x_{iw} - x_{iu}) \right]^{|\mathcal{B}|/|\mathcal{B}_i|}. \tag{24}$$

The expression between big brackets is the determinant of $\mathbb{V}_i\big[[\sigma_i, \tau_i]\big]$. As a matter of fact, $\mathbb{V}\big[[\sigma, \tau]\big] = V_1\big[[\sigma_1, \tau_1]\big] \otimes \cdots \otimes V_n\big[[\sigma_n, \tau_n]\big]$, and (24) may be confirmed via induction on n, using (21) and the well-known formula $\det(A \otimes B) = (\det A)^b (\det B)^a$ valid for square matrices A and B, of orders a and b, respectively (cf. [17]). □

4.2. **Explicit optimal testing sets.** Recall the concepts of *k-replacement* and *(proper) k-embedding* of Definition 3.

Theorem 12. *Let $\mathcal{P}_\mathcal{B}$ be a subspace of $k[x]$ with monomial basis $\mathcal{B} \subseteq \mathcal{M}$. Suppose that k satisfies $|k| \geqslant \max_{i \in [n]}(|\mathcal{B}_i| + \operatorname{sign} \min \mathcal{B}_i)$ and consider the following prescribed properties of a k-replacement $\mathcal{X}_\mathcal{B}^{\mathrm{var}} \to k$, $x_{ij} \rightsquigarrow \overline{x}_{ij}$:*

(a) If $\min \mathcal{B}_i > 0$, then $\overline{x}_{it} \neq 0$ for all $t \in \mathcal{B}_i$, and all $i \in [n]$;
(b) If $\theta_{it} > \theta_{i0}$, then $\overline{x}_{it} \neq 0$, for all $i \in [n]$.

If $\mathcal{B}$ is a σ-lower grid (resp., τ-upper grid), there exists a proper k^n-embedding $\mathcal{X}_\mathcal{B} \to k^n$ satisfying (a) (resp., (b)), and the image $\overline{\mathcal{X}}_\mathcal{B} \subseteq k^n$ of any such proper k^n-embedding is an optimal $\mathcal{P}_\mathcal{B}$-testing set.

Proof. In the σ-lower grid case we only have to make sure that k is large enough to accommodate a k-replacement of $\mathcal{X}^{\mathrm{var}}_{\mathcal{B}}$ that does not annihilate the prime factors $(x_{iw}-x_{iu})$ and x_{it} occurring in the expression (19). For a fixed i, we have two cases. In case $\sigma_i(=\min \mathcal{B}_i)=0$ we only have to fulfill the conditions $\overline{x}_{iw}-\overline{x}_{iu}\neq 0$, for $u<w\in\mathcal{B}_i$; so it is enough to have $|k|\geqslant|\mathcal{B}_i|$. In case $\sigma_i>0$, we also have to satisfy $\overline{x}_{it}\neq 0$ for all $t\in\mathcal{B}_i$; for this purpose $|k|\geqslant|\mathcal{B}_i|+1$ is enough. Thus the desired k-replacement exists if $|k|\geqslant\max_{i\in[n]}(|\mathcal{B}_i|+\operatorname{sign}\min\mathcal{B}_i)$.

Suppose $\mathcal{B}$ is a τ-upper grid. Note that x_{i0} is *not* a prime factor of (19). For a fixed i, $|k|\geqslant|\mathcal{B}_i|$ is enough to fulfill the conditions $\overline{x}_{iw}-\overline{x}_{iu}\neq 0$, for $u<w\in\mathcal{B}_i$. In case $\min\mathcal{B}_i=0$, it is enough to have $|k|\geqslant|\mathcal{B}_i|$ to fulfill the previous and the further conditions $\overline{x}_{it}\neq 0$, by letting $\overline{x}_{i0}=0$. In case $\min\mathcal{B}_i>0$, we must have $\overline{x}_{it}\neq 0$ for all $T\in\mathcal{B}_i$; so $|k|\geqslant|\mathcal{B}_i|+1$ is enough for that purpose. Therefore our theorem follows from Theorem 10. □

