

\$(d, \sigma)\$-VERONESE VARIETY AND SOME APPLICATIONS

N. DURANTE¹, G. LONGOBARDI², AND V. PEPE³

ABSTRACT. Let \$\mathbb{K}\$ be the Galois field \$\mathbb{F}_{q^t}\$ of order \$q^t\$, \$q = p^h\$, \$p\$ a prime, \$A = \text{Aut}(\mathbb{K})\$ be the automorphism group of \$\mathbb{K}\$ and \$\sigma = (\sigma_0, \dots, \sigma_{d-1}) \in A^d\$, \$d \ge 1\$. In this paper the following generalization of the Veronese map is studied:

$$\nu_{d,\sigma} : \langle v \rangle \in \text{PG}(n-1, \mathbb{K}) \longrightarrow \langle v^{\sigma_0} \otimes v^{\sigma_1} \otimes \dots \otimes v^{\sigma_{d-1}} \rangle \in \text{PG}(n^d-1, \mathbb{K}).$$

Its image will be called the \$(d, \sigma)\$-Veronese variety \$\mathcal{V}_{d,\sigma}\$. For \$d = t\$, \$\sigma\$ a generator of \$\text{Gal}(\mathbb{F}_{q^t}|\mathbb{F}_q)\$ and \$\sigma = (1, \sigma, \sigma^2, \dots, \sigma^{t-1})\$, the \$(t, \sigma)\$-Veronese variety \$\mathcal{V}_{t,\sigma}\$ is the variety studied in [19, 12, 14] and it will be denoted by \$\mathcal{V}_{t,\sigma}\$. Such a variety is the Grassmann embedding of the Desarguesian spread of \$\text{PG}(nt-1, \mathbb{F}_q)\$ and it has been used to construct codes [6] and (partial) ovoids of quadrics, see [12, 15]. We will show that \$\mathcal{V}_{d,\sigma}\$ is the Grassmann embedding of a normal rational scroll and we will prove that it has the property that any \$d+1\$ points of it are linearly independent. As applications we give a characterization of \$d+2\$ linearly dependent points of \$\mathcal{V}_{d,\sigma}\$ and we show how such a property is interesting for a linear code \$\mathcal{C}_{d,\sigma}\$ that can be associated to the variety. Moreover for some choices of parameters, \$\mathcal{V}_{p,\sigma}\$, for every \$p\$, is the normal rational curve and for \$p = 2\$, it can be also the Segre's arc of \$\text{PG}(3, q^t)\$, giving in both cases an MDS code. For \$p = 3\$ \$\mathcal{V}_{p,\sigma}\$ can be also a \$|\mathcal{V}_{p,\sigma}|\$-track giving an almost MDS code.

1. INTRODUCTION

Let \$V\$ be an \$n\$-dimensional vector space over a field \$\mathbb{K}\$, we will denote by \$\text{PG}(V)\$ as well as \$\text{PG}(n-1, \mathbb{K})\$ the projective space induced by it.

The Veronese variety \$\mathcal{V}_d\$ of degree \$d\$ and dimension \$n-1\$ is a classical algebraic variety widely studied over fields of any characteristic and it is the image of the Veronese map:

$$\nu_d : (x_0, x_1, \dots, x_{n-1}) \in \text{PG}(n-1, \mathbb{K}) \longrightarrow (\dots, X_I, \dots) \in \text{PG}\left(\binom{n+d-1}{d} - 1, \mathbb{K}\right)$$

where \$X_I\$ ranges over all the possible monomials of degree \$d\$ in \$x_0, x_1, \dots, x_{n-1}\$. The Veronese map can be defined also by:

$$\nu_d : \langle v \rangle \in \text{PG}(n-1, \mathbb{K}) \longrightarrow \langle v \otimes v \otimes \dots \otimes v \rangle \in \text{PG}\left(\binom{n+d-1}{d} - 1, \mathbb{K}\right).$$

Now, let \$V_i\$ be \$n_i\$-dimensional vector spaces over the field \$\mathbb{K}\$, \$i = 0, 1, \dots, d-1\$. A Segre variety of type \$(n_0, n_1, \dots, n_{d-1})\$ in \$\text{PG}(\otimes_{i=0}^{d-1} V_i)\$ is the set

$$(1) \Sigma_{n_0-1, n_1-1, \dots, n_{d-1}-1} = \{ \langle v_0 \otimes v_1 \otimes \dots \otimes v_{d-1} \rangle \mid v_i \in V_i \setminus \{0\}, i = 0, 1, \dots, d-1 \}$$

If $n_0 = \dots = n_{d-1} = n$, we write $\Sigma_{(n-1)^d}$ instead of $\Sigma_{n-1, n-1, \dots, n-1}$. Then it is clear that \mathcal{V}_d turns out to be a linear section of the Segre variety product of $\text{PG}(n-1, \mathbb{K})$ for itself d times.

If ζ is a collineation of $\text{PG}(V^{\otimes d})$ fixing $\Sigma_{(n-1)^d}$, then there exist $\zeta_i, i = 0, 1, \dots, d-1$ collineations of $\text{PG}(V)$, with the same companion field automorphism, and a permutation τ on $\{0, 1, \dots, d-1\}$ such that:

$$(v_0 \otimes v_1 \otimes \dots \otimes v_{d-1})^\zeta = v_{\tau(0)}^{\zeta_0} \otimes v_{\tau(1)}^{\zeta_1} \otimes \dots \otimes v_{\tau(d-1)}^{\zeta_{d-1}}$$

(for a proof of this in positive characteristic see, e.g., [21]).

Let \mathcal{L}_h be the set of all projective subspaces of dimension h of $\text{PG}(n-1, \mathbb{K})$, and consider

$$g_{n,h} : X = \langle v_0, v_1, v_2, \dots, v_h \rangle \in \mathcal{L}_h \longrightarrow \langle v_0 \wedge v_1 \wedge v_2 \wedge \dots \wedge v_h \rangle \in \text{PG}(\wedge^{h+1} V).$$

This map is called *Grassmann embedding* and its image $\mathcal{G}_{n,h}(V)$ is called *Grassmannian of subspaces of dimension h* of $\text{PG}(V)$. It is well-known that $\mathcal{G}_{n,h}(V)$ is an algebraic variety which is the complete intersection of certain quadrics, see [7].

