ГОДИШНИК НА СОФИЙСКИЯ УНИВЕРСИТЕТ „СВ. КЛИМЕНТ ОХРИДСКИ“
ФАКУЛТЕТ ПО МАТЕМАТИКА И ИНФОРМАТИКА
Том 111

ANNUAL OF SOFIA UNIVERSITY “ST. KLIMENT OHRIDSKI”
FACULTY OF MATHEMATICS AND INFORMATICS
Volume 111

TANGENT CODES

AZNIV K. KASPARIAN AND EVGENIYA D. VELIKOVA

The present article studies the finite Zariski tangent spaces to an affine variety X as linear codes, in order to characterize their typical or exceptional properties by global geometric conditions on X. We provide procedures for optimizing one of the parameters length, dimension or minimum distance of a single code by families of tangent codes.

Keywords: Zariski tangent space, minimum distance of a tangent code, genus reduction of a tangent code

2020 Mathematics Subject Classification: Primary: 94B27, 14G50; Secondary: 14G17, 11T71

1. Introduction

Codes with additional structure are usually equipped with a priori properties, which facilitate their characterization and decoding. For instance, algebro-geometric Goppa codes allowed Tsfasman, Vlădut and Zink to improve the asymptotic Gilbert-Varshamov bound on the information rate for a fixed relative minimum distance (cf. [11]). Justesen, Larsen, Elbrønd, Jensen, Havemose, Høholdt, Skorobogatov, Vlădut, Krachkovskii, Porter, Duursma, Feng, Rao and others developed efficient algorithms for decoding Goppa codes after obtaining the error support of the received word (Pellikaan's [8] is a survey on these results). Duursma's considerations from [3] imply that the averaged homogeneous weight enumerator of Goppa codes, associated with a complete set of representatives of the linear equivalence classes of divisors of fixed degree is related to the ζ-polynomial of the underlying curve (cf. [6] for the exact formulation). The realizations of codes by points of a Grassmannian, a determinantal variety or a modification of an arc provide other examples for exploiting “an extra structure” on the objects under study.

DOI: 10.60063/GSU.FMI.111.91-114

The present article interprets the finite Zariski tangent spaces to an affine variety X, defined over a finite field $\mathbb{F}_q$ as linear codes, in order to control the length, the dimension and the minimum distance of these codes by the equations of X. A series of extremal problems from coding theory minimizes the genus $g := n+1-k-d > 0$ of a not MDS $\mathbb{F}_q$-linear $[n,k,d]$-code C. We "deform" any such C into infinite families of linear codes with parameters $[n-1,k,d]$, $[n,k+1,d]$, $[n,k,d+1]$, called respectively a length, a dimension or an weight reductions of C. All of these families decrease the genus by 1.

The parity check matrices of the tangent codes to an affine variety X are the values of the Jacobian matrix of a generating set of the absolute ideal of X. That suggests their possible applications to the theory of convolutional codes (cf. [2, Ch. 9]). Tangent codes to appropriate families of affine varieties seem suitable for studying optimization and asymptotic problems on linear codes, due to their "geometrically integrable dynamical nature".

Here is a synopsis of the paper. Section 2 comprises some preliminaries on the Zariski topology and the Zariski tangent spaces $T_a(X,\mathbb{F}_{q^m})$ to an affine variety X. Our research starts in Section 3 by studying the minimum distance $d(T_a(X,\mathbb{F}_{q^m}))$ of a finite Zariski tangent space $T_a(X,\mathbb{F}_{q^m})$ to an irreducible affine variety $X/\mathbb{F}_q \subset \overline{\mathbb{F}_q}^n$, defined over $\mathbb{F}_q$. Proposition 3.2 (i) establishes that if X has some tangent code of minimum distance $\geq d+1$ then "almost all" finite Zariski tangent spaces to X are of minimum distance $\geq d+1$. The existence of a non-finite puncturing $\Pi_\gamma\colon X \to \Pi_\gamma(X)$ at $|\gamma| = d$ coordinates prohibits tangent codes of minimum distance $\geq d+1$, according to Proposition 3.2 (ii). Proposition 3.2 (iii) provides two sufficient conditions for the presence of a lower bound $d+1$ on "almost all" tangent codes to X. For an arbitrary $\mathbb{F}_q$-linear $[n,k,d]$-code C, Corollary 3.3 from Subsection 3.1 designs such a "twisted embedding" of $\overline{\mathbb{F}_q^k}$ in $\overline{\mathbb{F}_q}^n$, tangent to $C = T_{0^n}(X,\mathbb{F}_q)$ at the origin 0^n, whose finite Zariski tangent spaces "reproduce" the parameters $[n,k,d]$ of at "almost all the points" of X. By Proposition 3.4, for any family $\pi\colon \mathcal{C} \to \mathbb{F}_q^n$ of linear codes $\pi^{-1}(a) = \mathcal{C}(a) \subset \mathbb{F}_q^n$ there is an explicit (not necessarily irreducible) affine variety $X \subset \overline{\mathbb{F}_q}^n$, whose Zariski tangent spaces $T_a(X,\mathbb{F}_q) \subseteq \mathcal{C}(a)$ are contained in the members of the family for $\forall a \in \mathbb{F}_q^n$.

Chapter 4 is devoted to the construction of families of genus reductions of an $\mathbb{F}_q$-linear $[n,k,d]$-code C of genus $g := n+1-k-d > 0$. These are parameterized by Zariski open, Zariski dense subsets of affine spaces and defined by explicit polynomial parity check matrices. The length reduction of C with parameters $[n-1,k,d]$ consists of "almost all" tangent codes to the image $\Pi_n(X)$ of the puncturing $\Pi_n\colon X \to \Pi_n(X)$ of a "twisted embedding" of $\overline{\mathbb{F}_q^k}$ in $\overline{\mathbb{F}_q^n}$, at the last coordinate. The dimension reductions of C with parameters $[n,k+1,d]$ are parameterized by "almost all the points" of $\overline{\mathbb{F}_q}^{2(n-k)}$. Their parity check matrices are obtained by projecting the columns of a parity check matrix $H \in M_{(n-k)\times n}(\mathbb{F}_q)$ of C on appropriate hyperplanes in $\overline{\mathbb{F}_q}^{n-k}$. The existence of a polynomial parity check matrix of weight reductions of C with parameters $[n,k,\geq d+1]$ is established by an induction on the columns of the corresponding parity check matrices.

A work in progress focuses on simultaneous decoding of tangent codes with fixed error support and on the duals of the tangent codes. It relates some standard operations on tangent codes with appropriate operations of the associated affine varieties and constructs morphisms of affine varieties, whose differentials are Hamming isometries of the corresponding tangent codes.

2. Algebraic geometry preliminaries

Let $\overline{\mathbb{F}_q} = \cup_{m=1}^{\infty} \mathbb{F}_{q^m}$ be the algebraic closure of the finite field $\mathbb{F}_q$ with q elements and $\overline{\mathbb{F}_q}^n$ be the n-dimensional affine space over $\overline{\mathbb{F}_q}$. An affine variety $X \subset \overline{\mathbb{F}_q}^n$ is the common zero set

$$X = V(f_1, \ldots, f_m) = \{a \in \overline{\mathbb{F}_q}^n \mid f_1(a) = \cdots = f_m(a) = 0\}$$

of polynomials $f_1, \ldots, f_m \in \overline{\mathbb{F}_q}[x_1, \ldots, x_n]$. We say that $X \subset \overline{\mathbb{F}_q}^n$ is defined over $\mathbb{F}_q$ and denote $X/\mathbb{F}_q \subset \overline{\mathbb{F}_q}^n$ if the absolute ideal

$$I(X, \overline{\mathbb{F}_q}) := \{f \in \overline{\mathbb{F}_q}[x_1, \ldots, x_n] \mid f(a) = 0, \forall a \in X\}$$

of X is generated by polynomials $f_1, \ldots, f_m \in \mathbb{F}_q[x_1, \ldots, x_n]$ with coefficients from $\mathbb{F}_q$.

The affine subvarieties of X form a family of closed subsets. The corresponding topology is referred to as the Zariski topology on X. The Zariski closure $\overline{M}$ of a subset $M \subseteq X$ is defined as the intersection of the Zariski closed subsets Z of X, containing M. It is easy to observe that $\overline{M} = VI(M, \overline{\mathbb{F}_q})$ is the affine variety of the absolute ideal $I(M, \overline{\mathbb{F}_q}) \lhd \overline{\mathbb{F}_q}[x_1, \ldots, x_n]$ of M. A subset $M \subseteq X$ is Zariski dense if its Zariski closure $\overline{M} = X$ coincides with X. A property $\mathcal{P}(a)$, depending on a point $a \in \overline{\mathbb{F}_q}^n$ holds at a generic point of an affine variety $X \subset \overline{\mathbb{F}_q}^n$ if there is a Zariski dense subset $M \subseteq X$, such that $\mathcal{P}(a)$ is true for all $a \in M$.

An affine variety $X \subset \overline{\mathbb{F}_q}^n$ is irreducible if any decomposition $X = Z_1 \cup Z_2$ into a union of Zariski closed subsets $Z_j \subseteq X$ has $Z_1 = X$ or $Z_2 = X$. This holds exactly when the absolute ideal $I(X, \overline{\mathbb{F}_q}) \lhd \overline{\mathbb{F}_q}[x_1, \ldots, x_n]$ of X is prime, i.e., $fg \in I(X, \overline{\mathbb{F}_q})$ for $f, g \in \overline{\mathbb{F}_q}[x_1, \ldots, x_n]$ requires $f \in I(X, \overline{\mathbb{F}_q})$ or $g \in I(X, \overline{\mathbb{F}_q})$. A prominent property of the irreducible affine varieties X is the Zariski density of an arbitrary non-empty Zariski open subset $U \subseteq X$. This is equivalent to $U \cap W \neq \varnothing$ for any non-empty Zariski open subsets $U \subseteq X$ and $W \subseteq X$.

For an arbitrary irreducible affine variety $X/\mathbb{F}_q \subset \overline{\mathbb{F}_q}^n$, defined over $\mathbb{F}_q$ and an arbitrary constant field $\mathbb{F}_q \subseteq F \subseteq \overline{\mathbb{F}_q}$, the affine coordinate ring

$$F[X] := F[x_1, \ldots, x_n]/I(X, F)$$

of X over F is an integral domain. The fraction field

$$F(X) := \left\{ \frac{\varphi_1}{\varphi_2} \,\middle|\, \varphi_1, \varphi_2 \in F[X],\ \varphi_2 \neq 0 \in F[X] \right\}$$

of $F[X]$ is called the function field of X over F. The points $a \in X$ correspond to the maximal ideals $I(a, \overline{\mathbb{F}_q}) \triangleleft \overline{\mathbb{F}_q}[x_1, \ldots, x_n]$, containing $I(X, \overline{\mathbb{F}_q})$. For any F-rational point $a \in X(F) := X \cap F^n$ the localization

$$\mathcal{O}_a(X, F) := \left\{ \frac{\varphi_1}{\varphi_2} \,\middle|\, \varphi_1, \varphi_2 \in F[X],\ \varphi_2(a) \neq 0 \right\}$$

of $F[X]$ at $F[X] \setminus (I(a, F)/I(X, F))$ is the local ring of a in X over F. An F-linear derivation $D_a \colon \mathcal{O}_a(X, F) \to F$ at $a \in X(F)$ is an F-linear map, subject to Leibnitz-Newton rule $D_a(\psi_1\psi_2) = D_a(\psi_1)\psi_2(a) + \psi_1(a)D_a(\psi_2)$, $\forall \psi_1, \psi_2 \in \mathcal{O}_a(X, F)$. The F-linear space

$$T_a(X, F) := \mathrm{Der}_a(\mathcal{O}_a(X, F), F)$$

of the F-linear derivations $D_a \colon \mathcal{O}_a(X, F) \to F$ at $a \in X(F)$ is called the Zariski tangent space to X at a over F.

In order to derive a coordinate description of $T_a(X, F)$, note that any F-linear derivation $D_a \colon \mathcal{O}_a(X, F) \to F$ at $a \in X(F)$ restricts to an F-linear derivation $D_a \colon F[X] \to F$ at a. According to

$$D_a(\varphi_1) = D_a\left(\frac{\varphi_1}{\varphi_2}\right)\varphi_2(a) + \frac{\varphi_1(a)}{\varphi_2(a)} D_a(\varphi_2)$$

for all $\varphi_1, \varphi_2 \in F[X]$ with $\varphi_2(a) \neq 0$, any F-linear derivation $D_a \colon F[X] \to F$ at $a \in X(F)$ has unique extension to an F-linear derivation $D_a \colon \mathcal{O}_a(X, F) \to F$ at a. In such a way, there arises an F-linear isomorphism

$$T_a(X, F) \simeq \mathrm{Der}_a(F[X], F).$$

Any F-linear derivation $D_a \colon F[X] \to F$ of the affine ring $F[X]$ of X at $a \in X(F)$ lifts to an F-linear derivation $D_a \colon F[x_1, \ldots, x_n] \to F$ of the polynomial ring at a, vanishing on the ideal $I(X, F)$ of X over F. If $I(X, F) = \langle f_1, \ldots, f_m \rangle_F \triangleleft F[x_1, \ldots, x_n]$ is generated by $f_1, \ldots, f_m \in F[x_1, \ldots, x_n]$, then for arbitrary $g_1, \ldots, g_m \in F[x_1, \ldots, x_n]$ one has

$$D_a\left(\sum_{i=1}^{m} f_i g_i\right) = \sum_{i=1}^{m} D_a(f_i) g_i(a)$$

and the Zariski tangent space

$$T_a(X, F) \simeq \{D_a \in \mathrm{Der}_a(F[x_1, \ldots, x_n], F) \mid D_a(f_1) = \cdots = D_a(f_m) = 0\}$$

to X at a consists of the derivations $D_a \colon F[x_1, \ldots, x_n] \to F$ at a, vanishing on $f_1, \ldots, f_m$. In such a way, the coordinate description of $T_a(X, F)$ reduces to the coordinate description of

$$\mathrm{Der}_a(F[x_1, \ldots, x_n], F) = \mathrm{Der}_a(F[\overline{\mathbb{F}_q}^n], F) = T_a(\overline{\mathbb{F}_q}^n, F).$$