5. Optimal testing sets over finite fields

In this section k is a finite field, also denoted $\mathbb{F}_q$ to highlight the cardinality $|k|=q$. The concept of testing set is related with polynomial functions rather than with polynomials defined as formal expressions. The mapping $\Phi: k[x]\to k^{k^n}$ that transforms a polynomial f into the polynomial function $\xi\rightsquigarrow f(\xi)$ is a homomorphism of k-algebras. The kernel of Φ is the ideal of vanishing polynomials. The following facts are well-known (check [6], [8] and the excellent survey [18]). The Fermat Little Theorem tells that x_i^q and x_i produce the same polynomial function, in other words $x_i^q-x_i$ lies in $\ker\Phi$. As a matter of fact, $\ker\Phi$ is generated by the polynomials $x_i^q-x_i$ for $i\in\{1,\dots,n\}$. So, for positive integers a and b, the monomials x_i^a and x_i^b produce the same polynomial function if and only if $a\equiv b \mod (q-1)$. A polynomial is said to be a *reduced polynomial* whenever the degrees in each variable are all $<q$. Thus any polynomial is equivalent modulo $\ker\Phi$ to a reduced polynomial. Moreover, the set $\mathcal{R}$ of all reduced polynomials is a vector subspace of $k[x]$, and we have

$$k[x]=\mathcal{R}\oplus\ker\Phi.$$

A fundamental fact is that any member of k^{k^n} is a polynomial function. As a consequence $\mathcal{R}$, k^{k^n} and $k[x]/\ker\Phi$ are isomorphic k-spaces; so we may identify a reduced polynomial with the corresponding polynomial function. The *reduction* of a set $\mathcal{P}$ of polynomials, denoted $\mathcal{P}_{\mathrm{red}}$, is the set of polynomial functions (or reduced polynomials) afforded by the elements of $\mathcal{P}$. If $\mathcal{P}$ is a vector space then $\mathcal{P}_{\mathrm{red}}$ is a vector space as well, and $\dim\mathcal{P}_{\mathrm{red}}\leqslant\dim\mathcal{P}$. If $\mathcal{P}$ is a monomial space with monomial basis $\mathcal{B}$, then $\mathcal{B}_{\mathrm{red}}$ is a monomial basis of $\mathcal{P}_{\mathrm{red}}$, in other words $(\mathcal{P}_{\mathcal{B}})_{\mathrm{red}}=\mathcal{P}_{\mathcal{B}_{\mathrm{red}}}$.

We know that the cardinality of an optimal $\mathcal{P}$-testing set equals $\dim\mathcal{P}_{\mathrm{red}}$. So one may wonder why in Theorems 4 and 12 the cardinality of the optimal $\mathcal{P}$-testing sets equal $\dim\mathcal{P}$. The reason is that if the field is large enough with respect to $\mathcal{B}$, $\mathcal{P}_{\mathcal{B}}$ and $\mathcal{P}_{\mathcal{B}_{\mathrm{red}}}$ are isomorphic. More precisely:

Proposition 13. *Consider the following conditions involving a field $k=\mathbb{F}_q$ and a grid $\mathcal{B}$:*
(a) $|k|\geqslant\max_{i\in[n]}(|\mathcal{B}_i|+\operatorname{sign}\min\mathcal{B}_i)$;
(b) $\dim\mathcal{P}_{\mathcal{B}}=\dim\mathcal{P}_{\mathcal{B}_{\mathrm{red}}}$.
Then (a) implies (b). If $\mathcal{B}$ is a σ-lower grid or a τ-upper grid, then (a) and (b) are equivalent.

Proof. (a) $\Rightarrow$ (b). Suppose (b) is false, i.e. $|\mathcal{B}|>|\mathcal{B}_{\mathrm{red}}|$. There exist $\alpha,\beta\in\mathcal{B}$, such that $\alpha\neq\beta$ and $(x^\alpha)_{\mathrm{red}}=(x^\beta)_{\mathrm{red}}$. So for some $i\in[n]$ we have $\alpha_i\neq\beta_i$ and $(x_i^{\alpha_i})_{\mathrm{red}}=(x_i^{\beta_i})_{\mathrm{red}}$. We may assume $0<\alpha_i<\beta_i$. By Little Fermat $\alpha_i\equiv\beta_i \mod (q-1)$; therefore $\beta_i-\alpha_i\geqslant q-1$ and $\beta_i\geqslant q$. In case $\min\mathcal{B}_i=0$, we get $0,\beta_i\in\mathcal{B}_i$, and so $q<|\mathcal{B}_i|$; in case $\min\mathcal{B}_i>0$, we get $q<|\mathcal{B}_i|+1$. In both cases, (a) is false.

