Applicable Algebra in Engineering, Communication and Computing (2024) 35:71–118
https://doi.org/10.1007/s00200-023-00619-1

ORIGINAL PAPER

Exploring implications of Trace (Inversion) formula and Artin algebras in extremal combinatorics

Luis M. Pardo[1]

Received: 14 October 2022 / Accepted: 11 July 2023 / Published online: 13 August 2023

Abstract

This note is just a modest contribution to prove several classical results in Combinatorics from notions of Duality in some Artinian K-algebras (mainly through the Trace Formula), where K is a perfect field of characteristics not equal to 2. We prove how several classic combinatorial results are particular instances of a Trace (Inversion) Formula in finite $\mathbb{Q}$-algebras. This is the case with the Exclusion-Inclusion Principle (in its general form, both with direct and reverse order associated to subsets inclusion). This approach also allows us to exhibit a basis of the space of null t-designs, which differs from the one described in Theorem 4 of Deza and Frankl (Combinatorica 2:341–345, 1982). Provoked by the elegant proof (which uses no induction) in Frankl and Pach (Eur J Comb 4:21–23, 1983) of the Sauer–Shelah–Perles Lemma, we produce a new one based only in duality in the $\mathbb{Q}$-algebra $\mathbb{Q}[V_n]$ of polynomials functions defined on the zero-dimensional algebraic variety of subsets of the set $[n] := \{1, 2, \ldots, n\}$. All results are equally true if we replace $\mathbb{Q}[V_n]$ by $K[V_n]$, where K is any perfect field of characteristics $\neq 2$. The article connects results from two fields of mathematical knowledge that are not usually connected, at least not in this form. Thus, we decided to write the manuscript in a self-contained survey-like style, although it is not a survey paper at all. Readers familiar with Commutative Algebra probably know most of the proofs of the statements described in section 2. We decided to include these proofs for those potential readers not so familiar with this framework.

Keywords Zero-dimensional algebras · Trace Inversion formula · VC dimension · Sauer–Shelah–Perles Lemma

✉ Luis M. Pardo
luis.m.pardo@gmail.com; luis.pardo@unican.es

[1] Depto. de Matemáticas, Estadística y Computación, Facultad de Ciencias, Universidad de Cantabria, Avda. Los Castros, s/n, 39071 Santander, Cantabria, Spain

1 Introduction and summary of the main outcomes

In words of M.F. Atiyah, *Duality in mathematics is not a theorem, but a "principle"*. The present manuscript deepens in this direction by showing various classical results of extremal Combinatorics as particular cases of duality-related properties in some Artinian K-algebras. The manuscript does not pretend to give new results but rather to contextualize (by new proofs) some known results in a framework of duality. Our main outcomes were motivated and inspired by the proof of the Sauer–Shelah–Perles Lemma done in [12]. We may summarize these pages by saying: *As other classical results of Combinatorics, Frankl-Pach proof of Sauer–Shelah–Perles Lemma may be rewritten as a duality result within the context of finite K-algebras*. We do not aim to give simpler proofs but to explore how this kind of statements may be naturally embedded in the more abstract context of duality and trace in zero-dimensional K-algebras. We have tried to be as self-contained as possible, exhibiting self-contained proofs, with detailed descriptions of every argument. We just assume that the reader is familiar with elementary contents of Commutative Algebra such as the first two chapters of the classical [4], for instance.

Besides, this manuscript also pretends to be just another contribution to what was called *"The Polynomial Method"* in [26] (originated in [10] or [2], see also [23] and references therein). This term encompasses all those new theorems or new proofs (of eventually known results) in Combinatorics by using multivariate polynomials (and their properties) as the main argument. Here, we contribute with a modest "polynomial method" new proof of the famous Sauer–Shelah–Perles Lemma, introduced by Sauer ([24]) and Shelah ([25], who also gave credit to M. Perles).

Finally, there is a third motivation to write this more abstract approach to the topic. Many practitioners of Computational Learning usually claim that both the notion of VC-dimension and the bounds provided by Sauer–Shelah–Perles's Lemma are somehow excessive for their practical learning algorithms: they may achieve good results with less sample points than those provided by these notions and statements. We believe that a revision of the foundational bounds of computational learning is required. Of course, approaches based on alternatives to VC-dimension (as the separation bounds in [14], the teaching dimension in [16] and its references or the notions of dimension for multi-class learning as in [7] and references therein) are of great relevance. Our manuscript strongly differs from the approach from elementary Commutative Algebra to Sauer–Shelah–Perles Lemma done in [20], where Hilbert function is emphasized. For the moment, this manuscript just contributes by adding a bit more of abstraction to prove upper bounds to the growth function, expecting that this may shed some more light to the topic in future research.

The terms duality and trace here may be introduced in the following terms. Let K be a perfect field of characteristics $\neq 2$ and A an Artinian (also finite) K-algebra (i.e. a K-algebra which is a K-vector space of finite dimension). Classically, elements in A have Trace and Norm (see Definition 2), defined through the multiplication K-endomorphism they define on A. This yields a symmetric bilinear form:

$$\begin{array}{rccc} \mathrm{Tr}_{A} : & A\times A & \longrightarrow & K \\ & (x,y) & \longmapsto & Tr(xy), \end{array}$$

where $Tr(xy)$ is the classical trace of the element $xy \in A$. We focus on the case where $A = K[W]$ is the ring of polynomial functions with values in K on a zero-dimensional K-rational algebraic set W (i.e. when $W \subseteq K^n$). In this case, the trace is a non-degenerate symmetric bilinear form determined by the points of W (see Sect. 2 for details). Note that this trace differs from the trace discussed in [11].

As W is a K-rational zero-dimensional algebraic set, we have that $K[W] = K^W$ (i.e. every function with range in K is a polynomial function) and, additionally, due to the Chinese Remainder Theorem, we have:

$$\dim_K(K[W]) = \deg(W) = \sharp(W),$$

where $\deg(W)$ is the degree of W (see [15], for instance). In particular, every basis $\mathscr{B}$ of $K[W]$ may be indexed by W. Namely, if $\mathscr{B} \subseteq K[W]$ is a basis of $K[W]$ as K-vector space, the elements of $\mathscr{B}$ may be described as:

$$\mathscr{B} := \{v_x \ : \ x \in W\}.$$

A dual basis of $\mathscr{B}$ with respect to the trace is any basis $\mathscr{B}^* := \{w_y \ : \ y \in W\}$, such that

$$\mathrm{Tr}_{K[W]}(v_x, w_y) = \delta_{x,y},$$

where $\delta_{x,y}$ is Kronecker's delta function with indices in W. We prove that when W is K-rational, every basis $\mathscr{B}$ of $K[W]$ admits a dual basis with respect to this trace (an elementary proof is exhibited in Proposition 6).

Given a basis $\mathscr{B} := \{v_x \ : \ x \in W\}$ of $K[W]$ and a polynomial function $f \in K[W]$, we define the dual transform of f with respect to the basis $\mathscr{B}$ as the polynomial function $f^*_{\mathscr{B}} \in K[W]$ given by the following identity:

$$f^*_{\mathscr{B}}(x) := \mathrm{Tr}_{K[W]}(f, v_x) \in K, \ \forall x \in W.$$

Note that this dual transform is simply the (polynomial) function that describes the coefficients of f with respect to a dual basis of $\mathscr{B}$, provided that such a dual basis exists. This is described by our Trace (Inversion) Formula (2.7): Assuming a basis $\mathscr{B}$ as above and a basis $\mathscr{B}^* := \{v^*_y \ : \ y \in W\}$ dual to $\mathscr{B}$ with respect to the trace, the following equality holds:

$$f = \sum_{x\in W} f^*_{\mathscr{B}}(x) v^*_x, \tag{1.1}$$

Namely, for every $z \in W$ we have the *Trace (Inversion) Formula*:

$$f(z) = \sum_{x\in W} f^*_{\mathscr{B}}(x) v^*_x(z) = \sum_{x\in W} \mathrm{Tr}_{K[W]}(f, v_x) v^*_x(z). \tag{1.2}$$

We call it Trace (Inversion) Formula because at some of our applications this Trace Formula behaves like Möbius Inversion Formula. This Formula immediately follows from the existence of dual basis with respect to this trace and we then see how this is linked to Combinatorics.

Let $[n] := \{1, \ldots, n\}$ be a finite set with n elements, $2^{[n]}$ be the set of all its subsets and define the zero-dimensional $\mathbb{Q}$-rational algebraic set:

$$V_n := \{(x_1, \ldots, x_n) \in \mathbb{Q}^n \ : \ x_i^2 - x_i = 0, \ 1 \leq i \leq n\}.$$

Now, we consider the $\mathbb{Q}$-algebra $\mathbb{Q}[V_n]$ of polynomial functions defined in V_n with values in $\mathbb{Q}$. We have chosen $\mathbb{Q}$ for simplicity, but all our results equally hold for $K[V_n]$ where K is any perfect field of characteristics different to 2. We also consider the ideal

$$I(V_n) := \{f \in \mathbb{Q}[X_1, \ldots, X_n] \ : \ f(V_n) = 0\} = (X_1^2 - X_1, \ldots, X_n^2 - X_n),$$

and we have the classical identification $\mathbb{Q}[V_n] := \mathbb{Q}[X_1, \ldots, X_n]/I(V_n)$. As V_n is finite we obviously have $\mathbb{Q}[V_n] = \mathbb{Q}^{V_n}$.

The reader immediately observes that $V_n = 2^{[n]}$ and, hence, we may denote with similar symbols the elements $Y \in V_n$ and the subsets $Y \subseteq [n]$. From our hypothesis, the trace $\mathrm{Tr}_n := \mathrm{Tr}_{\mathbb{Q}[V_n]}$ is a non-degenerate symmetric bilinear form defined on $\mathbb{Q}[V_n] \times \mathbb{Q}[V_n]$.

In these pages we study some bases of $\mathbb{Q}[V_n]$ as $\mathbb{Q}$-vector space:

- *The monomial basis*, which is denoted in the following form: For every subset $S \in 2^{[n]}$ we consider the monomial

  $$P_S(X_1, \ldots, X_n) := \prod_{i \in S} X_i \in \mathbb{Q}[X_1, \ldots, X_n],$$

  where $\mathbb{Q}[X_1, \ldots, X_n]$ is the ring of polynomials in n variables with coefficients in $\mathbb{Q}$. This monomial defines a polynomial function $p_S : V_n \longrightarrow \mathbb{Q}$ under the usual rule $p_S := P_S + I(V_n)$. Then, the following is a well-known basis of $\mathbb{Q}[V_n]$ as $\mathbb{Q}$-vector space:

  $$\mathscr{B}_1 := \{p_S \ : \ S \subseteq [n]\} \subseteq \mathbb{Q}[V_n].$$

- *The Anti-monomial basis,* For every subset $S \in 2^{[n]}$ we consider the multivariate polynomial

  $$Q_S := \prod_{i \in [n] \setminus S} (1 - X_i) \in \mathbb{Q}[X_1, \ldots, X_n],$$

  where $[n] \setminus S$ is the complement of S in $[n]$. Each of these polynomials defines a polynomial function $q_S : V_n \longrightarrow \mathbb{Q}$ that, as usual, corresponds to $q_S := Q_S + I(V_n) \in \mathbb{Q}[V_n]$. The following is also a basis of $\mathbb{Q}[V_n]$ as $\mathbb{Q}$-vector space:

$$\mathscr{B}_2 := \{q_S \ : \ S \subseteq [n]\} \subseteq \mathbb{Q}[V_n].$$

Dual basis $\mathscr{B}_1^* := \{p_S^* \ : \ S \subseteq [n]\}$ and $\mathscr{B}_2^* := \{q_S^* \ : \ S \subseteq [n]\}$, respectively to $\mathscr{B}_1$ and $\mathscr{B}_2$, are exhibited in Propositions 11 and 13, as applications of the method to compute dual basis described in Sect. 2.3. Once we have computed these dual bases, we are in a position to prove that various classical Combinatorial results are simply particular instances of the Trace (Inversion) Formula (1.2) above.

(i) In Corollary 12 we prove that the Trace (Inversion) Formula described in (1.2) applied to the basis $\mathscr{B}_1$ and its dual $\mathscr{B}_1^*$ becomes the classical identity known as general form of the Inclusion–exclusion Principle (in a reverse order form). Namely, equality (1.2) becomes something that seems to resemble Möbius Inversion Formula:

For every $Y \subseteq [n]$ and for every $f \in \mathbb{Q}[V_n]$, we have:

$$f(Y) := \sum_{Y \subseteq S} (-1)^{\sharp(S\setminus Y)} f^*_{\mathscr{B}_1}(S) = \sum_{Y \subseteq S} (-1)^{\sharp(S\setminus Y)} \left(\sum_{S \subseteq T} f(T) \right)$$

(ii) In Corollary 14 we prove that the Trace (Inversion) Formula described in (1.2) applied to the basis $\mathscr{B}_2$ and its dual $\mathscr{B}_2^*$ becomes the general form of the Inclusion-exclusion Principle. Namely, equality (1.2) becomes:

For every $Y \subseteq [n]$ and for every $f \in \mathbb{Q}[V_n]$, we have:

$$f(Y) := \sum_{S \subseteq Y} (-1)^{\sharp(Y\setminus S)} f^*_{\mathscr{B}_2}(S) = \sum_{S \subseteq Y} (-1)^{\sharp(Y\setminus S)} \left(\sum_{T \subseteq S} f(T) \right).$$

(iii) Besides, we prove in Proposition 15 that the following is a basis of the $\mathbb{Q}$-vector space of null t-designs associated to $[n]$ (as defined in [12]):

$$P_t^* := \{p_F^* \ : \ F \subseteq [n], \sharp(F) > t\}.$$

Observe that this is naturally a subset of the dual basis $\mathscr{B}_1^*$ of the monomial basis $\mathscr{B}_1$. Moreover, this basis differs from the one cited in [12] as described in Theorem 4 of [9].

Nevertheless, our main motivation was to prove Sauer–Shelah–Perles Lemma from duality techniques. We turn back to the family of polynomials forming the basis $\mathscr{B}_2$. These polynomials are strongly rich in information. Before all, we consider a simpler form of the upper bound in that classical Lemma. Let $\mathscr{F} \subseteq 2^{[n]}$ be a class of subsets of $[n]$ and consider the class of polynomial functions

$$Q_{\mathscr{F}} := \{q_F \ : \ F \in \mathscr{F}\} \subseteq \mathbb{Q}[V_n]. \tag{1.3}$$

The set V_n is endowed with the Hamming distance $d_H : V_n \times V_n \longrightarrow \mathbb{R}$ and we distinguish the closed balls centered at the origin $\mathbf{0} \in V_n$ defined by this Hamming distance:

$$W_d := B_H(\mathbf{0}, d) := \{Y \in V_n \ : \ d_H(Y, \mathbf{0}) \le d\}.$$

We have the ascending chain of closed balls (and algebraic subsets) of V_n:

$$W_0 \subsetneq W_1 \subsetneq W_2 \subsetneq \cdots \subsetneq W_n.$$

As $Q_{\mathscr{F}}$ is a family of $\mathbb{Q}$- linearly independent functions, then its cardinality equals the cardinality of $\mathscr{F}$. Given $r \in \{0, \dots, n\}$, we may define the following class of restrictions to W_i of the polynomial functions in $Q_{\mathscr{F}}$:

$$Q_{\mathscr{F},i} := \{q_F \restriction_{W_i} \ : \ F \in \mathscr{F}\} \subseteq \mathbb{Q}[W_i].$$

Note that $Q_{\mathscr{F},n} = Q_{\mathscr{F}}$. For every $i \in [n]$, let us also consider the $\mathbb{Q}$-vector space $\mathbb{Q}\langle Q_{\mathscr{F},i}\rangle$ spanned by $Q_{\mathscr{F},i}$ in $\mathbb{Q}[W_i]$.

As $W_i \subseteq W_{i+1}$ we have an onto morphism of $\mathbb{Q}$-algebras: $i_r^* \ : \ \mathbb{Q}[W_{i+1}] \longrightarrow \mathbb{Q}[W_i]$, which is simply the restriction to W_i of the polynomial functions in $\mathbb{Q}[W_{i+1}]$. Thus, the following is an increasing sequence of dimensions:

$$\dim_{\mathbb{Q}}\left(\mathbb{Q}\langle Q_{\mathscr{F},i}\rangle\right) \le \dim_{\mathbb{Q}}\left(\mathbb{Q}\langle Q_{\mathscr{F},i+1}\rangle\right).$$

Then, it make sense to introduce the following notion:

Definition 1 (Rank VC-dimension) With these notations, we define the rank VC-dimension of $\mathscr{F}$ as the minimum r such that $Q_{\mathscr{F},r}$ is a $\mathbb{Q}$-linearly independent family of polynomial functions in $\mathbb{Q}[W_r]$. Namely, the minimum r such that

$$\dim_{\mathbb{Q}}\left(\mathbb{Q}\langle Q_{\mathscr{F},r}\rangle\right) = \dim_{\mathbb{Q}}\left(\mathbb{Q}\langle Q_{\mathscr{F},n}\rangle\right) = \sharp(\mathscr{F}).$$

We denote by $RVCD(\mathscr{F})$ this rank VC-dimension of $\mathscr{F}$.

The term rank is coined because *RVCD* is related to the rank of some matrices depending on the polynomial functions in $Q_{\mathscr{F}}$. In Lemma 28 we show that

$$RVCD(\mathscr{F}) := \min\{r \in \{0, \dots, n\} \ : \ \operatorname{rank}(M_{\mathscr{F},r}) = \sharp(\mathscr{F})\},$$

where $M_{\mathscr{F},r} \in \mathscr{M}_{N\times\delta(r)}(\mathbb{Q})$, $N = \sharp(\mathscr{F})$ and $\delta(r) = \sharp(W_r)$, is a matrix built from the family $Q_{\mathscr{F}}$ evaluated at the points $S \in W_r$ (see Sect. 5 for a precise description).

Since $\mathbb{Q}\langle Q_{\mathscr{F},i}\rangle$ is a vector subspace of $\mathbb{Q}[W_i]$, the following Corollary immediately follows from these definitions:

Corollary 1 *If* $r = RVCD(\mathscr{F})$, *then we have* $\sharp(\mathscr{F}) = \sharp(Q_{\mathscr{F},n}) = \dim_{\mathbb{Q}}\left(\mathbb{Q}\langle Q_{\mathscr{F},r}\rangle\right)$. *And, hence,*

$$\sharp(\mathscr{F}) = \dim_{\mathbb{Q}}\left(\mathbb{Q}\langle Q_{\mathscr{F},r}\rangle\right) \le \dim_{\mathbb{Q}}\left(\mathbb{Q}[W_r]\right) = \sharp\left(W_r\right) = \sum_{i=0}^{RVCD(\mathscr{F})} \binom{n}{i}.$$

We consider the principal ideal $\mathfrak{q}_Y := (q_Y) := \{fq_Y \ : \ f \in \mathbb{Q}[V_n]\} \subseteq \mathbb{Q}[V_n]$, generated by $q_Y \in \mathscr{B}_2$, where $Y \subseteq [n]$ as center of our discussions in these pages.