In order to endow $T_a(\overline{\mathbb{F}_q}^n, F)$ with a basis over F, let us note that the polynomial ring

$$F[x_1, \ldots, x_n] = F[x_1 - a_1, \ldots, x_n - a_n] = \oplus_{i=0}^{\infty} F[x_1 - a_1, \ldots, x_n - a_n]^{(i)}$$

has a natural grading by the F-linear spaces $F[x_1-a_1,\dots,x_n-a_n]^{(i)}$ of the homogeneous polynomials on $x_1-a_1,\dots,x_n-a_n$ of degree $i\geq 0$. An arbitrary F-linear derivation $D_a\colon F[x_1,\dots,x_n]\to F$ at $a\in F^n$ vanishes on $F[x_1-a_1,\dots,x_n-a_n]^{(0)}=F$ and on the homogeneous polynomials $F[x_1-a_1,\dots,x_n-a_n]^{(i)}$ of degree $i\geq 2$. Thus, D_a is uniquely determined by its restriction to the n-dimensional space

$$F[x_1-a_1,\dots,x_n-a_n]^{(1)}=\mathrm{Span}_F(x_1-a_1,\dots,x_n-a_n)$$

over F. That enables to identify the Zariski tangent space

$$T_a(\overline{\mathbb{F}_q}^n,F)\simeq \mathrm{Der}_a(F[x_1,\dots,x_n],F)\simeq \mathrm{Hom}_F(F[x_1-a_1,\dots,x_n-a_n]^{(1)},F)$$

to $\overline{\mathbb{F}_q}^n$ at a with the space of the F-linear functionals on the homogeneous linear polynomials $F[x_1-a_1,\dots,x_n-a_n]^{(1)}$. Note that $x_1-a_1,\dots,x_n-a_n$ is a basis of $F[x_1-a_1,\dots,x_n-a_n]^{(1)}$ over F and denote by $\left(\frac{\partial}{\partial x_1}\right)_a,\dots,\left(\frac{\partial}{\partial x_n}\right)_a$ its dual basis. In other words, $\left(\frac{\partial}{\partial x_j}\right)_a\in T_a(\overline{\mathbb{F}_q}^n,F)$ are the uniquely determined F-linear functionals on $F[x_1-a_1,\dots,x_n-a_n]^{(1)}$ with

$$\left(\frac{\partial}{\partial x_j}\right)_a(x_i-a_i)=\delta_{ij}=\begin{cases}1 & \text{for } 1\leq i=j\leq n,\\ 0 & \text{for } 1\leq i\neq j\leq n.\end{cases}$$

As a result, the Zariski tangent space to X at $a\in X(F)$ over F can be described as the linear subspace

$$T_a(X,F)=\left\{v=\sum_{j=1}^n v_j\left(\frac{\partial}{\partial x_j}\right)_a \;\Big|\; \sum_{j=1}^n v_j\frac{\partial f_i}{\partial x_j}(a)=0,\ 1\leq i\leq m\right\}$$

of F^n for any generating set $f_1,\dots,f_m$ of $I(X,F)=\langle f_1,\dots,f_m\rangle_F$.

Definition 2.1. If $F=\mathbb{F}_{q^s}$ is a finite field and $X/\mathbb{F}_q\subset\overline{\mathbb{F}_q}^n$ is an arbitrary irreducible affine variety defined over $\mathbb{F}_q$ then the linear space $T_a(X,\mathbb{F}_{q^s})\subset\mathbb{F}_{q^s}^n$ over $\mathbb{F}_{q^s}$ is called a tangent code. The parity check matrix of that code is the Jacobian matrix

$$\frac{\partial f}{\partial x}=\frac{\partial(f_1,\dots,f_m)}{\partial(x_1,\dots,x_n)}=\begin{pmatrix}\frac{\partial f_1}{\partial x_1} & \dots & \frac{\partial f_1}{\partial x_n}\\ \frac{\partial f_m}{\partial x_1} & \dots & \frac{\partial f_m}{\partial x_n}\end{pmatrix}$$

of a generating set $f_1,\dots,f_m$ of $I(X,\mathbb{F}_{q^s})\lhd\mathbb{F}_{q^s}[x_1,\dots,x_n]$.

Let $X/\mathbb{F}_q\subset\overline{\mathbb{F}_q}^n$ be an irreducible affine variety, defined over $\mathbb{F}_q$ and $a=(a_1,\dots,a_n)\in X$. The minimal extension $\mathbb{F}_{q^{\delta(a)}}:=\mathbb{F}_q(a_1,\dots,a_n)$ of the basic field $\mathbb{F}_q$, which contains the components of a is called the definition field of a. If $\mathbb{F}_{q^{\delta(a_i)}}=\mathbb{F}_q(a_i)$ are the definition fields of $a_i\in\overline{\mathbb{F}_q}$ over $\mathbb{F}_q$, then $\delta(a)$ is the least common multiple of $\delta(a_1),\dots,\delta(a_n)$. Note that $a\in X(\mathbb{F}_{q^m}):=X\cap\mathbb{F}_{q^m}^n$ is an $\mathbb{F}_{q^m}$-rational point if and only if $\delta(a)$ divides m. For all $l\in\mathbb{N}$ the Zariski tangent spaces $T_a(X,\mathbb{F}_{q^{l\delta(a)}})$ have one and a same parity check matrix

$$\frac{\partial f}{\partial x}(a):=\frac{\partial(f_1,\dots,f_m)}{\partial(x_1,\dots,x_n)}(a)\in M_{m\times n}(\mathbb{F}_{q^{\delta(a)}})$$

and are uniquely determined by $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ as the tensor products

$$T_a(X, \mathbb{F}_{q^{l\delta(a)}}) = T_a(X, \mathbb{F}_{q^{\delta(a)}}) \otimes_{\mathbb{F}_{q^{\delta(a)}}} \mathbb{F}_{q^{l\delta(a)}}.$$

In particular, $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ and $T_a(X, \mathbb{F}_{q^{l\delta(a)}})$ have one and a same dimension $n - \mathrm{rk}_{\mathbb{F}_{q^{\delta(a)}}} \frac{\partial f}{\partial x}(a)$ over $\mathbb{F}_{q^{\delta(a)}}$, respectively, over $\mathbb{F}_{q^{l\delta(a)}}$. The minimum distances of $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ and $T_a(X, \mathbb{F}_{q^{l\delta(a)}})$ coincide, as far as they equal the minimal natural number d for which $\frac{\partial f}{\partial x}(a)$ has d linearly dependent columns. From now on, we write $\dim T_a(X, \mathbb{F}_{q^{\delta(a)}})$ for the dimension of $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ over $\mathbb{F}_{q^{\delta(a)}}$.

Let $X = X_1 \cup \cdots \cup X_s$ be a reducible affine variety and $a \in X_{i_1} \cap \cdots \cap X_{i_r}$ with $1 \leq i_1 < \cdots < i_r \leq s$ be a common point of $r \geq 2$ irreducible components X_{i_j} of X. In general, X_{i_j} have different Zariski tangent spaces at a and the union $T_a(X_{i_1}, \mathbb{F}_{q^{\delta(a)}}) \cup \cdots \cup T_a(X_{i_r}, \mathbb{F}_{q^{\delta(a)}})$ is not an $\mathbb{F}_{q^{\delta(a)}}$-linear subspace of $\mathbb{F}^n_{q^{\delta(a)}}$. That is why we give the following definition of a tangent code to a reducible variety.

Definition 2.2. If $X/\mathbb{F}_q \subset \overline{\mathbb{F}_q}^n$ is a reducible affine variety, defined over $\mathbb{F}_q$, then the tangent code $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ to X at $a \in X$ is the $\mathbb{F}_{q^{\delta(a)}}$-linear code of length n with parity check matrix

$$\frac{\partial f}{\partial x}(a) = \frac{\partial(f_1, \ldots, f_m)}{\partial(x_1, \ldots, x_n)}(a) \in M_{m\times n}(\mathbb{F}_{q^{\delta(a)}}),$$

for some generators $f_1, \ldots, f_m \in \mathbb{F}_q[x_1, \ldots, x_n]$ of $I(X, \overline{\mathbb{F}_q}) = \langle f_1, \ldots, f_m\rangle_{\overline{\mathbb{F}_q}}$.

For a systematic study of the Zariski tangent spaces to an affine variety see [1, 7, 9, 10] or [4].

3. Immediate properties of tangent codes construction

3.1. Typical minimum distance of a tangent code

Let us recall that the Hamming weight $w(x)$ of vector $x = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$ is the number of the non-zero components and $w(x) \in \{0, 1, \ldots, n\}$. The Hamming distance $d(x, y)$ between vectors $x, y \in \mathbb{F}_q^n$ is the number of the different components $x_i \neq y_i$ and $d\colon \mathbb{F}_q^n \times \mathbb{F}_q^n \to \{0, 1, \ldots, n\}$, where $d(x, y) := w(x - y)$.

For an arbitrary finite set S and an arbitrary natural number $t \leq |S|$ let us denote by $\binom{S}{t}$ the collection of the t-sets of S, i.e., the family of the unordered subsets of S of cardinality t. In the case of $S = \{1, \ldots, n\}$, we write $\binom{1,\ldots,n}{t}$ instead of $\binom{\{1,\ldots,n\}}{t}$. For an arbitrary subset $\gamma \in \binom{1,\ldots,n}{d}$ of $\{1, \ldots, n\}$ of cardinality d, the erasing

$$\Pi_\gamma\colon \overline{\mathbb{F}_q}^n \longrightarrow \overline{\mathbb{F}_q}^{n-d}$$

of the components $x_\gamma = (x_{\gamma_1}, \ldots, x_{\gamma_d})$, labeled by $\gamma = \{\gamma_1, \ldots, \gamma_d\}$ is called the puncturing at γ. If $\neg\gamma = \{1, \ldots, n\} \setminus \gamma = \{\delta_1, \ldots, \delta_{n-d}\}$ is the complement of γ, then

$$\Pi_\gamma(x_1, \ldots, x_n) = x_{\neg\gamma} = (x_{\delta_1}, \ldots, x_{\delta_{n-d}}).$$

Any codeword of a linear code $C \subset \mathbb{F}_q^n$, whose weight equals the minimum Hamming distance is in the kernel of some puncturing Π_γ of C at $\gamma \in \binom{1,\dots,n}{d}$. Note that the puncturing

$$\Pi_\gamma \colon T_a(X, \mathbb{F}_{q^{\delta(a)}}) \longrightarrow \Pi_\gamma T_a(X, \mathbb{F}_{q^{\delta(a)}}) \subseteq \mathbb{F}_{q^{\delta(a)}}^{n-|\gamma|}$$

of a finite Zariski tangent space to X coincides with the differential

$$\Pi_\gamma = (d\Pi_\gamma)_a \colon T_a(X, \mathbb{F}_{q^{\delta(a)}}) \longrightarrow T_{\Pi_\gamma(a)}(\Pi_\gamma(X), \mathbb{F}_{q^{\delta(a)}})$$

of the puncturing

$$\Pi_\gamma \colon X \longrightarrow \Pi_\gamma(X)$$

of the corresponding irreducible affine variety X. That allows to study the minimum distance of $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ by the global properties of the puncturing $\Pi_\gamma \colon X \to \Pi_\gamma(X)$ of X.

In order to formulate precisely, let us recall that a finite morphism $\varphi \colon X \to \varphi(X)$ is called separable if the finite extension $\overline{\mathbb{F}_q}(\varphi(X)) \subseteq \overline{\mathbb{F}_q}(X)$ of the corresponding function fields is separable. This means that the minimal polynomial $g_\xi(t) \in \overline{\mathbb{F}_q}(\varphi(X))[t]$ of an arbitrary element $\xi \in \overline{\mathbb{F}_q}(X)$ over $\overline{\mathbb{F}_q}(\varphi(X))$ has no multiple roots.

A morphism $\varphi \colon X \to \varphi(X)$ is infinitesimally injective at some point $a \in X$, if the differential $(d\varphi)_a \colon T_a(X, \mathbb{F}_{q^{\delta(a)}}) \to T_{\varphi(a)}(\varphi(X), \mathbb{F}_{q^{\delta(a)}})$ of φ at a is an $\mathbb{F}_{q^{\delta(a)}}$-linear embedding. Let us denote by $\operatorname{Inf}\operatorname{Inj}(\varphi)$ the set of the points $a \in X$, at which the morphism $\varphi \colon X \to \varphi(X)$ is infinitesimally injective.

Lemma 3.1. *Let us suppose that $X/\mathbb{F}_q \subset \overline{\mathbb{F}_q}^n$ is an irreducible affine variety, defined over $\mathbb{F}_q$ and*

$$\Pi_\gamma \colon X \longrightarrow \Pi_\gamma(X) \subseteq \overline{\mathbb{F}_q}^{n-d}$$

is its puncturing at $\gamma \in \binom{1,\dots,n}{d}$.

(i) *The infinitesimally injective locus*

$$\operatorname{Inf}\operatorname{Inj}(\Pi_\gamma) = X \setminus V\left(\det \frac{\partial f_\delta}{\partial x_\gamma} \,\middle|\, \delta \in \binom{1,\dots,m}{d}\right) \tag{3.1}$$

is a Zariski open subset of X.

(ii) *If the set $\operatorname{Inf}\operatorname{Inj}(\Pi_\gamma) \cap \Pi_\gamma^{-1}(\Pi_\gamma(X)^{\mathrm{smooth}}) \neq \varnothing$ is non-empty, then the puncturing $\Pi_\gamma \colon X \to \Pi_\gamma(X)$ is a finite morphism,*

$$\operatorname{Inf}\operatorname{Inj}(\Pi_\gamma) \cap \Pi_\gamma^{-1}(\Pi_\gamma(X)^{\mathrm{smooth}}) \subseteq X^{\mathrm{smooth}}$$

and the differentials

$$(d\Pi_\gamma)_a \colon T_a(X, \mathbb{F}_{q^{\delta(a)}}) \longrightarrow T_{\Pi_\gamma(a)}(\Pi_\gamma(X), \mathbb{F}_{q^{\delta(a)}})$$

are surjective at all the points $a \in \operatorname{Inf}\operatorname{Inj}(\Pi_\gamma) \cap \Pi_\gamma^{-1}(\Pi_\gamma(X)^{\mathrm{smooth}})$.