(b) $\Rightarrow$ (a) *when $\mathcal{B}$ is a τ-upper grid.* Suppose that (a) is false. For some $i\in[n]$, $q<|\mathcal{B}_i|+\operatorname{sign}\min\mathcal{B}_i$. In case $\min\mathcal{B}_i=0$, we have $q<|\mathcal{B}_i|$; thus $q\in[0,\tau_i]=\mathcal{B}_i$; there exists $\alpha\in\mathcal{B}$ such that $\alpha_i=1$; define $\beta\in\mathbb{N}_0^n$ by $\beta_i=q$ and $\beta_s=\alpha_s$, for $s\neq i$; clearly $(x^\alpha)_{\mathrm{red}}=(x^\beta)_{\mathrm{red}}$; moreover $\beta\in\mathcal{B}$, because $\beta\in[\alpha,\tau]$; so (b) is false. In case $\min\mathcal{B}_i>0$, we have $q\leqslant|\mathcal{B}_i|$; there

exists $\alpha \in \mathcal{B}$ such that $\alpha_i = \min \mathcal{B}_i$. Define $\beta \in \mathbb{N}_0^n$ by $\beta_i = \alpha_i + q - 1$ and $\beta_s = \alpha_s$, for $s \neq i$. As in the previous case, we conclude that (b) is false.

We proved $(b) \Rightarrow (a)$ when $\mathcal{B}$ is a τ-upper grid. For a σ-lower grid the proof is similar. □

The affine group of $\mathcal{P}$. The *affine group* $\mathrm{Aff}_n(k)$ consists of the invertible mappings $\omega : k^n \to k^n$ of the form $\xi \rightsquigarrow \omega(\xi) = A\xi + b$, where $A = (a_{rs})$ is an $[n]$-square nonsingular k-matrix, and $b \in k^n$. Each such map gives rise to a reversible change of variables in $k[x]$; namely, any $f(x_1 \ldots, x_n) \in k[x]$ is mapped to $f_\omega \in k[x]$, given by

$$f_\omega(x_1, \ldots, x_n) = f(\omega(x)) = f\big(\textstyle\sum_i a_{1i}x_i + b_1, \ldots, \sum_i a_{ni}x_i + b_n\big).$$

Taking $b = 0$, we get the general linear group $\mathrm{GL}_n(k) \subseteq \mathrm{Aff}_n(k)$

Let $\mathcal{P}$ be a finite dimensional subspace of $k[x]$. An *affine automorphism of* $\mathcal{P}$ is a member $\omega \in \mathrm{Aff}_n(k)$ such that $f \in \mathcal{P}$ implies $f_\omega \in \mathcal{P}$. The *affine group of* $\mathcal{P}$, denoted $\mathrm{Aff}_\mathcal{P}$, is the set of all such automorphisms.

Lemma 14.

(A) *The image of a $\mathcal{P}$-testing set by an affine automorphism of $\mathcal{P}$ is a $\mathcal{P}$-testing set.*

(B) *The affine group of $\mathcal{P}$ is a subgroup of the affine group of $\mathcal{P}_{\mathrm{red}}$.*

(C) *With the above notation, f and f_ω have the same degree.*

(D) *The whole $\mathrm{Aff}_n(k)$ is the affine group of both the space $k[x]^{\leqslant d}$ and its reduction.*

(E) *For a positive d, $\mathrm{GL}_n(k)$ is the affine group of both $\mathcal{H}_d$ and its reduction.*

Proof. (A) Choose any $\mathcal{P}$-testing set T. For any $f \in \mathcal{P}$ and $\omega \in \mathrm{Aff}_\mathcal{P}$, suppose $f(\omega(T)) = \{0\}$. We have $f_\omega \in \mathcal{P}$ and $f_\omega(T) = \{0\}$. As T is a $\mathcal{P}$-testing set, $f_\omega(k^n) = \{0\}$. Therefore $f(k^n) = \{0\}$. This shows $\omega(T)$ is a $\mathcal{P}$-testing set.

(B) Let $\omega \in \mathrm{Aff}_\mathcal{P}$ and $\rho \in \mathcal{P}_{\mathrm{red}}$. Then $\rho = f_{\mathrm{red}}$ for some $f \in \mathcal{P}$. We have $f_\omega \in \mathcal{P}$. The equation $\rho = f_{\mathrm{red}}$ means that, *as functionals* $k^n \to k$, ρ and f coincide. Thus $\rho \circ \omega$ and $f \circ \omega$ coincide. Therefore $\rho_\omega \in \mathcal{P}_{\mathrm{red}}$, and we finally have $\rho_\omega \in \mathrm{Aff}_{\mathcal{P}_{\mathrm{red}}}$.

(C) We obviously have $\deg f_\omega \leqslant \deg f$. Therefore, $\deg f = \deg f_{\omega\omega^{-1}} \leqslant \deg f_\omega \leqslant \deg f$.

(D) is an obvious consequence of (B) and (C).