This ideal $\mathfrak{q}_Y$ is isomorphic (as $\mathbb{Q}$-vector space) to the $\mathbb{Q}$-algebra $\mathbb{Q}[2^Y]$ of all polynomial functions defined on the box $2^Y \subseteq V_n$ of all subsets of Y (see Lemma 16). Thus, all that remains to prove the Sauer–Shelah–Perles Lemma is to prove that $VCD(\mathscr{F}) \geq RVCD(\mathscr{F})$. This is done in Corollary 30 by using a simplified argument that involves some of the aspects discussed in previous sections.

The short Sect. 6 is devoted to preserving "another" proof of the Sauer–Shelah–Perles Lemma. The variation with respect to the proof exhibited in Sect. 5 is that this proof here only uses duality techniques restricted to the principal ideal $\mathfrak{q}_Y$. This was our first approach. We kept it here since this was what the seminal paper [12] inspired to this author. The proof is not as simple as the one exhibited in Sect. 5, but simplification was not the main motivation of these pages.

We reconsider the bases $\mathscr{B}_1$ and $\mathscr{B}_2$ and their dual bases $\mathscr{B}_1^*$ and $\mathscr{B}_2^*$. Thus, we introduce two "dual" transforms that, in turn, become two automorphisms of $\mathbb{Q}[V_n]$ as $\mathbb{Q}$-vector space of finite dimension:

- The dual transform based on the monomial basis $\mathscr{B}_1$:

$$\begin{array}{rcl} \mathscr{D}_1 : \mathbb{Q}[V_n] & \longrightarrow & \mathbb{Q}[V_n] \\ f & \longmapsto & (f)^*_{\mathscr{B}_1}, \end{array} \tag{1.4}$$

  where, for every $S \subseteq [n]$ we have:

$$\mathscr{D}_1(f)(S) := \operatorname{Tr}_n(f, p_S),$$

  and p_S is the element of basis $\mathscr{B}_1$ determined by $S \subseteq [n]$.
- Another dual transform based on $\mathscr{B}_2^*$, that we call *Frankl-Pach dual transform:*

$$\begin{array}{rcl} \mathscr{D}_2 : \mathfrak{q}_Y & \longrightarrow & \mathfrak{q}_Y \\ f & \longrightarrow & (f)^*_{\mathscr{B}_2^*}, \end{array} \tag{1.5}$$

  where, for every $S \subseteq [n]$ we have:

$$\mathscr{D}_2(f)(S) := \operatorname{Tr}_n(f, q_S^*),$$

  and q_S^* is the element of the dual basis $\mathscr{B}_2^*$ determined by $S \subseteq [n]$.

We call $\mathscr{D}_2$ the *Frankl-Pach dual transform* since it is implicit in the proof of the main outcome in [12]. In fact, the essential aspect of proof in [12] of Sauer–Shelah–Perles Lemma is, in our language, the following statement:

Proposition 2 *With these notations, $\mathscr{D}_2$ is the inverse of $\mathscr{D}_1$. Namely, for all $f \in \mathbb{Q}[V_n]$ we have:*

$$f = \mathscr{D}_1\big(\mathscr{D}_2(f)\big) = \mathscr{D}_2\big(\mathscr{D}_1(f)\big) = \sum_{S\subseteq[n]} f^*_{\mathscr{B}_1}(S)p_S^* = \sum_{S\subseteq[n]} f^*_{\mathscr{B}_2}(S)q_S^*.$$

Moreover, for every $Y \subseteq [n]$, the restrictions to the ideal $\mathfrak{q}_Y$ of $\mathscr{D}_1$ and $\mathscr{D}_2$ are also $\mathbb{Q}$-vector space automorphisms of $\mathfrak{q}_Y$, each inverse of the other.

This is proved as Proposition 32 in Sect. 6. From this statement, in Corollary 33, we also conclude $VCD(\mathscr{F}) \geq RVCD(\mathscr{F})$ just using duality and Proposition 2. Hence, Sauer–Shelah–Perles Lemma follows.

The manuscript is structured as follows. Section 2 is devoted to state the basic notions and some classical facts of trace and duality in finite K-algebras. Section 3 is devoted to establish the basic facts of the algebraic set V_n. In Sects. 3.3 and 3.4 we prove two forms of the General Inclusion–exclusion Principle as immediate instances of the Trace (Inversion) Formula. In Sect. 4 we deal with the principal ideal $\mathfrak{q}_Y$, the ideals $\mathfrak{q}_{\mathscr{F}}$ and its main properties. In Sect. 5 we discuss rank VC dimension and introduce a first and simple proof of Sauer–Shelah–Perles Lemma (see Corollary 30). Finally, Sect. 6 is devoted to state what [12] inspired to this author: The proofs of Proposition 2 and Corollary 33.

We insist on the aspects of the style chosen to write this manuscript. The aim of these pages is to connect two fields of the mathematical knowledge which are not usually connected and, certainly, not in the form we present here. Thus, we have written the text as self-contained as possible. In this sense, potential readers with a classical knowledge of Commutative Algebra can skip reading the elementary proofs described in Sect. 2. In exchange, readers with different cultural backgrounds who might be interested in its content can access it.

2 Trace and duality in Artinian *K*-algebras of *K*-rational zero-dimensional varieties

2.1 Some terminology and general properties

This Subsection is devoted to a brief summary of Duality and Trace in zero-dimensional K-algebras associated to K-rational varieties, when K is a perfect field. Readers familiar with elementary Commutative Algebra may skip proofs which are quite elementary.

Let K be a perfect field of characteristics different to 2, $\mathbb{K}$ its algebraic closure and A an Artinian K-algebra. An Artinian K-algebra (also called zero-dimensional K-algebra or finite, depending of the context) is a K-algebra which is a K-vector space of finite dimension. For every element $a \in A$, we may consider the endomorphism of A as K-vector space η_a defined by multiplying by a:

$$\begin{array}{rrcl} \eta_a : & A & \longrightarrow & A \\ & x & \longmapsto & ax. \end{array}$$

Definition 2 (Trace and Norm) With these notations, for every $a \in A$ we define:

(i) The trace of a as element in A as the trace of the endomorphism η_a:

$$\mathrm{Tr}(a) := Trace(\eta_a) \in K.$$

(ii) The norm of a as element in A, as the determinant of the endomorphism η_a:

$\mathrm{Norm}(a) := \det(\eta_a)$.

We thus define the symmetric bilinear trace of the K-algebra A as

$$\begin{array}{rcl} \mathrm{Tr}_{_A} : A \times A & \longrightarrow & K \\ (a, b) & \longmapsto & \mathrm{Tr}(\eta_a, \eta_b) = \mathrm{Tr}(ab). \end{array} \qquad (2.1)$$

Definition 3 With these notations, let $\mathscr{B} := \{v_i \ : \ i \in I\}$ be a basis of A as K-vector space, where $\sharp(I) = \dim_K(A)$. Let $\mathscr{B}^* := \{w_j \ : \ j \in I\}$ be another basis of A as K-vecor space with same set of indices. We say that $\mathscr{B}^*$ is a dual basis of $\mathscr{B}$ with respect to the $\mathrm{Tr}_{_A}$ if the following equality holds:

$$\mathrm{Tr}_{_A}(v_i, w_j) := \delta_{i,j}, \quad \forall i, j \in I,$$

where $\delta_{i,j}$ is Kronecker's delta function with indices in I.

The relevance of $\mathrm{Tr}_{_A}$ with respect to duality in A is spread along mathematical literature (the interested reader may follow [5, 13, 17] and references therein). We concentrate our terms in the simplest case of K-rational varieties.

With the same notations let $K[X_1, \dots, X_n]$ be the ring of polynomials in n variables with coefficients in K. A *K-definable algebraic set* is a subset $W \subseteq \mathbb{K}^n$ such that there exist a family of polynomials $f_1, \dots, f_s \in K[X_1, \dots, X_n]$ such that

$$W := V_{\mathbb{A}}(f_1, \dots, f_s) := \{x \in \mathbb{K}^n \ : \ f_1(x) = \cdots = f_s(x) = 0\}.$$

As usual, W is of dimension zero if and only if it is a finite set. The cardinality of a zero-dimensional algebraic set W is called its degree and denoted by $\deg(W) = \sharp(W)$ (cf. [15], for instance). We call K-rational points of W the elements in $W_K := W \cap K^n$. When $W_K = W$, we say that W is a *K-rational algebraic set* and it is, obviously, K-definable.

We bijectively associate to every K-definable algebraic set W its (radical) ideal in $K[X_1, \dots, X_n]$ given by the following identity:

$$I_K(W) := \{f \in K[X_1, \dots, X_n] \ : \ f(x) = 0, \ \forall x \in W\}. \qquad (2.2)$$

When no confusion arises with the field K, we simply write $I(W)$.

A K-definable polynomial function on a K-definable algebraic set W is a function $f : W \longrightarrow K$ such that there is a polynomial $P \in K[X_1, \dots, X_n]$ satisfying:

$$f(x) := P(x_1, \dots, x_n), \ \forall x = (x_1, \dots, x_n) \in W.$$

We denote by $K[W]$ the ring of all K-definable polynomial functions over W. Note that if W is zero-dimensional and K-rational, every mapping $f : W \longrightarrow K$ is, in fact, a polynomial function. Namely, if W is a finite set we have:

$$K[W] = K^W.$$

The reader may easily verify that $K[W]$ is the residue ring:

$$K[W] = K[X_1, \dots, X_n]/I_K(W).$$

Observe that if W is K-definable and $\mathbb{K}$ its algebraic closure, the $\mathbb{K}$-algebra $\mathbb{K}[W]$ is obtained by extending scalars, namely $\mathbb{K}[W] = \mathbb{K} \otimes_K K[W]$ and bases of $K[W]$ as K-vector space extend to bases of $\mathbb{K}[W]$ as $\mathbb{K}$-vector space by the obvious transfrom $v \longmapsto 1 \otimes v$. The following is an immedaite consequence of the classical Chinese Remainder Theorem:

Theorem 3 *With these notations, the following is a* $\mathbb{K}$*-algebra isomorphism*:

$$\begin{array}{rcl} \varphi : \mathbb{K}[W] & \longrightarrow & \mathbb{K}^{\sharp(W)} \\ f & \longmapsto & (f(x) \ : \ x \in W), \end{array} \tag{2.3}$$

where $(f(x) \ : \ x \in W) \in \mathbb{K}^{\sharp(W)}$ *is the row vector whose coordinates are the values of the polynomial function* $f \in \mathbb{K}[W]$ *at the points* $x \in \mathbb{K}^n$.

Proof We just indicate the main argument. For every $x \in W$, we denote by $\mathfrak{m}_x$ the following maximal ideal in $\mathbb{K}[W]$:

$$\mathfrak{m}_x := I_{\mathbb{K}}(x) := \{f \in \mathbb{K}[W] \ : \ f(x) = 0\}.$$

The following is a ring epimorphism:

$$\begin{array}{rcl} eval_x : \mathbb{K}[W] & \longrightarrow & \mathbb{K} \\ f & \longmapsto & f(x), \end{array}$$

whose kernel is the ideal $\mathfrak{m}_x := \ker(eval_x)$. Thus, $\mathfrak{m}_x$ is a maximal ideal in $\mathbb{K}[W]$ and, hence, $\mathfrak{m}_x + \mathfrak{m}_y = \mathbb{K}[W]$ for all $x \neq y$, with $x, y \in W$. We thus have:

$$(0) = \bigcap_{x \in W} \mathfrak{m}_x.$$

Finally, the mapping φ cited at the statement becomes the ring isomorphism of the Chinese Remainder Theorem:

$$\begin{array}{rcl} \varphi : \mathbb{K}[W] = \mathbb{K}[W]/\bigcap_{x\in W} \mathfrak{m}_x & \longrightarrow & \prod_{x\in W}(\mathbb{K}/\mathfrak{m}_x) = \mathbb{K}^{\sharp(W)} \\ f & \longmapsto & (f(x) \ : \ x \in W), \end{array} \tag{2.4}$$

and this proves our statement. □

When W is a K-rational algebraic set, we do not need the algebraic closure since every $x \in W$ satisfies $x \in K^n$. This yields the following immediate Corollary:

Corollary 4 *With the same notations, if W is a zero-dimensional K-rational algebraic set, the classical Chinese Remainder Theorem implies that the following is a ring isomorphism and an isomorphism of K-vector spaces:*

$$\begin{array}{rccc} \varphi : & K[W] & \longrightarrow & K^{\sharp(W)} \\ & f & \longmapsto & (f(x)\ :\ x \in W), \end{array} \tag{2.5}$$

where $(f(x)\ :\ x \in W) \in K^{\sharp(W)}$ is the row vector whose coordinates are the values of the polynomial function $f \in K[W]$ at the points $x \in K^n$.

In particular, we have:

$$\dim_K(K[W]) = \deg(W) = \sharp(W), \;\; \dim_{\mathbb{K}}(\mathbb{K}[W]) = \deg(W) = \sharp(W).$$

Additionally, every basis $\mathscr{B}$ of $K[W]$ may be indexed by W (no matter how the elements of the basis $\mathscr{B}$ are linked to the points of W). Namely, if $\mathscr{B} \subseteq K[W]$ is a basis of $K[W]$ as K-vector space, we may always described the elements in $\mathscr{B}$ as:

$$\mathscr{B} := \{v_x\ :\ x \in W\}.$$

Moreover, this isomorphism is the key to prove the following classical result:

Corollary 5 *If $W \subseteq K^n$ is a zero-dimensional K-rational algebraic set, for every $f \in K[W]$, the endomorphism η_f is diagonalizable over K. Moreover, the Jordan canonical form of η_f over K is the diagonal matrix $Diag(f(x)\ :\ x \in W) \in \mathscr{M}_{\sharp(W)}(K)$ and the trace and determinant of η_f satisfy:*

$$\mathrm{Tr}(\eta_f) = \sum_{x \in W} f(x) \in K, \;\; \det(\eta_f) := \prod_{x \in W} f(x) \in K.$$

Let us denote by $\mathrm{Tr}_{_W} := \mathrm{Tr}_{_{K[W]}}$ the symmetric bilinear form on $K[W]$ associated to the trace mapping in Equation (2.1) above. Accordingly, given two bases $\mathscr{B} := \{v_x\ :\ x \in W\}$ and $\mathscr{B}^* := \{w_x\ :\ x \in W\}$ of $K[W]$ as K-vector space, with indices in W, we say that $\mathscr{B}$ and $\mathscr{B}^*$ are dual bases with respect to trace if and only if

$$\mathrm{Tr}_{_W}(v_x, w_y) = \delta_{x,y}, \; \forall x, y \in W,$$

where $\delta_{x,y}$ is again Kronecker's delta function with indices in W.

We believe that the following statement is well-known and it is the translation to K-rational varieties of Lemma B.6 of [23]. Again, we include the proof in order to be as self-contained as possible:

Proposition 6 *Let $W \subseteq K^n$ a zero-dimensional K-rational algebraic variety. Then, $\mathrm{Tr}_{_W}\ :\ K[W] \times K[W] \longrightarrow K$ is a non-degenerate symmetric bilinear form. Moreover, for every basis $\mathscr{B} \subseteq K[W]$ as K-vector space there is a dual basis $\mathscr{B}^*$ of $\mathscr{B}$ with respect to* $\mathrm{Tr}_{_W}$.

Proof Firstly, we prove the existence of dual basis $\mathscr{B}^*$ for every basis $\mathscr{B}$ of $K[W]$. Because of the isomorphism φ described in Identity (2.5), we know that a list of polynomial functions $\mathscr{B} := \{v_1, \dots, v_D\} \subseteq K[W]$ is a basis if and only if the following matrix (vanderMonde-like matrix) is a regular matrix:

$$vdM(\mathscr{B}) := \begin{pmatrix} v_1(x_1) & \cdots & v_1(x_D) \\ \vdots & \ddots & \vdots \\ v_D(x_1) & \cdots & v_D(x_D) \end{pmatrix},$$

where $W = \{x_1, \dots, x_D\}$ and $D = \sharp(W) = \deg(W)$. For every i, $1 \leq i \leq D$, let e_k be the k-th vector of the "canonical" basis of K^D. Let $\omega_i := (\omega_{i,1}, \dots, \omega_{i,D}) \in K^D$ be the unique solution of the following linear system of equations:

$$vdM(\mathscr{B}) \begin{pmatrix} \omega_{i,1} \\ \vdots \\ \omega_{i,D} \end{pmatrix} = e_i^T,$$

where e_i^T is the transposed matrix of the vector e_i (i.e. in column notation). Then, by the isomorphism φ of Identity (2.5) there exist $w_i \in K[W]$ such that:

$$\varphi(w_i) = (w_i(x_1), \dots, w_i(x_D)) = (\omega_{i,1}, \cdots, \omega_{i,D}) = \omega_i.$$

The family $\mathscr{B}^* := \{w_1, \dots, w_D\}$ is the "dual" basis of $\mathscr{B}$, since

$$\mathrm{Tr}_{_W}(v_i, w_j) = \sum_{k=1}^{D} v_i(x_k) w_j(x_k) = (v_i(x_1), \dots, v_i(x_d)) \begin{pmatrix} w_j(x_1) \\ \vdots \\ w_j(x_D) \end{pmatrix} = \delta_{i,j}.$$

Obviously, the fact that $\mathscr{B}^*$ is a dual basis of $\mathscr{B}$ with respect to $\mathrm{Tr}_{_W}$ implies that $\mathrm{Tr}_{_W}$ is a non-degenerate bilinear form:

Given $v := \sum_{i=1}^{D} \lambda_i v_i \in K[W] \setminus \{0\}$, there is some $j \in \{1, \dots, D\}$ such that $\lambda_j \neq 0$ and, hence,

$$\mathrm{Tr}_{_W}(v, w_j) = \sum_{i=1}^{D} \lambda_i \mathrm{Tr}_{_W}(v_i, w_j) = \lambda_j \neq 0,$$

which means that $\mathrm{Tr}_{_W}$ is non-degenerate as bilinear form. □

2.2 Trace (inversion) formula

With the same notations as in the previous Subsection, we restrict ourselves to $K[W]$, where $W \subseteq K^n$ is a zero-dimensional K-rational algebraic set (i.e. when

Proposition 6 holds). This subsection is devoted to state Trace (Inversion) Formula, which is the key element that motivated this manuscript. Trace (Inversion) Formula is an almost immediate consequence of the existence of dual basis. We just prove it in order to fix notations:

Definition 4 (*Dual transform of a function with respect to* Tr_W *and a fixed basis*) Given a basis $\mathscr{B} := \{v_x \ : \ x \in W\}$ of $K[W]$, and a polynomial function $f \in K[W]$ we may also define the dual transform of f with respect to the basis $\mathscr{B}$ and Tr_w as the polynomial function $f^*_{\mathscr{B}} \in K[W]$ given by the following identity:

$$\begin{array}{rccc} f^*_{\mathscr{B}} : & W & \longrightarrow & K \\ & x & \longmapsto & \mathrm{Tr}_w(f, v_x) \end{array} \tag{2.6}$$

Proposition 7 *With these notations, let* $\mathscr{B}^* := \{v^*_x \ : \ x \in W\}$ *be a dual basis of* $\mathscr{B}$ *with respect to* Tr_w *and let* $f \in K[W]$. *Then, the coefficients of* f *as linear combination of elements of* $\mathscr{B}^*$ *are exactly the values of the dual transform at the points in W. Namely, we have*

$$f := \sum_{x\in W} \lambda_x v^*_x = \sum_{x\in W} f^*_{\mathscr{B}}(x) v^*_x,$$

with $\lambda_x = f^*_{\mathscr{B}}(x) = \mathrm{Tr}_w(f, v_x)$.