(iii) *If the puncturing* $\Pi_\gamma\colon X \to \Pi_\gamma(X)$ *is a finite separable morphism then the intersection* $\operatorname{Inf}\operatorname{Inj}(\Pi_\gamma) \cap \Pi_\gamma^{-1}(\Pi_\gamma(X)^{\mathrm{smooth}}) \neq \varnothing$ *is a Zariski dense subset of* X. *In particular, for a finite* $\Pi_\gamma\colon X \to \Pi_\gamma(X)$, *whose degree* $\deg \Pi_\gamma := [\overline{\mathbb{F}_q}(X)\colon \overline{\mathbb{F}_q}(\Pi_\gamma(X))]$ *is relatively prime to* $p = \mathrm{char}\mathbb{F}_q$, *the subset* $\varnothing \neq \operatorname{Inf}\operatorname{Inj}(\Pi_\gamma) \cap \Pi_\gamma^{-1}(\Pi_\gamma(X)^{\mathrm{smooth}}) \subseteq X$ *is Zariski dense.*

Proof. (i) The kernel of the differential

$$(d\Pi_\gamma)_a\colon T_a(X, \mathbb{F}_{q^{\delta(a)}}) \longrightarrow T_{\Pi_\gamma(a)}(\Pi_\gamma(X), \mathbb{F}_{q^{\delta(a)}})$$

consists of the tangent vectors $v(a) \in T_a(X, \mathbb{F}_{q^{\delta(a)}})$ with $\operatorname{Supp}(v(a)) \subseteq \gamma$. Thus, $\ker(d\Pi_\gamma) \neq \{0^n\}$ exactly when $\operatorname{rk} \frac{\partial f}{\partial x_\gamma}(a) < d$. That justifies

$$X \setminus \operatorname{Inf}\operatorname{Inj}(\Pi_\gamma) = X \cap V\left(\det \frac{\partial f_\delta}{\partial x_\gamma} \,\middle|\, \delta \in \binom{1,\dots,m}{d}\right),$$

whereas (3.1).

(ii) Let us recall that $\dim T_a(X, \mathbb{F}_{q^{\delta(a)}}) \geq \dim X = k$ at all the points $a \in X$. If $a \in \operatorname{Inf}\operatorname{Inj}(\Pi_\gamma) \cap \Pi_\gamma^{-1}(\Pi_\gamma(X)^{\mathrm{smooth}})$, then

$$(d\Pi_\gamma)_a\colon T_a(X, \mathbb{F}_{q^{\delta(a)}}) \longrightarrow T_{\Pi_\gamma(a)}(\Pi_\gamma(X), \mathbb{F}_{q^{\delta(a)}})$$

is injective and $\dim T_{\Pi_\gamma(a)}(\Pi_\gamma(X), \mathbb{F}_{q^{\delta(a)}}) = \dim \Pi_\gamma(X)$. Combining with the inequality $\dim \Pi_\gamma(X) \leq \dim X$, one obtains

$$\begin{aligned}\dim X &\leq \dim T_a(X, \mathbb{F}_{q^{\delta(a)}}) = \dim (d\Pi_\gamma)_a T_a(X, \mathbb{F}_{q^{\delta(a)}}) \\ &\leq \dim T_{\Pi_\gamma(a)}(\Pi_\gamma(X), \mathbb{F}_{q^{\delta(a)}}) = \dim \Pi_\gamma(X) \leq \dim X.\end{aligned}$$

Therefore $(d\Pi_\gamma)_a T_a(X, \mathbb{F}_{q^{\delta(a)}}) = T_{\Pi_\gamma(a)}(\Pi_\gamma(X), \mathbb{F}_{q^{\delta(a)}})$, $\dim X = \dim T_a(X, \overline{\mathbb{F}_q})$ and the dimensions $\dim \Pi_\gamma(X) = \dim X$ coincide. In other words, the differential $(d\Pi_\gamma)_a\colon T_a(X, \mathbb{F}_{q^{\delta(a)}}) \longrightarrow T_{\Pi_\gamma(a)}(\Pi_\gamma(X), \mathbb{F}_{q^{\delta(a)}})$ is surjective, $a \in X^{\mathrm{smooth}}$ is a smooth point and $\Pi_\gamma\colon X \to \Pi_\gamma(X)$ is a finite morphism.

(iii) Without loss of generality, assume that $\gamma = \{1, \dots, d\}$, whereas $\neg\gamma := \{1, \dots, n\} \setminus \gamma = \{d+1, \dots, n\}$. Note that the puncturing $\Pi_\gamma\colon X \to \Pi_\gamma(X)$ is a finite morphism if and only if $\overline{x_s} := x_s + I(X, \overline{\mathbb{F}_q}) \in \overline{\mathbb{F}_q}(X)$ are algebraic over $\overline{\mathbb{F}_q}(\Pi_\gamma(X)) = \overline{\mathbb{F}_q}(\overline{x_{\neg\gamma}})$ for all $1 \leq s \leq d$. Let $g_s(x_s) \in \overline{\mathbb{F}_q}(\Pi_\gamma(X))[x_s]$ be the minimal polynomial of $\overline{x_s}$ over $\overline{\mathbb{F}_q}(\Pi_\gamma(X))$ and $f_s(x_s, x_{\neg\gamma}) \in \overline{\mathbb{F}_q}[x_s, x_{\neg\gamma}]$ be the product of g_s with the least common multiple of the denominators of the coefficients of g_s. Then $f_s(x_s, x_{\neg\gamma})$ is irreducible in $\overline{\mathbb{F}_a}[x_s, x_{\neg\gamma}]$ and defined up to a multiple from $\overline{\mathbb{F}_q}^*$. Moreover, $f_s(x_s, x_{\neg\gamma}) \in I(X, \overline{\mathbb{F}_q})$ is of minimal degree $\deg_{x_s} f_s(x_s, x_{\neg\gamma}) = \deg g_s(x_s) = \deg_{\overline{\mathbb{F}_q}(\Pi_\gamma(X))} \overline{x_s}$ with respect to x_s. According to $f_1, \dots, f_d \in I(X, \overline{\mathbb{F}_q})$, the Zariski tangent space $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ at an arbitrary point $a \in X$ is contained in the $\mathbb{F}_{q^{\delta(a)}}$-linear code $C(a)$ with parity check matrix

$$\frac{\partial(f_1, \dots, f_d)}{\partial(x_1, \dots, x_n)}(a) = \begin{pmatrix} \frac{\partial f_1}{\partial x_1}(a) & \cdots & 0 & \frac{\partial f_1}{\partial x_{d+1}}(a) & \cdots & \frac{\partial f_1}{\partial x_n}(a) \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & \frac{\partial f_d}{\partial x_d}(a) & \frac{\partial f_d}{\partial x_{d+1}}(a) & \cdots & \frac{\partial f_d}{\partial x_n}(a) \end{pmatrix}.$$

Note that $\Pi_\gamma^{-1}(\Pi_\gamma(X)^{\mathrm{smooth}})$ is a non-empty, Zariski open, Zariski dense subset of the irreducible affine variety X and $\operatorname{Inf}\operatorname{Inj}(\Pi_\gamma) \subseteq X$ is Zariski open by (i), so that the intersection $\operatorname{Inf}\operatorname{Inj}(\Pi_\gamma) \cap \Pi_\gamma^{-1}(\Pi_\gamma(X)^{\mathrm{smooth}}) = \varnothing$ only when $\operatorname{Inf}\operatorname{Inj}(\Pi_\gamma) = \varnothing$. We claim that $\operatorname{Inf}\operatorname{Inj}(\Pi_\gamma) = \varnothing$ requires the inseparability of $\overline{x_s} := x_s + I(X, \overline{\mathbb{F}_q}) \in \overline{\mathbb{F}_q}(X)$ over $\overline{\mathbb{F}_q}(\Pi_\gamma)$ for some $1 \leq s \leq d$. This suffices for $\operatorname{Inf}\operatorname{Inj}(\Pi_\gamma) \cap \Pi_\gamma^{-1}(\Pi_\gamma(X)^{\mathrm{smooth}}) \neq \varnothing$ in the case of a finite separable morphism $\Pi_\gamma \colon X \to \Pi_\gamma(X)$. The inseparability of $\overline{x_s} := x_s + \in I(X, \overline{\mathbb{F}_q}) \in \overline{\mathbb{F}_q}(X)$ over $\overline{\mathbb{F}_q}(\Pi_\gamma)$ holds only when $p = \mathrm{char}\mathbb{F}_q$ divides the degree

$$\deg_{\overline{\mathbb{F}_q}(\Pi_\gamma(X))} \overline{x_s} := [\overline{\mathbb{F}_q}(\Pi_\gamma(X))(\overline{x_s}) \colon \overline{\mathbb{F}_q}(\Pi_\gamma(X))]$$

of $\overline{x_s}$ over $\overline{\mathbb{F}_q}(\Pi_\gamma(X))$. Bearing in mind that the degree $\deg_{\overline{\mathbb{F}_q}(\Pi_\gamma(X))} \overline{x_s}$ of $\overline{x_s}$ divides the degree $\deg \Pi_\gamma = [\overline{\mathbb{F}_q}(X) \colon \overline{\mathbb{F}_q}(\Pi_\gamma(X))]$ of Π_γ, one concludes that the intersection $\operatorname{Inf}\operatorname{Inj}(\Pi_\gamma) \cap \Pi_\gamma^{-1}(\Pi_\gamma(X)^{\mathrm{smooth}}) \neq \varnothing$ is non-empty in the case of $\gcd(\deg \Pi_\gamma, p) = 1$.

By the very definition of an etale morphism, $\operatorname{Inf}\operatorname{Inj}(\Pi_\gamma) = \varnothing$ amounts to the existence of a nowhere vanishing vector field $v \colon X \to \coprod\limits_{a \in X} T_a(X, \mathbb{F}_{q^{\delta(a)}})$ with $\operatorname{Supp} v(a) \subseteq \gamma$ for all $a \in X$. Then $v(a) \in C(a)$ for all $a \in X$ and $\operatorname{rk} \frac{\partial(f_1, \ldots, f_d)}{\partial(x_1, \ldots, x_d)}(a) < d$. Thus,

$$\det \frac{\partial(f_1, \ldots, f_d)}{\partial(x_1, \ldots, x_d)}(a) = \prod_{s=1}^{d} \frac{\partial f_s}{\partial x_s}(a) = 0 \quad \text{for} \quad \forall a \in X$$

and $\prod\limits_{s=1}^{d} \frac{\partial f_s}{\partial x_s} \in I(X, \overline{\mathbb{F}_q})$. The absolute ideal $I(X, \overline{\mathbb{F}_q}) \lhd \overline{\mathbb{F}_q}[x_1, \ldots, x_n]$ of the irreducible affine variety X is prime, so that there is $1 \leq s \leq d$ with $\frac{\partial f_s}{\partial x_s} \in I(X, \overline{\mathbb{F}_q})$. Since $f_s(x_s, x_{\neg\gamma}) \in I(X, \overline{\mathbb{F}_q})$ is of minimal $\deg_{x_s} f_s(x_s, x_{\neg\gamma})$ and $\deg_{x_s} \frac{\partial f_s(x_s, x_{\neg\gamma})}{\partial x_s} < \deg_{x_s} f_s(x_s, x_{\neg\gamma})$, there follows $\frac{\partial f_s(x_s, x_{\neg\gamma})}{\partial x_s} \equiv 0_{\overline{\mathbb{F}_q}} \in \overline{\mathbb{F}_q}[x_s, x_{\neg\gamma}]$. As a result, $\frac{\partial g_s(x_s)}{\partial x_s} \equiv 0$ and $\overline{x_s}$ is inseparable over $\overline{\mathbb{F}_q}(\Pi_\gamma(X))$. □

Note that Lemma 3.1 (ii) is a sort of a generalization of the Implicit Function Theorem, according to which a puncturing $\Pi_\gamma \colon X \to \Pi_\gamma(X)$ with an injective differential at some $a \in \Pi_\gamma^{-1}(\Pi_\gamma(X))^{\mathrm{smooth}}$ is a finite morphism.

For an arbitrary irreducible affine variety $X/\mathbb{F}_q \subset \overline{\mathbb{F}_q}^n$, defined over $\mathbb{F}_q$, let us denote by

$$X^{(\leq d)} := \{a \in X \mid d(T_a(X, \mathbb{F}_{q^{\delta(a)}})) \leq d\}$$

the set of the points $a \in X$, at which the finite Zariski tangent spaces are of minimum distance $\leq d$. Similarly, put

$$X^{(d)} := \{a \in X \mid d(T_a(X, \mathbb{F}_{q^{\delta(a)}})) = d\} \text{ and } X^{(\geq d)} := \{a \in X \mid d(T_a(X, \mathbb{F}_{q^{\delta(a)}})) \geq d\}.$$

The next proposition establishes that if an irreducible affine variety X admits a tangent code $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ of minimum distance $\geq d+1$ then "almost all" finite Zariski tangent spaces to X are of minimum distance $\geq d+1$. If there is a non-finite puncturing $\Pi_\gamma \colon X \to \Pi_\gamma(X)$ at $|\gamma| = d$ variables, we show that all the tangent codes to X are of minimum distance $\leq d$. When all the puncturings $\Pi_\gamma \colon X \to \Pi_\gamma(X)$ at

$|\gamma| = d$ variables are finite and separable, the minimum distance of a finite Zariski tangent space to X is bounded below by $d+1$ at "almost all" points of X.