(E) From (B) and (C) we get $\mathrm{GL}_n(k) \subseteq \mathrm{Aff}_{\mathcal{H}_d} \subseteq \mathrm{Aff}_{\mathcal{H}_{d,\mathrm{red}}}$. So we only need to prove that no translation $\tau : x \rightsquigarrow x + b$ by a nonzero $b \in k^n$ lies in $\mathrm{Aff}_{\mathcal{H}_{d,\mathrm{red}}}$. To check this, note that $b_s \neq 0$ for some $s \in [n]$. The monomial x_s^d lies in $\mathcal{H}_d$ and its reduction is $x_s^e \in \mathcal{H}_{d,\mathrm{red}}$, where e is a positive exponent. τ maps the homogeneous monomial x_s^e to the non-homogeneous polynomial $(x_s + b_s)^e = x_s^e + \cdots + b_s^e$. As $\mathcal{H}_d$ is a monomial space $\mathcal{H}_{d,\mathrm{red}}$ is monomial as well. So all monomials in the expansion of $(x_s + b_s)^e$ lie in $\mathcal{H}_{d,\mathrm{red}}$, in particular the nonzero constant b_s^e. However all monomials of $\mathcal{H}_{d,\mathrm{red}}$ have positive degrees. So τ does not lie in $\mathrm{Aff}_{\mathcal{H}_{d,\mathrm{red}}}$. □

The examples to follow are relevant to Coding Theory. So we borrow some concepts and language from that area (e.g. [8, 4, 23]). The *code* determined by a subspace $\mathcal{P} \subseteq k[x]$, denoted $\mathsf{C}_\mathcal{P}$, is the set of the q^n-tuples, the *codewords*,

$$\big(\varphi(t) : t \in k^n\big), \tag{25}$$

with φ running over $\mathcal{P}$. Up to isomorphism, $\mathsf{C}_\mathcal{P}$ is $\mathcal{P}_{\mathrm{red}}$. So $\mathsf{C}_\mathcal{P}$ is an evaluation code in the sense that the encoding of a "message" φ is obtained by evaluating a function at all points of a fixed finite set of points, the whole k^n in our case.

Thus the dimension of $\mathsf{C}_\mathcal{P}$ is $\dim \mathcal{P}_{\mathrm{red}}$. We may replace $\mathcal{P}$ with $\mathcal{P}_{\mathrm{red}}$, or else assume that $\mathcal{P}$ is a subspace of k^{k^n}; this only changes the formal indexation of the words, not the code itself. In case $\mathcal{P}$ is a monomial space with monomial basis $\mathcal{B}$, then the reduction $\mathcal{P}_{\mathrm{red}}$ is also a monomial space, whose monomial basis is the reduction $\mathcal{B}_{\mathrm{red}}$. We shall consider two relevant families of codes associated wth monomial spaces, namely the generalized Reed-Muller (GRM) codes and the Projective generalized Reed-Muller (PGRM) codes.

Generalized Reed-Muller codes. Let d be a positive integer. The *GRM code of order d* over the field $\mathbb{F}_q$, usually denoted by $\mathsf{C}_d(n,q)$, or $\mathsf{C}_{d,q}$ for short, is the code corresponding to $k[x]^{\leqslant d}$, the vector space of polynomials of degrees $\leqslant d$ (cf. [8, p. 409], [4, p. 71]), which has monomial basis

$$\mathcal{B}_d := \left\{ x_1^{i_1} \cdots x_n^{i_n} \,:\, i_1 + \cdots + i_n \leqslant d \right\}.$$

The monomial basis of $\mathsf{C}_{d,q}$ is therefore the set

$$\mathcal{B}_{d,\mathrm{red}} := \left\{ x_1^{i_1} \cdots x_n^{i_n} \,:\, i_1 + \cdots + i_n \leqslant d, \text{ and } 0 \leqslant i_s < q \text{ for all } s \right\}. \tag{26}$$

The dimension of $\mathsf{C}_{d,q}$ is thus the cardinality of (26). In [4, p. 72] the reader may find a proof of the following formula based on the inclusion-exclusion principle:

$$\dim \mathsf{C}_{d,q} = \sum_{s=0}^{n} (-1)^s \binom{n}{s} \sum_{i=0}^{d} \binom{i - sq + n - 1}{n-1}. \tag{27}$$

Therefore, this number is the cardinality of the optimal $k[x]^{\leqslant d}$-testing sets.