Proof The statement is immediate, but we prove it for completeness of the manuscript. Assume you have:

$$f := \sum_{x\in W} \lambda_x v^*_x,$$

with $\lambda_x \in K$. Then, as Tr_w is bilinear and $\mathscr{B}^*$ is a dual basis of $\mathscr{B}$ with respect to Tr_w, we have:

$$\mathrm{Tr}_w(f, v_y) = \sum_{x\in W} \lambda_x \mathrm{Tr}_w(v^*_x, v_y) = \sum_{x\in W} \lambda_x \delta_{x,y} = \lambda_y,$$

as stated. □

Thus, we may introduce a certain Trace Formula to evaluate a polynomial function $f \in K[W]$ as follows:

Trace (Inversion) Formula: For every $f \in K[W]$ and for every $z \in W$ we have:

$$f(z) = \sum_{x\in W} f^*_{\mathscr{B}}(x) v^*_x(z) = \sum_{x\in W} \mathrm{Tr}_w(f, v_x) v^*_x(z). \tag{2.7}$$

I have used the term "Inversion" since at some coming places it may be used as an inversion method very close to Möbius Inversion Formula.

2.3 Constructing dual bases in the case of Cartesian product varieties

Although Proposition 6 proves that every basis $\mathscr{B}$ of $K[W]$ has a dual basis, we wish to present an explicit form of constructing dual basis in the case of zero-dimensional varieties obtained as Cartesian products. This generalizes the method described as Lemma B.7 of [23]. We restrict our method to K-rational varieties although it is easily generalizable for every product of zero-dimensional K-definable varieties.

Let $W_i \subseteq K^{n_i}$, $1 \leq i \leq m$, be a family of zero-dimensional K-rational varieties. Let us consider the algebraic K-rational algebraic set given as the Cartesian product $W := \prod_{i=1}^{n} W_i \subseteq K^n$, where $n := \sum_{i=1}^{m} n_i$. In what concerns degree (or cardinality), we obviously have

$$\deg(W) = \sharp(W) = \prod_{i=1}^{m} \deg(W_i) = \prod_{i=1}^{m} \deg(W_i).$$

We consider the K-algebra $K[W]$ of polynomial functions on W. This K-algebra is given as the tensor product of the respective K-algebras $K[W_1], \ldots, K[W_m]$. Namely we have:

$$K[W] := K[W_1] \otimes_K \cdots \otimes_K K[W_m].$$

As the dimension of $K[W]$ as K-vector space equals the degree of W and we have:

$$\dim_K(K[W]) = \prod_{i=1}^{n} \dim_K(K[W_i]) = \deg(W).$$

Given a list of polynomial functions $\varphi_1 \in K[W_1], \ldots, \varphi_m \in K[W_m]$, we denote the tensor product of these mappings by:

$$\otimes_{i=1}^{m} \varphi_i := \varphi_1 \otimes \cdots \otimes \varphi_m \in K[W].$$

The reader may see the polynomial function $\otimes_{i=1}^{m} \varphi_i$ as follows:

$$\begin{array}{rrcl} \otimes_{i=1}^{m} \varphi_i : & W = \prod_{j=1}^{m} W_i & \longrightarrow & K \\ & (\zeta_1, \ldots, \zeta_m) & \longmapsto & \prod_{j=1}^{m} \varphi_j(\zeta_j). \end{array} \tag{2.8}$$

Some authors prefer to use the notation $\prod_{i=1}^{m} \varphi_i := \otimes_{i=1}^{m} \varphi_i$. We use both depending on the context.

Let $(D) := (D_1, \ldots, D_m) \in \mathbb{N}^m$ be a list of non-negative integers. For every list of positive integers $(k) := (k_1, \ldots, k_m) = \mathbb{N}^m$ we write $(k) \preceq (D)$ if and only if $1 \leq k_i \leq D_i$ for every i, $1 \leq i \leq m$. Given $(k) := (k_1, \ldots, k_m) \preceq (D)$ and $(r) := (r_1, \ldots, r_m) \preceq (D)$, we denote by $\delta_{(k),(r)}$ Kronecker's symbol of values (k) and (r), i.e.

$$\delta_{(k),(r)} := \begin{cases} 1, & \text{if and only if} k_i = r_i, \text{for all} i, 1 \leq i \leq m \\ 0, & \text{otherwise}, \end{cases}$$

Let us now consider a family of basis of each $K[W_i]$ as K-vector spaces. Assume that these bases are given by:

$$\mathscr{B}_i := \{\varphi_1^{(i)}, \dots, \varphi_{D_i}^{(i)}\},\ 1 \le i \le m,$$

where $D_i := \deg(W_i)$. Then, it is well-known that the following is a basis of $K[W]$ as K-vector space:

$$\mathscr{B} := \{\Phi_{(k)} := \otimes_{i=1}^m \varphi_{k_i}^{(i)}\ :\ (k) = (k_1, \dots, k_m) \preceq (D)\}. \tag{2.9}$$

The following statement shows how to construct dual basis for $\mathscr{B}$ with respect to Tr_W .

Proposition 8 *With the same notations as above, for every i, $1 \le i \le m$, let $\mathscr{B}_i^* \subseteq K[W_i]$ be a dual basis of $\mathscr{B}_i$ with respect to the trace Tr_{W_i} in $K[W_i]$. Assume that the elements of $\mathscr{B}_i^*$ have the following form:*

$$\mathscr{B}_i^* := \{\psi_1^{(i)}, \dots, \psi_{D_i}^{(i)}\}.$$

Then, the following is a dual basis of $\mathscr{B}$ for the trace Tr_W as bilinear mapping defined on $K[W]$:

$$\mathscr{B}^* := \{\Psi_{(r)} := \otimes_{i=1}^{(m)} \psi_{k_i}^{(i)}\ :\ (r) := (r_1, \dots, r_m) \preceq (D)\}.$$

In particular, for every $(k), (r) \preceq (D)$, the following holds:

$$\mathrm{Tr}_W(\Phi_{(k)}, \Psi_{(r)}) = \delta_{(k),(r)}. \tag{2.10}$$

Proof The fact that W is a Cartesian product is crucial in this proof. We proceed by induction in m. The case $m = 1$ being immediate, assume that $m \ge 2$.

According to the definition of the trace function $\mathrm{Tr}_W : K[W] \times K[W] \longrightarrow K$, we have:

$$\mathrm{Tr}_W(\Phi_{(k)}, \Psi_{(r)}) = \sum_{\zeta \in W} \big(\Phi_{(k)}\Psi_{(r)}\big)(\zeta) = \sum_{\zeta \in W} \big(\Phi_{(k)}(\zeta)\big)\big(\Psi_{(r)}(\zeta)\big).$$

Additionally, according to the definition of the elements $\mathscr{B}$ and $\mathscr{B}^*$, we have:

$$\mathrm{Tr}_W(\Phi_{(k)}, \Psi_{(r)}) = \sum_{\zeta \in W} \Big(\otimes_{i=1}^m \varphi_{k_i}^{(i)}\Big)(\zeta)\Big(\otimes_{i=1}^m \psi_{r_i}^{(i)}\Big)(\zeta).$$

As $W = \prod_{i=1}^m W_i$ and following Identity (2.8), we have:

$$\mathrm{Tr}_W(\Phi_{(k)}, \Psi_{(r)}) = \sum_{\zeta_1 \in W_1} \cdots \sum_{\zeta_m \in W_m} \left(\prod_{i=1}^m \varphi_{k_i}^{(i)}(\zeta_i)\right)\left(\prod_{i=1}^m \psi_{r_i}^{(i)}(\zeta_i)\right).$$

As K is a commutative field, we may rewrite this last identity by:

$$\mathrm{Tr}_{W}(\Phi_{(k)}, \Psi_{(r)}) = \sum_{\zeta_1 \in W_1} \cdots \sum_{\zeta_m \in W_m} \prod_{i=1}^{m} \left(\varphi_{k_i}^{(i)}(\zeta_i) \psi_{r_i}^{(i)}(\zeta_i) \right).$$

We also have:

$$\mathrm{Tr}_{W}(\Phi_{(k)}, \Psi_{(r)}) = \sum_{\zeta_1 \in W_1} \varphi_{k_1}^{(1)}(\zeta_1) \psi_{r_1}^{(1)}(\zeta_1) \left(\sum_{\zeta_2 \in W_2} \cdots \sum_{\zeta_m \in W_m} \prod_{i=2}^{m} \left(\varphi_{k_i}^{(i)}(\zeta_i) \psi_{r_i}^{(i)}(\zeta_i) \right) \right).$$

Let us denote by R_{m-1} the following sum

$$R_{m-1} := \left(\sum_{\zeta_2 \in W_2} \cdots \sum_{\zeta_m \in W_m} \prod_{i=2}^{m} \left(\varphi_{k_i}^{(i)}(\zeta_i) \psi_{r_i}^{(i)}(\zeta_i) \right) \right).$$

Let $W' := \prod_{i=2}^{m} W_i$ the zero-dimensional algebraic set that “forgets” W_1. Let $\mathrm{Tr}_{W'} : K[W'] \times K[W'] \longrightarrow K$ be the trace of W' which is also a Cartesian product. Let us denote by $(D') := (D_2, \ldots, D_m)$ and for $(k) \preceq (D)$, let us denote by $(k') := (k_2, \ldots, k_m) \preceq (D')$ and $(r') := (r_2, \ldots, r_m) \preceq (D')$. Accordingly, let us denote by

$$\Phi_{(k')} := \otimes_{i=2}^{m} \varphi_{k_i}^{(i)} \in K[W'], \;\; \Psi_{(r')} := \otimes_{i=2}^{m} \varphi_{r_i}^{(i)} \in K[W'].$$

Applying the inductive hypothesis, the following holds:

$$R_{m-1} := \mathrm{Tr}_{W'}(\Phi_{(k')}, \Psi_{(r')}) = \delta_{(k'),(r')},$$

where $\delta_{(k'),(r')}$ is Kronecker’s delta as above. Hence, have proved:

$$\mathrm{Tr}_{W}(\Phi_{(k)}, \Psi_{(r)}) = \left(\sum_{\zeta_1 \in W_1} \varphi_{k_1}^{(1)}(\zeta_1) \psi_{r_1}^{(1)}(\zeta_1) \right) R_{m-1} = Tr_{W_1}(\varphi_{k_1}^{(1)}, \psi_{r_1}^{(1)}) \delta_{(k'),(r')},$$

where $Tr_{W_1} : K[W_1] \longrightarrow K$ is the trace in $K[W_1]$. As $\mathscr{B}_1^*$ is the dual basis of $\mathscr{B}_1$ in $K[W_1]$ with respect to Tr_{W_1}, we conclude:

$$\mathrm{Tr}_{W}(\Phi_{(k_1,\ldots,k_m)} \Psi_{(r_1,\ldots,r_m)}) = \delta_{k_1,r_1} \delta_{(k'),(r')} = \delta_{(k),(r)},$$

where δ_{k_1,r_1} is Kronecker’s delta function. and we have proved Identity (2.10).

We immediately conclude that $\mathscr{B}^*$ is a basis and it is a dual basis of $\mathscr{B}$ with respect to the non-degenerate bilinear function Tr_{W}. □

3 The $\mathbb{Q}$-rational algebraic set $2^{[n]}$: basis, trace, duality and immediate applications in Combinatorics

3.1 The $\mathbb{Q}$-rational algebraic set of subsets of a finite set

Let $[n] = \{1, \dots, n\}$ be a set of cardinality n. Denote by $2^{[n]}$ the class of all its subsets and by $\mathbb{F}_2[[n]]$ the $\mathbb{F}_2$-algebra formed by all the characteristic (also called indicator) functions $\chi_{_Y}$ determined by subsets $Y \in 2^{[n]}$.

We consider the following $\mathbb{Q}$-rational zero-dimensional algebraic set of degree $\deg(V_n) = 2^n$ (see [22] for other usages of this algebraic set):

$$V_n := \{(x_1, \dots, x_n) \in \mathbb{K}^n \ : \ x_i^2 - x_i = 0, \ 1 \le i \le n\} = \{0,1\}^n \subseteq \mathbb{K}^n.$$

It is easy to verify that V_n is a smooth complete intersection since we have:

$$I_{\mathbb{Q}}(V_n) = (X_1^2 - X_1, \dots, X_n^2 - X_n),$$

and the Jacobian determinant of this family of polynomials is a unit in $\mathbb{Q}[V_n]$.

Additionally, we obviously have the identification:

$$2^{[n]} \cong \mathbb{F}_2[[n]] \cong V_n,$$

just identifying subsets $Y \subseteq [n]$ with the graph $Gr(\chi_{_Y}) \subseteq \{0,1\}^n$ of its characteristic function, viewed as point in V_n. Just to help the reader, we denote by the same symbol the subset $Y \subseteq [n]$ and the point $Y := (y_1, \dots, y_n) \in V_n$, where

$$y_i := \begin{cases} 1, & \text{if } i \in Y \\ 0, & \text{otherwise} \end{cases}$$

We may see a finite family of subsets $\mathscr{F} \subseteq 2^{[n]}$ as a $\mathbb{Q}$-rational zero-dimensional algebraic subset of V_n.

Let us denote by $\mathrm{Tr}_{_n} := \mathrm{Tr}_{_{V_n}} : \mathbb{Q}[V_n] \times \mathbb{Q}[V_n] \longrightarrow \mathbb{Q}$ the non-degenerate symmetric bilinear form defined by the trace on $\mathbb{Q}[V_n] \times \mathbb{Q}[V_n]$ as in the previous section. From Proposition 6 we know that every basis $\mathscr{B}$ of $\mathbb{Q}[V_n]$ as $\mathbb{Q}$-vector space has a dual basis $\mathscr{B}^*$ with respect to $\mathrm{Tr}_{_n}$ and Trace (Inversion) Formula (2.7) holds in $\mathbb{Q}[V_n]$. Finally, it is clear that $V_n := \{0,1\}^n$ is the Cartesian product of n $\mathbb{Q}$-rational varieties. All these remarks yield the following Corollary that summarizes the main properties we proved before:

Corollary 9 *Let $\mathscr{B} := \{v_Y \ : \ Y \in 2^{[n]}\}$ be any basis of $\mathbb{Q}[V_n]$ as $\mathbb{Q}$-vector space. Then we have*:

(i) *There is a dual basis $\mathscr{B}^* := \{v_Y^* \ : \ Y \in 2^{[n]}\}$ of $\mathscr{B}$ in $\mathbb{Q}[V_n]$ with respect to* $\mathrm{Tr}_{_n}$.

(ii) *The Trace (Inversion) Formula holds for the dual transform. Namely, for every $f \in \mathbb{Q}[V_n]$ the following equality holds in $\mathbb{Q}[V_n]$*:

$$f = \sum_{Y\in 2^{[n]}} f^*_{\mathscr{B}}(Y)v^*_Y.$$

(iii) *The method of constructing dual bases described in Sect.* 2.3 *applies to bases of* $\mathbb{Q}[V_n]$.

Next, we proceed by applying these techniques to several bases of $\mathbb{Q}[V_n]$ which will be used in the sequel:

3.2 An example of self-dual basis: Atomic characteristic functions in $2^{[n]}$

For every $S \subseteq [n]$, we consider the characteristic (sometimes called indicator) function of the atom $\{S\} \in 2^{V_n}$, i.e. the following functions:

$$\begin{array}{rcl} \chi_{_{\{S\}}} : V_n = 2^{[n]} & \longrightarrow & \mathbb{Q} \\ T & \longmapsto & \begin{cases} 1, & \text{if} S = T \\ 0, & \text{otherwise} \end{cases} \end{array} \tag{3.1}$$

Let the reader observe that $\chi_{_{\{S\}}} \in \mathbb{Q}[V_n]$ differs from the characteristic function $\chi_{_S} \in \mathbb{F}_2[U]$.

Proposition 10 (**Self-dual basis of atoms**) *With these notations, the polynomial function* $\chi_{_{\{S\}}}$ *are idempotent elements in* $\mathbb{Q}[V_n]$ (*i.e.* $(\chi_{_{\{S\}}})^2 - \chi_{_{\{S\}}} = 0$ *in* $\mathbb{Q}[V_n]$).

(i) *The set of characteristic functions of atoms in* V_n *defines a basis* $\mathscr{B}_0$ *of* $\mathbb{Q}[V_n]$ *as* $\mathbb{Q}$-*vector space, where*:

$$\mathscr{B}_0 := \{\chi_{_{\{S\}}} : S \in V_n = 2^{[n]}\}.$$

(ii) *The basis* $\mathscr{B}_0$ *is self-dual* (*i.e.* $\mathscr{B}_0$ *is a dual basis of itself*). *Namely, if* $\mathrm{Tr}_{_n}$ *is the trace in* $\mathbb{Q}[V_n]$, *for every* $S, T \in V_n$ *we have*:

$$\mathrm{Tr}_{_n}(\chi_{_{\{S\}}}, \chi_{_{\{T\}}}) = \delta_{S,T},$$

where, as before, $\delta_{S,T}$ is Kronecker's delta function.

Proof Observe that $\mathscr{B}_0$ spans $\mathbb{Q}[V_n]$ since for every function $f \in \mathbb{Q}[V_n]$ we have:

$$f := \sum_{S\subseteq[n]} f(S)\chi_{_{\{S\}}}.$$

As $\sharp(\mathscr{B}_0) = 2^n = \dim_{\mathbb{Q}}(\mathbb{Q}[V_n])$, then it must be a basis of this $\mathbb{Q}$-vector space. This yields Claim *i*).