Let \mathbb{K} be the Galois field \mathbb{F}_{q^t} of order q^t , $A = \text{Aut}(\mathbb{K})$ be the automorphism group of \mathbb{K} and $\sigma = (\sigma_0, \dots, \sigma_{d-1}) \in A^d, d \geq 1$. The aim of this paper is to study the following generalization of the Veronese map:

$$\nu_{d,\sigma} : \langle v \rangle \in \text{PG}(n-1, \mathbb{K}) \longrightarrow \langle v^{\sigma_0} \otimes v^{\sigma_1} \otimes \dots \otimes v^{\sigma_{d-1}} \rangle \in \text{PG}(n^d - 1, \mathbb{K})$$

and its image will be called here the (d, σ) -*Veronese variety* $\mathcal{V}_{d,\sigma}$. For $d = t$, σ a generator of $\text{Gal}(\mathbb{F}_{q^t} | \mathbb{F}_q)$ and $\sigma = (1, \sigma, \sigma^2, \dots, \sigma^{t-1})$, the (t, σ) -Veronese variety $\mathcal{V}_{t,\sigma}$ is the variety studied in [19, 12, 14] and it will be called $\mathcal{V}_{t,\sigma}$. Such a variety is the Grassmann embedding of the Desarguesian spread of $\text{PG}(nt-1, \mathbb{F}_q)$ and it has been used to construct codes [6] and (partial) ovoids of quadrics, see [12, 15].

Here we study the most general case. We will show what is the span of the variety and its automorphisms group, we will prove that it is the Grassmann embedding of a normal rational scroll and it has the property that any $d+1$ points of $\mathcal{V}_{d,\sigma}$ are in general position, i.e., any $d+1$ points of $\mathcal{V}_{d,\sigma}$ are linearly independent. Moreover, we give a characterization of $d+2$ linearly dependent points of $\mathcal{V}_{d,\sigma}$ and we show how such a property is interesting for a linear code that can be associated to the variety.

An $[n, k]$ -linear code \mathcal{C} is a subspace of the vector space \mathbb{F}_q^n of dimension k . The *weight* of a codeword is the number of its elements that are nonzero and the *Hamming distance* between two codewords is the number of elements in which they differ. The distance d of a linear code is the minimum distance between distinct codewords and it is equals to the minimum weight. A linear code of length n , dimension k , and minimum distance d is called an $[n, k, d]$ -code. A matrix H of order $(n-k) \times n$ such that

$$\mathbf{x}H^T = \mathbf{0} \quad \text{for all } \mathbf{x} \in \mathcal{C}$$

is called a *parity check matrix* for \mathcal{C} . The minimum weight, and hence the minimum distance, of \mathcal{C} is at least w if and only if any $w-1$ columns of H are linearly independent [13, Theorem 10, p. 33]. Each linear $[n, k, d]$ -code \mathcal{C} satisfies the following inequality

$$d \leq n - k + 1,$$

called *Singleton bound*. If $d = n - k + 1$, \mathcal{C} is called *maximum distance separable* or *MDS*, while if $d = n - k$ the code is called *almost MDS*. These can be related to some subsets of points in the projective space. More precisely, \mathcal{C} is an $[n, k, d]$ -linear code if and only if the columns of its parity check matrix H can be seen as n points in $\text{PG}(n - k - 1, q)$ each $d - 1$ of which are in general position, [4, Theorem 1]. Then, the existence of MDS or almost MDS linear codes is equivalent to the existence of arcs or track in projective spaces.

Definition 1.1. An n -arc is a set of n points in $\text{PG}(r, q)$ such that $r + 1$ of them are in general position. An m -track is a set of m points in $\text{PG}(r, q)$ such that every r of them are in general position.

Here, if H is the matrix whose columns are the coordinates vectors of the points of the variety $\mathcal{V}_{d, \sigma}$, we get a code $\mathcal{C}_{d, \sigma}$ and we study the minimum distance of it and we can characterize the codewords of minimum weight. (for an overview on this topic, see, e.g., [2]).

2. THE VARIETY $\mathcal{V}_{d, \sigma}$

Let $V = V(n, \mathbb{K})$ be an n -dimensional vector space over the field \mathbb{K} and $\text{PG}(V) = \text{PG}(n - 1, \mathbb{K})$ be the induced projective space. In particular, if \mathbb{K} is the Galois field of order q^t , we will denote the projective space by $\text{PG}(n - 1, q^t)$.

Let $A = \text{Aut}(\mathbb{K})$ be the automorphism group of \mathbb{K} and $\sigma = (\sigma_0, \dots, \sigma_{d-1}) \in A^d$, $d \geq 1$, and define the map

$$(2) \quad \nu_{d, \sigma} : \langle v \rangle \in \text{PG}(V) \longrightarrow \langle v^{\sigma_0} \otimes v^{\sigma_1} \otimes \dots \otimes v^{\sigma_{d-1}} \rangle \in \text{PG}(V^{\otimes d}).$$

Without loss of generality, we may assume that $\sigma_0 = 1$. It is clear that the map $\nu_{d, \sigma}$ is an injection of $\text{PG}(V)$ into $\text{PG}(V^{\otimes d})$ by the injectivity of the Segre map.

We will call $\nu_{d, \sigma}$ the (d, σ) -Veronese embedding and, as defined before, its image $\mathcal{V}_{d, \sigma}$ the (d, σ) -Veronese variety. Then $\mathcal{V}_{d, \sigma}$ is a rational variety of $\text{PG}(N - 1, \mathbb{K})$, $N = n^d$, of dimension $n - 1$.

Here a collineation ζ of $\text{PG}(V^{\otimes d})$ fixing $\mathcal{V}_{d, \sigma}$ is such that:

$$(v \otimes v^{\sigma_1} \otimes \dots \otimes v^{\sigma_{d-1}})^{\zeta} = v^{\zeta_0} \otimes v^{\sigma_1 \circ \zeta_1} \otimes \dots \otimes v^{\sigma_{d-1} \circ \zeta_{d-1}}$$

where ζ_i , $i = 0, 1, \dots, d - 1$ are collineations of $\text{PG}(V)$ such that $\zeta_i = \sigma_i^{-1} \circ \zeta_0 \circ \sigma_i$ (so the collineations ζ_i 's have all the same companion automorphism of ζ_0).