Proposition 3.2. *Let $X/\mathbb{F}_q \subset \overline{\mathbb{F}_q}^n$ be an irreducible affine variety of dimension $k \in \mathbb{N}$, defined over $\mathbb{F}_q$.*

(i) *For an arbitrary natural number $d \leq n-k+1$ the locus*

$$X^{(\geq d+1)} = \cap_{\gamma \in \binom{1,\dots,n}{d}} \operatorname{Inf}\operatorname{Inj}(\Pi_\gamma) = X \setminus V\left(\prod_{i \in \binom{1,\dots,n}{d}} \det \frac{\partial f_{\varphi(i)}}{\partial x_i} \,\middle|\, \varphi\colon \binom{1,\dots,n}{d} \to \binom{1,\dots,m}{d} \right)$$

is a Zariski open subset of X.

(ii) *If there is a non-finite puncturing $\Pi_\gamma\colon X \to \Pi_\gamma(X)$ at $|\gamma| = d$ coordinates, then $X = X^{(\leq d)}$. Moreover, in the case of $X^{(d)} \neq \varnothing$ the locus $X^{(d)} = X^{(\geq d)}$ is a Zariski dense, Zariski open subset of X.*

(iii) *If for any $\gamma \in \binom{1,\dots,n}{d}$ the puncturing $\Pi_\gamma\colon X \to \Pi_\gamma(X)$ is finite and separable, then the subset $X^{(\geq d+1)} \subseteq X$ is Zariski dense. In particular, if for any $\gamma \in \binom{1,\dots,n}{d}$ the puncturing $\Pi_\gamma\colon X \to \Pi_\gamma(X)$ is a finite morphism with $\gcd(\deg \Pi_\gamma, \operatorname{char}\mathbb{F}_q) = 1$ for $\deg \Pi_\gamma := [\overline{\mathbb{F}_q}(X)\colon \overline{\mathbb{F}_q}(\Pi_\gamma(X))]$, then $X^{(\geq d+1)}$ is a Zariski dense subset of X.*

Proof. (i) Let us observe that $a \in X^{(\geq d+1)}$ if and only if there is no tangent vector $v \in T_a(X, \mathbb{F}_{q^{\delta(a)}}) \setminus \{0^n\}$ with $\operatorname{Supp}(v) \subseteq \gamma$ for some $\gamma \in \binom{1,\dots,n}{d}$. That amounts to

$$\ker(d\Pi_\gamma)_a = \{v \in T_a(X, \mathbb{F}_{q^{\delta(a)}}) \mid \operatorname{Supp}(v) \subseteq \gamma\} = \{0^n\}$$

and holds exactly when $a \in \operatorname{Inf}\operatorname{Inj}(\Pi_\gamma)$ for all $\gamma \in \binom{1,\dots,n}{d}$.

Let $I(X, \overline{\mathbb{F}_q}) = \langle f_1, \dots, f_m \rangle \lhd \overline{\mathbb{F}_q}[x_1, \dots, x_n]$ be generated by some polynomials $f_1, \dots, f_m \in \mathbb{F}_q[x_1, \dots, x_n]$. Then $a \in X^{(\geq d+1)}$ exactly when any d-tuple of columns of $\frac{\partial f}{\partial x}(a)$ is linearly independent. In other words, $\operatorname{rk} \frac{\partial f}{\partial x_i}(a) = \operatorname{rk} \frac{\partial (f_1,\dots,f_m)}{\partial (x_{i_1},\dots,x_{i_d})}(a) = d$ for all $i \in \binom{1,\dots,n}{d}$. By $k = \dim X \geq n-m$ there follows $m \geq n-k \geq d$ and $\operatorname{rk} \frac{\partial f}{\partial x_i}(a) = d$ is equivalent to $\det \frac{\partial f_\gamma}{\partial x_i}(a) \neq 0$ for some $\gamma \in \binom{1,\dots,m}{d}$. Thus,

$$\begin{aligned} X^{(\geq d+1)} &= \cap_{i \in \binom{1,\dots,n}{d}} \left[\cup_{\gamma \in \binom{1,\dots,m}{d}} \left(X \setminus V\left(\det \frac{\partial f_\gamma}{\partial x_i} \right) \right) \right] \\ &= \cap_{i \in \binom{1,\dots,n}{d}} \left[X \setminus V\left(\det \frac{\partial f_\gamma}{\partial x_i} \,\middle|\, \gamma \in \binom{1,\dots,m}{d} \right) \right] \\ &= X \setminus \cup_{i \in \binom{1,\dots,n}{d}} V\left(\det \frac{\partial f_\gamma}{\partial x_i} \,\middle|\, \gamma \in \binom{1,\dots,m}{d} \right) \\ &= X \setminus V\left(\prod_{i \in \binom{1,\dots,n}{d}} \det \frac{\partial f_{\varphi(i)}}{\partial x_i} \,\middle|\, \varphi\colon \binom{1,\dots,n}{d} \to \binom{1,\dots,m}{d} \right), \end{aligned} \tag{3.2}$$

where $\varphi\colon \binom{1,\dots,n}{d} \to \binom{1,\dots,m}{d}$ vary over all the maps of the collection of the subsets of $\{1,\dots,n\}$ of cardinality d in the family of the subsets of $\{1,\dots,m\}$ of cardinality d. The last equality in (3.2) follows from

$$\cup_{i\in\binom{1,\dots,n}{d}} V(S_i) = V\left(\prod_{i\in\binom{1,\dots,n}{d}} S_i\right)$$

for

$$\prod_{i\in\binom{1,\dots,n}{d}} S_i := \left\{\prod_{i\in\binom{1,\dots,n}{d}} g_i \mid g_i \in S_i\right\}, \quad S_i := \left\{\det \frac{\partial f_\gamma}{\partial x_i}\middle| \gamma \in \binom{1,\dots,m}{d}\right\}.$$

(ii) We claim that at any point $a \in \Pi_\gamma^{-1}(\Pi_\gamma(X)^{\mathrm{smooth}})$ the Zariski tangent space $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ contains a non-zero word, supported by γ. To this end, it suffices to establish that the differential

$$(d\Pi_\gamma)_a\colon T_a(X,\mathbb{F}_{q^{\delta(a)}}) \longrightarrow T_{\Pi_\gamma(a)}(\Pi_\gamma(X),\mathbb{F}_{q^{\delta(a)}})$$

of Π_γ at a is non-injective. Assume the opposite, i.e., that $\ker(d\Pi_\gamma)_a = 0$. Then

$$k \le \dim T_a(X,\mathbb{F}_{q^{\delta(a)}}) \le \dim T_{\Pi_\gamma(a)}(\Pi_\gamma(X),\mathbb{F}_{q^{\delta(a)}}) = \dim \Pi_\gamma(X).$$

The morphism $\Pi_\gamma\colon X \to \Pi_\gamma(X)$ is not finite, so that $\dim \Pi_\gamma(X) < \dim X = k$. That leads to a contradiction and implies that $\ker(d\Pi_\gamma)_a \neq 0$ at any point $a \in \Pi_\gamma^{-1}(\Pi_\gamma(X)^{\mathrm{smooth}})$. As a result, $\Pi_\gamma^{-1}(\Pi_\gamma(X)^{\mathrm{smooth}}) \subseteq X^{(\le d)}$. According to (i), $X^{(\le d)}$ is a Zariski closed subset of X. The non-empty, Zariski open, Zariski dense subset $\Pi_\gamma^{-1}(\Pi_\gamma(X)^{\mathrm{smooth}})$ of X is Zariski dense, so that

$$X = \overline{\Pi_\gamma^{-1}(\Pi_\gamma(X)^{\mathrm{smooth}})} \subseteq \overline{X^{(\le d)}} = X^{(\le d)},$$

whereas $X = X^{(\le d)}$. Now, $X^{(d)} = X^{(\le d)} \cap X^{(\ge d)} = X \cap X^{(\ge d)} = X^{(\ge d)}$ is a Zariski open subset of X, whereas Zariski dense for $X^{(d)} \neq \varnothing$.

(iii) According to Lemma 3.1 (iii), if $\Pi_\gamma\colon X \to \Pi_\gamma(X)$ is a finite separable morphism or a finite morphism with $\gcd(\deg \Pi_\gamma, \mathrm{char}\mathbb{F}_q) = 1$, then $\operatorname{Inf}\operatorname{Inj}(\Pi_\gamma) \cap \Pi_\gamma^{-1}(\Pi_\gamma(X)^{\mathrm{smooth}}) \neq \varnothing$. In particular, $\operatorname{Inf}\operatorname{Inj}(\Pi_\gamma) \neq \varnothing$. Since $\operatorname{Inf}\operatorname{Inj}(\Pi_\gamma)$ is Zariski open by Lemma 3.1 (i), the finite intersection $X^{(\ge d+1)} = \cap_{\gamma\in\binom{1,\dots,n}{d}} \operatorname{Inf}\operatorname{Inj}(\Pi_\gamma)$ of the non-empty, Zariski open subsets $\operatorname{Inf}\operatorname{Inj}(\Pi_\gamma) \subseteq X$ is a non-empty, Zariski open, Zariski dense subset of the irreducible affine variety X. □

The above proposition reveals that for any point $a \in X^{(d)}$ there exists a d-tuple of indices $\gamma \in \binom{1,\dots,n}{d}$, such that $\Pi_\gamma\colon X \to \Pi_\gamma(X)$ is not infinitesimally injective at a.

3.2. Reproducing the dimension and the minimum distance of a code

For an arbitrary $\mathbb{F}_q$-linear $[n,k,d]$-code C we provide explicit equations of a twisted embedding of $\overline{\mathbb{F}_q}^k$ in $\overline{\mathbb{F}_q}^n$, whose tangent codes $T_a(X,\mathbb{F}_{q^{\delta(a)}})$ at a generic point reproduce the length n, the dimension k and the minimum distance d of C.

If not specified otherwise, $H=(H_1\dots H_n)$ is a parity check matrix of the linear code under consideration. For any $\lambda\in\binom{1,\dots,n}{t}$ we denote by H_λ the columns of H, labeled by λ. If $\mu\in\binom{1,\dots,m}{s}$, then $H_{\mu,\lambda}$ is the collection of the rows of H_λ, labeled by μ.

Corollary 3.3. *Let C be an $\mathbb{F}_q$-linear $[n,k,d]$-code and $\sigma\in\binom{1,\dots,n}{d}$ be the support of a non-zero word $c\in C\setminus\{0^n\}$. Then there is a smooth irreducible k-dimensional affine variety $X/\mathbb{F}_q\subset\overline{\mathbb{F}_q}^n$, isomorphic to $\overline{\mathbb{F}_q}^k$, such that $0^n\in X$, $T_{0^n}(X,\mathbb{F}_q)=C$ and $c\in T_a(X,\mathbb{F}_{q^{\delta(a)}})$ for all $a\in X$.*

In particular, $X=X^{(\le d)}$, so that $X^{(d)}=X^{(\ge d)}\neq\varnothing$ is a Zariski open, Zariski dense subset of X and $T_a(X,\mathbb{F}_{q^{\delta(a)}})$ are $[n,k,d]$-codes for all $a\in X^{(d)}$.

Proof. Let $H\in M_{(n-k)\times n}(\mathbb{F}_q)$ be a parity check matrix of the code C with columns $H_s\in M_{(n-k)\times 1}(\mathbb{F}_q)$ and $\sigma'=\sigma\setminus\{\sigma_d\}$ for some $\sigma_d\in\sigma$. Since C is of minimum distance d, the columns of H, labeled by σ' are linearly independent. Bearing in mind that H is of $\mathrm{rk}(H)=n-k$, one concludes the existence of $\tau\in\binom{\{1,\dots,n\}\setminus\sigma}{n-k-d+1}$, such that the square matrix $H_{\sigma'\cup\tau}=(H_{\sigma'}H_\tau)\in M_{(n-k)\times(n-k)}(\mathbb{F}_q)$ is non-singular. If $s\in\sigma\cup\tau$ and $1\le i\le n-k$, then let $f_{i,s}(x_s):=H_{i,s}x_s$. For $s\in\{1,\dots,n\}\setminus(\sigma\cup\tau)$ and $1\le i\le n-k$ take

$$f_{i,s}(x_s):=H_{i,s}x_s+\sum_{r=2}^{m_{i,s}}b_{i,s,r}x_s^r\in\mathbb{F}_q[x_s]$$

for some $m_{i,s}\in\mathbb{N}\setminus\{1\}$ and $b_{i,s,r}\in\mathbb{F}_q$, $\forall 2\le r\le m_{i,s}$. Consider

$$f_i(x_1,\dots,x_n):=\sum_{s=1}^{n}f_{i,s}(x_s)=\sum_{s=1}^{n}H_{i,s}x_s+\sum_{s\in\{1,\dots,n\}\setminus(\sigma\cup\tau)}\sum_{r=2}^{m_{i,s}}b_{i,s,r}x_s^r$$

for all $1\le i\le n-k$ and the affine variety $X:=V(f_1,\dots,f_{n-k})\subset\overline{\mathbb{F}_q}^n$, defined over $\mathbb{F}_q$. Let us denote $\rho:=\{1,\dots,n\}\setminus(\sigma'\cup\tau)$ and observe that $f_i(x_1,\dots,x_n)=0$ are equivalent to

$$\sum_{s\in\sigma'\cup\tau}H_{i,s}x_s=g_i(x_\rho)\quad\text{for some}\quad g_i(x_\rho)\in\mathbb{F}_q[x_\rho]\quad\text{and all } 1\le i\le n-k.$$

Viewing $x_{\sigma'\cup\tau}$ as a column of variables, labeled by $\sigma'\cup\tau\in\binom{1,\dots,n}{n-k}$, one can write the equations of X in the form

$$H_{\sigma'\cup\tau}\,x_{\sigma'\cup\tau}=\begin{pmatrix}g_1(x_\rho)\\ \vdots\\ g_{n-k}(x_\rho)\end{pmatrix}.$$

The invertibility of $H_{\sigma'\cup\tau}$ allows to represent the equations of X in the form

$$x_{\sigma'\cup\tau} = (H_{\sigma'\cup\tau})^{-1} \begin{pmatrix} g_1(x_\rho) \\ \vdots \\ g_{n-k}(x_\rho) \end{pmatrix}.$$

Thus, the puncturing $\Pi_{\sigma'\cup\tau}\colon X \to \overline{\mathbb{F}_q}^k$ at $\sigma'\cup\tau \in \binom{1,\dots,n}{n-k}$ is biregular, with inverse

$$(\Pi_{\sigma'\cup\tau})^{-1}(x_\rho) = \left((H_{\sigma'\cup\tau})^{-1} \begin{pmatrix} g_1(x_\rho) \\ \vdots \\ g_{n-k}(x_\rho) \end{pmatrix}, x_\rho \right).$$

In particular, X is a smooth irreducible affine variety of dimension $\dim X = k$.