From Corollary 5 we know that:

$$\mathrm{Tr}_n(\chi_{\{S\}}, \chi_{\{T\}}) := \sum_{Y \in V_n} \chi_{\{S\}}(Y)\chi_{\{T\}}(Y),$$

and, from the definition of the functions $\chi_{\{S\}}$ and $\chi_{\{T\}}$ above, we immediately conclude:

$$\mathrm{Tr}_n(\chi_{\{S\}}, \chi_{\{T\}}) = \delta_{S,T},$$

which proves Claim *ii*). □

3.3 The example of monomial basis: dual basis, inversion formula and a "reverse order" general inclusion–exclusion principle

For every subset $S \in 2^{[n]}$ we consider the monomial

$$P_S(X_1, \ldots, X_n) := \prod_{i \in S} X_i = \prod_{i=1}^{n} X_i^{\mu_i} \in \mathbb{Q}[X_1, \ldots, X_n], \tag{3.2}$$

where the point $S \in V_n$ has coordinates $S = (\mu_1, \ldots, \mu_n) \in \{0, 1\}^n$. This monomial defines a polynomial function on V_n that we denote by $p_S := P_S + I_{\mathbb{Q}}(V_n) \in \mathbb{Q}[V_n]$. The following statement summarizes the main properties satisfied by these polynomial functions:

Proposition 11 *With these notations, we have:*

(i) *The polynomial function $p_S : V_n \longrightarrow \mathbb{Q}$ satisfies for every $Y \subseteq [n]$:*

$$p_S(Y) = \begin{cases} 1, & \text{if}\, S \subseteq Y \\ 0, & \text{other wise,} \end{cases} \tag{3.3}$$

In particular, all polynomial functions p_S are idempotent elements in $\mathbb{Q}[V_n]$.

(ii) *The set $\mathscr{B}_1 := \{p_S \ : \ S \in V_n = 2^{[n]}\}$ of monomial functions is a basis of $\mathbb{Q}[V_n]$ as $\mathbb{Q}$-vector space.*

(iii) *The set $\mathscr{B}_1^* := \{p_S^* \ : \ S \in V_n = 2^{[n]}\}$ is a dual basis of $\mathscr{B}_1$ with respect to* Tr_n, *where*

$$p_S^* := \prod_{i \in S}(2X_i - 1) \prod_{j \in X \setminus S}(1 - X_j) + I_K(V_n) \in \mathbb{Q}[V_n].$$

(iv) *The polynomial functions in this dual basis satisfy:*

$$p_S^*(Y) = \begin{cases} (-1)^{\sharp(S \setminus Y)} & \text{if}\, Y \subseteq S \\ \quad 0, & \text{otherwise} \end{cases} \tag{3.4}$$

Proof Claim *i*) is merely a verification, whereas Claim *ii*) follows from the fact that $\{X_1^2 - X_1, \ldots, X_n^2 - X_n\}$ is a Gröbner basis of the ideal $I_K(V_n)$ with respect to many natural monomial orders (as "degree+lexicographic", see [8] for this terminology, if required). As for Claim *iii*), observe that the basis $\mathscr{B}_1$ is the basis of the tensor product $\mathbb{Q}[V_n] = \mathbb{Q}[W_1] \otimes_{\mathbb{Q}} \cdots \otimes_{\mathbb{Q}} \mathbb{Q}[W_n]$, constructed according to the method described in Identity (2.9), where $W_i = \{0, 1\}$ and the basis of $\mathbb{Q}[W_i]$ is given by $\mathscr{B}_{1,i} := \{1 + I_{\mathbb{Q}}(W_i), X_i + I_{\mathbb{Q}}(W_i)\}$. Let Tr_{W_i} be the trace associated to the algebraic set W_i. It is immediate to verify that a dual basis of $\mathscr{B}_{1,i}$, with respect to Tr_{W_i}, is given by

$$\mathscr{B}_{1,i}^* := \{(1 - X_i) + I_{\mathbb{Q}}(W_i), (2X_i - 1) + I_{\mathbb{Q}}(W_i)\}.$$

Then, applying the method of Proposition 8 of Sect. 2.3, we conclude that the following is a dual basis of $\mathscr{B}_1$ with respect to Tr_n:

$$\mathscr{B}_1^* := \{\prod_{i\in S}(2X_i - 1) \prod_{j\in X\setminus S}(1 - X_j) + I_{\mathbb{Q}}(V_n) \in \mathbb{Q}[V_n] \ : \ S \in 2^{[n]}\}.$$

Claim *iv*) immediately follows from the form of p_S^*. □

The Trace (Inversion) Formula for this basis $\mathscr{B}_1$ is a very familiar "principle" of Combinatorics: Inclusion–exclusion Principle (in its reverse order form).

Corollary 12 (Duality, monomial basis and inclusion–exclusion principle (in reverse order form)) *With the same notations as above, let $f \in \mathbb{Q}[V_n]$ be any (polynomial) function defined on $2^{[n]}$. We have:*

(i) *For every $S \subseteq [n]$, the following equality holds:*

$$\mathrm{Tr}_n(f, p_S) = \sum_{S\subseteq Y} f(Y).$$

In particular, if $f_{\mathscr{B}_1}^* \in \mathbb{Q}[V_n]$ is the dual transform of f with respect to the basis $\mathscr{B}_1$ and and Tr_n we have:

$$f_{\mathscr{B}_1}^*(S) = \sum_{S\subseteq T} f(T).$$

(ii) *We also have:*

$$f := \sum_{S\subseteq[n]} f_{\mathscr{B}_1}^*(S) p_S^*.$$

(iii) *"Reverse order" of the General Inclusion–exclusion Principle: For every $Y \subseteq [n]$ we have*

$$f(Y) := \sum_{Y\subseteq S}(-1)^{\sharp(S\setminus Y)} f^*_{\mathscr{B}_1}(S) = \sum_{Y\subseteq S}(-1)^{\sharp(S\setminus Y)}\left(\sum_{S\subseteq T} f(T)\right),$$

(iv) *For every $T \subseteq [n]$ we have*

$$\chi_{\{T\}} := \sum_{T\subseteq S}(-1)^{\sharp(S\setminus T)} p_S. \tag{3.5}$$

Proof Most of the claims are immediate from the definitions and previous results. Anyway. we introduce indications of the proof to explain how our previous results apply. From Corollary 5, we know that:

$$\mathrm{Tr}_n(f, p_S) := \sum_{Y\in V_n} f(Y) p_S(Y).$$

From Equation (3.3) of Proposition 11 we know that $p_S(Y) = 1$ is and only if $S \subseteq Y$, being zero otherwise. Thus, we conclude

$$f^*_{\mathscr{B}_1}(S) := \mathrm{Tr}_n(f, p_S) := \sum_{S\subseteq Y} f(Y).$$

Claim *iii*) immediately follows from the Trace (Inversion) Formula (2.7) above. Claim *iv*) is simply Claim *iii*), just using the standard presentation fo Inclusion–exclusion Principles and the evaluation of the polynomial function p^*_S described in Identity (3.4).

Claim *iv*) is also the Trace (Inversion) Formula but changing the roles of $\mathscr{B}_1$ and $\mathscr{B}^*_1$. Namely, there exists some linear combination:

$$\chi_{\{T\}} := \sum_{S\subseteq [n]} \lambda_{S,T} p_S,$$

where $\lambda_{S,T} \in \mathbb{Q}$. Because $\mathscr{B}^*_1$ is a dual basis of $\mathscr{B}_1$ with respect to the trace, we have:

$$\lambda_{S,T} := \mathrm{Tr}_n(\chi_{\{T\}}, p^*_S) = \sum_{W\subseteq [n]} \chi_{\{T\}}(W) p^*_S(W) = p^*_S(T).$$

According to Identity (3.4), we conclude Equality (3.5):

$$\lambda_{S,T} = p^*_S(T) = \begin{cases} (-1)^{\sharp(S\setminus T)} & \text{if } T \subseteq S \\ 0, & \text{otherwise.} \end{cases}$$

And this proves Claim *iv*). □

3.4 The example of anti-monomial basis: dual basis, inversion formula and the general form of the Inclusion–exclusion principle

Let us now consider the following polynomial mapping defined on the algebraic set V_n:

$$\begin{array}{rccc} \Psi : & V_n & \longrightarrow & V_n \\ & (x_1, \dots, x_n) & \longmapsto & (1 - x_1, \dots, 1 - x_n). \end{array} \tag{3.6}$$

This is obviously a biregular isomorphism whose inverse is itself $\Psi^{-1}(y_1, \dots, y_n) = (1 - y_1, \dots, 1 - y_n) = \Psi(y_1, \dots, y_n)$. Moreover, for every $S \in V_n$ $\Psi(S)$ is the complement of S in $[n]$ (i.e. $\Psi(S) = [n] \setminus S$). This biregular isomorphism induces an $\mathbb{Q}$-algebra isomorphism by composition:

$$\begin{array}{rccc} \psi := \Psi_* : & \mathbb{Q}[V_n] & \longrightarrow & \mathbb{Q}[V_n] \\ & f & \longmapsto & f \circ \Psi \end{array} \tag{3.7}$$

Now, for every $S \in V_n$ we introduce the following polynomial functions $q_S \in \mathbb{Q}[V_n]$:

$$q_S := \prod_{i \in [n] \setminus S} (1 - X_i) + I(V_n) \in \mathbb{Q}[V_n]. \tag{3.8}$$

We obviously have that the following identity holds for every $S \subseteq [n]$:

$$\psi(p_S) = q_{[n] \setminus S}.$$

In particular, as $\mathscr{B}_1$ was a basis (the monomial basis), the class $\mathscr{B}_2 := \{q_S \ : \ S \in V_n\}$ is also a basis of $\mathbb{Q}[V_n]$ as $\mathbb{Q}$-vector space. The following statement resumes some of the properties satisfied by the elements of the basis $\mathscr{B}_2$:

Proposition 13 *With these notations, we have:*

(i) *The polynomial function $q_S : V_n \longrightarrow \mathbb{Q}$ satisfies for every $Y \subseteq [n]$:*

$$q_S(Y) = \begin{cases} 1, & \text{if } Y \subseteq S \\ 0, & \text{other wise} \end{cases} \tag{3.9}$$

In particular, for every $S \subseteq [n]$, the polynomial function q_S is an idempotent element of $\mathbb{Q}[V_n]$.

(ii) For every $S \subseteq [n]$, $q_S(Y) := p_{([n] \setminus S)}(\mathbf{1} - Y)$, where $\mathbf{1} = (1, \dots, 1) \in V_n$ is associated to $[n]$ as element in V_n and $[n] \setminus S$ is the complement of S in $[n]$.

(iii) The set $\mathscr{B}_2 := \{q_S \ : \ S \in V_n = 2^{[n]}\}$ is a basis of $\mathbb{Q}[V_n]$ as $\mathbb{Q}$-vector space.

(iv) The set $\mathscr{B}_2^* = \{q_S^* \ : \ S \subseteq [n]\}$ is a dual basis of $\mathscr{B}_2$ with respect to Tr_n, where

$$q_S^* := \prod_{i \in S} X_i \prod_{j \in [n] \setminus S} (1 - 2X_j) + I_{\mathbb{Q}}(V_n) \in \mathbb{Q}[V_n].$$

(v) *The polynomial functions in this dual basis satisfy:*

$$q_S^*(Y) = \begin{cases} (-1)^{\sharp(Y \setminus S)}, & \text{if } S \subseteq Y \\ 0, & \text{otherwise.} \end{cases} \tag{3.10}$$

Proof Claims *i*) and *v*) are mere verifications from the definitions of q_S and q_S^*. Just for helping the reader, let us see *v*). Let $Y \subseteq [n]$ be a subset and denote also by Y the point $Y := (y_1, \dots, y_n) \in V_n$, where $y_i = 1$ if and only if $i \in Y$. Let us consider the polynomial functions of the family $\mathscr{B}_2 := \{q_S^* \ : \ S \subseteq [n]\}$.

If $S \subseteq Y$, then the following equality holds:

$$q_S^*(Y) = \prod_{i \in S} y_i \prod_{j \in Y \setminus S} (1 - 2y_j) \prod_{k \in [n] \setminus Y} (1 - 2y_k).$$

Then, we have:

- If $i \in S \subseteq Y$, then $y_i = 1$ and, hence, $\prod_{i \in S} y_i = 1$.
- If $j \in Y \setminus S$, then $y_i = 1$ and, hence, $\prod_{j \in Y \setminus S}(1 - 2y_i) = (-1)^{\sharp(Y \setminus S)}$.
- If $j \in [n] \setminus Y$, then $y_i = 0$ and, hence, $\prod_{k \in X \setminus Y}(1 - 2y_k) = 1$.

Thus, if $S \subseteq Y$ we have: $q_S^*(Y) = (-1)^{\sharp(Y \setminus S)}$.

On the other hand, if $S \nsubseteq Y$, then there is some $i \in S \setminus Y$ and, hence, $\prod_{i \in S} y_i = 0$ which implies $q_S^*(Y) = 0$. An this proves Claim *v*).

With the same notations of $Y := (y_1, \dots, y_n) \in V_n$, such that $y_i = 1$ of and only if $i \in Y$, we have:

$$q_S(Y) = \prod_{i \in [n] \setminus S} (1 - y_i) \in \mathbb{Q}.$$

From the definition of the polynomials p_T (Identity 3.2) we obviously have:

$$q_S(Y) = p_{[n] \setminus S}(1 - y_1, \dots, 1 - y_n) = p_{[n] \setminus S}(\mathbf{1} - Y),$$

and Claim *ii*) follows. Note that the following is a $\mathbb{Q}$-algebra isomorphism:

$$\begin{array}{rccc} \psi \ : & \mathbb{Q}[V_n] & \longrightarrow & \mathbb{Q}[V_n] \\ & f & \longmapsto & f(\mathbf{1} - Y). \end{array}$$

Thus Claim *ii*) implies that $\mathscr{B}_2 := \psi(\mathscr{B}_1)$ and, hence, $\mathscr{B}_2$ is a basis of $\mathbb{Q}[V_n]$ as $\mathbb{Q}$ -vector space, concluding Claim *iii*).

Taking $W_i := \{0, 1\}$, we have that $V_n := \prod_{i=1}^n W_i = \{0, 1\}^n$ is a Cartesian product Q-rational algebraic set. Let Tr_{W_i} be the trace associated to the algebraic set W_i. There is a natural basis of $\mathbb{Q}[W_i]$ given by $\mathscr{B}_{2,i} := \{\overline{1}, \overline{(1 - X_i)}\}$, where $\overline{1} := 1 + I(W_i)$ and $\overline{(1 - X_i)} := (1 - X_i) + I(W_i)$ are respectively the polynomial functions in $\mathbb{Q}[W_i]$ defined by 1 and $(1 - X_i)$. As simple verification sows that the dual basis of $\mathscr{B}_{2,i}$ with respect to Tr_{W_i} is given by:

$$B_{2,i}^* := \{\overline{X_i}, \overline{1 - 2X_i}\} \subseteq \mathbb{Q}[W_i].$$

In other words, we have:

$$\mathrm{Tr}_{W_i}(\overline{X_i}, \overline{X_i}) = 1, \mathrm{Tr}_{W_i}(\overline{X_i}, \overline{1 - X_i}) = 0,$$
$$\mathrm{Tr}_{W_i}(\overline{X_i}, \overline{1 - 2X_i}) = 0,\ \mathrm{Tr}_{W_i}(\overline{1 - X_i}, \overline{1 - 2X_i}) = 1.$$

Then, Proposition 8 proves that the following is a dual basis of $\mathscr{B}_2$:

$$\{\psi_1 \otimes \cdots \otimes \psi_n \ : \ \psi_i \in \mathscr{B}_{2,i}^*\}.$$

This last basis is simply the set $\mathscr{B}_2^* = \{q_S^* \ : \ S \subseteq [n]\}$ described above, as the reader may easily verify. And this proves Claim *iv*). □

We also observe that the Trace (Inversion) Formula applied to the basis $\mathscr{B}_2$, yields the standard formulation of the general form of the Inclusion–exclusion Principle.

Corollary 14 (Duality, anti-monomial basis and inclusion–exclusion principle in general form) *With the same notations as above, let* $f \in \mathbb{Q}[V_n]$ *be any* (*polynomial*) *function defined on* $2^{[n]}$. *We have*:

(i) *For every* $S \subseteq [n]$, *the dual transform* $f^*_{\mathscr{B}_2}$ *of* f *with respect to the basis* $\mathscr{B}_2$ *and* Tr_n, *satisfies*:

$$f^*_{\mathscr{B}_2}(S) = \mathrm{Tr}_n(f, q_S) = \sum_{T \subseteq S} f(T).$$

(ii) *We also have*:

$$f := \sum_{S \subseteq [n]} f^*_{\mathscr{B}_2}(S) q_S^*.$$

(iii) *General form of the Inclusion–exclusion Principle:*

$$f(Y) := \sum_{S \subseteq Y} (-1)^{\sharp(Y \setminus S)} f^*_{\mathscr{B}_2}(S) = \sum_{S \subseteq Y} (-1)^{\sharp(Y \setminus S)} \left(\sum_{T \subseteq S} f(T) \right),$$

(iv) *For every* $T \subseteq [n]$, *we also have*:

$$\chi_{\{T\}} := \sum_{S \subseteq T} (-1)^{\sharp(T \setminus S)} q_S. \tag{3.11}$$

Proof Claim *i*) follows from the previous Proposition. Claim *ii*) is the Trace (Inversion) Formula (2.7).

Claim *iii*) follows just applying Claim *ii*) to any subset $Y \subseteq [n]$. We have:

$$f(Y) := \sum_{S\subseteq[n]} f^*_{\mathscr{B}_2}(S) q^*_S(Y).$$

According to Equality (3.10) of the preceding Proposition, we know that $q^*_S(Y)=0$ if $S \nsubseteq Y$ and that $q^*_S(Y)=(-1)^{\sharp(Y\setminus S)}$ if $S\subseteq Y$. Thus, using Claim *i*) we conclude:

$$f(Y) := \sum_{S\subseteq Y} (-1)^{\sharp(Y\setminus S)} f^*_{\mathscr{B}_2}(S) = \sum_{S\subseteq Y} (-1)^{\sharp(Y\setminus S)} \left(\sum_{T\subseteq S} f(T) \right),$$

which is the usual General Inclusion–exclusion Principle.