Applying the map:

$$(v \otimes v^{\sigma_1} \otimes \dots \otimes v^{\sigma_{d-1}})^{\zeta} = v^{\zeta_0} \otimes v^{\sigma_1 \circ \zeta_1} \otimes \dots \otimes v^{\sigma_{d-1} \circ \zeta_{d-1}}$$

with general ζ_i , we get a subvariety of $\Sigma_{(n-1)^d}$ projectively equivalent to $\mathcal{V}_{d, \sigma}$.

Although many of the results also hold in the case of a general field, from now on it will be assumed, that \mathbb{K} is the Galois field \mathbb{F}_{q^t} of q^t elements and $\sigma = (\sigma_0, \sigma_1, \dots, \sigma_{d-1}) \in G^d$ with $G = \text{Gal}(\mathbb{F}_{q^t} | \mathbb{F}_q)$. Moreover, since any element $\sigma_i \in G$ is a map of the type $\sigma_i : x \mapsto x^{q^{h_i}}$ with $0 \leq h_i < t$ and $0 \leq i \leq d - 1$, hereafter we

will suppose that

$$\boldsymbol{\sigma} = \underbrace{(\sigma_0, \dots, \sigma_0)}_{d_0 \text{ times}}, \underbrace{(\sigma_1, \dots, \sigma_1)}_{d_1 \text{ times}}, \dots, \underbrace{(\sigma_m, \dots, \sigma_m)}_{d_m \text{ times}}$$

where $0 = h_0 < h_1 < \dots < h_m < t$ and we will consider the vector $d_{\boldsymbol{\sigma}} = (d_0, d_1, \dots, d_m)$ where d_j is the occurrence of σ_j in $\boldsymbol{\sigma}$, $0 \leq j \leq m$. Clearly $d_0 + d_1 + \dots + d_m = d$. If $\boldsymbol{\sigma} \in G^d$, the integer

$$(3) \quad |\boldsymbol{\sigma}| = \sum_{i=0}^{d-1} q^{h_i} = \sum_{i=0}^m d_i q^{h_i}.$$

will be called *norm* of $\boldsymbol{\sigma}$. Since we consider the rings of polynomials over \mathbb{F}_{q^t} actually as the quotient $\mathbb{F}_{q^t}[x_0, x_1, \dots, x_{n-1}]/(x_0^{q^t} - x_0, x_1^{q^t} - x_1, \dots, x_{n-1}^{q^t} - x_{n-1})$, from now on we assume that $|\boldsymbol{\sigma}| < q^t$, so that distinct polynomials will be distinct functions over \mathbb{F}_{q^t} . Note that the $(d, \boldsymbol{\sigma})$ -Veronese variety $\mathcal{V}_{d, \boldsymbol{\sigma}}$ has as many points as $\text{PG}(n-1, q^t)$.

Let $\{e_i \mid i = 0, 1, \dots, nd-1\}$ be the canonical basis of $V(nd, \mathbb{F}_{q^t}) = V(nd, q^t)$ and let $\Pi \cong \text{PG}(n-1, q^t)$ be the subspace of $\text{PG}(nd-1, q^t)$ spanned by $\{\langle e_i \rangle \mid i \leq n-1\}$. Let ϕ be the collineation of $\text{PG}(nd-1, q^t)$ such that

$$\langle e_i \rangle \mapsto \langle e_{i+n} \rangle,$$

where the subscripts are taken mod nd . As in [6], we observe that for any $\langle v_i \rangle \in \Pi^{\phi^t}$,

$$v_0 \wedge v_1 \wedge v_2 \wedge \dots \wedge v_{d-1} = v_0 \otimes v_1 \otimes v_2 \otimes \dots \otimes v_{d-1}.$$

Therefore, $\mathcal{V}_{d, \boldsymbol{\sigma}}$ is the Grassman embedding of the d -fold normal rational scroll $S_{n-1, n-1, \dots, n-1} = \{\langle P^{\sigma_0}, P^{\phi \sigma_1}, P^{\phi^2 \sigma_2}, \dots, P^{\phi^{d-1} \sigma_{d-1}} \rangle \mid P \in \Pi\}$ of $\text{PG}(nd-1, q^t)$ (see [7, Ch.8] for a definition of normal rational scroll).

Example 2.1. Let $\boldsymbol{\sigma} = \mathbf{1}$, the identity of the product group A^d , the $\boldsymbol{\sigma}$ -Veronese variety $\mathcal{V}_{d, \boldsymbol{\sigma}}$ is the classical Veronese variety of degree d and $\mathcal{V}_{d, \boldsymbol{\sigma}} \subset \text{PG}(N-1, q^t)$ with $N = \binom{n+d-1}{d}$. Moreover, in this case, $\mathcal{V}_{d, \boldsymbol{\sigma}}$ is the Grassmann embedding of $S_{n-1, n-1, \dots, n-1} = \{\langle P, P^\phi, P^{\phi^2}, \dots, P^{\phi^{d-1}} \rangle \mid P \in \Pi\}$, i.e. the Segre variety $\Sigma_{n-1, d-1}$ of $\text{PG}(nd-1, q^t)$ (see again [7, Ch.8]).