Corollary 15. *Take any k-replacement $\mathcal{X}^{\mathrm{var}}_{\mathcal{B}_{d,\mathrm{red}}} \to k$, $x_{ij} \mapsto \overline{x}_{ij}$, such that, for each $i \in [n]$, $\overline{x}_{i0}, \overline{x}_{i1}, \ldots, \overline{x}_{i,\min\{d,q-1\}}$ are pairwise distinct. Then the following subset of k^n*

$$T = \{(\overline{x}_{1\alpha_1}, \ldots, \overline{x}_{n\alpha_n}) \,:\, \alpha_1 + \cdots + \alpha_n \leqslant d, \text{ and } 0 \leqslant \alpha_s < q \text{ for all } s \in [n]\} \tag{28}$$

is an optimal $\mathsf{C}_d(n,q)$-testing set. The family of all sets T obtained from k-replacements as described is invariant under translations. For any such set T and any $\omega \in \mathrm{GL}_n(k)$, $\omega(T)$ is an optimal $\mathsf{C}_d(n,q)$-testing set.

Proof. The basis $\mathcal{B}_{d,\mathrm{red}}$ given by (26) is clearly a lower grid of $\mathbb{N}_0^n$. The projection of $\mathcal{B}_{d,\mathrm{red}}$ on the i-th coordinate is $(\mathcal{B}_{d,\mathrm{red}})_i = [0, \min\{d, q-1\}]$. Therefore the restriction imposed by Theorem 12 upon $|k| = q$ is satisfied, and property (a) of that theorem is vacuously true. Moreover, the conditions imposed on $\overline{x}_{i0}, \overline{x}_{i1}, \ldots, \overline{x}_{i,\min\{d,q-1\}}$ tell us that the given k-replacement induces a proper k^n-embedding $\mathcal{X}_{\mathcal{B}_{d,\mathrm{red}}} \to k^n$. So the first part of the corollary follows easily from Theorem 12.

The invariance under translations follows from the fact that the translate $T + v$, where $v = (v_i) \in k^n$, is obtained from the map $x_{ij} \rightsquigarrow \overline{x}_{ij} + v_i$, that is also a k-replacement inducing a proper k^n-embedding of $\mathcal{X}_{\mathcal{B}_{d,\mathrm{red}}}$. The assertion relative to $\omega(T)$ follows from Lemma 14(D). □

Projective Generalized Reed-Muller codes. For the case of the space $\mathcal{H}_d$, the d-th homogeneous component of the graded ring $k[x]$, we consider two closely related codes: the *affine* code $\mathsf{C}_{\mathcal{H}_d}$, with codewords as defined in (25), and the projective version of a GRM code as given in [23] under the notation $\mathsf{PC}_d(n,q)$. The monomial basis of $\mathcal{H}_d$ is the set of monomials of degree d; the monomial basis of $\mathcal{H}_{d,\mathrm{red}}$ is the reduction of the former basis, namely the set

$$\left\{ x_1^{i_1} \cdots x_n^{i_n} \,:\, \textstyle\sum_s i_s \leqslant d,\ \sum_s i_s \equiv d \mod (q-1), \text{ and } 0 \leqslant i_1, \ldots, i_n < q \right\}. \tag{29}$$

The dimension of $\mathsf{C}_{\mathcal{H}_d}$ is thus the cardinality of this set. This number has been determined in [23, Theorem 1] with the following outcome:

$$\dim \mathcal{H}_{d,\mathrm{red}} = \sum_{\substack{0 < t \leqslant d \\ t \equiv d \bmod (q-1)}} \sum_{j=0}^{n} (-1)^j \binom{n}{j} \binom{t - jq + n - 1}{n-1}.$$

So this number is the cardinality of the optimal $\mathcal{H}_d$-testing sets.

For the projective code $\mathsf{PC}_d(n,q)$ we start with the same space $\mathcal{H}_d$ but the evaluation process is different from that of $\mathsf{C}_{\mathcal{H}_d}$. While the latter evaluates homogeneous polynomials at the points of k^n, $\mathsf{PC}_d(n,q)$ evaluates those polynomials at the points of the projective space $\mathbb{P}^{n-1}(k)$. This is done by the usual embedding of $\mathbb{P}^{n-1}(k)$ into k^n, which consists in choosing a single representative from each point of $\mathbb{P}^{n-1}(k)$. This reduces the length of the code from q^n to

$(q^n-1)/(q-1)$, a drastic cut if $q \gg 2$. The matrix of the projective code $\mathsf{PC}_d(n,q)$, call it P, is obtained from the matrix A of the affine code $\mathsf{C}_{\mathcal{H}_d}$ after the following operations are performed: (i) the column of A indexed by the zero vector is eliminated; (ii) for each point $U \in \mathbb{P}^{n-1}(k)$, the $q-1$ columns of A indexed by the elements of U (that are pairwise proportional) are replaced by a chosen one of them. The column spaces of A and P are obviously the same. So the dimensions of the two codes are the same as well.