Claim *iv*) is also the Trace (Inversion) Formula but changing the roles of $\mathscr{B}_s$ and $\mathscr{B}_2^*$. Namely, there exists some linear combination:

$$\chi_{_{\{T\}}} := \sum_{S\subseteq[n]} \lambda_{S,T} q_S,$$

where $\lambda_{S,T}\in\mathbb{Q}$. Because $\mathscr{B}_2^*$ is a dual basis of $\mathscr{B}_2$ with respect to the trace, we have:

$$\lambda_{S,T} := \operatorname{Tr}_n(\chi_{\{T\}}, q^*_S) = \sum_{W\subseteq[n]} \chi_{\{T\}}(W) q^*_S(W) = q^*_S(T).$$

According to Identity (3.10), we conclude Equality (3.11):

$$\lambda_{S,T} := \begin{cases} (-1)^{\sharp(T\setminus S)}, & \text{if } S\subseteq T \\ 0, & \text{otherwise} \end{cases}$$

□

3.5 The example of the vector subspace of Null *t*-designs: just another explicit basis

We now exhibit the role of the basis $\mathscr{B}_1$ in $\mathbb{Q}[V_n]$ which is related to *Null t-designs*, discussed in [12] and references therein. We review the notion here.

Definition 5 With the same notations as in previous sections, a function $f : 2^{[n]} \longrightarrow \mathbb{Q}$ is called a null *t*-design if for every $A\subseteq[n]$, such that $\sharp(A)\le t$ the following equality holds:

$$\sum_{A\subseteq Y} f(Y) = 0.$$

Let us consider $W_t := B_H(\mathbf{0}, t) \subseteq V_n$ the closed ball with center $\mathbf{0}$ and radius t with respect to Hamming distance in V_n. Then, we have:

Proposition 15 *With these notations, the following properties hold for every function $f : 2^{[n]} \longrightarrow \mathbb{Q}$:*

(i) *The function $f \in \mathbb{Q}[V_n]$ is a null t-design if and only if the following holds:*

$$\mathrm{Tr}_{n}(f, p_A) = 0, \ \forall A \in W_t.$$

(ii) *A function $f : 2^{[n]} \longrightarrow \mathbb{Q}$ is a null t-design if and only if f belongs to the $\mathbb{Q}$-vector space spanned by the following family of linearly independent polynomials:*

$$P_t^* := \{p_F^* \ : \ F \subseteq [n], F \notin W_t\}.$$

Proof According to Claim *i*) of Proposition 11, we know that for every $A \in W_t$ the following holds:

$$\mathrm{Tr}_{n}(f, p_A) = \sum_{A \subseteq Y} f(Y) = 0.$$

Hence, Claim *i*) is a tautology.

As for Claim *ii*), observe that $\mathscr{B}_1^*$ is a basis of $\mathbb{Q}[V_n]$. Now, every function $f \in \mathbb{Q}[V_n]$ admits a description of the form:

$$f := \sum_{F \subseteq [n]} \mu_F^* p_F^*,$$

where $\mu_F^* \in \mathbb{Q}$. Since $\mathscr{B}_1^*$ is a basis dual to $\mathscr{B}_1$ with respect to Tr_{n} and f is a Null t-design we have that

$$\mu_A^* := \mathrm{Tr}_{n}(f, p_A) = 0, \ \forall A \in W_t.$$

Thus, we immediately conclude that the class of null t-designs on $\mathbb{Q}[V_n]$ is contained in the $\mathbb{Q}$-vector space spanned by P_t^*.

Conversely, its is easy to see that P_t^* is made of null t-designs of $\mathbb{Q}[V_n]$: As $\mathscr{B}_1^*$ is a basis dual to $\mathscr{B}_1$ we have that

$$\mathrm{Tr}_{V_n}(p_F^*, p_A) = 0, \quad \forall A \neq F.$$

In particular, if $F \notin W_t$ and $A \in W_t$, we obviously have $A \neq F$ and, hence, given $p_F^* \in P_t^*$ we have:

$$\mathrm{Tr}_{n}(p_F^*, p_A) = 0, \quad \forall A \in W_t,$$

which proves that P_t^* is a finite set of null t-designs. □

Note that this basis differs from the one cited in [12] and described in Theorem 4 of [9].

4 The principal ideals $\mathfrak{q}_Y$ and closedness downward

4.1 The principal ideals $\mathfrak{q}_Y$

With the same notations as in previous subsections, given $Y \subseteq [n]$, we may view the class $2^Y \subseteq V_n$ of the subsets of Y as a zero-dimensional algebraic subset of V_n:

$$2^Y := \{S \in V_n \ : \ S \subseteq Y\} = \{(x_1, \dots, x_n) \in V_n \ : \ x_j = 0, \ \forall j \notin Y\},$$

where, as in previous sections, we identified subsets $S \subseteq [n]$ and points $S \in V_n$. Some authors prefer to call the class 2^Y as the *$\sharp(Y)$-dimensional box determined by Y*. We denote by $I(2^Y) \subseteq \mathbb{Q}[V_n]$ the ideal of polynomial functions in $\mathbb{Q}[V_n]$ that vanish in 2^Y and we obviously have the following isomorphism:

$$\mathbb{Q}[V_n]/I(2^Y) = \mathbb{Q}[2^Y] := \{f \ : \ 2^Y \longrightarrow \mathbb{Q} \ : \ f \text{is a function}\}.$$

We have also identified the class 2^Y and the class of the characteristic functions of subsets in 2^Y:

$$2^Y \cong \mathbb{F}_2[Y] := \{\chi_{_S} \ : \ S \subseteq Y\}.$$

Thus, given $\mathscr{F} \subseteq 2^{[n]}$ and $Y \subseteq [n]$, we may consider the restriction mapping:

$$\begin{array}{rcl} \rho_Y \ : \ 2^{[n]} & \longrightarrow & \mathbb{F}_2[Y] \\ T & \longmapsto & \chi_{_T} \restriction_{_Y} . \end{array}$$

Some authors denote by $\mathscr{F} \restriction_{_Y}$ the family of restrictions $\rho_Y(\mathscr{F})$, i.e. the class of all restrictions to Y of any subset $\mathscr{F} \subseteq 2^{[n]}$ of binary functions defined on $[n]$.

Definition 6 [28] With these notations, given $Y \subseteq [n]$ and $\mathscr{F} \subseteq V_n$, we say that $\mathscr{F}$ shatters Y if and only if the following equality holds:

$$\rho_Y(\mathscr{F}) = \mathbb{F}_2[Y] = 2^Y.$$

We define the Vapnik-Chervonenkis dimension of $\mathscr{F}$ as the maximum cardinality of any subset Y such that $\mathscr{F}$ shatters Y. We denote by *VCD*($\mathscr{F}$) the Vapnik-Chervonenkis dimension of $\mathscr{F} \subseteq V_n$.

Next, we introduce the following principal ideal in $\mathbb{Q}[V_n]$:

$$\mathfrak{q}_Y := (q_Y) := \{f q_Y \ : \ f \in \mathbb{Q}[V_n]\}, \tag{4.1}$$

where q_Y is the polynomial function introduced in Sect. 3.4.

Lemma 16 *For every $f \in \mathbb{Q}[V_n]$, the following holds for every subsets $S, Y \subseteq [n]$:*

$$(fq_Y)(S) = \begin{cases} f(S), & \text{if } S \subseteq Y \\ 0, & \text{otherwise.} \end{cases} \qquad (fp_Y)(S) = \begin{cases} f(S), & \text{if } Y \subseteq S \\ 0, & \text{otherwise.} \end{cases} \tag{4.2}$$

In particular, we may identify fq_Y with the restriction of f to 2^Y (i.e. $f\restriction_{2^Y} \in \mathbb{Q}[2^Y]$) and we have:

$$\mathfrak{q}_Y = \{f \in \mathbb{Q}[V_n] \ : \ f(T) = 0, \forall T \nsubseteq Y\} = I(\mathscr{O}_Y),$$

where $\mathscr{O}_Y := V_n \setminus 2^Y = \{S \in V_n \ : \ q_Y(S) = 0\}$ is the set (a distinguished open set for some authors) of all subsets of $[n]$ not contained in Y. We also have a decomposition as direct sum of vectors subspaces of $\mathbb{Q}[V_n]$ given by

$$\mathbb{Q}[V_n] \cong \mathfrak{q}_Y \oplus I(2^Y), \tag{4.3}$$

which also yields an isomorphism as $\mathbb{Q}$-vector spaces between $\mathbb{Q}[2^Y]$ and $\mathfrak{q}_Y$.

Proof Identities in (4.2) immediately follow from their definitions. These identities imply, in particular, that $\mathfrak{q}_Y \subseteq I(\mathscr{O}_Y)$. Conversely, given $f \in I(\mathscr{O}_Y) \subseteq \mathbb{Q}[V_n]$, let us consider the polynomial function $g := fq_Y$. As f vanishes outside 2^Y, Identities (4.2) imply that $g(S) = f(S)$ for all $S \in V_n$ and, hence, $f = fq_Y \in \mathfrak{q}_Y$. In order to prove the isomorphism of Equation (4.3), just observe that for every $f \in \mathbb{Q}[V_n]$, then $f - fq_Y \in I_{\mathbb{Q}}(2^Y)$ and that $\mathfrak{q}_Y \cap I_{\mathbb{Q}}(2^Y) = (0)$. □

For every $\mathscr{F} \subseteq V_n$ we introduce the following class of functions:

$$Q_{\mathscr{F}} := \{q_G \ : \ G \in \mathscr{F}\}. \tag{4.4}$$

As $Q_{\mathscr{F}} \subseteq \mathscr{B}_2$ (which is a basis of $\mathbb{Q}[V_n]$) the family $Q_{\mathscr{F}}$ is a family of linearly independent functions and its cardinality equals the cardinality of $\mathscr{F}$ (i.e. $\sharp(Q_{\mathscr{F}}) = \sharp(\mathscr{F})$). With the same notations we also introduce:

$$\mathscr{F}^{(\max)} := \{F \in \mathscr{F} \ : \ F \text{is maximal in } \mathscr{F} \text{with respect to } \subseteq\} \subseteq \mathscr{F}. \tag{4.5}$$

Finally, for every subset $\mathscr{F} \subseteq V_n$ we introduce the following notations:

- The ideal $\mathfrak{q}_{\mathscr{F}} \subseteq \mathbb{Q}[V_n]$ generated by $Q_{\mathscr{F}}$:

$$\mathfrak{q}_{\mathscr{F}} := (q_F \ : \ F \in \mathscr{F}). \tag{4.6}$$

- The vector space $W_{\mathscr{F}} \subseteq \mathbb{Q}[V_n]$ spanned by $Q_{\mathscr{F}}$:

$$W_{\mathscr{F}} := \mathbb{Q}\langle q_F \ : \ F \in \mathscr{F}\rangle. \tag{4.7}$$

We obviously have that $\mathfrak{q}_Y$ is the ideal $\mathfrak{q}_{\{Y\}}$, the subspace $W_{\mathscr{F}} \subseteq \mathfrak{q}_{\mathscr{F}}$ and the dimension of $W_{\mathscr{F}}$ as $\mathbb{Q}$-vector space is $\sharp(\mathscr{F})$ since the elements in $Q_{\mathscr{F}}$ are linearly independent over $\mathbb{Q}$. We firstly prove the following long proposition that summarizes other main properties of the principal ideal $\mathfrak{q}_Y$:

Proposition 17 *With these notations, we have:*

(i) *For every $Z, Y \subseteq [n]$, the following property holds in $\mathbb{Q}[V_n]$:*

$$q_Z q_Y = q_{Z\cap Y}.$$

(ii) *Also for every* $Z, Y \subseteq [n]$ *the following are equivalent claims*:

(a) $Z \subseteq Y$.
(b) q_Y *divides* q_Z *in* $\mathbb{Q}[V_n]$.
(c) $\mathfrak{q}_Z \subseteq \mathfrak{q}_Y$.

(iii) *The isomorphism between* $\mathbb{Q}[2^Y]$ *and* $\mathfrak{q}_Y$ *is an isomorphism as* $\mathbb{Q}[V_n]$*-modules.*

(iv) *The following are basis of* $\mathfrak{q}_Y$ *as* $\mathbb{Q}$*-vector space*:

$$\mathscr{B}_{0,2^Y} := \{\chi_{\{T\}} \ : \ T \subseteq Y\}, \ \ \mathscr{B}_{2,2^Y} := \{q_T \ : \ T \subseteq Y\}.$$

(v) *The ideal* $I(2^Y)$ *is the annihilator in* $\mathbb{Q}[V_n]$ *of the ideal* $\mathfrak{q}_Y$:

$$I(2^Y) := Ann_{\mathbb{Q}[V_n]}(\mathfrak{q}_Y) := \{f \in \mathbb{Q}[V_n] \ : \ fq_Y = 0\},$$

and $\{q_T^* \ : \ T \not\subseteq Y\} \subseteq I(2^Y)$.

(vi) *Given* $\mathscr{F} \subseteq 2^{[n]}$, *a subset* $Y \subseteq [n]$, *let us denote by* $Q_{\mathscr{F},Y}$ *the class of polynomial functions*:

$$Q_{\mathscr{F},Y} := \{q_F q_Y \ : \ F \in \mathscr{F}\} \subseteq \mathfrak{q}_Y.$$

Then, $\mathscr{F}$ shatters Y if and only if $Q_{\mathscr{F},Y}$ is a basis of $\mathfrak{q}_Y$ as $\mathbb{Q}$-vector space. In particular, $\mathscr{F}$ shatters Y if and only if

$$2^{\sharp(Y)} \leq \sharp\big(Q_{\mathscr{F},Y}\big).$$

In particular, VC dimension may be characterised as follows:

$$\begin{aligned} VCD(\mathscr{F}) &= \max\{\sharp(Y) \ : \ 2^{\sharp(Y)} \leq \sharp\big(Q_{\mathscr{F},Y}\big)\} = \\ &= \max\{\sharp(Y) \ : \ Q_{\mathscr{F},Y} \text{ is a } \mathbb{Q} - \text{basis of } \mathfrak{q}_Y \text{asvct.sp.}\}. \end{aligned}$$

Proof We proof each claim separately:

- *Claim (i):* Immediate follows from Identity (3.9).
- *Claim (ii):* The equivalence between (b) and (c) is obvious by the definitions of $\mathfrak{q}_Y$ and $\mathfrak{q}_Z$. Claim i) immediately yields $(a) \Longrightarrow (c)$. As for the implication $(b) \Longrightarrow (a)$, assume that $q_Z = fq_Y$ for some $f \in \mathbb{Q}[V_n]$. If $Z \not\subseteq Y$, then we would have:

  $$1 = q_Z(Z) = f(Z)q_Y(Z) = f(Z) \cdot 0 = 0,$$

  which is impossible.
- *Claim (iii):* The canonical projection $p : \mathbb{Q}[V_n] \longrightarrow \mathbb{Q}[2^Y]$ induces:

  $$\begin{aligned} \varphi : \mathfrak{q}_Y &\longrightarrow \mathbb{Q}[2^Y] \\ f &\longmapsto f \restriction_{2^Y}. \end{aligned}$$

Obviously this is a $Q[V_n]$-morphism.

- *Claim (iv):* It is obvious since 2^Y may be identified with V_m, where $m = \sharp(Y)$, and using Propositions 10 and 13.
- *Claim (v):* Given any function $f \in \mathbb{Q}[V_n]$, if f vanishes at all points $S \in 2^Y$, then, we have that

$$fq_Y(S) = 0, \ \forall S \in 2^Y.$$

Additionally, we know that

$$fq_Y(T) = 0, \ \forall T \notin 2^Y.$$

Thus, if $f \in I_{\mathbb{Q}}(2^Y)$, then $fq_Y \in \mathbb{Q}[V_n]$ is the null polynomial function and, hence, $f \in Ann_{\mathbb{Q}[V_n]}(q_Y)$. Conversely, if $f \in Ann_{\mathbb{Q}[V_n]}(2^Y)$, then

$$0 = fq_Y(S) = f(S), \ \forall S \subseteq Y,$$

and, hence, $f \in I(2^Y)$.

The second claim is obvious from Identity (3.10).

- *Claim (vi):* Observe that $\mathscr{F}$ shatters Y if and only if the following two sets are equal:

$$Q_{\mathscr{F},Y} = \{q_{F\cap Y} \ : \ F \in \mathscr{F}\} = \{q_S \ : \ S \subseteq Y\}.$$

Hence, implication $\Longrightarrow$ is obvious. The converse implication follows since the dimension of $\mathfrak{q}_Y$ as $\mathbb{Q}$-vector space equals the dimension of $\mathbb{Q}[2^Y]$ and this dimension is $2^{\sharp(Y)}$. Thus, if $Q_{\mathscr{F},Y}$ is a basis of $\mathfrak{q}_Y$ as $\mathbb{Q}$-vector space, we conclude $\sharp(Q_{\mathscr{F},Y}) = 2^{\sharp(Y)}$. As $Q_{\mathscr{F},Y}$ is always included in $\{q_S \ : \ S \subseteq Y\}$, if both finite sets have the same cardinality they must be equal and, hence, $\mathscr{F}$ shatters Y. The last claim of *vi*) follows by these arguments.

The last claim of the statement immediately follows from Claim *vi*). □

4.2 Closed downward algebraic subsets of V_n are in bijection with ideals $\mathfrak{q}_{\mathscr{F}} \subseteq \mathbb{Q}[V_n]$

This subsection explains the role of the ideals $\mathfrak{q}_{\mathscr{F}}$ introduced above in terms of closed downward systems of generators.

Definition 7 With the same notations as above, let $\mathscr{F} \subseteq V_n$ be a subset. We say that $\mathscr{F}$ is closed downward if for every $F, Y \in V_n$, if $Y \in \mathscr{F}$ and $F \subseteq Y$, then $F \in \mathscr{F}$.

We follow the same notations as in the previous subsection.

Lemma 18 *Let $\mathscr{F} \subseteq V_n$ be a subset. Then, we have:*

$$\mathfrak{q}_{\mathscr{F}} = (q_{Y_1}, \ldots, q_{Y_r}) := \mathfrak{q}_{Y_1} + \cdots + \mathfrak{q}_{Y_r},$$

where

$$\mathscr{F}^{(\max)} = \{Y_1, \dots, Y_r\},$$

and $\mathscr{F}^{(\max)} \subseteq \mathscr{F}$ *is the set defined in Identity* (4.5).