Example 2.2. Let σ be a generator of $\text{Gal}(\mathbb{F}_{q^t}|\mathbb{F}_q)$ and $\boldsymbol{\sigma} = (1, \sigma, \dots, \sigma^{t-1})$, then we get the algebraic variety introduced in [19, 12, 14] and we will refer to it as the SLP-variety $\mathcal{V}_{t, \boldsymbol{\sigma}}$. Let $\hat{\sigma}$ be the semi-linear collineation $\phi \circ \sigma$ of $\text{PG}(nt-1, q^t)$ of order t , then $\text{Fix}(\hat{\sigma}) \subset \text{PG}(nt-1, q^t)$ is a subgeometry $\cong \text{PG}(nt-1, q)$ ¹ and a subspace of $\text{PG}(nt-1, q^t)$ intersects the subgeometry in a subspace of the same dimension if and only if it is set-wise fixed by $\hat{\sigma}$ (see [12]). In this case, $S_{n-1, n-1, \dots, n-1} = \{\langle P, P^{\hat{\sigma}}, P^{\hat{\sigma}^2}, \dots, P^{\hat{\sigma}^{t-1}} \rangle \mid P \in \Pi\}$, and hence its $(t-1)$ -spaces are set-wise fixed by $\hat{\sigma}$. Also, $S_{n-1, n-1, \dots, n-1} \cap \text{Fix}(\hat{\sigma})$ is the Desarguesian $(t-1)$ -spread of $\text{PG}(nt-1, q) = \text{Fix}(\hat{\sigma}) \subset \text{PG}(nt-1, q^t)$. Therefore, $\mathcal{V}_{t, \boldsymbol{\sigma}}$ is the Grassmann embedding of the Desarguesian spread of $\text{PG}(nt-1, q)$. In this case, in fact, $\mathcal{V}_{t, \boldsymbol{\sigma}}$ turns out to be a variety of the subgeometry $\text{PG}(n^t-1, q) \subset \text{PG}(n^t-1, q^t)$ point-wise fixed by the semi-linear collineation of order t of $\text{PG}(n^t-1, q^t)$ induced by $\hat{\sigma}$:

$$v_0 \otimes v_1 \otimes \dots \otimes v_{t-1} \mapsto v_{t-1}^{\hat{\sigma}} \otimes v_0^{\hat{\sigma}} \otimes \dots \otimes v_{t-2}^{\hat{\sigma}}.$$

¹By $\text{Fix}(\hat{\sigma})$ we denote the set of points fixed by $\hat{\sigma}$.

By (2), a point of $\text{PG}(n-1, q^t)$ with homogeneous coordinates $(x_0, x_1, \dots, x_{n-1})$ is mapped by $\nu_{d, \sigma}$ into a point of coordinates

$$\left(\dots, \prod_{j=0}^m X_{I_j}^{\sigma_j}, \dots \right)$$

where X_{I_j} is a monomial of degree d_j in the variables x_0, x_1, \dots, x_{n-1} . Hence, the (d, σ) -Veronese variety $\mathcal{V}_{d, \sigma}$ is contained in a projective space of rank $N = N_0 N_1 \cdots N_m$, with $N_j = \binom{n+d_j-1}{d_j}$, $j = 0, 1, \dots, m$.

Suppose that $d_i \sigma_i \neq d_j \sigma_j \ \forall i \neq j$, then we get exactly N distinct monomials of type $\prod_{j=0}^m X_{I_j}^{\sigma_j}$. This is not the case anymore if $d_i \sigma_i = d_j \sigma_j$ for some $i \neq j$. For

example, if $q = 2$, $\sigma = (1, 1, 2)$, then $d_0 = 2, d_1 = 1$ and hence $d_0 = d_1 \sigma_1$. Then $(x_0, x_1) \otimes (x_0, x_1) \otimes (x_0^2, x_1^2) = (x_0^4, x_0^2 x_1^2, x_0^3 x_1, x_0 x_1^3, x_0^3 x_1, x_0 x_1^3, x_0^2 x_1^2, x_1^4)$, hence we get 5 distinct monomials and $\mathcal{V}_{3, \sigma}$ is in fact contained in a projective space of rank less than $N = 6$.

Recall that an r -hypersurface of $\text{PG}(n-1, q^t)$ is a set of points such that their coordinates vanish an r -form of $\mathbb{F}_{q^t}[X_0, \dots, X_{n-1}]$. If $r = 2$, an r -hypersurface is called *quadric*. In [20], it is shown a lower bound on the degree of an r -hypersurface \mathcal{D} of $\text{PG}(n-1, q^t)$ after which \mathcal{D} could contain all points of the projective space. More precisely,

Theorem 2.3. [20] *If an r -hypersurface \mathcal{D} of $\text{PG}(n-1, q^t)$ contains all the points of the space, then $r \geq q^t + 1$.*

Let I be a multi-index of the form $I = I_0 I_1 \cdots I_m$, where I_j is a multi-index corresponding to a monomial in x_0, x_1, \dots, x_{n-1} of degree d_j . Once we have labelled the coordinates of $\text{PG}(N-1, q^t)$ according to the multi-index I , we can define a natural linear map ψ that sends the hyperplane of $\text{PG}(N-1, q^t)$ of equation $\sum_I a_I z_I = 0$ to the σ -hypersurface of equation

$$\sum_I a_I \prod_{j=0}^m X_{I_j}^{\sigma_j} = 0.$$

If $d_i \sigma_i \neq d_j \sigma_j \ \forall i \neq j$, then ψ is injective and hence to each hyperplane corresponds a non-identically zero σ -hypersurface. Then, by Theorem 2.3, we get the following result.

Theorem 2.4. *Let $\sigma \in G^d$ with $d_\sigma = (d_0, d_1, \dots, d_m)$. If $|\sigma| < q^t$ and $d_i \sigma_i \neq d_j \sigma_j$, then the (d, σ) -Veronese variety $\mathcal{V}_{d, \sigma}$ is not contained in any hyperplane of $\text{PG}(N-1, q^t)$.*

In the following, we generalize some results proved in [5] for the SLP-variety.

Theorem 2.5. *Let $\Pi_0, \Pi_1, \dots, \Pi_{d-1}$ be proper subspaces of $\text{PG}(n-1, q^t)$ and suppose that $P \in \text{PG}(n-1, q^t)$ is not contained in any of them. Then, $P^{\nu_{d, \sigma}}$ is not contained in $\langle \Pi_0^{\nu_{d, \sigma}}, \Pi_1^{\nu_{d, \sigma}}, \dots, \Pi_{d-1}^{\nu_{d, \sigma}} \rangle$.*

Proof. Recall that the dual space of $V(n^d, q^t)$, denoted by $V(n^d, q^t)^*$, is spanned by the simple tensors $l_0^* \otimes l_1^* \otimes \cdots \otimes l_{d-1}^*$, with $l_i^* \in V(n, q^t)^*$, and $l_0^* \otimes l_1^* \otimes \cdots \otimes l_{d-1}^*$ evaluated in $u_0 \otimes u_1 \otimes \cdots \otimes u_{d-1}$ is $l_0^*(u_0) l_1^*(u_1) \cdots l_{d-1}^*(u_{d-1}) \in \mathbb{F}_{q^t}$.