The tangent spaces $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ at all the points $a \in X$ are linear codes of length n and dimension k, whose parity check matrices $\frac{\partial(f_1,\dots,f_{n-k})}{\partial(x_1,\dots,x_n)}(a)$ have columns $H_{\sigma\cup\tau}$, labeled by $\sigma\cup\tau \in \binom{1,\dots,n}{n-k+1}$. That is why $c \in C$ with $\mathrm{Supp}(c) = \sigma$ belongs to $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ for $\forall a \in X$ and the minimum distance $d(T_a(X, \mathbb{F}_{q^{\delta(a)}})) \le d$ at $\forall a \in X$. In other words, $X = X^{(\le d)}$. By the very construction of $f_i(x_1,\dots,x_n)$ one has $0^n \in X$ and $\frac{\partial(f_1,\dots,f_{n-k})}{\partial(x_1,\dots,x_n)}(0^n) = H$, whereas $T_{0^n}(X, \mathbb{F}_q) = C$. As a result, $0^n \in X^{(d)} = X^{(\ge d)}$ is non-empty and the Zariski tangent space $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ at a generic $a \in X$ is an $[n, k, d]$-code. □

The above proposition reveals that a single linear code C does not reflect global properties of the affine varieties X, tangent to C at some point $a \in X$. It illustrates how the equations of X govern the behavior of a generic tangent code to X.

3.3. Inscription of Zariski tangent spaces in families of linear codes

Proposition 3.4. *Let $\mathcal{C} \to S$ be a family of $\mathbb{F}_q$-linear codes $\mathcal{C}(a) \subset \mathbb{F}_q^n$, $a \in S$ of arbitrary dimension and minimum distance, parameterized by a subset $S \subseteq \mathbb{F}_q^n$. Then there exists a (not necessarily irreducible) affine variety $X \subseteq \overline{\mathbb{F}_q}^n$, containing all the $\mathbb{F}_q$-rational points $\mathbb{F}_q^n$ of $\overline{\mathbb{F}_q}^n$ and such that $T_a(X, \mathbb{F}_q) \subseteq \mathcal{C}(a)$ at $\forall a \in S$.*

Proof. Let $\mathcal{H} \to S$ be a family of parity-check matrices $\mathcal{H}(a) \in M_{(n-k)\times n}(\mathbb{F}_q)$ of $\mathcal{C}(a) \subset \mathbb{F}_q^n$ for all $a \in S$ and denote by $\mathcal{H}(a)_{ij} \in \mathbb{F}_q$ the entries of these matrices. For an arbitrary $\beta \in \mathbb{F}_q$, consider the Lagrange basis polynomial

$$L^\beta_{\mathbb{F}_q}(t) := \prod_{\alpha\in\mathbb{F}_q\setminus\{\beta\}} \frac{t-\alpha}{\beta-\alpha}$$

with $L^\beta_{\mathbb{F}_q}(t)(\beta) = 1$ and $L^\beta_{\mathbb{F}_q}(t)\big|_{\mathbb{F}_q\setminus\{\beta\}} = 0$. Straightforwardly,

$$L^0_{\mathbb{F}_q}(t) = -t^{q-1} + 1 \quad \text{and} \quad L^\beta_{\mathbb{F}_q}(t) = -t^{q-1} - \sum_{s=1}^{q-2} \beta^{-s} t^s, \quad \forall \beta \in \mathbb{F}_q^*.$$

Let us denote by

$$\Phi_p\colon \overline{\mathbb{F}_q}^n \longrightarrow \overline{\mathbb{F}_q}^n, \quad \Phi_p(a_1,\dots,a_n)=(a_1^p,\dots,a_n^p), \quad \forall a=(a_1,\dots,a_n)\in \overline{\mathbb{F}_q}^n$$

the Frobenius automorphism of degree $p=\mathrm{char}\mathbb{F}_q$ and consider

$$f_i(x_1,\dots,x_n) := \sum_{b\in\Phi_p(S)}\left[\sum_{j=1}^{n}\mathcal{H}(\Phi_p^{-1}(b))_{ij}(x_j-x_j^q)\right]L_{\mathbb{F}_q}^{b_1}(x_1^p)\dots L_{\mathbb{F}_q}^{b_n}(x_n^p)\in\mathbb{F}_q[x_1,\dots,x_n]$$

for $1\le i\le n-k$. The affine algebraic set $X:=V(f_1,\dots,f_{n-k})\subset\overline{\mathbb{F}_q}^n$ is claimed to satisfy the announced conditions. First of all, X passes through all the $\mathbb{F}_q$-rational points $\mathbb{F}_q^n$ of the affine space $\overline{\mathbb{F}_q}^n$, since $\forall a=(a_1,\dots,a_n)\in\mathbb{F}_q^n$ has components $a_j=a_j^q$ and $f_i(a_1,\dots,a_n)=0$ for $\forall 1\le i\le n-k$. The partial derivatives of f_i are $\frac{\partial f_i}{\partial x_j}=\sum\limits_{b\in\Phi_p(S)}\mathcal{H}(\Phi_p^{-1}(b))_{ij}L_{\mathbb{F}_q}^{b_1}(x_1^p)\dots L_{\mathbb{F}_q}^{b_n}(x_n^p)$ and their values at $a\in S\subseteq\mathbb{F}_q^n$ equal $\frac{\partial f_i}{\partial x_j}(a)=\mathcal{H}(\Phi_p^{-1}\Phi_p(a))_{ij}=\mathcal{H}(a)_{ij}$. Note that the composition of Lagrange interpolation polynomials with the Frobenius automorphism Φ_p is designed in such a way that to adjust

$$\frac{\partial(f_1,\dots,f_{n-k})}{\partial(x_1,\dots,x_n)}(a)=\mathcal{H}(a)$$

at all the points $a\in S$. By $f_1,\dots,f_{n-k}\in I(X,\overline{\mathbb{F}_q})=r(\langle f_1,\dots,f_{n-k}\rangle)$ for the radical $r(\langle f_1,\dots,f_{n-k}\rangle)\lhd\overline{\mathbb{F}_q}[x_1,\dots,x_n]$ of $\langle f_1,\dots,f_{n-k}\rangle\lhd\overline{\mathbb{F}_q}[x_1,\dots,x_n]$, the Zariski tangent space $T_a(X,\mathbb{F}_q)\subseteq\mathcal{C}(a)$ to X at an arbitrary point $a\in S$ is contained in the linear code $\mathcal{C}(a)$ with parity check matrix $\frac{\partial(f_1,\dots,f_{n-k})}{\partial(x_1,\dots,x_n)}(a)$. □

4. Families of genus reductions of a code

The genus of an $\mathbb{F}_q$-linear $[n,k,d]$-code C is defined as the deviation $g:=n+1-k-d$ of its parameters from the equality in the Singleton Bound $n+1-k-d\ge 0$. One of the problems in coding theory is to obtain a linear code C' of genus $g'=g-1\ge 0$ from the given linear code C of genus $g\ge 1$. We say that C' is a genus reduction of C. There are three standard ways for construction of a genus reduction C'. These are, respectively, the length, the dimension and the weight reductions of C with parameters $[n-1,k,d]$, $[n,k+1,d]$, $[n,k,d+1]$. In the next three subsections we use the set up of tangent codes, in order to construct families of length, dimension and weight reductions of C, parameterized by appropriate Zariski dense subsets of affine spaces over $\overline{\mathbb{F}_q}$.

4.1. A family of length reductions of a linear code

Here is a simple lemma from coding theory, which will be used for the construction of a family of length reductions of a linear code.

Lemma 4.1. *Let C be an $\mathbb{F}_q$-linear code of genus $g = n+1-k-d > 0$ with a parity check matrix $H = (H_1 \dots H_n) \in M_{(n-k)\times n}(\mathbb{F}_q)$. If*

$$H_n \notin \cup_{\lambda \in \binom{1,\dots,n-1}{d-1}} \mathrm{Span}_{\mathbb{F}_q}(H_\lambda), \tag{4.1}$$

then the image $\Pi_n(C) \subset \mathbb{F}_q^{n-1}$ of the puncturing $\Pi_n \colon C \to \Pi_n(C)$ of the last component is an $\mathbb{F}_q$-linear $[n-1,k,d]$-code.

Proof. If $H_n \notin \cup_{\lambda \in \binom{1,\dots,n-1}{d-1}} \mathrm{Span}_{\mathbb{F}_q}(H_\lambda)$ and $c = (c_1, \dots, c_n) \in C$ is a word of weight $\mathrm{wt}(c) = d$, then $c_n = 0$ and $\mathrm{Supp}(c) \in \binom{1,\dots,n-1}{d}$. As a result, $\mathrm{wt}(\Pi_n(c)) = \mathrm{wt}(c) = d$ and $\Pi_n(C) \subset \mathbb{F}_q^{n-1}$ is of minimum distance d. Let us suppose that there is a non-zero $c \in \ker(\Pi_n) \cap C = \{(0^{n-1}, c_n) \in C\}$. Then $H_n = 0^n \in \cap_{\lambda \in \binom{1,\dots,n-1}{d-1}} \mathrm{Span}_{\mathbb{F}_q}(H_\lambda)$. The contradiction with the assumption (4.1) reveals that $\ker(\Pi_n) \cap C = \{0^n\}$ and $\dim_{\mathbb{F}_q} \Pi_n(C) = \dim_{\mathbb{F}_q}(C) = k$. □

Recall that a linear code $C \subset \mathbb{F}_q^n$ is non-degenerate if it is not contained in a coordinate hyperplane $V(x_i) = \{a \in \mathbb{F}_q^n \mid a_i = 0\}$ for some $1 \le i \le n$.

Proposition 4.2. *Let C be a non-degenerate $\mathbb{F}_q$-linear $[n,k,d]$-code of genus $g = n+1-k-d > 0$. Then there exist a finite extension $\mathbb{F}_{q^m} \supseteq \mathbb{F}_q$, a smooth irreducible affine variety $X/\mathbb{F}_{q^m} \subset \overline{\mathbb{F}_q}^n$, isomorphic to $\overline{\mathbb{F}_q}^k$ and a Zariski dense subset $S \subseteq X$, such that $0^n \in S$, $T_{0^n}(X, \mathbb{F}_{q^m}) = C \otimes_{\mathbb{F}_q} \mathbb{F}_{q^m}$, the puncturing $\Pi_n \colon X \to \Pi_n(X)$ at x_n is a finite morphism and the images*

$$(d\Pi_n)_a T_a(X, \mathbb{F}_{q^{\delta(a)}}) = T_{\Pi_n(a)}(\Pi_n(X), \mathbb{F}_{q^{\delta(a)}})$$

of the puncturings of $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ at all the points $a \in S$ are $[n-1,k,d]$-codes.

Proof. Let $H' \in M_{(n-k)\times n}(\mathbb{F}_q)$ be a parity check matrix of C with columns H'_j for all $1 \le j \le n$. There is no loss in assuming that $H'_{k+1}, \dots, H'_n$ are linearly independent and form the identity matrix I_{n-k}. Any finite union of proper $\overline{\mathbb{F}_q}$-linear subspaces of the linear space $M_{(n-k)\times 1}(\overline{\mathbb{F}_q})$ over the infinite field $\overline{\mathbb{F}_q}$ has non-empty complement and there exists

$$c = \begin{pmatrix} c_1 \\ \vdots \\ c_{n-k} \end{pmatrix} \in M_{(n-k)\times 1}(\overline{\mathbb{F}_q}) \setminus \left\{ \left[\cup_{\lambda \in \binom{1,\dots,n-1}{d-1}} \mathrm{Span}_{\overline{\mathbb{F}_q}}(H'_\lambda) \right] \cup V(y_{n-k}) \right\}.$$

Let us denote by $\mathbb{F}_{q^m} := \mathbb{F}_q(c_1, \dots, c_{n-k})$ the definition field of c, put $p := \mathrm{char}\mathbb{F}_q$ for the characteristic of $\mathbb{F}_q$ and consider the affine variety $X := V(f_1, \dots, f_{n-k}) \subset \overline{\mathbb{F}_q}^n$, cut by the polynomials

$$f_i(x_1, \dots, x_k, x_{k+i}, x_n) := \sum_{s=1}^{k} H'_{i,s} x_s + x_{k+i} + c_i x_n^{p+1} \quad \text{for} \quad \forall 1 \le i \le n-k.$$

In order to construct a biregular morphism $X \to \overline{\mathbb{F}_q}^k$, note that $c_{n-k} \neq 0$ by the very choice of c and

$$X = V\left(f_i - \frac{c_i}{c_{n-k}} f_{n-k}, f_{n-k} \,\middle|\, 1 \leq i \leq n-k-1\right).$$

The equations

$$f_i(x_1, \ldots, x_k, x_{k+i}, x_n) - \frac{c_i}{c_{n-k}} f_{n-k}(x_1, \ldots, x_k, x_n) = \sum_{s=1}^{k} \left(H'_{i,s} - \frac{c_i}{c_{n-k}} H'_{n-k,s}\right) x_s + x_{k+i} - \frac{c_i}{c_{n-k}} x_n = 0$$

for $\forall 1 \leq i \leq n-k-1$ are equivalent to $x_{k+i} = \psi_{k+i}(x_1, \ldots, x_k, x_n)$ for

$$\psi_{k+i}(x_1, \ldots, x_k, x_n) := \sum_{s=1}^{k} \left(\frac{c_i}{c_{n-k}} H'_{n-k,s} - H'_{i,s}\right) x_s + \frac{c_i}{c_{n-k}} x_n,$$