It is easy to check that if $T \subseteq k^n$ is an optimal $\mathcal{H}_d$-testing set, then all points of T are nonzero; moreover, replacing each point $t \in T$ by a proportional point $\lambda_t t$, $\lambda_t \neq 0$, the new set is also an optimal homogeneous d-testing set. So we may consider T as a subset of $\mathbb{P}^{n-1}(k)$ with no violation of the optimal testing property.

The set of the monomials with total degree d is the monomial basis of the space $\mathcal{H}_d$. For $n > 1$ and $d > 0$, that basis is neither a σ-lower set nor a σ-upper set. Thus, essentially, Theorem 12 does not apply to that case. We illustrate the expected difficulties with a simple example.

We consider the case $n = 2$, $d = 4$ over the field $\mathbb{F}_3 = \{0,1,2\}_{\bmod 3}$, and try to find an optimal $\mathcal{H}_4$-testing set in ${\mathbb{F}_3}^2$. The monomial basis of $\mathcal{H}_4$ is $\mathcal{B} = \{x_2^4, x_1x_2^3, x_1^2x_2^2, x_1^3x_2, x_1^4\}$. So the reduced basis is, in lexicographic order, $\mathcal{B}_{\mathrm{red}} = \{x_2^2,\, x_1x_2,\, x_1^2,\, x_1^2x_2^2\}$. Following the construction of Section 2, we get

$$\mathbb{V}[\mathcal{B}_{\mathrm{red}}] = \begin{bmatrix} x_{22}^2 & x_{21}^2 & x_{20}^2 & x_{22}^2 \\ x_{10}x_{22} & x_{11}x_{21} & x_{12}x_{20} & x_{12}x_{22} \\ x_{10}^2 & x_{11}^2 & x_{12}^2 & x_{12}^2 \\ x_{10}^2x_{22}^2 & x_{11}^2x_{21}^2 & x_{12}^2x_{20}^2 & x_{12}^2x_{22}^2 \end{bmatrix} = \begin{bmatrix} w^2 & v^2 & u^2 & w^2 \\ aw & bv & cu & cw \\ a^2 & b^2 & c^2 & c^2 \\ a^2w^2 & b^2v^2 & c^2u^2 & c^2w^2 \end{bmatrix},$$

where, for better readability, we have replaced the x_{ij} with non subscripted variables according to $(a,b,c) := (x_{10}, x_{11}, x_{12})$ and $(u,v,w) := (x_{20}, x_{21}, x_{22})$. According to an *ad hoc* computer program, the irreducible factorization of $\det \mathbb{V}[\mathcal{B}_{\mathrm{red}}]$ has the form $cw(a-c)(u-w)\cdot\varphi$, where the factor φ is given by:

$$\varphi = c^2bw^2v + cbaw^2v - cb^2wv^2 - c^2awv^2 - cb^2w^2u - b^2aw^2u + c^2bwvu + cbawvu - c^2av^2u + b^2av^2u.$$

Our problem now is to replace (a,b,c,u,v,w) in ${\mathbb{F}_3}^6$, so that $\det \mathbb{V}[\mathcal{B}_{\mathrm{red}}] \neq 0$. By brute force we determine that there are 24 distinct solutions to this problem, but the complexity of φ leaves us with no hint on a systematic way to determine such a solution, much less for higher values of the parameters q, n, d. However we may circumvent this inconvenience over the field $\mathbb{F}_2$.

The case of the two-element field. Recall from the Introduction that R. Livné's result [19, Theorem 4.3, p. 256] involves, among other ingredients, the identification of testing sets for the space $\mathcal{H}_3$ of cubic homogeneous polynomial functions over the field $k = \mathbb{F}_2$. Here we consider the general case $\mathcal{H}_d$ of any degree $d > 0$. In this case we have a simple way to get explicit (optimal) $\mathcal{H}_d$-testing sets. The monomial basis of $\mathcal{H}_{d,\mathrm{red}}$ as given in (29), is the set

$$\begin{aligned} \mathcal{S}_d &= \{x_1^{\alpha_1}\cdots x_n^{\alpha_n} : \alpha_i \in \{0,1\},\ 0 < \textstyle\sum_s \alpha_s \leqslant d\} \\ &= \{x_{i_1}\cdots x_{i_s} : 1 \leqslant i_1 < \cdots < i_s \leqslant n,\ 1 \leqslant s \leqslant d\}. \end{aligned}$$

Clearly, over $\mathbb{F}_2$, $\mathcal{H}_{d-1,\mathrm{red}} \subset \mathcal{H}_{d,\mathrm{red}} \subset \mathsf{C}_{d,2}$. So a testing set for $\mathsf{C}_{d,2}$ (resp., $\mathcal{H}_{d,\mathrm{red}}$) is a testing set for any $\mathcal{H}_{e,\mathrm{red}}$ for any $e \leqslant d$. Besides, note that $1 \notin \mathcal{S}_d$ (recall 1 is the monomial represented by $(0,\ldots,0) \in \mathbb{N}_0^n$). On the other hand, according to (26), the monomial basis of $\mathsf{C}_{d,2}$ is $\mathcal{S}_d \cup \{1\}$. This situation is the object of the following simple result.