For every $i \in \{0, 1, \dots, d-1\}$, take an $l_i^* \in V(n, q^t)^*$ such that l_i^* vanishes on $\Pi_i^{\sigma_i}$ and not in P^{σ_i} . Then the hyperplane defined by $l_0^* \otimes l_1^* \otimes \dots \otimes l_{d-1}^*$ contains the points of $\Pi_j^{\nu_{d,\sigma}} \forall j = 0, 1, \dots, d-1$ and it does not contain the point $P^{\nu_{d,\sigma}}$. \square

Corollary 2.6. *Any $d+1$ points of $\mathcal{V}_{d,\sigma}$, $d \geq 2$, are in general position.*

Proof. It is enough to take the Π_i 's of dimension 0. \square

Corollary 2.7. *A set of $d+2$ linearly dependent points of $\mathcal{V}_{d,\sigma}$ is the (d, σ) -Veronese embedding of points contained in a line of $\text{PG}(n-1, q^t)$.*

Proof. The statement needs to be proved for $n > 2$. Let $P_0, P_1, \dots, P_d, P_{d+1}$ be $d+2$ points whose embedding is linearly dependent. Let $\Pi_i := P_i$ for $i = 2, \dots, d+1$ and let $\Pi_1 = \langle P_0, P_1 \rangle$. Suppose that $P_i \notin \Pi_1$, with $i = 2, \dots, d+1$, then by Theorem 2.5,

$$P_i^{\nu_{d,\sigma}} \notin \langle \Pi_1^{\nu_{d,\sigma}}, \Pi_2^{\nu_{d,\sigma}}, \dots, \Pi_{i-1}^{\nu_{d,\sigma}}, \Pi_{i+1}^{\nu_{d,\sigma}}, \dots, \Pi_{d+1}^{\nu_{d,\sigma}} \rangle,$$

but by hypothesis

$$P_i^{\nu_{d,\sigma}} \in \langle P_0^{\nu_{d,\sigma}}, P_1^{\nu_{d,\sigma}}, \dots, P_{i-1}^{\nu_{d,\sigma}}, P_{i+1}^{\nu_{d,\sigma}}, \dots, P_{d+1}^{\nu_{d,\sigma}} \rangle \subset \langle \Pi_1^{\nu_{d,\sigma}}, \Pi_2^{\nu_{d,\sigma}}, \dots, \Pi_{i-1}^{\nu_{d,\sigma}}, \Pi_{i+1}^{\nu_{d,\sigma}}, \dots, \Pi_{d+1}^{\nu_{d,\sigma}} \rangle,$$

a contradiction. \square

In order to prove the next Corollary, we need the following

Lemma 2.8. [11] *Let $d < |\mathbb{K}|$. Let S be a set of $d+2$ subspaces of $\text{PG}(2d-1, \mathbb{K})$ of dimension $d-1$, pairwise disjoint, linearly dependent as points of the Grassmannian and such that any $d+1$ elements of S are linearly independent. Then a line intersecting 3 elements of S intersects all of them.*

Since we have assumed $|\sigma| < q^t$, Lemma 2.8 always applies to $\mathcal{V}_{d,\sigma}$.

Corollary 2.9. *A set of $d+2$ linearly dependent points of $\mathcal{V}_{d,\sigma}$ is the Grassmann embedding of $(d-1)$ -subspaces of the normal rational scroll $S_{1,1,\dots,1} \subset \text{PG}(2d-1, q^t)$ such that a line intersecting 3 of them must intersect all of them.*

Proof. By Corollary 2.7, a set $\{P_0^{\nu_{d,\sigma}}, P_1^{\nu_{d,\sigma}}, \dots, P_{d+1}^{\nu_{d,\sigma}}\}$ of $d+2$ linearly dependent points of $\mathcal{V}_{d,\sigma}$ is such that P_0, P_1, \dots, P_{d+1} are contained in the same line, hence $\{P_0^{\nu_{d,\sigma}}, P_1^{\nu_{d,\sigma}}, \dots, P_{d+1}^{\nu_{d,\sigma}}\}$ is contained in a variety $\mathcal{V}_{d,\sigma}$ of dimension 1.

Hence, $\{P_0^{\nu_{d,\sigma}}, P_1^{\nu_{d,\sigma}}, \dots, P_{d+1}^{\nu_{d,\sigma}}\}$ is the Grassmann embedding of the $(d-1)$ -subspaces of the normal rational scroll $S_{1,1,\dots,1} \subset \text{PG}(2d-1, q^t)$. Then the result follows from Corollary 2.6 and Lemma 2.8. \square

Theorem 2.10. *A set of $d+2$ linearly dependent points of $\mathcal{V}_{d,\sigma}$ is the σ -Veronese embedding of points on a subline $\cong \text{PG}(1, q')$, where $\mathbb{F}_{q'}$ is the largest subfield of \mathbb{F}_{q^t} fixed by σ_i in σ .*

Proof. Let $\langle u_i \otimes u_i^{\sigma_1} \otimes \dots \otimes u_i^{\sigma_{d-1}} \rangle$, $i = 0, 1, \dots, d+1$ be $d+2$ linearly dependent points of $\mathcal{V}_{d,\sigma}$, and by Corollary 2.7, we can assume $\mathcal{V}_{d,\sigma}$ to be of dimension 1. Then, embed $\text{PG}(1, q^t)$ as the subspace of $\text{PG}(2d-1, q^t)$ spanned by $\langle e_0 \rangle, \langle e_1 \rangle$, say Π , and hence we can write

$$u_i \otimes u_i^{\sigma_1} \otimes \dots \otimes u_i^{\sigma_{d-1}} = u_i \wedge u_i^{\phi \sigma_1} \wedge \dots \wedge u_i^{\phi^{d-1} \sigma_{d-1}}.$$