$\forall 1 \leq i \leq n-k-1$. We claim the existence of $1 \leq s \leq k$ with $H'_{n-k,s} \neq 0$, since otherwise the last row of the parity check matrix H' of C is $(0^{n-1}, 1)$ and the non-degenerate code C is contained in the coordinate hyperplane with equation $x_n = 0$. Up to a permutation of the first k components of $\overline{\mathbb{F}_q}^n$, we assume that $H'_{n-k,k} \neq 0$. Then $f_{n-k}(x_1, \ldots, x_k, x_n) = 0$ is equivalent to $x_k = \psi_k(x_1, \ldots, x_{k-1}, x_n)$ for

$$\psi_k(x_1, \ldots, x_{k-1}, x_n) := -(H'_{n-k,k})^{-1} \left(\sum_{s=1}^{k-1} H'_{n-k,s} x_s + x_n + c_{n-k} x_n^{p+1}\right).$$

Thus, $X \subset \overline{\mathbb{F}_q}^n$ is cut by the equations

$$x_k - \psi_k(x_1, \ldots, x_{k-1}, x_n) = 0,$$
$$x_{k+i} - \psi_{k+i}(x_1, \ldots, x_{k-1}, \psi_k(x_1, \ldots, x_{k-1}, x_n), x_n) = 0 \quad \text{for} \quad \forall 1 \leq i \leq n-k-1$$

and the puncturing Π_α at $\alpha = \{k, k+1, \ldots, n-1\} \in \binom{1,\ldots,n}{n-k}$ provides a biregular morphism $\Pi_\alpha \colon X \to \overline{\mathbb{F}_q}^k$. In particular, X is a smooth irreducible affine variety, defined over $\mathbb{F}_{q^m}$. Note that the puncturing $\Pi_n \colon X \to \Pi_n(X)$ at x_n is a finite morphism, as far as the equation

$$f_{n-k}(x_1, \ldots, x_k, x_n) = \sum_{s=1}^{k} H'_{n-k,s} x_s + x_n + c_{n-k} x_n^{p+1} = 0$$

implies the algebraic dependence of the element $x_n + I(X, \overline{\mathbb{F}_q}) \in \overline{\mathbb{F}_q}(X)$ over the function field $\overline{\mathbb{F}_q}(\Pi_n(X)) = \overline{\mathbb{F}_q}(x_1 + I(X, \overline{\mathbb{F}_q}), \ldots, x_{n-1} + I(X, \overline{\mathbb{F}_q}))$.

For the rest of the proof, $T_a(X, \mathbb{F}_{q^{\delta(a)}})$, respectively, $T_{\Pi_n(a)}(\Pi_n(X), \mathbb{F}_{q^{\delta(a)}})$ are the Zariski tangent spaces over the definition fields $\mathbb{F}_{q^{\delta(a)}} := \mathbb{F}_{q^m}(a_1, \ldots, a_n)$ of $a \in X$ over $\mathbb{F}_{q^m}$. Note that

$$\frac{\partial(f_1, \ldots, f_{n-k})}{\partial x}(x_1, \ldots, x_n) = (H'_1 \ldots H'_{n-1} H_n(x_n)) = \frac{\partial f}{\partial x}(x_n) \tag{4.2}$$

with $H_n(x_n) = H'_n + x_n^p c$ depends only on x_n. The columns of the Jacobian matrix $\frac{\partial(f_1,\dots,f_{n-k})}{\partial x}(x_n)$, labeled by $\beta = \{k+1,\dots,n\} \in \binom{1,\dots,n}{n-k}$ form the matrix

$$\frac{\partial(f_1,\dots,f_{n-k})}{\partial x_\beta}(x_n) = \begin{pmatrix} 1 & 0 & \cdots & 0 & c_1 x_n^p \\ 0 & 1 & \cdots & 0 & c_2 x_n^p \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & c_{n-k-1} x_n^p \\ 0 & 0 & \cdots & 0 & 1 + c_{n-k} x_n^p \end{pmatrix}$$

with determinant $\det \frac{\partial(f_1,\dots,f_{n-k})}{\partial x_\beta}(x_n) = 1 + c_{n-k} x_n^p$. Thus, at any point $a \in X \setminus V(c_{n-k} x_n^p + 1)$, the matrix $\frac{\partial(f_1,\dots,f_{n-k})}{\partial x}(a_n) \in M_{(n-k)\times n}(\mathbb{F}_{q^{\delta(a)}})$ is of rank $\operatorname{rk} \frac{\partial f}{\partial x}(a_n) = n-k$. According to

$$f_1,\dots,f_{n-k} \in I(X, \overline{\mathbb{F}_q}) = IV(f_1,\dots,f_{n-k}) = r(\langle f_1,\dots,f_{n-k}\rangle) \lhd \overline{\mathbb{F}_q}[x_1,\dots,x_n],$$

the Zariski tangent space $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ at $a \in X$ is contained in the linear code $\mathcal{C}(a)$ with parity check matrix $\frac{\partial(f_1,\dots,f_{n-k})}{\partial x}(a)$. Since X is smooth, $\dim T_a(X, \mathbb{F}_{q^{\delta(a)}}) = \dim X = k$ at $\forall a \in X$ and $\frac{\partial(f_1,\dots,f_{n-k})}{\partial x}(a)$ is a parity check matrix of $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ if and only if $\operatorname{rk} \frac{\partial(f_1,\dots,f_{n-k})}{\partial x}(a) = n-k$. In particular, $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ has parity check matrix $\frac{\partial(f_1,\dots,f_{n-k})}{\partial x}(a)$ at all the points a of the non-empty, Zariski open, Zariski dense subset $X \setminus V(c_{n-k} x_n^p + 1)$ of X. Note that $0^n \in X = V(f_1,\dots,f_{n-k})$ and $0^n \notin V(c_{n-k} x_n^p + 1)$, so that $T_{0^n}(X, \mathbb{F}_{q^m})$ has parity check matrix $\frac{\partial(f_1,\dots,f_{n-k})}{\partial x}(0) = H'$ and $T_{0^n}(X, \mathbb{F}_{q^m}) = C \otimes_{\mathbb{F}_q} \mathbb{F}_{q^m}$.

Let $\Pi_n \colon \mathcal{C}(a) \to \Pi_n \mathcal{C}(a)$ be the puncturing at n and S_o be the set of those $a \in X$, at which $\Pi_n \mathcal{C}(a)$ is an $[n-1,k,d]$-code. By Lemma 4.1,

$$S_o \supseteq \left\{ a \in X \mid H_n(a_n) \notin \cup_{\lambda \in \binom{1,\dots,n-1}{d-1}} \operatorname{Span}_{\mathbb{F}_{q^{\delta(a)}}}(H'_\lambda) \right\},$$

whereas

$$Y := X \setminus S_o \subseteq Z := \left\{ a \in X \mid H_n(a_n) \in \cup_{\lambda \in \binom{1,\dots,n-1}{d-1}} \operatorname{Span}_{\overline{\mathbb{F}_q}}(H'_\lambda) \right\}.$$

We claim that Z is a proper Zariski closed subset of X. If so, then $X \setminus Z$ is a non-empty, Zariski open, Zariski dense subset of X and has non-empty, Zariski open, Zariski dense intersection $U := (X \setminus Z) \cap [X \setminus V(c_{n-k} x_n^p + 1)]$ with the Zariski open subset $X \setminus V(c_{n-k} x_n^p + 1) \neq \varnothing$ of the irreducible affine variety X. That suffices for $S' := S_o \cap [X \setminus V(c_{n-k} x_n^p + 1)] \supseteq U$ to be a Zariski dense subset of X, containing 0^n and such that $(d\Pi_n)_a T_a(X, \mathbb{F}_{q^{\delta(a)}})$ are $[n-1,k,d]$-codes at all $a \in S'$.

Towards the study of Z, let

$$Z_\lambda := \{ a \in X \mid H_n(a_n) \in \operatorname{Span}_{\overline{\mathbb{F}_q}}(H'_\lambda) \} = \{ a \in X \mid \operatorname{rk}(H'_\lambda H_n(a_n)) < d \}$$

for $\lambda \in \binom{1,\dots,n-1}{d-1}$ and represent $Z = \cup_{\lambda \in \binom{1,\dots,n-1}{d-1}} Z_\lambda$. If $\mu \in \binom{1,\dots,n-k}{d}$ and

$$g_{\mu,\lambda}(x_n) := \det \frac{\partial f_\mu}{\partial(x_\lambda, x_n)}(x_n) \in \mathbb{F}_{q^m}[x_n]$$

is the determinant of the matrix

$$\frac{\partial f_\mu}{\partial(x_\lambda, x_n)}(x_n) = (H'_{\mu,\lambda}H'_{\mu,n}(x_n)) = (H'_{\mu,\lambda}H'_{\mu,n} + x_n^p c_{\mu,n})$$

formed by the rows of $(H'_\lambda H_n(x_n))$, labeled by $\mu \in \binom{1,\dots,n-k}{d}$, then

$$Z_\lambda = X \cap V\left(g_{\mu,\lambda}(x_n) \,\middle|\, \forall \mu \in \binom{1,\dots,n-k}{d}\right)$$

is a Zariski closed subset of X and, therefore, $Z = \cup_{\lambda\in\binom{1,\dots,n-1}{d-1}} Z_\lambda$ is Zariski closed in X. The assumption

$$\cup_{\lambda\in\binom{1,\dots,n-1}{d-1}} Z_\lambda = Z = X$$

for the irreducible affine variety X requires

$$X = Z_\lambda \subseteq V\left(g_{\mu,\lambda}(x_n) \,\middle|\, \forall \mu \in \binom{1,\dots,n-k}{d}\right)$$

for some $\lambda \in \binom{1,\dots,n-1}{d-1}$. Recall that the puncturing $\Pi_\alpha : X \longrightarrow \overline{\mathbb{F}_q}^k$ at the $(n-k)$-tuple $\alpha = \{k, k+1, \dots, n-1\}$ is biregular and consider the sequence of affine varieties

$$\Pi_\alpha^{-1}(0^{k-1} \times \overline{\mathbb{F}_q}) \subseteq X \subseteq V\left(g_{\mu,\lambda}(x_n) \,\middle|\, \forall \mu \in \binom{1,\dots,n-k}{d}\right),$$

where $0^{k-1} \times \overline{\mathbb{F}_q} = V(x_1, \dots, x_{k-1}) \subset \overline{\mathbb{F}_q}^k$. Then $g_{\mu,\lambda}(x_n) \equiv 0$ for all $\mu \in \binom{1,\dots,n-k}{d}$, which holds exactly when $\det(H'_{\mu,\lambda}H'_{\mu,n}) = 0$ and $\det(H'_{\mu,\lambda}c_\mu) = 0$ for all $\mu \in \binom{1,\dots,n-k}{d}$. As a result, $\operatorname{rk}(H'_\lambda c) < d$ for $H'_\lambda \in M_{(n-k)\times(d-1)}(\mathbb{F}_q)$ of $\operatorname{rk} H'_\lambda = d-1$ and $c \in \operatorname{Span}_{\overline{\mathbb{F}_q}}(H'_\lambda)$. That contradicts the choice of c and shows that $Z \subsetneq X$ is a proper Zariski closed subset of X.

Note that the puncturing $\Pi_n \colon X \to \Pi_n(X)$ has injective differentials

$$(d\Pi_n)_a \colon T_a(X, \mathbb{F}_{q^{\delta(a)}}) \longrightarrow T_{\Pi_n(a)}(\Pi_n(X), \mathbb{F}_{q^{\delta(a)}}) \quad \text{at} \quad \forall a \in U,$$

so that the non-empty, Zariski open, Zariski dense subset $U \subseteq X$ is contained in the infinitesimally injective locus of Π_n, i.e., $U \subseteq \operatorname{Inf}\operatorname{Inj}(\Pi_n)$. Intersecting U with the non-empty, Zariski open subset $\Pi_n^{-1}(\Pi_n(X)^{\text{smooth}})$ of the irreducible affine variety X, one obtains a non-empty, Zariski open, Zariski dense subset $W := U \cap \Pi_n^{-1}(\Pi_n(X)^{\text{smooth}}) \subseteq X$. Then

$$S := S' \cap \Pi_n^{-1}(\Pi_n(X)^{\text{smooth}}) = S_o \cap [X \setminus V(c_{n-k}x_n^p + 1)] \cap \Pi_n^{-1}(\Pi_n(X)^{\text{smooth}}) \supseteq W$$

is such a Zariski dense subset of X that

$$(d\Pi_n)_a T_a(X, \mathbb{F}_{q^{\delta(a)}}) = T_{\Pi_n(a)}(\Pi_n(X), \mathbb{F}_{q^{\delta(a)}})$$

are $[n-1, k, d]$-codes for all $a \in S$ according to Lemma 3.1 (ii). □

4.2. A family of dimension reductions of a linear code

The next proposition provides a family of dimension reductions of an $\mathbb{F}_q$-linear $[n,k,d]$-code C of genus $g = n+1-k-d > 0$, which is parameterized by a non-empty, Zariski open, Zariski dense subset of $\overline{\mathbb{F}_q}^{2(n-k)}$. The codes from the family are not tangent to a specific affine variety. We choose a parity check matrix of the original $[n,k,d]$-code C and project it on various hyperplanes in $\overline{\mathbb{F}_q}^{n-k}$, in order to obtain parity check matrices of $[n,k+1,d]$-codes over finite extensions of $\mathbb{F}_q$.