Proof Inclusion $\supseteq$ is obvious since $q_{Y_i} \in Q_{\mathscr{F}}$ for every $i \in \{1, \dots, r\}$. On the other hand, given $F \in \mathscr{F}$, there must be some maximal element Y_i such that $F \subseteq Y_i$. Using Claim *i*) of Proposition 17, we have that $q_F = q_F q_{Y_i} \in \mathfrak{q}_{Y_i}$ and we have proved the inclusion of ideals $\mathfrak{q}_{\mathscr{F}} \subseteq \mathfrak{q}_{Y_1} + \cdots + \mathfrak{q}_{Y_r}$. □

We may introduce the downward closure of a subset $\mathscr{F} \subseteq 2^{[n]}$ as follows:

Definition 8 (*Closure downward*) Given $\mathscr{F} \subseteq 2^{[n]}$ we define the downward closure of $\mathscr{F}$ as the set

$$\overline{\mathscr{F}}^{d} := \{Y \in 2^{[n]} \ : \ \exists F \in \mathscr{F},\ Y \subseteq F\}.$$

The following statement summarizes the main properties of subsets of V_n that are closed downward:

Proposition 19 *Let* $\mathscr{F} \subseteq V_n$ *be a algebraic subset of* V_n. *The following properties are equivalent*:

(i) $\mathscr{F}$ *is closed downward.*

(ii) $\mathscr{F}$ *is a finite union of boxes, i.e. there exist* $Z_1, \dots, Z_s \in V_n$ *such that*

$$\mathscr{F} = \bigcup_{j=1}^{s} 2^{Z_j}.$$

(iii) $\mathscr{F}$ *is the finite union of the boxes determined by its maximal elements, i.e.*

$$\mathscr{F} = \bigcup_{i=j}^{r} 2^{Y_j},$$

where $\mathscr{F}^{(\max)} = \{Y_1, \dots, Y_r\}$.

(iv) *The vector subspace* $W_{\mathscr{F}}$ *associated to* $\mathscr{F}$ *is an ideal in* $\mathbb{Q}[V_n]$.

(v) *The following equality holds*:

$$W_{\mathscr{F}} = \mathfrak{q}_{\mathscr{F}} = \mathfrak{q}_{Y_1} + \cdots + \mathfrak{q}_{Y_r} = (q_{Y_1}, \dots, q_{Y_r}),$$

where $\mathscr{F}^{(\max)} = \{Y_1, \dots, Y_r\}$.

(vi) *For every* $i \in [n]$ *and for every* $F \in \mathscr{F}$, $(1 - X_i)q_F \in W_{\mathscr{F}}$.

(vii) *For every* $i \in [n]$ *and for every* $f \in W_{\mathscr{F}}$, $(1 - X_i)f \in W_{\mathscr{F}}$.

In particular, if $\mathscr{F}$ is closed downward we have

$$VCD(\mathscr{F}) := \max\{\sharp(F) \ : \ F \in \mathscr{F}\} = \max\{\sharp(Y) \ : \ Y \in \mathscr{F}^{(\max)}\}.$$

and

$$\mathscr{F} \subseteq B_H(0, VCD(\mathscr{F})),$$

where $B_H(\mathbf{0}, i) \subseteq V_n$ *is the closed ball with center* $\mathbf{0} = \emptyset \in V_n$ *and radius* i *with respect to the Hamming distance.*

Proof The equivalences between i), ii) and iii) are immediate. As for the other equivalences, we have:

- $(i) \Longrightarrow (iv)$: Assume that $\mathscr{F}$ is closed downward. let us consider $f \in W_{\mathscr{F}}$ and $g \in \mathbb{Q}[V_n]$. As $Q_{\mathscr{F}}$ is a basis of $W_{\mathscr{F}}$ as vector subspace of $\mathbb{Q}[V_n]$ there exists $\{\lambda_F \ : \ F \in \mathscr{F}\} \subseteq \mathbb{Q}$ such that

$$f = \sum_{F \in \mathscr{F}} \lambda_F q_F \in W_{\mathscr{F}}.$$

On the other hand, $\mathscr{B}_2 := \{q_Y \ : \ Y \subseteq [n]\}$ is a basis of $\mathbb{Q}[V_n]$ as vector space. Then, there exists $\{\mu_Y \ : \ Y \in V_n\} \subseteq \mathbb{Q}$ such that

$$g = \sum_{Y \in V_n} \mu_Y q_Y.$$

Then, from Claim i) of Proposition 17 we conclude

$$gf = \sum_{F \in \mathscr{F}, Y \in V_n} \lambda_F \mu_Y q_F q_Y = \sum_{F \in \mathscr{F}, Y \in V_n} \lambda_F \mu_Y q_{F \cap Y}.$$

As $\mathscr{F}$ is closed downward, for every $F \in \mathscr{F}$ and every $Y \in V_n$, $F \cap Y \in \mathscr{F}$ and, hence, $q_{F \cap Y} \in Q_{\mathscr{F}} \subseteq W_{\mathscr{F}}$. Thus, we conclude that $gf \in W_{\mathscr{F}}$ and $W_{\mathscr{F}}$ must be an ideal in $\mathbb{Q}[V_n]$.
- $(iv) \Longleftrightarrow (v)$: From the previous Lemma we already know that:

$$\mathfrak{q}_{\mathscr{F}} = \mathfrak{q}_{Y_1} + \cdots + \mathfrak{q}_{Y_r} = (q_{Y_1}, \ldots, q_{Y_r}).$$

Thus, as $W_{\mathscr{F}} \subseteq \mathfrak{q}_{\mathscr{F}}$ and $\{q_{Y_1}, \ldots, q_{Y_r}\} \subseteq Q_{\mathscr{F}} \subseteq W_{\mathscr{F}}$, if $W_{\mathscr{F}}$ is an ideal, then it must be equal to $\mathfrak{q}_{\mathscr{F}}$. The converse is immediate.
- $(v) \Longrightarrow (vi)$: As $W_{\mathscr{F}}$ is an ideal, multiplying by $1 - X_i$ remains in $W_{\mathscr{F}}$ and vi) follows.
- $(vi) \Longrightarrow (i)$: Again, from Claim i) of Proposition 17, since every element in $\mathbb{Q}[V_n]$ is idempotent, we conclude that

$$(1 - X_i) q_F = \begin{cases} q_F, & \text{if } i \notin F, \\ q_{F \setminus \{i\}}, & \text{if } i \in F, \end{cases} \tag{4.8}$$

and, hence, $(1 - X_i)q_F = q_{F\setminus\{i\}}$, for every $F \subseteq [n]$. Moreover, we observe that for every $Z \subseteq [n]$, $q_Z \in W_{\mathscr{F}}$ if and only if $Z \in \mathscr{F}$. Note that if $q_Z \in W_{\mathscr{F}}$, there exist $\{\lambda_F \ : \ F \in \mathscr{F}\} \subseteq \mathbb{Q}$ such that

$$q_Z = \sum_{F\in\mathscr{F}} \lambda_F q_F.$$

Thus, if $Z \notin \mathscr{F}$, we would have a non-trivial linear combination of elements in the basis $\mathscr{B}_2$ equal to 0:

$$q_Z + \sum_{F\in\mathscr{F}} (-\lambda_F)q_F = 0.$$

And this cannot be possible. Thus, claim *vi*) means that for every $F \in \mathscr{F}$ and for every $i \in [n]$, $F \setminus \{i\} \in \mathscr{F}$. Obviously, this means that given $F \in \mathscr{F}$ and given $Y \subseteq F$, then $Y \in \mathscr{F}$ and $\mathscr{F}$ is closed downward.

- (*vi*) $\Longleftrightarrow$ (*vii*): This is also obvious by identical arguments to those used in the previous implication. If $f \in W_{\mathscr{F}}$, then there exists $\{\lambda_F \ : \ F \in \mathscr{F}\} \subseteq \mathbb{Q}$ such that

$$f = \sum_{F\in\mathscr{F}} \lambda_F q_F.$$

Thus,

$$(1 - X_i)f = \sum_{F\in\mathscr{F}} \lambda_F (1 - X_i)q_F,$$

and because of *vi*) we conclude that $(1 - x_i)f \in W_{\mathscr{F}}$. The converse is trivial.

As for the last claim, if $\mathscr{F}$ is closed downward, the VC dimension of $\mathscr{F}$ is determined by the cardinality of the maximal box 2^Y contained in $\mathscr{F}$ and the equality follows. From claims *ii*) or *iii*), it is clear that if $\mathscr{F}$ is closed downward all its elements $F \in \mathscr{F}$ belong to some box 2^{Y_i} and hence, $\sharp(F) \leq \sharp(Y_i) \leq VCD(\mathscr{F})$. Thus, we conclude that $\mathscr{F} \subseteq B_H(\mathbf{0}, VCD(\mathscr{F}))$ as claimed. □

Whereas the vector subspace $W_{\mathscr{F}}$ is determined (and determines) the class $\mathscr{F}$ (because $Q_{\mathscr{F}} \subseteq \mathscr{B}_2$ is a family of linearly independent functions), the ideal $\mathfrak{q}_{\mathscr{F}}$ is determined (and determines) the class $\mathscr{F}^{(\max)}$ of maximal elements in $\mathscr{F} \subseteq 2^{[n]}$. Also the ideal $\mathfrak{q}_{\mathscr{F}}$ is determined (and determines) the downward closure $\overline{\mathscr{F}}^d$. This is explained in the following statements.

Lemma 20 *Let $\mathscr{F}, \mathscr{G} \subseteq 2^{[n]}$ be two subsets of V_n. Then, $\mathfrak{q}_{\mathscr{F}} \subseteq \mathfrak{q}_{\mathscr{G}}$ if and only if for all $F \in \mathscr{F}$ there exists $G \in \mathscr{G}$ such that $F \subseteq G$.*

Proof Assume the following property holds:

$$\forall F \in \mathscr{F}, \ \exists G \in \mathscr{G}, \ F \subseteq G.$$

Then, for every $q_F \in Q_{\mathscr{F}}$, then there is $G \in \mathscr{G}$ such that $F \subseteq G$. According to Claim *ii*) of Proposition 17, we have that $q_G \mid q_F$ in $\mathbb{Q}[V_n]$. Thus, we have that $\mathfrak{q}_{\mathscr{F}} \subseteq \mathfrak{q}_{\mathscr{G}}$ as wanted.

As for the converse, assume that $\mathfrak{q}_{\mathscr{F}} \subseteq \mathfrak{q}_{\mathscr{G}}$ and consider $F \in \mathscr{F}$. Then, $q_F \in \mathfrak{q}_G$ and, then, there exists $\{f_G \ : \ G \in \mathscr{G}\} \subseteq \mathbb{Q}[V_n]$ such that

$$q_F = \sum_{G\in\mathscr{G}} f_G q_G.$$

As $\mathscr{B}_2$ is a basis of $\mathbb{Q}[V_n]$ as vector space, for every $G \in \mathscr{G}$ there exists $\{\lambda_{Y,G} \ : \ Y \in V_n\} \subseteq \mathbb{Q}$ such that

$$f_G := \sum_{Y\in V_n} \lambda_{Y,G} q_Y.$$

Thus, we conclude:

$$q_F = \sum_{G\in\mathscr{G}, Y\in V_n} \lambda_{Y,G} q_Y q_G = \sum_{G\in\mathscr{G}, Y\in V_n} \lambda_{Y,G} q_{Y\cap G}.$$

If $F \nsubseteq G$ for all $G \in \mathscr{G}$ we would have a non-trivial linear combination of elements in $\mathscr{B}_2$ equal to zero:

$$q_F + \sum_{G\in\mathscr{G}, Y\in V_n} (-\lambda_{Y,G}) q_{Y\cap G} = 0,$$

which cannot be possible. Then, there must be some $Y \in V_n$ and $G \in \mathscr{G}$ such that $F = Y \cap G$. Hence, $F \subseteq G$ and the Lemma follows. □

Proposition 21 *Let $\mathscr{F}, \mathscr{G} \subseteq 2^{[n]}$ be two subsets of V_n. Then, the following are equivalent properties*:

(i) $\mathfrak{q}_{\mathscr{F}} = \mathfrak{q}_{\mathscr{G}}$.
(ii) $\mathscr{F}^{(\max)} = \mathscr{G}^{(\max)}$.
(iii) $\overline{\mathscr{F}}^d = \overline{\mathscr{G}}^d$.

In particular, the mapping $\mathscr{F} \longmapsto \mathfrak{q}_{\mathscr{F}}$ is a bijection between the the subsets of $2^{[n]}$ which are closed downward and the ideals of the form $\mathfrak{q}_{\mathscr{F}}$.

Proof First of all, the implication *ii*) $\Longrightarrow$ *i*) immediately follows from Lemma 18 above. As for the implication *i*) $\Longrightarrow$ *ii*), assume that $\mathfrak{q}_{\mathscr{F}} = \mathfrak{q}_{\mathscr{G}}$ and let $F \in \mathscr{F}^{(\max)}$. Because of Lemma 20, as $\mathfrak{q}_{\mathscr{F}} \subseteq \mathfrak{q}_{\mathscr{G}}$, there must be $G \in \mathscr{G}$ such that $F \subseteq G$. Then, there will be $G' \in \mathscr{G}^{(\max)}$ such that $F \subseteq G'$. Again, since $\mathfrak{q}_{\mathscr{G}} \subseteq \mathfrak{q}_{\mathscr{F}}$ too, there must be $F' \in \mathscr{F}$ such that $G' \subseteq F'$ and, hence $F \subseteq G \subseteq G' \subseteq F'$. As $F \in \mathscr{F}^{(\max)}$ is maximal in $\mathscr{F}$, then $F = G = G' = F'$. In particular $F = G' \in \mathscr{G}^{(\max)}$ and we have $\mathscr{F}^{(\max)} \subseteq \mathscr{G}^{(\max)}$. Changing the roles of $\mathscr{G}^{(\max)}$ and $\mathscr{F}^{(\max)}$, we conclude the equality of both sets, and, hence, *ii*) follows from *i*). The equivalence between *ii*) and *iii*) is obvious since two subsets $\mathscr{F}, \mathscr{G} \subseteq 2^{[n]}$ have the same downward closure if and only if their maximal elements are the same. □

The following statement explains the difference between the ideal $\mathfrak{q}_{\mathscr{F}}$ and the vector subspace $W_{\mathscr{F}}$.

Corollary 22 *Given* $\mathscr{F} \subseteq 2^{[n]}$ *the following equality holds*:

$$\dim_{\mathbb{Q}} \left(\mathfrak{q}_{\mathscr{F}}/W_{\mathscr{F}}\right) = \sharp\left(\overline{\mathscr{F}}^{d}\right) - \sharp(\mathscr{F}),$$

where $\dim_{\mathbb{Q}}$ *means the dimension as vector space and* U/V *stands for the quotient of vector spaces* $V \subseteq U$.

Proof That is immediate by comparing the basis $Q_{\overline{\mathscr{F}}^{d}}$ of $\mathfrak{q}_{\mathscr{F}}$ and $Q_{\mathscr{F}}$ of $W_{\mathscr{F}}$. □

4.3 Monomial ideals in $\mathbb{Q}[V_n]$ and closed upward algebraic subsets of V_n

Monomial ideals is a standard subject of research in symbolic methods used in Computational Algebraic Geometry (see, for instance, [19, 27] and references therein). A monomial ideal in $\mathbb{Q}[V_n]$ is an ideal generated by some monomials in this $\mathbb{Q}$-algebra. Namely, given $\mathscr{G} \subseteq V_n$ the monomial ideal generated by the monomials associated to $\mathscr{G}$ is the ideal:

$$\mathfrak{p}_{\mathscr{G}} := \left(p_S \ : \ S \in \mathscr{G}\right).$$

Let $\psi : \mathbb{Q}[V_n] \longrightarrow \mathbb{Q}[V_n]$ be the biregular $\mathbb{Q}$-algebra isomorphism introduced at Identity (3.7). The reader may easily see that this $\mathbb{Q}$-algebra isomorphism satisfies the following identity for every $\mathscr{G} \subseteq V_n$:

$$\psi(\mathfrak{p}_{\mathscr{G}}) = \mathfrak{q}_{C(\mathscr{G})}, \tag{4.9}$$

where $C(\mathscr{G}) := \{[n]\setminus S \in V_n \ : \ S \in \mathscr{G}\} \subseteq V_n$ is the class of complements of the sets in $\mathscr{G}$. This suggests the idea of considering algebraic subsets of V_n which are closed upward.

Definition 9 With these notations a subset $\mathscr{G} \subseteq V_n$ is closed upward if the following holds:

$$\forall G \in \mathscr{G}, \ \forall Z \in V_n, \ G \subseteq Z \implies Z \in \mathscr{G}.$$

Observe that for every $\mathscr{G} \subseteq V_n$, $\mathscr{G}$ is closed upward if and only if $C(\mathscr{G})$ is closed downward. Similarly to what we did in the previous section, we may also consider the closure upward of a class $\mathscr{G} \subseteq V_n$ as follows:

$$\overline{\mathscr{G}}^{u} := \{Z \in V_n \ : \ \exists G \in \mathscr{G},\ G \subseteq Z\}. \tag{4.10}$$

For an atom $\mathscr{G} := \{G\}$, we may consider its upward closure which is given by the following identity:

$$\overline{\{G\}}^{u} := \{Z \in V_n \ : \ G \subseteq Z\}.$$

Similarly, we may also consider the class $\mathscr{G}^{(\min)}$ of minimal subsets in a class $\mathscr{G} \subseteq V_n$ with respect to $\subseteq$. We obviously have that $\mathscr{G}$ is closed upward if and only if the following equality holds:

$$G = \overline{\mathscr{G}}^{u} = \bigcup_{G \in \mathscr{G}^{(\min)}} \overline{\{G\}}^{u}.$$

In fact, observe that the following relates closures upward and downward for every subset $\mathscr{G} \subseteq V_n$:

$$\overline{\mathscr{G}}^{u} := C\left(\overline{C(\mathscr{G})}^{d}\right).$$

The proof is straightforward and we omit it.

Having in mind these identities we easily conclude from Proposition 21 the following relation between monomial ideals in $\mathbb{Q}[V_n]$ and closed upward subclasses of $2^{[n]}$:

Proposition 23 *With these notations, let $\mathscr{F}, \mathscr{G} \subseteq 2^{[n]}$ two classes of subsets of $[n]$. Then, the following claims are equivalent:*

(i) *The monomial ideals they generate are equal, i.e. $\mathfrak{p}_{\mathscr{F}} = \mathfrak{p}_{\mathscr{G}}$.*
(ii) *Both sets have same the minimal elements, i.e. $\mathscr{F}^{(\min)} = \mathscr{G}^{(\min)}$.*
(iii) *The upward closures of both sets agree, i.e. $\overline{\mathscr{F}}^{u} = \overline{\mathscr{G}}^{u}$.*

In particular, the mapping $\mathscr{G} \longmapsto \mathfrak{p}_{\mathscr{G}}$ is a bijection between the closed upward subsets of $2^{[n]}$ and the monomial ideals of $\mathbb{Q}[V_n]$.

Although this statement is probably known, we include it because it can illustrate the connection between the ideals generated by elements in the two bases $\mathscr{B}_1$ and $\mathscr{B}_2$. Monomial ideals, being more popular, are related to ideals of the type $\mathfrak{p}_{\mathscr{F}}$. While the main interest of this manuscript concerns the ideals $\mathfrak{q}_{\mathscr{F}}$ and their relation with Combinatorics.