Proposition 16. *For any field k and any finite set $\mathcal{S}$ of monomials such that $1 \notin \mathcal{S}$, we have: $U \subseteq k^n$ is a $\mathcal{P}_{\mathcal{S}}$-testing set if and only if $U \cup \{0\}$ is a $\mathcal{P}_{\mathcal{S}\cup\{1\}}$-testing set. This is also true when the expression "testing set" is replaced with "optimal testing set".*

Proof. Let U be a $\mathcal{P}_{\mathcal{S}}$-testing set, and assume $\psi \in \mathcal{P}_{\mathcal{S}\cup\{1\}}$ vanishes on $U\cup\{0\}$; then ψ vanishes on U and, as $\psi(0)=0$, ψ lies in $\mathcal{P}_{\mathcal{S}}$; so ψ vanishes on k^n. Conversely let $U\cup\{0\}$ be a $\mathcal{P}_{\mathcal{S}\cup\{1\}}$-testing set, and assume $\psi \in \mathcal{P}_{\mathcal{S}}$ vanishes on U; as $1 \notin \mathcal{S}$, ψ vanishes on $U\cup\{0\}$; so ψ vanishes on k^n. The claim concerning optimal testing sets is easily proved arguing with cardinalities of reduced bases. In fact, $(\mathcal{S}\cup\{1\})_{\mathrm{red}} = \mathcal{S}_{\mathrm{red}}\cup\{1\}$; therefore, as no member of $\mathcal{S}$ has reduced form 1, we have $|(\mathcal{S}\cup\{1\})_{\mathrm{red}}| = |\mathcal{S}_{\mathrm{red}}| + 1$. The rest is easy. □

In the case $k=\mathbb{F}_2$ we give a neat form to Corollary 15 and get a nice family of optimal testing sets for homogeneous polynomials.

Theorem 17. *Let T_d be the set of those members of $\mathbb{F}_2^n$ that have at most d entries equal to 1. For any $\omega \in \mathrm{Aff}_n(\mathbb{F}_2)$, $\omega(T_d)$ is an optimal testing set for polynomials over $\mathbb{F}_2$ of degrees $\leqslant d$, as well as a testing set for homogeneous polynomials over $\mathbb{F}_2$ of degree d.*

For any $v \in T_d$, and any $\omega \in \mathrm{GL}_n(\mathbb{F}_2)$, the set $\omega(v+T_d)\smallsetminus\{0\}$ is an optimal testing set for homogeneous polynomials over $\mathbb{F}_2$ of degree d.

Proof. The only restriction Corollary 15 puts on the $\mathbb{F}_2$-replacement is $\{\overline{x}_{i0},\overline{x}_{i1}\}=\{0,1\}$, i.e. $\overline{x}_{i1}=\overline{x}_{i0}+1$. We choose $(\overline{x}_{10},\dots,\overline{x}_{n0})$ arbitrarily in $\mathbb{F}_2^n$. As $q=2$ the integers α_i in (28) all lie in $\{0,1\}$. We shall view $\alpha=(\alpha_1,\dots,\alpha_n)$ also as a member of $\mathbb{F}_2^n$. If $\alpha_i=0$, then $\overline{x}_{i\alpha_i}=\overline{x}_{i0}$; if $\alpha_i=1$, then $\overline{x}_{i\alpha_i}=\overline{x}_{i1}=\overline{x}_{i0}+1$. Therefore

$$(\overline{x}_{1\alpha_1},\dots,\overline{x}_{n\alpha_n}) = (\overline{x}_{10},\dots,\overline{x}_{n0})+\alpha.$$

In (28) α runs over T_d. So in case $q=2$ the set (28) is $(\overline{x}_{10},\dots,\overline{x}_{n0})+T_d$, which is, by Corollary 15, an optimal testing set for $\mathbb{F}_2$-polynomials of degrees $\leqslant d$.