Proposition 4.3. *Let us suppose that C is an $\mathbb{F}_q$-linear $[n,k,d]$-code of genus $g = n+1-k-d > 0$. Then there exist a Zariski open, Zariski dense subset $\mathcal{W} \subset \overline{\mathbb{F}_q}^{2(n-k)}$ and a family $\mathcal{C} \to \mathcal{W}$ of $\mathbb{F}_{q^{\delta(u,v)}}$-linear $[n,k+1,d]$-codes $\mathcal{C}(u,v)$, containing C for any $(u,v) \in \mathcal{W}$, $u,v \in \overline{\mathbb{F}_q}^{n-k}$.*

Proof. Let $H = (H_1 \dots H_n) \in M_{(n-k)\times n}(\mathbb{F}_q)$ be a parity check matrix of C with columns $H_1,\dots,H_n \in \mathbb{F}_q^{n-k}$. For any $\lambda \in \binom{1,\dots,n}{d-1}$ let us consider $Z_\lambda := \mathrm{Span}_{\overline{\mathbb{F}_q}}(H_\lambda) \simeq \overline{\mathbb{F}_q}^{d-1}$ as an irreducible affine subvariety of $M_{(n-k)\times 1}(\overline{\mathbb{F}_q}) \simeq \overline{\mathbb{F}_q}^{n-k}$ and put

$$V(Q) := \left\{ (u,v) \in \overline{\mathbb{F}_q}^{n-k} \times \overline{\mathbb{F}_q}^{n-k} \mid Q(u,v) = \langle u,v\rangle = \sum_{s=1}^{n-k} u_s v_s = 0 \right\}$$

for the quadric in $\overline{\mathbb{F}_q}^{2(n-k)}$, given by the inner product in $\overline{\mathbb{F}_q}^{n-k}$. Observe that $Z_\lambda \times \overline{\mathbb{F}_q}^{n-k}$, $V(Q)$ and, therefore,

$$Z := V(Q) \cup \left(\cup_{\lambda \in \binom{1,\dots,n}{d-1}} Z_\lambda \times \overline{\mathbb{F}_q}^{n-k} \right)$$

are proper affine subvarieties of $\overline{\mathbb{F}_q}^{2(n-k)}$, due to the irreducibility of the affine space $\overline{\mathbb{F}_q}^{2(n-k)}$ and the assumption $g > 0$. Thus, $\mathcal{W} := \overline{\mathbb{F}_q}^{2(n-k)} \setminus Z$ is a non-empty, Zariski open, Zariski dense subset of $\overline{\mathbb{F}_q}^{2(n-k)}$. For any $(u,v) \in \mathcal{W}$ with $u,v \in \overline{\mathbb{F}_q}^{n-k}$, note that $u \notin \cup_{\lambda \in \binom{1,\dots,n}{d-1}} Z_\lambda = \cup_{\lambda \in \binom{1,\dots,n}{d-1}} \mathrm{Span}_{\overline{\mathbb{F}_q}}(H_\lambda)$ and

$$u \notin \mathcal{H}_v := \{ z \in \overline{\mathbb{F}_q}^{n-k} \mid \langle z,v\rangle = 0 \}$$

for the hyperplane $\mathcal{H}_v \subset \overline{\mathbb{F}_q}^{n-k}$ with gradient vector v. That allows to consider the $\overline{\mathbb{F}_q}$-linear maps

$$\mathcal{L}_{u,v} \colon \overline{\mathbb{F}_q}^{n-k} \longrightarrow \mathcal{H}_v,$$
$$\mathcal{L}_{u,v}(y) := y - \frac{\langle y,v\rangle}{\langle u,v\rangle} u \quad \text{for} \quad \forall y \in \overline{\mathbb{F}_q}^{n-k}, \quad \forall (u,v) \in \mathcal{W},$$

which project $\overline{\mathbb{F}_q}^{n-k}$ on $\mathcal{H}_v$, parallel to $\ker \mathcal{L}_{u,v} = \mathrm{Span}_{\overline{\mathbb{F}_q}}(u)$. Here we use that for any $z \in \mathcal{H}_v$ one has $\mathcal{L}_{u,v}(z) = z$. Let us consider the definition field $\mathbb{F}_{q^{\delta(u,v)}} =$

$\mathbb{F}_q(u_1,\dots,u_{n-k},v_1,\dots,v_{n-k})$ of $(u,v)\in\mathcal{W}$ over $\mathbb{F}_q$ and the matrix $H(u,v):=(\mathcal{L}_{u,v}(H_1)\dots\mathcal{L}_{u,v}(H_n))\in M_{(n-k)\times n}(\mathbb{F}_{q^{\delta(u,v)}})$. The linear code $\mathcal{C}(u,v)$ with parity check matrix $H(u,v)$ contains C, as far as the $\overline{\mathbb{F}_q}$-linear map $\mathcal{L}_{u,v}$ transforms any non-trivial linear dependence $\sum\limits_{s=1}^{n}c_sH_s=0^{n-k}$ of the columns of H into a non-trivial linear dependence relation $\sum\limits_{s=1}^{n}c_s\mathcal{L}_{u,v}(H_s)=0^{n-k}$ of the columns of $H(u,v)$. In particular, $\mathcal{C}(u,v)$ contains words of weight d and the minimum distance $d(\mathcal{C}(u,v))\le d$. If there is a non-zero word $a\in\mathcal{C}(u,v)\backslash\{0^n\}$ with $\mathrm{Supp}(a)\subseteq\lambda=\{\lambda_1,\dots,\lambda_{d-1}\}\in\binom{1,\dots,n}{d-1}$, then $0^n=\sum\limits_{s=1}^{d-1}a_{\lambda_s}\mathcal{L}_{u,v}(H_{\lambda_s})=\mathcal{L}_{u,v}\left(\sum\limits_{s=1}^{d-1}a_{\lambda_s}H_{\lambda_s}\right)$, whereas $\sum\limits_{s=1}^{d-1}a_{\lambda_s}H_{\lambda_s}\in\ker\mathcal{L}_{u,v}=\mathrm{Span}_{\overline{\mathbb{F}_q}}(u)$ and $\sum\limits_{s=1}^{d-1}a_{\lambda_s}H_{\lambda_s}=\lambda_0u$ for some $\lambda_0\in\overline{\mathbb{F}_q}$. According to $u\notin\mathrm{Span}_{\overline{\mathbb{F}_q}}(H_\lambda)$, there follow $\lambda_0=0$ and $\mathrm{rk}\,H_\lambda=\mathrm{rk}(H_{\lambda_1},\dots,H_{\lambda_{d-1}})<d-1$. That contradicts the fact that C is of minimum distance d and shows that $\mathcal{C}(u,v)$ is of minimum distance $d(\mathcal{C}(u,v))=d$ for $\forall(u,v)\in\mathcal{W}$.

There remains to be checked that $\mathrm{rk}\,H(u,v)=n-k-1$ for all $(u,v)\in\mathcal{W}$, in order to derive that $\dim\mathcal{C}(u,v)=k+1$ and to conclude the proof of the proposition. To this end, note that $\mathcal{L}_{u,v}(H_s)\in\mathcal{H}_v$ for $\forall1\le s\le n$, whereas $\mathrm{Span}_{\overline{\mathbb{F}_q}}(\mathcal{L}_{u,v}(H_1),\dots,\mathcal{L}_{u,v}(H_n))\subseteq\mathcal{H}_v$ and $\mathrm{rk}\,H(u,v)\le\dim_{\overline{\mathbb{F}_q}}\mathcal{H}_v=n-k-1$. On the other hand, $H_s=\mathcal{L}_{u,v}(H_s)+\frac{\langle H_s,v\rangle}{\langle u,v\rangle}u$ for all $1\le s\le n$ imply that

$$\overline{\mathbb{F}_q}^{n-k}=\mathrm{Span}_{\overline{\mathbb{F}_q}}(H_1,\dots,H_n)\subseteq\mathrm{Span}_{\overline{\mathbb{F}_q}}(\mathcal{L}_{u,v}(H_1),\dots,\mathcal{L}_{u,v}(H_n),u).$$

If $\mathrm{rk}\,H(u,v)\le n-k-2$, then

$$n-k\le\dim_{\overline{\mathbb{F}_q}}\mathrm{Span}_{\overline{\mathbb{F}_q}}(\mathcal{L}_{u,v}(H_1),\dots,\mathcal{L}_{u,v}(H_n),u)\le\mathrm{rk}\,H(u,v)+1\le n-k-1$$

is an absurd, justifying $\mathrm{rk}\,H(u,v)=n-k-1$ and $\dim\mathcal{C}(u,v)=k+1$ for all $(u,v)\in\mathcal{W}:=\overline{\mathbb{F}_q}^{2(n-k)}\setminus\left[V(Q)\cup\left(\cup_{\lambda\in\binom{1,\dots,n}{d-1}}Z_\lambda\times\overline{\mathbb{F}_q}^{n-k}\right)\right]$, $u,v\in\overline{\mathbb{F}_q}^{n-k}$. □

4.3. A family of weight reductions of a linear code

Let C be a linear $[n,k,d]$-code, which is not MDS. The next proposition establishes the existence of a family $\mathcal{C}\to U$ of $[n,k]$-codes $\mathcal{C}(a)$, $a\in U$ of minimum distance $\ge d+1$, parameterized by a non-empty, Zariski open, Zariski dense subset $U\subseteq\overline{\mathbb{F}_q}^n$. The codes from $\mathcal{C}$ are defined by a polynomial parity check matrix in n variables, but are not tangent to a specific affine subvariety of $\overline{\mathbb{F}_q}^n$.

Proposition 4.4. *Let us suppose that C is an $\mathbb{F}_q$-linear $[n,k,d]$-code of genus $g=n+1-k-d>0$. Then there exist a finite extension $\mathbb{F}_{q^m}\supseteq\mathbb{F}_q$, a non-empty, Zariski open, Zariski dense subset $U\subseteq\overline{\mathbb{F}_q}^n$ and a family $\mathcal{C}\to\overline{\mathbb{F}_q}^n$ of linear codes $\mathcal{C}(a)\subset\mathbb{F}_{q^{\delta(a)}}^n$ over the definition fields $\mathbb{F}_{q^{\delta(a)}}$ of $a\in\overline{\mathbb{F}_q}^n$ over $\mathbb{F}_{q^m}$, such that $\mathcal{C}(0^n)=C\otimes_{\mathbb{F}_q}\mathbb{F}_{q^m}$ and $\mathcal{C}(a)$ are of length n, dimension k and minimum distance $\ge d+1$ at all the points $a\in U$.*

Proof. Let $H' = (H'_1 \dots H'_n) \in M_{(n-k)\times n}(\mathbb{F}_q)$ be a parity check matrix of $C \subseteq \mathbb{F}_q^n$, whose first $n-k$ columns form a non-singular square matrix $(H'_1, \dots, H'_{n-k}) \in \mathrm{GL}(n-k, \mathbb{F}_q)$. By an induction on $d \le j \le n$, we choose appropriate $c_d, \dots, c_n \in M_{(n-k)\times 1}(\overline{\mathbb{F}_q})$, in order to set

$$H_j := H'_j \ \text{ for } \ 1 \le j \le d-1,$$
$$H_j(x_j) := H'_j + x_j c_j \ \text{ for } \ d \le j \le n$$

and to obtain a polynomial matrix

$$H(x_d, \dots, x_n) = (H'_1 \dots H'_{d-1} H_d(x_d) \dots H_n(x_n)) \in M_{(n-k)\times n}(\overline{\mathbb{F}_q}[x_d, \dots, x_n]).$$

Let $\mathbb{F}_{q^m} = \mathbb{F}_q(c_{ij} \mid 1 \le i \le n-k,\ d \le j \le n)$ be the common definition field of all the entries of $c_d, \dots, c_n$ over $\mathbb{F}_q$. At any point $a \in \overline{\mathbb{F}_q}^n$, define $\mathcal{C}(a)$ to be the linear code over the definition field $\mathbb{F}_{q^{\delta(a)}} = \mathbb{F}_{q^m}(a_1, \dots, a_n)$ of a over $\mathbb{F}_{q^m}$, with parity check matrix $H(a) = H(a_d, \dots, a_n) \in M_{(n-k)\times n}(\mathbb{F}_{q^{\delta(a)}})$. Our choice of $H(x_d, \dots, x_n)$ is such that $H(0^n) = H'$, whereas $\mathcal{C}(0^n) = C \times_{\mathbb{F}_q} \mathbb{F}_{q^m}$. It suffices to show the existence of non-empty, Zariski open, Zariski dense subsets $U' \subseteq \overline{\mathbb{F}_q}^n$, $U'' \subseteq \overline{\mathbb{F}_q}^n$, such that $\mathcal{C}(a)$ are of minimum distance $\ge d+1$ at all $a \in U'$ and $\mathcal{C}(b)$ are of dimension k at all $b \in U''$. Then $U := U' \cap U'' \subseteq \overline{\mathbb{F}_q}^n$ is a non-empty, Zariski open, Zariski dense subset, over which the codes $\mathcal{C}(a)$, $a \in U$ are of length n, dimension k and minimum distance $\ge d+1$. Regardless of the choice of $c_d, \dots, c_n \in M_{(n-k)\times 1}(\overline{\mathbb{F}_q})$, let $\gamma := \{1, \dots, n-k\}$ and note that

$$U'' := \overline{\mathbb{F}_q}^n \setminus V\left(\det H_\gamma(x_d, \dots, x_{n-k})\right)$$

is a Zariski open subset of $\overline{\mathbb{F}_q}^n$ with $\dim \mathcal{C}(b) = k$ at all $b \in U''$. Since $0^n \in U''$, the set U'' is non-empty and, therefore, Zariski dense in $\overline{\mathbb{F}_q}^n$.