We stress out that ϕ^j and σ_j commute. Let $S_i := \langle u_i, u_i^{\phi^{\sigma_1}}, \dots, u_i^{\phi^{d-1}\sigma_{d-1}} \rangle$, for all $i = 0, 1, \dots, d+1$. Then take a point $P \in S_0$ such that $P \notin \langle \Pi^{\phi^h}, h \neq j \rangle$ for any fixed $j \in \{0, 1, \dots, d-1\}$. The subspace $\langle P, S_1 \rangle$ intersects S_2 in a point, say R . Let ℓ be the line spanned by P and R . Then ℓ has non empty intersection with S_1 as well. Hence, by Corollary 2.9, ℓ has non empty intersection with all the S_i 's. By the choice of P , the line ℓ is not contained in any $\langle \Pi^{\phi^h}, h \neq j \rangle$ for a fixed $j \in \{0, 1, \dots, d-1\}$. If ℓ intersects $\langle \Pi^{\phi^h}, h \neq j \rangle$ for some $j \in \{0, 1, \dots, d-1\}$, then it would be projected to a unique point of Π^{ϕ^j} from $\langle \Pi^{\phi^h}, h \neq j \rangle$. Since $u_i \neq u_h \forall i \neq h$, then $u_i^{\sigma_j} \neq u_h^{\sigma_j} \forall i \neq h$ and ℓ can be projected on a unique point only if $\ell \cap S_i$ is in $\langle \Pi^{\phi^h}, h \neq j \rangle$ for all the S_i 's except one, a contradiction. Indeed, the point $\ell \cap S_i = \langle \lambda_0 u_i + \lambda_1 u_i^{\phi^{\sigma_1}} + \dots + \lambda_{d-1} u_i^{\phi^{d-1}\sigma_{d-1}} \rangle$ and the projection of $\ell \cap S_i$ over Π^{ϕ^j} is the point $\langle u_i^{\phi_j^{\sigma_j}} \rangle$, so h_j cannot be zero. Therefore, $\ell \cap \langle \Pi^{\phi^h}, h \neq j \rangle = \emptyset$ for any fixed $j \in \{0, 1, \dots, r-1\}$. Hence the projection of ℓ on a Π^{ϕ^j} is an isomorphism of lines, say p_j and $(\ell \cap S_i)^{p_j} = \langle u_i^{\phi_j^{\sigma_j}} \rangle$. By $(\ell \cap S_i)^{p_j \phi^{-j}} = (\ell \cap S_i)^{p_0 \sigma_j}$ we get that $(\ell \cap S_i)^{p_0}$ is fixed by the semi-linear collineation $\sigma_j \phi^j p_j^{-1} p_0$. If a semi-linear collineation of $\Pi \cong \text{PG}(1, q^t)$ fixes at least 3 points, then it fixes a subline $\cong \text{PG}(1, q')$, where $\mathbb{F}_{q'}$ is the subfield of \mathbb{F}_{q^t} fixed by σ_j . This is true for all σ_j in σ . \square

Finally, since the algebraic variety $\Sigma_{(n-1)^a}$ has dimension $d(n-1)$ and degree $\binom{d(n-1)}{n-1, n-1, \dots, n-1} = \frac{(d(n-1))!}{d^{n-1}}$, a general subspace of $\text{PG}(N-1, q^t)$ of codimension $d(n-1)$ contains at most $\frac{(d(n-1))!}{d^{n-1}}$ points of $\mathcal{V}_{d, \sigma}$.

Moreover, the Segre variety is smooth and hence the tangent space $T_P(\Sigma_{(n-1)^a})$ to $\Sigma_{(n-1)^a}$ at a point $P = \langle v_0 \otimes v_1 \otimes \dots \otimes v_{d-1} \rangle$ has dimension $d(n-1)$ and it is spanned by the d subspaces $\langle \langle v_0 \otimes v_1 \otimes \dots \otimes v_{i-1} \otimes u_i \otimes v_{i+1} \otimes \dots \otimes v_{d-1} \rangle : \langle u_i \rangle \in \text{PG}(n-1, q^t) \rangle \cong \text{PG}(n-1, q^t)$. These subspaces pairwise intersect only in P and they are the maximal subspaces contained in $\Sigma_{(n-1)^a}$ through the point P , and $\Sigma_{(n-1)^a}$ does not share with $\mathcal{V}_{d, \sigma}$ the property proved in Corollary 2.6. We have, in fact, $T_P(\Sigma_{(n-1)^a}) \cap \mathcal{V}_{d, \sigma} = P$ for each $P \in \mathcal{V}_{d, \sigma}$.

3. THE CODE $\mathcal{C}_{d, \sigma}$

As we have seen before, the SLP-variety turns out to be a variety of a subgeometry of order q , even though the array σ is defined on a finite field of order q^t , hence among all the possible choice of σ and n , for q 'big enough' $\mathcal{V}_{t, \sigma}$ is the variety with the most 'dense' set of points of a projective space with the property that any $d+1$ points are independent. In this case, since $d = t$ and, as proved in [5], $t+2$ linearly dependent points are contained in a normal rational curve of degree t of $\text{PG}(t, q)$, $q > t$.

For the classical Veronese variety of degree d , hence for $\sigma = 1$, Corollary 2.10 implies that $d+2$ linearly dependent points are contained in the Veronese embedding of degree d of a line, hence in a normal rational curve of degree d of $\text{PG}(d, q^t)$.

Finally, we get that for a general (d, σ) -Veronese variety, if $d+2 > q'+1$, with q' defined as in Corollary 2.10, every $d+2$ points of $\mathcal{V}_{d, \sigma}$ are linearly independent, hence, for 'small' q' , it provides a dense set of points with that property. More precisely, we get $\frac{q^{nt}-1}{q^t-1}$ points in $\text{PG}(N-1, q^t)$ such that any $d+2$ of them are

²Here, if f and g are collineations fg stands for $g \circ f$.

in general position. Sets of points with properties of this sort are studied for their connections with linear codes, more precisely

Definition 3.1. Let $\mathcal{V}_{d,\sigma}$ be a (d, σ) -Veronese variety and denote by $\mathcal{C}_{d,\sigma}$ the code whose parity check matrix H of order $N \times \binom{q^{nt}-1}{q^t-1}$ has columns that are the coordinate vectors of the points of the variety $\mathcal{V}_{d,\sigma}$.

Clearly, the order of the columns of H is arbitrary, so that Definition 3.1 makes sense only up to code equivalence, as a permutation of the columns that is not usually an automorphism of the code, see [5, Remark 3.3].