4.4 The technique of shifting in terms of ideals and subspaces: the "distance" to the closed downward subset of the same cardinality

In [14], D. Haussler used the technique of "shifting" to produce a proof of Suaer-Shelah-Perles Lemma. This technique seems to appear first in [11] and (independently) in [1]. The technique consists in performing a chain of shifts on a given set $\mathscr{F}$ that transforms $\mathscr{F}$ into a new subset $\mathscr{F}'$ with the same cardinality, smaller VC dimension and such that $\mathscr{F}'$ is closed downward. In our language, this yields a series of transformations of $\mathscr{F}$ that minimizes the distance between $W_{\mathscr{F}}$ and $\mathfrak{q}_{\mathscr{F}}$. We must cite the work [18], and references therein, who also worked an algebraic description of the shifting technique in terms of Göbner basis and monomial ideals.

We just want to emphasize the role played by the ideals $\mathfrak{q}_{\mathscr{F}}$ and the subspaces $W_{\mathscr{F}}$ in relation to the shifting technique.

Definition 10 With the same notations as above, for every $\mathscr{F} \subseteq 2^{[n]}$ and every $i \in [n]$, we say that $\mathscr{F}$ is closed with respect to i if the following property holds:

$$\forall F \in \mathscr{F},\ F \setminus \{i\} \in \mathscr{F}. \tag{4.11}$$

According to our discussions in the previous section we easily conclude:

Lemma 24 *With these notations, given $\mathscr{F} \subseteq 2^{[n]}$ we have:*

(i) *For each $i \in [n]$, the following properties are equivalent:*

(a) *$\mathscr{F}$ is closed with respect to i,*
(b) *For all $F \in \mathscr{F}$, $(1 - X_i)q_F \in W_{\mathscr{F}}$,*
(c) *Forall $f \in W_{\mathscr{F}}$, $(1 - X_i)f \in W_{\mathscr{F}}$.*

(ii) *If $\mathscr{F}$ is closed with respect to i for all $i \in [n]$, then $\mathscr{F}$ is closed downward, $W_{\mathscr{F}} = \mathfrak{q}_{\mathscr{F}}$, and the following also holds:*

- *$VCD(\mathscr{F}) \leq \max\{\sharp(Y) \ :\ Y \in \mathscr{F}^{(\max)}\}$,*
- *$\mathscr{F} \subseteq B_H(\mathbf{0}, VCD(\mathscr{F}))$.*

In particular, if $\mathscr{F}$ is closed with respect to i for all $i \in [n]$, $d = VCD(\mathscr{F})$, then Sauer–Shelah–Perles upper bound holds:

$$\sharp(\mathscr{F}) \leq \sharp(B_H(\mathbf{0}, d)) \leq \sum_{i=0}^{d} \binom{n}{i}.$$

Proof In order to prove Claim *i*) simply recall that $\{q_G \ :\ G \in \mathscr{F}\}$ is a $\mathbb{Q}$-linearly independent family of polynomial functions and that Identity (4.8) holds. Thus, $\mathscr{F}$ is closed with respect to i if and only if for all $F \in \mathscr{F}$, $(1 - X_i)q_F \in W_{\mathscr{F}}$. Similar arguments to those Proposition 19 yield the other claims. □

Thus, we may view this shifting technique as a way to transform a given family $\mathscr{F} \subseteq 2^{[n]}$ into another one $S_i(\mathscr{F}) \subseteq 2^{[n]}$ with the same cardinality which is closed with respect to $i \in [n]$. This transformation works as follows:

Given $\mathscr{F} \subseteq 2^{[n]}$ and given $i \in [n]$, define

$$\mathscr{F}_i^+ := \{F \in \mathscr{F} \ : \ F \setminus \{i\} \in \mathscr{F}\},$$

and

$$\mathscr{F}_i^- := \mathscr{F} \setminus \mathscr{F}_i^+.$$

We then define:

$$S_i(\mathscr{F}) := \mathscr{F}_i^+ \cup \{F \setminus \{i\} \ : \ F \in \mathscr{F}_i^-\}. \tag{4.12}$$

Obviously, by construction $S_i(\mathscr{F})$ is closed with respect to i. Moreover, they have the same cardinality since the following is an injective mapping:

$$\begin{array}{rcl} S_i : \mathscr{F} & \longmapsto & 2^{[n]} \\ F & \longmapsto & \begin{cases} F, & \text{if } F \in \mathscr{F}_i^+, \\ F \setminus \{i\}, & \text{otherwise.} \end{cases} \end{array} \tag{4.13}$$

The following statement resumes some of the elementary properties of this transformation:

Proposition 25 *The following properties hold*:

(i) *S_i is a bijection between $\mathscr{F}$ and $S_i(\mathscr{F})$ whose definition depends on $\mathscr{F}$.*

(ii) *$VCD(S_i(\mathscr{F})) \leq VCD(\mathscr{F})$.*

(iii) *For every $i, j \in [n]$, if $\mathscr{F}$ is closed with respect to $j \in [n]$, then $S_i(\mathscr{F})$ is closed both with respect to i and j.*

(iv) *The following is an equality between vector subspaces of* $\mathbb{Q}[V_n]$:

$$W_{S_i(\mathscr{F})} = W_{\mathscr{F}_i^+} \oplus \mathbb{Q}\langle\{(1 - X_i)q_F \ : \ F \in \mathscr{F}_i^-\}\rangle.$$

(v) *The following is an inclusion between ideals*:

$$\mathfrak{q}_{S_i(\mathscr{F})} \subseteq \mathfrak{q}_{\mathscr{F}},$$

and equality holds if and only if $\mathscr{F}^{(\max)} \subseteq \mathscr{F}_i^+$.

(vi) *The transformation S_i "reduces" the distance between $\mathfrak{q}_{\mathscr{F}}$ and $W_{\mathscr{F}}$. Namely, either $\mathfrak{q}_{S_i(\mathscr{F})} = \mathfrak{q}_{\mathscr{F}}$ or*

$$\dim_{\mathbb{Q}} \left(\mathfrak{q}_{S_i(\mathscr{F})}/W_{S_i(\mathscr{F})}\right) < \dim_{\mathbb{Q}} \left(\mathfrak{q}_{\mathscr{F}}/W_{\mathscr{F}}\right).$$

Proof Claim *i*) is obvious, whereas Claim *ii*) is an easy exercise (which was already in [14]). The remaining claims are also easy to prove from the definitions. □

Let the reader observe that the notation S_i is somehow improper since S_i depends both on i and $\mathscr{F}$. We keep this improper notation assuming that the reader may understand the subtle differences. Thus, given any word $\omega = i_1 \cdots i_r \in [n]^*$, we denote by $S_\omega(\mathscr{F})$ the subset of $2^{[n]}$ given (with this improper notation) by:

$$S_\omega(\mathscr{F}) := S_{i_1}\left(S_{i_2}\left(\cdots\left(S_{i_r}(\mathscr{F})\right)\cdots\right)\right).$$

One may easily prove by induction (using Claim *iii*) of the previous Proposition) that if $\omega \in [n]^*$ and $J \subseteq [n]$ is such that $\omega \in J^*$, then for all $j \in J$, $S_\omega(\mathscr{F})$ is closed with respect to j. We thus conclude:

Proposition 26 *There is some $\omega \in [n]^*$ such that $S_\omega(\mathscr{F})$ is closed with respect to any $i \in [n]$. In particular, we have that*

$$S_i(S_\omega(\mathscr{F})) = S_\omega(\mathscr{F}),\ \forall i \in [n],$$

and, hence, the following properties also hold:

(i) $VCD(S_\omega(\mathscr{F})) \leq VCD(\mathscr{F})$,

(ii) $S_\omega(\mathscr{F})$ is closed downward,

(iii) $\mathfrak{q}_{S_\omega(\mathscr{F})} = W_{S_\omega(\mathscr{F})}$,

(iv) $\dim_{\mathbb{Q}}(\mathfrak{q}_{S_\omega(\mathscr{F})}/W_{S_\omega(\mathscr{F})}) = 0$.

(v) $\dim_{\mathbb{Q}}(W_{S_\omega(\mathscr{F})}) = \sharp(S_\omega(\mathscr{F})) = \sharp(\mathscr{F}) = \dim_{\mathbb{Q}}(W_{\mathscr{F}})$.

In particular, Sauer–Shelah–Perles upper bound holds for $\mathscr{F}$:

$$\sharp(\mathscr{F}) \leq \sum_{i=0}^{VCD(\mathscr{F})} \binom{n}{i}.$$

Given a word $\omega = i_1 \cdots i_r \in [n]^*$, denote by $\omega_k := i_k \cdots i_r \in [n]^*$ the word obtained by eliminating the prefix of length $k-1$ in ω, where $\omega_{r+1} = \lambda$ is the empty word. We have a descending chain of ideals:

$$\mathfrak{q}_{\mathscr{F}} = \mathfrak{q}_{S_{\omega_{r+1}}(\mathscr{F})} \supseteq \mathfrak{q}_{S_{\omega_r}(\mathscr{F})} \supseteq \cdots \supseteq \mathfrak{q}_{S_{\omega_1}(\mathscr{F})} \supseteq \mathfrak{q}_{S_{\omega_0}(\mathscr{F})} = \mathfrak{q}_{S_\omega(\mathscr{F})}.$$

This chain corresponds to a descending chain of dimensions:

$$\dim_{\mathbb{Q}}\left(\mathfrak{q}_{\mathscr{F}}/W_{\mathscr{F}}\right) \geq \dim_{\mathbb{Q}}\left(\mathfrak{q}_{S_{\omega_r}(\mathscr{F})}/W_{S_{\omega_r}(\mathscr{F})}\right) \geq \cdots \geq \dim_{\mathbb{Q}}\left(\mathfrak{q}_{S_\omega(\mathscr{F})}/W_{S_\omega(\mathscr{F})}\right) = 0.$$

The following is an immediate consequence of our approach which is rather similar to the statements in Lemma 1 of [6]:

Corollary 27 *For every $\mathscr{F} \subseteq 2^{[n]}$, there is $\mathscr{G} \subseteq 2^{[n]}$ such that the following properties hold:*

(i) $VCD(\mathscr{G}) \leq VCD(\mathscr{F})$,
(ii) $\sharp(\mathscr{G}) = \sharp(\mathscr{F})$,
(iii) *$\mathscr{G}$ is closed downward and* $W_{\mathscr{G}} = \mathfrak{q}_{\mathscr{G}} \subseteq \mathfrak{q}_{\mathscr{F}}$.

All in all, the shifting technique is a transformation that goes downward (by modifying unstable elements of $\mathscr{F}$) instead of adding missed subsets to compute the downward closure of $\mathscr{F}$. In some still unprecise sense to be still explored, the length of the shortest word ω that satisfies the previous Proposition measures the minimum distance of $\mathscr{F}$ to a closed downward set $\mathscr{G}$ of the same cardinality.

5 The principal ideal $\mathfrak{q}_Y$ and Sauer–Shelah–Perles Lemma: rank VC dimension

We are now in conditions to prove Sauer–Shelah–Perles Lemma. We have the ascending chain of closed balls in V_n with respect to the Hamming distance:

$$W_0 \subsetneq W_1 \subsetneq W_2 \subsetneq \cdots \subsetneq W_n,$$

where $W_i := B_H(\mathbf{0}, i) \subseteq V_n$ is the closed ball with center $\mathbf{0} \in V_n$ and radius i with respect to the Hamming distance. Take the class $Q_{\mathscr{F}} \subseteq \mathbb{Q}[V_n]$ defined in Identity (4.4) above.

Given $r \in \{0, \ldots, n\}$, we may define the following subclasses of polynomial functions:

$$Q_{\mathscr{F},r} := \{q_F \restriction_{W_r} \ : \ F \in \mathscr{F}\} \subseteq \mathbb{Q}[W_r]. \tag{5.1}$$

Note that $Q_{\mathscr{F},n} = Q_{\mathscr{F}}$.

Every inclusion $i_r : W_r \hookrightarrow W_{r+1}$ induces a natural onto morphism of $\mathbb{Q}$-algebras:

$$\begin{array}{rccl} i_r^* : & \mathbb{Q}[W_{r+1}] & \longrightarrow & \mathbb{Q}[W_r] \\ & f & \longmapsto & f \restriction_{W_r} . \end{array}$$

Definition 11 (*Rank VC-dimension*) With these notations, we define the rank VC-dimension of $\mathscr{F}$ as the minimum r such that $Q_{\mathscr{F},r}$ is a $\mathbb{Q}$-linearly independent family of polynomial functions in $\mathbb{Q}[W_r]$. Namely, the minimum r such that

$$\dim_{\mathbb{Q}} \left(\mathbb{Q}\langle Q_{\mathscr{F},r}\rangle\right) = \dim_{\mathbb{Q}} \left(\langle Q_{\mathscr{F},n}\rangle\right),$$

where $\mathbb{Q}\langle Q_{\mathscr{F},i}\rangle$ is the vector subspace spanned by $Q_{\mathscr{F},i}$ in $\mathbb{Q}[W_i]$. We denote by $RVCD(\mathscr{F})$ this rank VC-dimension of $\mathscr{F}$.

The term rank is coined because $RVCD$ is related to the rank of some matrices. Namely, assume $N := \sharp(\mathscr{F}) \in \mathbb{N}$, and for every non-negative integer $d \in \mathbb{N}$ define

$\delta(d) := \deg(W_d) = \sharp(W_d)$. We consider a matrix $M_{\mathscr{F},d} \in \mathscr{M}_{N\times\delta(d)}(\mathbb{Q})$ whose rows $\rho_{F,d}$, for $F \in \mathscr{F}$, are given by the following rule:

$$\rho_{F,d} := \left(q_F(S) \ : \ S \in W_d\right) \in \mathbb{Q}^{\delta}.$$

Thus, the matrix may be described by:

$$M_{\mathscr{F},d} := \left(\rho_{F,d}\right)_{F\in\mathscr{F}} \in \mathscr{M}_{N\times\delta(d)}(\mathbb{Q}).$$

The rank of these matrices is clearly a monotone increasing function: for every d we have that:

$$\operatorname{rank}(M_{\mathscr{F},d}) \leq \operatorname{rank}(M_{\mathscr{F},d+1}).$$

The following Lemma shows the relation between *RVCD* and the ranks of these matrices:

Lemma 28 *With these notations, we have*:

(i) $\operatorname{rank}(M_{\mathscr{F},n}) = \sharp(\mathscr{F})$.

(ii) *We have*

$$\operatorname{rank}(M_{\mathscr{F},r}) = \dim_{\mathbb{Q}}\left(\mathbb{Q}\langle Q_{\mathscr{F},r}\rangle\right),$$

In particular, we have

$$RVCD(\mathscr{F}) := \min\{r \in \{0,\dots,n\} \ : \ \operatorname{rank}(M_{\mathscr{F},r}) = \sharp(\mathscr{F})\}.$$

Proof Claim *i*) is immediate ($W_n = V_n$) and Claim *ii*) is an almost immediate consequence of the Chinese Remainder Theorem applied to $\mathbb{Q}[W_r]$ (see Identity (2.5)). Namely, we have an isomorphism between the elements of $\mathbb{Q}[W_r]$ and the vectors of their values at the points of W_r:

$$q_F \longleftrightarrow \rho_{F,r} := \left(q_F(S) \ : \ S \in W_r\right) \in \mathbb{Q}^{\delta(r)}.$$

Then, the family of elements $Q_{\mathscr{F},r}$ is linearly independent in $\mathbb{Q}[W_r]$ if and only if the following are linearly independent vectors in $\mathbb{Q}^{\delta(r)}$:

$$\{\rho_{F,r} \ : \ F \in \mathscr{F}\}.$$

this simply means Claim *ii*). The last equality is an immediate consequence of *ii*) and the definition of *RVCD*. □

We are now in conditions to prove Corollary 1 as stated at the Introduction:

Lemma 29 *If* $r = RVCD(\mathscr{F})$, *then we have* $\sharp(\mathscr{F}) = \sharp(Q_{\mathscr{F},n}) = \dim_{\mathbb{Q}}\left(\mathbb{Q}\langle Q_{\mathscr{F},r}\rangle\right)$. *And, hence*,

$$\sharp(\mathscr{F}) = \dim_{\mathbb{Q}}\left(\mathbb{Q}\langle Q_{\mathscr{F},r}\rangle\right) \leq \dim_{\mathbb{Q}}\left(\mathbb{Q}[W_r]\right) = \sharp\left(W_r\right) = \sum_{i=0}^{RVCD(\mathscr{F})} \binom{n}{i}.$$

Proof That is immediate from the definitions. As $\mathbb{Q}\langle Q_{\mathscr{F},r}\rangle$ is a vector subspace of $\mathbb{Q}[W_r]$ and as the dimension of $\mathbb{Q}\langle Q_{\mathscr{F},r}\rangle$ equals the cardinality of $\mathscr{F}$, we obviously have the claimed inequality. □

From these estimates, to conclude the standard form of Sauer–Shelah–Perles Lemma we just need to proof that $VCD(\mathscr{F}) \geq RVCD(\mathscr{F})$ for every $\mathscr{F} \subseteq V_n$. This is done in the following Corollary that includes the classical form of Sauer–Shelah–Perles Lemma:

Corollary 30 *With these notations*, $VCD(\mathscr{F}) \geq RVCD(\mathscr{F})$ *and*, *hence*, *the following inequality holds*:

$$\sharp(\mathscr{F}) \leq \sum_{i=0}^{VCD(\mathscr{F})} \binom{n}{i}. \tag{5.2}$$

Proof Assume that $r = RVCD(\mathscr{F})$. As $RVCD$ is a minimum, we have:

- The family $Q_{\mathscr{F},r}$ is a $\mathbb{Q}$-linearly independent family of elements in $\mathbb{Q}[V_n]$.
- The family $Q_{\mathscr{F},r-1}$ is a $\mathbb{Q}$-linearly dependent family of elements in $\mathbb{Q}[V_n]$.