By an induction on $d \le j \le n$, we choose $c_j \in M_{(n-k)\times 1}(\overline{\mathbb{F}_q})$ and show the existence of a non-empty, Zariski open, Zariski dense subset $U_j \subseteq \overline{\mathbb{F}_q}^j$ with $\mathrm{rk}\, H_\beta(u) = d$ for all $\beta \in \binom{1,\dots,j}{d}$ and all $u \in U_j$. Then $U' := U_n$ will be a non-empty, Zariski open, Zariski dense subset of $\overline{\mathbb{F}_q}^n$, such that $\mathcal{C}(a)$ is of minimum distance $\ge d+1$ at all $a \in U'$. To this end, let $j = d$, $\lambda := \{1, \dots, d-1\}$ and note that $\mathrm{Span}_{\overline{\mathbb{F}_q}}(H'_\lambda) \simeq \overline{\mathbb{F}_q}^{d-1}$ is a proper subspace of $M_{(n-k)\times 1}(\overline{\mathbb{F}_q}) \simeq \overline{\mathbb{F}_q}^{n-k}$, according to $g > 0$. That allows to choose

$$c_d \in M_{(n-k)\times 1}(\overline{\mathbb{F}_q}) \setminus \mathrm{Span}_{\overline{\mathbb{F}_q}}(H'_\lambda)$$

and to put $H_d(x_d) := H'_d + x_d c_d$. The family $\{H_d(a_d)\}_{a_d \in \overline{\mathbb{F}_q}}$ of columns is claimed to have at most one common entry $H_d(\kappa_d)$ with $\mathrm{Span}_{\overline{\mathbb{F}_q}}(H'_\lambda)$, so that $\mathrm{rk}\, H_{\lambda\cup\{d\}}(x_d) = d$ at all the points of the non-empty, Zariski open, Zariski dense subset $U_d := \overline{\mathbb{F}_q}^{d-1} \times (\overline{\mathbb{F}_q} \setminus \{\kappa_d\})$ of $\overline{\mathbb{F}_q}^d$. Indeed, if $H_d(x_d) \notin \mathrm{Span}_{\overline{\mathbb{F}_q}}(H'_\lambda)$ for all $x_d \in \overline{\mathbb{F}_q}$, there is nothing to be proved. In the case of $H_d(\kappa_d) \in \mathrm{Span}_{\overline{\mathbb{F}_q}}(H'_\lambda)$ for some $\kappa_d \in \overline{\mathbb{F}_q}$, let us move the origin of $M_{(n-k)\times 1}(\overline{\mathbb{F}_q})$ at $H_d(\kappa_d) \in M_{(n-k)\times 1}(\overline{\mathbb{F}_q})$. The 1-dimensional linear

subspace $H_d(x_d)$ of the $(n-k)$-dimensional space $M_{(n-k)\times 1}(\overline{\mathbb{F}_q})$ intersects the $(d-1)$-dimensional linear subspace $\mathrm{Span}_{\overline{\mathbb{F}_q}}(H'_\lambda)$ in more than one point if and only if it is contained in $\mathrm{Span}_{\overline{\mathbb{F}_q}}(H'_\lambda)$. Then for arbitrary $x_d \neq y_d$ from $\overline{\mathbb{F}_q}$, one has $(x_d - y_d)c_d \in \mathrm{Span}_{\overline{\mathbb{F}_q}}(H'_\lambda)$, contrary to the choice of $c_d \notin \mathrm{Span}_{\overline{\mathbb{F}_q}}(H'_\lambda)$. That provides the base of the induction.

Suppose that $d+1 \leq j \leq n$ and $c_d, \ldots, c_{j-1} \in M_{(n-k)\times 1}(\overline{\mathbb{F}_q})$ have been chosen in such a way that there exists a non-empty, Zariski open, Zariski dense subset $U_{j-1} \subseteq \overline{\mathbb{F}_q}^{j-1}$ with $\mathrm{rk}\, H_\beta(u) = d$ for all $\beta \in \binom{1,\ldots,j-1}{d}$ and all $u \in U_{j-1}$. Fix an arbitrary $u \in U_{j-1}$ and choose

$$c_j \in M_{(n-k)\times 1}(\overline{\mathbb{F}_q}) \setminus \left[\cup_{\lambda\in\binom{1,\ldots,j-1}{d-1}} \mathrm{Span}_{\overline{\mathbb{F}_q}}(H_\lambda(u))\right]. \tag{4.3}$$

The existence of c_j is due to the fact that $\cup_{\lambda\in\binom{1,\ldots,j-1}{d-1}} \mathrm{Span}_{\overline{\mathbb{F}_q}}(H_\lambda(u))$ is a finite union of proper subspaces $\mathrm{Span}_{\overline{\mathbb{F}_q}}(H_\lambda(u)) \simeq \overline{\mathbb{F}_q}^{d-1}$ of the linear space $M_{(n-k)\times 1}(\overline{\mathbb{F}_q}) \simeq \overline{\mathbb{F}_q}^{n-k}$ over the infinite field $\overline{\mathbb{F}_q}$. We claim that

$$W_{j-1} := \{w \in U_{j-1} \mid c_j \notin \cup_{\lambda\in\binom{1,\ldots,j-1}{d-1}} \mathrm{Span}_{\overline{\mathbb{F}_q}}(H_\lambda(w))\}$$

is a Zariski open subset of U_{j-1}. Indeed,

$$\begin{aligned} U_{j-1} \setminus W_{j-1} &= \cup_{\lambda\in\binom{1,\ldots,j-1}{d-1}} \{t \in U_{j-1} \mid c_j \in \mathrm{Span}_{\overline{\mathbb{F}_q}}(H_\lambda(t))\} \\ &= \cup_{\lambda\in\binom{1,\ldots,j-1}{d-1}} \{t \in U_{j-1} \mid \mathrm{rk}(H_\lambda(t)c_j) = d-1\}, \end{aligned}$$

as far as $\mathrm{rk}\, H_\beta(u) = d$ for all $\beta \in \binom{1,\ldots,j-1}{d}$ and all $u \in U_{j-1}$ implies $\mathrm{rk}\, H_\lambda(t) = d-1$ for all $\lambda \in \binom{1,\ldots,j-1}{d-1}$ and all $t \in U_{j-1}$. Denoting by Σ_d^{d-1} the set of the maps $\mu\colon \binom{1,\ldots,j-1}{d-1} \to \binom{1,\ldots,n-k}{d}$ and putting

$$Y_j := V\left(\prod_{\lambda\in\binom{1,\ldots,j-1}{d-1}} \det(H_{\mu(\lambda),\lambda}c_{\mu(\lambda),j}) \,\middle|\, \forall \mu \in \Sigma_d^{d-1}\right),$$

one concludes that

$$\begin{aligned} U_{j-1} \setminus W_{j-1} &= \cup_{\lambda\in\binom{1,\ldots,j-1}{d-1}} \left\{t \in U_{j-1} \mid \det(H_{\nu,\lambda}(t)c_{\nu,j}) = 0,\ \forall \nu \in \binom{1,\ldots,n-k}{d}\right\} \\ &= \cup_{\lambda\in\binom{1,\ldots,j-1}{d-1}} \left[U_{j-1} \cap V\left(\det(H_{\nu,\lambda}c_{\nu,j}) \mid \forall \nu \in \binom{1,\ldots,n-k}{d}\right)\right] \\ &= U_{j-1} \cap Y_j \end{aligned}$$

is a Zariski closed subset of U_{j-1}, so that $W_{j-1} = U_{j-1} \setminus Y_j$ is Zariski open in U_{j-1}. According to $u \in W_{j-1}$ for the point $u \in U_{j-1}$, used in the choice (4.3) of c_j, $W_{j-1} \neq \varnothing$ is non-empty and, therefore, Zariski dense in $\overline{\mathbb{F}_q}^{j-1}$. Note that

$$\begin{aligned} U_j &:= \left\{(w, w_j) \in \overline{\mathbb{F}_q}^{j-1} \times \overline{\mathbb{F}_q} \mid \mathrm{rk}\, H_\beta(w, w_j) = d, \quad \forall \beta \in \binom{1,\ldots,j}{d}\right\} \\ &= \left\{(w, w_j) \in W_{j-1} \times \overline{\mathbb{F}_q} \mid \mathrm{rk}(H_\lambda(w)H_j(w_j)) = d, \quad \forall \lambda \in \binom{1,\ldots,j-1}{d-1}\right\} \end{aligned}$$

has complement

$$(W_{j-1}\times\overline{\mathbb{F}_q})\setminus U_j = \cup_{\lambda\in\binom{1,\dots,j-1}{d-1}}\left\{(w,w_j)\in W_{j-1}\times\overline{\mathbb{F}_q}\mid \operatorname{rk}(H_\lambda(w)H_j(w_j))<d\right\}$$
$$= \cup_{\lambda\in\binom{1,\dots,j-1}{d-1}}\left\{(w,w_j)\in W_{j-1}\times\overline{\mathbb{F}_q}\mid h_{\nu,\lambda}(w,w_j)=0,\ \forall\nu\in\tbinom{1,\dots,n-k}{d}\right\},$$

where $h_{\nu,\lambda}(x_d,\dots,x_j) := \det(H_{\nu,\lambda}(x_d,\dots,x_{j-1})H_{\nu,j}(x_j))\in\overline{\mathbb{F}_q}[x_d,\dots,x_j]$. If

$$Z_j := V\left(\prod_{\lambda\in\binom{1,\dots,j-1}{d-1}} h_{\mu(\lambda),\lambda}(x_d,\dots,x_j)\,\middle|\,\forall\mu\in\Sigma_d^{d-1}\right),$$

then

$$(W_{j-1}\times\overline{\mathbb{F}_q})\setminus U_j = (W_{j-1}\times\overline{\mathbb{F}_q})\cap\left[\cup_{\lambda\in\binom{1,\dots,j-1}{d-1}}V\left(h_{\nu,\lambda}\mid\forall\nu\in\tbinom{1,\dots,n-k}{d}\right)\right]$$
$$= (W_{j-1}\times\overline{\mathbb{F}_q})\cap Z_j$$

is Zariski closed in $W_{j-1}\times\overline{\mathbb{F}_q}$, so that $U_j = (W_{j-1}\times\overline{\mathbb{F}_q})\setminus Z_j$ is Zariski open in $W_{j-1}\times\overline{\mathbb{F}_q}$ and in $\overline{\mathbb{F}_q}^j$. The assumption $U_j=\varnothing$ implies $W_{j-1}\times\overline{\mathbb{F}_q}\subseteq Z_j$ and holds exactly when

$$h_{\mu(\lambda),\lambda} = \det(H_{\mu(\lambda),\lambda}(x_d,\dots,x_{j-1})H'_{\mu(\lambda)j} + x_j c_{\mu(\lambda)j})$$
$$= \det(H_{\mu(\lambda),\lambda}(x_d,\dots,x_{j-1})H'_{\mu(\lambda)j}) + x_j\det(H_{\mu(\lambda),\lambda}(x_d,\dots,x_{j-1})c_{\mu(\lambda)j})$$

is independent of x_j for all $\lambda\in\binom{1,\dots,j-1}{d-1}$ and all $\mu\colon\binom{1,\dots,j-1}{d-1}\to\binom{1,\dots,n-k}{d}$. That, in turn, is equivalent to $\det(H_{\nu,\lambda}(x_d,\dots,x_{j-1})c_{\nu j})=0$ for all $\nu\in\binom{1,\dots,n-k}{d}$ and all $\lambda\in\binom{1,\dots,j-1}{d-1}$ and specializes to $\det(H_{\nu,\lambda}(u)c_{\nu j})=0$ at the point $u\in U_{j-1}$, used in the choice (4.3) of c_j. As a result, $\operatorname{rk}(H_\lambda(u)c_j)<d$ for all $\lambda\in\binom{1,\dots,j-1}{d-1}$. The inductive hypothesis $\operatorname{rk}H_\beta(u)=d$ for all $\beta\in\binom{1,\dots,j-1}{d}$ requires $\operatorname{rk}H_\lambda(u)=d-1$ for all $\lambda\in\binom{1,\dots,j-1}{d-1}$ and $\operatorname{rk}(H_\lambda(u)c_j)<d$ is equivalent to $c_j\in\operatorname{Span}_{\overline{\mathbb{F}_q}}(H_\lambda(u))$ for all $\lambda\in\binom{1,\dots,j-1}{d-1}$. That contradicts the choice (4.3) of c_j and shows that $U_j\neq\varnothing$ is a non-empty, Zariski open, Zariski dense subset of $\overline{\mathbb{F}_q}^j$. □

Acknowledgements. The first author is partially supported by Contract 80-10-99/26.04.2023 of the Science Foundation of Sofia University "St. Kliment Ohridski".

References

[1] M. C. Beltrametti, E. Carletti, D. Gallarati, and G. M. Bragadin, Lectures on curves, surfaces and projective varieties (A classical view of algebraic geometry), European Mathematical Society Textbooks, Zürich, 2009.

[2] R. Blahut, Algebraic codes for data transmission, Cambridge University Press, 2003.

[3] I. Duursma, Weight distribution of geometric Goppa codes, Trans. Amer. Math. Soc. 351 (1999) 3609–3639.

[4] J. Harris, Algebraic geometry – A first course, Graduate Texts in Mathematics, Springer, 1992.
[5] W. C. Huffman, V. Pless, Fundamentals of error correcting codes, Cambridge University Press, 2003.
[6] A. Kasparian and I. Marinov, Duursma's reduced polynomial, Adv. Math. Commun. 11(4) (2017) 647–669.
[7] K. O'Grady, A first course in algebraic geometry, 2012.
[8] R. Pellikaan, On the efficient decoding of algebraic-geometric codes, in: Eurocode 92, ed. by P. Camion, P. Charpin and S. Harari, Udine, CISM Courses and Lectures 339, Springer, Wien, 1993, 231–253.
[9] M. Reid, Undergraduate Algebraic Geometry, London Mathematical Society Student Texts, 1989.
[10] I. R. Shafarevich, Basic Algebraic Geometry, v.1, 2, Nauka, Moscow, 1988 (in Russian).
[11] M. A. Tsfasman, S. G. Vlădut, and T. Zink, Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound, Math. Nachr. 109 (1982) 21–28.

Received on September 18, 2023
Accepted on February 13, 2024

Azniv K. Kasparian and Evgeniya D. Velikova

Faculty of Mathematics and Informatics
Sofia University "St. Kliment Ohridski"
5, James Bourchier Blvd.
1164 Sofia
BULGARIA

E-mails: kasparia@fmi.uni-fofia.bg
velikova@fmi.uni-sofia.bg