Definition 3.2. The support of a codeword $\mathbf{w} \in \mathcal{C}_{d,\sigma}$ is the set of the points of the variety $\mathcal{V}_{d,\sigma}$ corresponding to the non-zero positions of \mathbf{w} .

As showed in [5, Theorem 3.5], the following result holds

Theorem 3.3. *Let $\sigma \in G^d$ with $d_\sigma = (d_0, d_1, \dots, d_m)$, $|\sigma| < q^t$ and $d_i\sigma_i \neq d_j\sigma_j$ for any $i, j = 0, 1, \dots, d-1$ and let $\mathbb{F}_{q'}$ be the largest subfield fixed by σ_i 's. If $d < q'$ then the code $\mathcal{C}_{d,\sigma}$ has length $r = \frac{q^{nt}-1}{q^t-1}$ and parameters $[r, r - N, d + 2]$.*

Proof. Since $|\mathcal{V}_{d,\sigma}| = |\text{PG}(n-1, q^t)|$ the code $\mathcal{C}_{d,\sigma}$ has length $\frac{q^{nt}-1}{q^t-1}$. Moreover, since $\mathcal{V}_{d,\sigma}$ is not contained in any hyperplane of $\text{PG}(N-1, q^t)$, the rank of the $N \times r$ matrix H is maximal and so the dimension of the code is $r - N$. By Corollary 2.6 guarantees that any $d + 1$ columns of H are linearly independent; thus, by [13, Theorem 10, p. 33], the minimum distance of $\mathcal{C}_{d,\sigma}$ is at least $d + 2$. The image under $\nu_{d,\sigma}$ of the canonical subline $\text{PG}(1, q')$ of $\text{PG}(n-1, q^t)$ determines a submatrix H' of H with many repeated rows; indeed, the points represented in H constitute a normal rational curve $\text{PG}(d, q')$ and it follows that any $d + 2$ such points are necessarily dependent. Hence, the minimum distance is exactly $d + 2$. \square

Now, as in [5, Theorem 3.7], by the characterizations of sets of $d + 2$ points of $\mathcal{V}_{d,\sigma}$ which are linearly dependent yields a characterization of the minimum weight codewords of the associated code. More precisely,

Theorem 3.4. *A codeword $\mathbf{w} \in \mathcal{C}_{d,\sigma}$ has minimum weight if and only if its support consists of $d + 2$ points contained in the image of a subline $\text{PG}(1, q')$, $d < q'$, where $\mathbb{F}_{q'}$ is the largest subfield of \mathbb{F}_{q^t} fixed by σ_i for all σ_i in σ .*

Note that, by Theorem 2.10, if $\mathbb{F}_{q'}$ is the largest subfield of \mathbb{F}_{q^t} fixed by σ_i , for all σ_i in σ and $d \geq q'$, then the code $\mathcal{C}_{d,\sigma}$ is a linear code with minimum distance at least $d + 3$. Recalling the Singleton bound, in this case, $d(\mathcal{C}_{d,\sigma}) \leq N + 1$. If that bound is reached, then it is an MDS code. Then let

$$N = \binom{d_0 + n - 1}{d_0} \binom{d_1 + n - 1}{d_1} \cdots \binom{d_m + n - 1}{d_m}$$

with $\sum_{i=0}^m d_i = d$.

If $n = 2$, then $N = \prod_{i=0}^m (d_i + 1)$ and the minimum is reached for $m = 1, d_0 = d - 1, d_1 = 1$, so $N = 2d$.

So, if σ is such that $\text{Fix}(\sigma) \cap \mathbb{F}_{q^t} = \mathbb{F}_p$, where p is the characteristic of the field, since we should have $d > p - 1$, the smallest possible $d = p$. Therefore, for $d = p$,

$$(4) \quad \sigma = \underbrace{(1, 1, \dots, 1)}_{p-1 \text{ times}}, \sigma$$

and one gets that $\mathcal{V}_{d,\sigma}$ is a set of $q^t + 1$ points in $\text{PG}(2p - 1, q^t)$ such that any $p + 2$ of them are in general position. So the code $\mathcal{C}_{d,\sigma}$ is a $[q^t + 1, q^t - 2p + 1]$ -linear code with minimum distance at least $p + 3$ and the Singleton bound $2p + 1$. Now,

- if $\sigma : x \mapsto x^p$, then $\mathcal{V}_{p,\sigma}$ is the normal rational curve of $\text{PG}(2p - 1, q^t)$; hence $\mathcal{C}_{p,\sigma}$ is an MDS code. Furthermore for $p \in \{2, 3\}$, beside the normal rational curve, the following can also occur
- for $p = 2$, $\mathcal{V}_{2,\sigma}$ is the Segre arc, the only arc that is not a normal rational curve (see [3]); hence $\mathcal{C}_{2,\sigma}$ is an MDS code.
- for $p = 3$, $\mathcal{V}_{3,\sigma}$ is a $(3^{et} + 1)$ -track of $\text{PG}(5, 3^{et})$; hence $\mathcal{C}_{3,\sigma}$ is a so called *almost MDS* code, [4]. (See next Theorem 3.5).

Theorem 3.5. *Let $q = 3^e$ and $\sigma : x \in \mathbb{F}_{q^t} \mapsto x^{3^h} \in \mathbb{F}_{q^t}$, $1 < h < t$ and $\text{gcd}(h, et) = 1$. Then $\mathcal{C}_{3,\sigma}$ with $\sigma = (1, 1, \sigma)$ is an almost MDS.*

Proof. By the previous considerations, since the $[q^t + 1, q^t - 5]$ -code $\mathcal{C}_{d,\sigma}$ has distance at least 6, the result follows showing the existence of 6 columns of H linearly dependent or equivalently that there exists 6 points linearly dependent of the set

$$\mathcal{V}_{3,\sigma} = \{(1, z, z^2, z^{3^h}, z^{3^h+1}, z^{3^h+2}) : z \in \mathbb{F}_{q^t}\} \cup \{(0, 0, 0, 0, 0, 1)\}.$$

Suppose that any 6 points of $\mathcal{V}_{3,\sigma}$ with $\sigma = (1, 1, \sigma)$ are linearly independent, hence $\mathcal{V}_{3,\sigma}$ is an arc of $\text{PG}(5, q^t)$. By [10], $\mathcal{V}_{3,\sigma}$ must be projectively equivalent to rational normal curve

$$\{(1, y, y^2, y^3, y^4, y^5) : y \in \mathbb{F}_{q^t}\} \cup \{(0, 0, 0, 0, 0, 1)\}.$$

Since the normal rational curve has a 3-transitive automorphisms group, we can always assume that there is a collineation of $\text{PG}(5, q^t)$ fixing $(0, 0, 0, 0, 0, 1)$ and $(1, 0, 0, 0, 0, 0)$. Moreover, w.l.o.g. we can assume that this collineation has the identity as companion automorphism.