Then, there exists $\underline{\lambda} := (\lambda_F \ : \ F \in \mathscr{F}) \in \mathbb{Q}^{\sharp(\mathscr{F})}\setminus\{0\}$ such that if we consider $Q := \sum_{F\in\mathscr{F}} \lambda_F q_F \in \mathbb{Q}[V_n]$, the following two properties hold:

$$Q \restriction_{W_r} \in \mathbb{Q}[W_r] \setminus \{0\}. \tag{5.3}$$

$$Q \restriction_{W_{r-1}} \equiv 0. \tag{5.4}$$

Then, there must exist some $Y \in W_r \setminus W_{r-1}$ such that $Q(Y) \neq 0$, whereas Q vanishes at all proper subsets of Y. Then, let us consider the element $Qq_Y \in \mathfrak{q}_Y$. Observe that the following equality holds:

$$Q(Y)\chi_{\{Y\}} = Qq_Y,$$

where $Q(Y) \in \mathbb{Q}$ is a non-zero rational number. Just for explaining this equality: Observe that if $T \subseteq [n]$ is such that $T \nsubseteq Y$, then $q_Y(T) = 0$ and $Qq_Y(T) = 0$. On the other hand, if $S \subsetneq Y$, then $Q(S) = 0$ and, hence, we also have $Qq_Y(S) = 0$. Finally, $Qq_Y(Y) = Q(Y) = Q(Y)\chi_{\{Y\}}(Y)$ and the two polynomial functions are equal. From this equality and Claim *i*) of Proposition 17 we have:

$$Q(Y)\chi_{\{Y\}} = Qq_Y := \sum_{F\in\mathscr{F}} \lambda_F q_F q_Y = \sum_{F\in\mathscr{F}} \lambda_F q_{F\cap Y} = \sum_{S\subseteq Y} \left(\sum_{\substack{F \in \mathscr{F} \\ F\cap Y = S}} \lambda_F \right) q_{F\cap Y}.$$

On the other and, from Identity (3.11) we have:

$$\chi_{\{Y\}} := \sum_{S\subseteq Y} (-1)^{\sharp(Y\setminus S)} q_S.$$

Thus, as $\{q_S \ : \ S \subseteq Y\}$ is a family of linearly independent polynomial functions,we conclude for every $S \subseteq Y$:

$$(-1)^{\sharp(Y\setminus S)} = \left(\sum_{\substack{F \in \mathscr{F} \\ F\cap Y = S}} \lambda_F \right),$$

and, hence, Y is shattered by $\mathscr{F}$ with $\sharp(Y) = r$. This implies $VCD(\mathscr{F}) \geq r$ as wanted. The inequality immediately follows from the one given in Lemma 29. □

6 Frankl–Pach dual transform

In this last section, we proceed to discuss another proof of Sauer–Shelah–Perles Lemma. The variation here just uses duality techniques (as introduced in previous pages). All this manuscript was motivated by the proof of Sauer–Shelah–Perles Lemma in [12]. After reading that proof, this author was convinced that all that proof may be re-obtained by simply using only duality techniques in finite $\mathbb{Q}$-algebras. The content in this final section is just to prove that this author was not wrong in his intuition. And that is why we keep it in this manuscript in spite of the simpler proof of the previous section. We first consider the following two transforms:

(i) First of all, we consider the dual transform induced by the basis $\mathscr{B}_1$:

$$\begin{array}{rcll} \mathscr{D}_1 := (\cdot)^*_{\mathscr{B}_1} : \mathbb{Q}[V_n] & \longrightarrow & \mathbb{Q}[V_n] \\ f & \longmapsto & (f)^*_{\mathscr{B}_1}. \end{array} \tag{6.1}$$

(ii) Secondly, we consider the dual transform induced by the dual basis of $\mathscr{B}_2^*$.

$$\begin{array}{rcll} \mathscr{D}_2 := (\cdot)^*_{\mathscr{B}_2^*} : \mathbb{Q}[V_n] & \longrightarrow & \mathbb{Q}[V_n] \\ f & \longrightarrow & (f)^*_{\mathscr{B}_2^*}, \end{array} \tag{6.2}$$

We call $\mathscr{D}_2$ the *Frankl-Pach dual Transform* since, in our opinion, this dual transform explains the main contriution of [12].

Lemma 31 *With the same notations as above, for every subset* $Y \subseteq [n]$ *and for every* $f \in \mathfrak{q}_Y$*, the following holds*:

(i) $\mathscr{D}_1(f) \in \mathfrak{q}_Y$.
(ii) $\mathscr{D}_2(f) \in \mathfrak{q}_Y$.

Additionally, for every $f \in \mathfrak{q}_Y$ the following equality holds:

$$f = \sum_{W \subseteq Y} \mathscr{D}_2(f)(W) q_W, \quad \forall f \in \mathfrak{q}_Y. \tag{6.3}$$

Proof We proof each claim separately:

- *Claim (i):* By Claim *i*) of Corollary 12, given $f \in \mathfrak{q}_Y$ and $S \not\subseteq Y$, we have:

$$\mathscr{D}_1(f)(S) = \sum_{S \subseteq T} f(T). \tag{6.4}$$

  Note that as $S \not\subseteq Y$, then $T \not\subseteq Y$, for all $T \supseteq S$. As $f \in \mathfrak{q}_Y$, we conclude that $f(T) = 0$, for all $T \supseteq S$ and Equation (6.4) becomes $\mathscr{D}_1(f)(S) = 0$ for all $S \not\subseteq Y$. Thus, by Lemma 16 we conclude that $\mathscr{D}_1(f) \in \mathfrak{q}_Y$ and the claim follows.
- *Claim (ii):* Finally, because of Claim *iii*) of Proposition 17 we know that $\mathscr{B}_{2,Y} := \{q_W \ : \ W \subseteq Y\}$ is a basis of $\mathfrak{q}_Y$ as $\mathbb{Q}$-vector space. Thus, for $f \in \mathfrak{q}_Y$ we have:

$$f = \sum_{W \subseteq Y} \mu_W q_W,$$

  for some $\mu_W \in \mathbb{Q}$. As $\mathscr{B}_2^*$ and $\mathscr{B}_2$ are dual bases, if $S \subseteq [n]$ is such that $S \not\subseteq Y$ we have:

$$\mathscr{D}_2(f)(S) := \operatorname{Tr}_n(f, q_S^*) = \sum_{W \subseteq Y} \mu_W \operatorname{Tr}_n(q_W, q_S^*) = \sum_{W \subseteq S} \mu_W \delta_{W,S} = 0,$$

  because $\delta_{W,S} = 0$ for $W \subseteq Y$ and $S \not\subseteq Y$. Thus, by Lemma 16 we conclude $\mathscr{D}_2(f) \in \mathfrak{q}_Y$. Additionally, for every $W \subseteq Y$, we also conclude

$$\mu_W := \operatorname{Tr}_n(f, q_W^*) = \mathscr{D}_2(f)(W),$$

  which yields Identity (6.3).

□

Remark 1 Let the reader observe that for $Y = [n]$, $q_{[n]} = 1$, $\mathfrak{q}_{[n]} = \mathbb{Q}[V_n]$ and Identity (6.3) becomes:

$$f = \sum_{S\subseteq[n]} \mathscr{D}_2(f)(S) q_S, \quad \forall f \in \mathbb{Q}[V_n], \tag{6.5}$$

which is simply Trace (Inversion) Formula (2.7) with dual bases $\mathscr{B}_2^*$ and $\mathscr{B}_2$ (i.e. in reverse order).

Proposition 32 *With these notations, $\mathscr{D}_2$ is the inverse of $\mathscr{D}_1$. Namely, for all $f \in \mathbb{Q}[V_n]$ we have:*

$$f = \mathscr{D}_1\big(\mathscr{D}_2(f)\big) = \mathscr{D}_2\big(\mathscr{D}_1(f)\big) = \sum_{S\subseteq[n]} f^*_{\mathscr{B}_1}(S) p^*_S = \sum_{S\subseteq[n]} f^*_{\mathscr{B}_2}(S) q^*_S.$$

Moreover, for every $Y \subseteq [n]$, the restrictions to the ideal $\mathfrak{q}_Y$ of $\mathscr{D}_1$ and $\mathscr{D}_2$ are also $\mathbb{Q}$-vector space automorphisms of $\mathfrak{q}_Y$, each inverse of the other.

Proof From Claim *i*) of Corollary 12 and for every $W \subseteq [n]$, the following holds:

$$\mathscr{D}_1\big(\mathscr{D}_2(f)\big)(W) = \mathrm{Tr}_n(\mathscr{D}_2(f), p_W) = \sum_{W\subseteq S} \mathscr{D}_2(f)(S).$$

As $q_S(W) = 1$ when $W \subseteq S$ and $q_S(W) = 0$ when $W \not\subseteq S$ (see Claim *i*) of Proposition 13) we also have:

$$\mathscr{D}_1\big(\mathscr{D}_2(f)\big)(W) = \sum_{S\subseteq[n]} \mathscr{D}_2(f)(S) q_S(W).$$

Fromm Identity (6.5) in Remark 1 we conclude:

$$\mathscr{D}_1\big(\mathscr{D}_2(f)\big)(W) = \sum_{S\subseteq[n]} \mathscr{D}_2(f)(S) q_S(W) = f(W).$$

Hence, $\mathscr{D}_1 \circ \mathscr{D}_2(f) = f$ for all $f \in \mathbb{Q}[V_n]$. As both of them are linear $\mathbb{Q}$-automorphisms, we also have $\mathscr{D}_1 \circ \mathscr{D}_2(f) = f$ for all $f \in \mathbb{Q}[V_n]$ and, the statement follows. The last two equalities are simply the Trace (Inversion) Formula respectively applied to $\mathscr{B}_1$ and $\mathscr{B}_2$. The last sentence of the statement immediately follows from Lemma 31. □

Our last result is an alternative proof of the fact $VCD(\mathscr{F}) \geq RVCD(\mathscr{F})$ (inspired in [12]). We just wish show how our previous Proposition (inspired in [12]) applies to give another proof Sauer–Shelah–Perles Lemma. The main aspect here is that we just use duality in its purest form to produce the wanted result. We follow notations of Sect. 5 above. Let $Q_{\mathscr{F}} \subseteq \mathbb{Q}[V_n]$ be the class defined in Identity (4.4) above.

Corollary 33 *With the same notations as above, given $Y \subseteq [n]$ such that $r = \sharp(Y) = RVCD(\mathscr{F})$, then $\mathscr{F}$ shatters Y and $VCD(\mathscr{F}) \geq r$.*

Proof As $r = \sharp(Y) = RVCD(\mathscr{F})$, there exist some list of rational coefficients: $\underline{\lambda} \in \mathbb{Q}^N \setminus \{0\}$ such that the following polynomial

$$Q := Q_{\underline{\lambda}} := \sum_{F \in \mathscr{F}} \lambda_F q_F \in \mathbb{Q}[V_n] \setminus \{0\},$$

be a non-zero-polinomial in $\mathbb{Q}[V_n]$ such that $Q(Y) \neq 0$ and it vanishes at any proper subset $S \subsetneq Y$.

Next, let us consider $S \subseteq Y$ and observe that for every $W \subseteq [n]$, we have $\mathscr{D}_2(q_S)(W) = \mathrm{Tr}_n(q_S, q_W^*) = \delta_{S,W}$. In other words,

$$\mathscr{D}_2(q_S) = \chi_{\{S\}}, \quad \forall S \subseteq Y.$$

Let us then consider $G := \mathscr{D}_2(Qq_Y) \in \mathfrak{q}_Y$. Denote by $f := \mathscr{D}_1(G) = Qq_Y \in \mathfrak{q}_Y$.

Applying Claim *iii*) of Corollary 12 (Reverse Inclusion-exclusion Principle) and Claim *iv*) of Proposition 11, one easily concludes for every $S \subseteq [n]$ that the following holds:

$$G(S) := \sum_{S \subseteq T \subseteq [n]} (-1)^{\sharp(T \setminus S)} \mathscr{D}_1(G)(T).$$

As $\mathscr{D}_1(G) = \mathscr{D}_1(\mathscr{D}_2(f)) = f = Qq_Y$, we conclude:

$$G(S) := \sum_{S \subseteq T \subseteq Y} (-1)^{\sharp(T \setminus S)} f(T) = (-1)^{\sharp(Y \setminus S)} f(Y) = (-1)^{\sharp(Y \setminus S)} Q(Y) \neq 0.$$

On the other hand, as in Corollary 30, we have that

$$G = \mathscr{D}_2(f) = \mathscr{D}_2(Qq_Y) = \mathscr{D}_2\left(\sum_{F \in \mathscr{F}} \lambda_F q_F q_Y\right) = \mathscr{D}_2\left(\sum_{F \in \mathscr{F}} \lambda_F q_{F \cap Y}\right).$$

As $\mathscr{D}_2$ is linear we also have

$$G := \sum_{S \subseteq Y} \left(\sum_{\substack{F \in \mathscr{F} \\ F \cap Y = S}} \lambda_F \right) \mathscr{D}_2(q_S) = \sum_{S \subseteq Y} \left(\sum_{\substack{F \in \mathscr{F} \\ F \cap Y = S}} \lambda_F \right) \chi_{\{S\}}.$$

Thus, for every $S \subseteq Y$,

$$\mathscr{D}_2(f)(S) = \left(\sum_{\substack{F \in \mathscr{F} \\ F \cap Y = S}} \lambda_F \right) = G(S) = (-1)^{\sharp(Y \setminus S)} Q(Y) \neq 0,$$

and, consequently, Y is shattered by $\mathscr{F}$. Hence, $VCD(\mathscr{F}) \geq \sharp(Y)$ and the claim follows. □

This proof of Corollary 33 differs from the proof exhibited in Sect. 5 just on the fact that we have avoided the "knowledge" of the product $f := Qq_Y$. Instead, we just used Proposition 32 and duality techniques. Certainly, the proof exhibited in Sect. 5 is simpler, but the one we have just discussed follows the spirit underlying the proof in [12].

Remark 2 Just a final observation for the reader. Due to the identities described at the beginning of Sect. 3.4, most of the arguments in Sects. 5 and 6 could be redone replacing the q_S by the p_S and adjusting the arguments. I chose to work with the basis $\mathscr{B}_2 := \{q_S \ : \ S \subseteq [n]\}$ because these pages are ultimately a tribute to [12], which I found very pleasant and interesting to read.

Acknowledgements The author wishes to thank an anonymous referee whose thorough work helped to improve the manuscript. In particular, the author wants to thank this anonymous referee for the idea of Corollary 30 which, in some sense, simplifies the proof of Corollary 33.

Funding Open Access funding provided thanks to the CRUE-CSIC agreement with Springer Nature.

References

1. Alon, N.: On the density of sets of vectors. Discrete Math. **46**, 199–202 (1983)
2. Alon, N.: Combinatorial Nullstellensatz. Comb. Probab. Comput. **8**, 7–29 (1999)
3. Atiyah, M.F.: *Duality in Mathematics and Physics*. Lecture notes from the Institut de Matematica de la Universitat de Barcelona (IMUB), (2007)
4. Atiyah, M.F., MacDonald, I.G.: Introduction to Commutative Algebra. Addison-Wesley, Boston (1969)
5. Becker, E., Cardinal, J.P., Roy, M.-F., Szafraniec, Z.: *Multivariate Bezoutians, Kronecker symbol and Eisenbud-Levine formula.* In: González Vega, L., Recio, T. (eds.), "Algorithms in Algebraic Geometry and Applications, Proc. MEGA'94", Progress in Mathematics **143**, pp. 79–104. Birkhäuser Verlag (1996)
6. Bollobás, B., Radcliffe, A.J.: Defect Sauer results. JCT A **72**, 189–202 (1995)
7. Brukhim, N., Carmon, D., Dinur, I., Moran, S., Yehudayoff, A.: A Characterization of Multiclass Learnability. Electr. Collq. Comput. Complex, TR22-035 (2022)
8. Cox, D.A., Little, J., O'Shea, D.: Ideals, Varieties, and Algorithms An Introduction to Computational Algebraic Geometry and Commutative Algebra. Springer Verlag, Berlin (1992)
9. Deza, M., Frankl, P.: On the vector space of 0-configurations. Combinatorica **2**, 341–345 (1982)
10. Dvir, Z.: On the size of Kakeya sets on finite fields. J. Am. Math. Soc. **22**, 1093–1097 (2009)

11. Frankl, P.: On the trace of finite sets. J. Comb. Theory Ser. A **34**, 41–45 (1983)
12. Frankl, P., Pach, J.: On the number of sets in a null t-design. Eur. J. Comb. **4**, 21–23 (1983)
13. Giusti, M., Heintz, J., Pardo, L. M., Sabia, J., Solerno, P., Smietansky, F.: Sur la Complexité du Théoréme des Zéros. In: Guddat, J. et al. (eds.), Approximation and Optimization **8**, pp. 274–329. Peter Lange Verlag (1995)
14. Haussler, D.: Sphere packing numbers for subsets of the Boolean n-cube with bounded Vapnik–Chervonenkis dimension. J. Comb. Theory Ser. A **69**, 217–232 (1995)
15. Heintz, J.: Definability and fast quantifier elimination in algebraically closed fields. Theor. Comput. Sci. **24**, 239–277 (1983)
16. Hu, L., Wu, R., Li, T., Wang, L.: Quadratic upper bound for recursive teaching dimension of finite VC classes. Proc. Mach. Learn. Res. **65**, 1–10 (2017)
17. Krick, T., Pardo, Luis M.: *A computational method for diophantine approximations*. In: González Vega, L., Recio,T. (eds.), Algorithms in Algebraic Geometry and Applications, Proc. MEGA'94", Progress in Mathematics **143**, pp. 193–253. Birkhäuser Verlag (1996)
18. Mészáros, T.: "*S–extremal set systems and Gröbner bases.*" MSc Thesis, Budapest University of Technology and Economics, (2010) http://math.bme.hu/~slovi/thesiswork.pdf
19. Miller, E., Sturmfels, B.: Combinatorial Commutative Algebra, Graduate Texts in Mathematics, vol. 227. Springer-Verlag, New York (2005)
20. Moran, S., Rashtchian, C.: Shattered Sets and the Hilbert Function. In: Faliszewski, P., Muscholl, A., Niedermeier, R. (eds.), Proceedings of the 41st International Symposium on Mathematical Foundations of Computer Science (MFCS 2016), Leibniz International Proceedings in Informatics (LIPIcs), (2016)
21. Natarajan, B.K.: On learning sets and functions. Mach. Learn. **4**, 67–97 (1989)
22. Pardo, L. M.: How lower and upper complexity bounds meet in elimination theory. In: Cohen, G., Giusti, M. Mora, T. (eds.), Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Lecture Notes in Computer Science **948**, pp. 33-69. Springer Verlag (1995)
23. Pardo, L.M., Sebastián, D.: A promenade through correct test sequences I: degree of constructible sets, Bézout's Inequality and density. J. Complex. **68**, 101588 (2022)
24. Sauer, N.: On the density of families of sets. J. Comb. Theory Ser. A **13**, 145–147 (1972)
25. Shelah, S.: A combinatorial problem; stability and order for models and theories in infinitary languages. Pac. J. Math. **41**, 247–261 (1972)
26. Tao, T.: Algebraic combinatorial geometry: the polynomial method in arithmetic combinatorics, incidence combinatorics, and number theory. EMS Surv. Math. Sci. **1**, 1–46 (2014)
27. Teissier, B.: Monomial ideals, binomial ideals, polynomial ideals. Trends Commut. Algebra **21**, 211–246 (2004)
28. Vapnik, V.N., Chervonenkis, A.. Ya..: On the uniform convergence of relative frequencies of rvents to their probabilities. Theory Probab. Appl. **16**, 264–280 (1971)