The first claim of our theorem now follows from Corollary 15 and Proposition 16. Thus, for any $v\in T_d$, the set $v+T_d$ is an optimal $\mathsf{C}_{d,2}$-testing set and $0\in v+T_d$; so Proposition 16 tells that $(v+T_d)\smallsetminus\{0\}$ is an optimal $\mathcal{H}_d$-testing set, and Lemma 14(E) does the rest. □

References

[1] Erhard Aichinger, Simon Grünbacher, and Paul Hametner. Zero testing and equation solving for sparse polynomials on rectangular domains. *Finite Fields Appl.*, 95:Paper No. 102379, 17, 2024.

[2] N. Alon and M. Tarsi. Colorings and orientations of graphs. *Combinatorica*, 12(2):125–134, 1992.

[3] Noga Alon. Combinatorial Nullstellensatz. volume 8, pages 7–29. 1999. Recent trends in combinatorics (Mátraháza, 1995).

[4] Ian F. Blake and Ronald C. Mullin. *The mathematical theory of coding.* Academic Press [Harcourt Brace Jovanovich, Publishers], New York-London, 1975.

[5] Sergio Caracciolo, Alan D. Sokal, and Andrea Sportiello. Algebraic/combinatorial proofs of Cayley-type identities for derivatives of determinants and Pfaffians. *Adv. in Appl. Math.*, 50(4):474–594, 2013.

[6] C. Chevalley. Démonstration d'une hypothèse de M. Artin. *Abh. Math. Sem. Univ. Hamburg*, 11(1):73–75, 1935.

[7] Michael Clausen, Andreas Dress, Johannes Grabmeier, and Marek Karpinski. On zero-testing and interpolation of k-sparse multivariate polynomials over finite fields. *Theoret. Comput. Sci.*, 84(2, Algorithms Automat. Complexity Games):151–164, 1991.

[8] P. Delsarte, J.-M. Goethals, and F. J. MacWilliams. On generalized Reed-Muller codes and their relatives. *Information and Control*, 16:403–442, 1970.

[9] Luis Dieulefait, Lucio Guerberoff, and Ariel Pacetti. Proving modularity for a given elliptic curve over an imaginary quadratic field. *Math. Comp.*, 79(270):1145–1170, 2010.

[10] Nira Dyn and Michael S. Floater. Multivariate polynomial interpolation on lower sets. *J. Approx. Theory*, 177:34–42, 2014.

[11] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983.

[12] Mariano Gasca and Thomas Sauer. Polynomial interpolation in several variables. volume 12, pages 377–410. 2000. Multivariate polynomial interpolation.

[13] Gene H. Golub and Charles F. Van Loan. *Matrix computations.* Johns Hopkins Studies in the Mathematical Sciences. Johns Hopkins University Press, Baltimore, MD, third edition, 1996.

[14] Alexey L. Gorodentsev. *Algebra. II. Textbook for students of mathematics*. Springer, Cham, 2017. Originally published in Russian, 2015.
[15] Loïc Grenié. Comparison of semi-simplifications of Galois representations. *J. Algebra*, 316(2):608–618, 2007.
[16] Dima Yu. Grigoriev, Marek Karpinski, and Michael F. Singer. Fast parallel algorithms for sparse multivariate polynomial interpolation over finite fields. *SIAM J. Comput.*, 19(6):1059–1063, 1990.
[17] Harold V. Henderson, Friedrich Pukelsheim, and Shayle R. Searle. On the history of the Kronecker product. *Linear and Multilinear Algebra*, 14(2):113–120, 1983.
[18] Jean-René Joly. Équations et variétés algébriques sur un corps fini. *Enseign. Math. (2)*, 19:1–117, 1973.
[19] Ron Livné. Cubic exponential sums and Galois representations. In *Current trends in arithmetical algebraic geometry (Arcata, Calif., 1985)*, volume 67 of *Contemp. Math.*, pages 247–261. Amer. Math. Soc., Providence, RI, 1987.
[20] Thomas Sauer. Lagrange interpolation on subgrids of tensor product grids. *Math. Comp.*, 73(245):181–190, 2004.
[21] Thomas Sauer. Polynomial interpolation in several variables: lattices, differences, and ideals. In *Topics in multivariate approximation and interpolation*, volume 12 of *Stud. Comput. Math.*, pages 191–230. Elsevier B. V., Amsterdam, 2006.
[22] Jean-Pierre Serre. Résumé des cours de 1984-1985. *Annuaire du Collège de France*, pages 85–90, 1985.
[23] Anders Bjært Sørensen. Projective Reed-Muller codes. *IEEE Trans. Inform. Theory*, 37(6):1567–1576, 1991.

CMUC, Department of Mathematics, University of Coimbra, 3000-143 Coimbra, Portugal
Email address: emsa@mat.uc.pt