Hence there must be $f_i(y) \in \mathbb{F}_{q^t}[y]$ of degree at most 5 and linearly independent such that

$$(f_0(y), f_1(y), f_2(y), f_3(y), f_4(y), f_5(y)) = (1, z, z^2, z^{3^h}, z^{3^h+1}, z^{3^h+2})$$

with $f_i(y)$ vanishing in 0 for $i \in \{1, 2, 3, 4, 5\}$ and $f_0(0) = 1$. So, $f_0(y) = 1$ for all $y \in \mathbb{F}_{q^t}$ and since $\deg f_0(y) \leq 5 < q^t$, then $f_0(y) = 1$. Note that $\deg f_i(y) \neq 0$ for $i = 1, 2, 3, 4, 5$ and

$$f_2(y) = f_1(y)^2 \pmod{y^{q^t} - y},$$

but $2 \deg f_1(y) \leq 10 < q^t$, and hence $f_2(y) = f_1(y)^2$ and $\deg f_1(y) \leq 2$. Similarly,

$$f_4(y) = f_1(y)^{3^h} \pmod{y^{q^t} - y},$$

but $3^h \deg f_1(y) \leq 3^h \cdot 2 < q^t$, so $f_4(y) = f_1(y)^{3^h}$ and $3^h \deg f_1(y) \leq 5$, obtaining $3^h \leq 5$, a contradiction. \square

Clearly, as p gets larger, the minimum distance gets smaller than the Singleton bound.

4. ACKNOWLEDGEMENT

The authors thank Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA - INdAM) for having supported this research.

REFERENCES

- [1] S. Ball, M. Lavrauw, Arcs in finite projective space, *Ems Surveys in Mathematical Sciences* **6(1–2)** (2019), 133–172.
- [2] E.R. Berlekamp, *Algebraic Coding Theory*, Mc Graw-Hill (1968).
- [3] L.R.A. Casse, A solution to B. Segre’s problem $I_{r,q}$. *Atti Accad. Naz. Lincei Rend.* **46** (1969), 13–20.
- [4] M.A. De Boer, Almost MDS codes *Des. Codes Cryptogr.* **9** (1996) 143–155.
- [5] L. Giuzzi, V. Pepe, Families of twisted tensor product codes, *Des. Codes Cryptogr.* **67** (2013), 375–384.
- [6] L. Giuzzi, V. Pepe, On some subvarieties of the Grassmann variety, *Linear Multilinear Algebra* **63** (2015), 2121–2134.
- [7] J. Harris, *Algebraic Geometry Book, A First Course*, Graduate Texts in Mathematics **133**, Springer-Verlag (1992).
- [8] J.W.P. Hirschfeld, *Projective Geometries over finite fields* (1990).
- [9] J.W.P. Hirschfeld, J.A. Thas, *General Galois Geometries*, Springer Monographs in Mathematics (2016).
- [10] H. Kaneta, T. Maruta An elementary proof and an extension of Thas’ theorem on k -arcs, *Math. Proc. Cambridge Philos. Soc.* **105(3)** (1989), 459–462.
- [11] G. Lunardon, Planar fibrations and algebraic subvarieties of the Grassmann variety, *Geom. Dedicata* **16** (1984), 291–313.
- [12] G. Lunardon, Normal Spreads, *Geom. Dedicata* **75** (1999), 245–261.
- [13] F.J. MacWilliams, N.J.A Sloane, *The Theory of Error Correcting Codes*, North-Holland, Amsterdam (1977).
- [14] V. Pepe, On the algebraic variety $\mathcal{V}_{r,t}$, *Finite Fields and Their Applications* **17(4)** (2011), 343–349.
- [15] V. Pepe, Desarguesian and Unitary complete partial ovoids, *J. Algebr. Comb.* **37** (2013), 503–522.
- [16] B. Segre, Curve razionali normali e k -archi negli spazi finiti, *Ann. Mat. Pura Appl.* **39** (1955), 357–379.
- [17] B. Segre, Ovals in a finite projective plane. *Canadian Journal of Mathematics* **7 (10)** (1955), 414–416.
- [18] B. Segre, Ovali e curve nei piani di Galois di caratteristica due, *Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Nat.* **8** (1962).
- [19] B. Segre, Teoria di Galois, fibrazioni proiettive e geometrie non desarguesiane, *Ann. Mat. Pura Appl.* **64** (1964), 1–76.
- [20] G. Tallini, Sulle ipersuperfici irriducibili d’ordine minimo che contengono tutti i punti di uno spazio di Galois $S_{r,q}$, *Rend. Mat. Appl.* **20(5)** (1961), 431–479.
- [21] R. Westwick, Transformations on tensor spaces, *Pac. J. Math.* **23** (1967), 613–620.

¹DIPARTIMENTO DI MATEMATICA E APPLICAZIONI “RENATO CACCIOPPOLI”, UNIVERSITÀ DEGLI STUDI DI NAPOLI “FEDERICO II”, VIA VICINALE CUPA CINTIA, 80126 NAPOLI, ITALY
Email address: ndurante@unina.it

²DIPARTIMENTO DI TECNICA E GESTIONE DEI SISTEMI INDUSTRIALI, UNIVERSITÀ DEGLI STUDI DI PADOVA, STRADELLA S. NICOLA, 3, 36100 VICENZA, ITALY
Email address: giovanni.longobardi@unipd.it

³DIPARTIMENTO DI SCIENZE DI BASE ED APPLICATE PER L’INGEGNERIA, ‘SAPIENZA’ UNIVERSITÀ DI ROMA, VIA ANTONIO SCARPA, 14, 00161 ROMA, ITALY
Email address: valepepe@sbai.uniroma1.it