Tangent Codes *

Azniv Kasparian

Section of Algebra, Department of Mathematics and Informatics
Kliment Ohridski University of Sofia
5 James Bouchier Blvd., Sofia 1164, Bulgaria
email: kasparia@fmi.uni-soifa.bg

Evgeniya Velikova

Section of Algebra, Department of Mathematics and Informatics
Kliment Ohridski University of Sofia
James Bouchier Blvd., Sofia 1164, Bulgaria
email: velikova@fmi.uni-sofia.bg

Abstract

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 decreasing the length, increasing the dimension or increasing the minimum distance of a single $\mathbb{F}_q$-linear code by families of codes, parameterized by "almost all" the points of affine spaces over the algebraic closure $\overline{\mathbb{F}_q}$ of $\mathbb{F}_q$. The article discusses simultaneous decoding of tangent codes with fixed error support. The duals of the tangent codes to X are realized by gradients of polynomials from the ideal of X.

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.[15]). 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 [11] is a survey on these results.) Duursma's considerations from [5] 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.[8] for the exact formulation). The realizations of codes by points of a

[*] *2010 Mathematics Subject Classification:* Primary: 94B27, 14G50; Secondary: 14G17, 11T71

Key words and phrases: Zariski tangent space, minimum distance of a tangent code, simultaneous decoding of tangent codes, gradient codes, genus reduction of a tangent code.

Grassmannian, a determinantal variety or a modification of an arc provide other examples for exploiting "an extra structure" on the objects under study.

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. We propose a procedure for simultaneous decoding of tangent codes with fixed error support $j = \{j_1, \ldots, j_t\}$. This could be useful when the probability for the occurrence of an error support j is considerably larger than the one for any other t-tuple of indices. The spaces of the received words with error support j are described as tangent codes to appropriate affine varieties Y_j. Under some special choices of the equations of X, the parity check matrices of the tangent codes to Y_j are obtained from the ones for the tangent codes to X by removing t rows and t columns. Nevertheless, our characterization of the spaces of received words with error support j has high complexity and reduces to an exhaustive search.

By the very definition, the parity check matrices of the tangent codes to an affine variety X are values of the Jacobian matrix of a generating set of the absolute ideal of X. We exploit this in Chapter 4 for ”deforming” an abstract $\mathbb{F}_q$-linear $[n, k, d]$-code C with genus $g := n+1-k-d > 0$ into three families of linear codes, whose parameters are, respectively, $[n-1, k, d]$, $[n, k+1, d]$ or $[n, k, d+1]$. The aforementioned families are parameterized, respectively, by ”almost all the points” of the affine spaces $\overline{\mathbb{F}_q}^k$, $\overline{\mathbb{F}_q}^{2(n-k)}$ or $\overline{\mathbb{F}_q}^n$ over the algebraic closure $\overline{\mathbb{F}_q}$ of $\mathbb{F}_q$. The members of these families are called, respectively, length, dimension and weight reductions of C and viewed as special cases of genus reductions of C. In general, our construction takes place over a finite extension of the basic field $\mathbb{F}_q$. However, it detects and realizes the possibility for being accomplished over $\mathbb{F}_q$ itself.

In an analogy with the algebro-geometric Goppa codes, which have best decoding capacity on the projective line $\mathbb{P}^1(\overline{\mathbb{F}_q})$, the tangent codes set up is most flexible on the affine varieties $X \subset \overline{\mathbb{F}_q}^n$, isomorphic to $\overline{\mathbb{F}_q}^k$. The reason for this is that the irreducibility of a generic affine variety X is very difficult to be gained by an explicit choice of the equations of X, while the construction of ”twisted embeddings” of $\overline{\mathbb{F}_q}^k$ can be done easily in various ways (compare the constructions from Corollary 3, Proposition 6 and Corollary 14). The above considerations can be viewed as a testimony for the lack of coding theory constructions, reflecting the advantages of the algebraic varieties of general type.

The tangent codes set up studies families of linear codes, whose parity check matrices are the values of a given polynomial matrix. That suggests their possible applications to the theory of convolutional codes (cf.Chapter 9 from [2]). Appropriate collections of finite Zariski tangent spaces to 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 $X/\mathbb{F}_a \subset \overline{\mathbb{F}_q}^n$, defined over $\mathbb{F}_q$. Proposition 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 $\Pi_\gamma : X \to \Pi_\gamma(X)$ at $|\gamma| = d$ coordinates prohibits tangent codes of minimum distance $\geq d+1$, according to Proposition 2 (ii). Proposition 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 from subsection 3.1 designs such a "twisted embedding" $\overline{\mathbb{F}_q}^k \xrightarrow{\simeq} X \subset \overline{\mathbb{F}_q}^n$, 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 4, for any family $\pi : \mathcal{C} \rightarrow \mathbb{F}_q^n$ 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 $g := n+1-k-d > 0$. Our family of length reductions of C with parameters $[n-1,k,d]$ consists of "almost all" tangent codes to the image $\Pi_n(X)$ of the puncturing $\Pi_n : X \rightarrow \Pi_n(X)$ of a "twisted embedding" $\overline{\mathbb{F}_q}^k \xrightarrow{\simeq} X \subset \overline{\mathbb{F}_q}^n$ at the last coordinate. The members of the other two families are also determined by their parity check matrices, but are not tangent to affine varieties. 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.

The last chapter 5 discusses the simultaneous decoding of tangent codes with fixed error support and the gradient codes. After fixing the coding theory set up of the decoding with fixed error support $j \in \binom{1,\ldots,n}{t}$, we identify the spaces $\mathrm{Err}(T_a(X, \mathbb{F}_{q^m}), j)$ of the received words with $T_a(X, \mathbb{F}_{q^m})$-error supported by j with the Zariski tangent spaces $T_a(Y_j, \mathbb{F}_{q^m})$ of an affine variety Y_j. If $\Pi_j : \overline{\mathbb{F}_q}^n \rightarrow \overline{\mathbb{F}_q}^{n-t}$ is the puncturing at j and $\overline{\Pi_j(X)}$ is the Zariski closure of $\Pi_j(X)$ in $\overline{\mathbb{F}_q}^{n-t}$ then $Y_j \simeq \overline{\mathbb{F}_q}^t \times \overline{\Pi_j(X)}$ is the cylinder with base $\overline{\Pi_j(X)}$ in $\overline{\mathbb{F}_q}^n$. In general, $\mathrm{Err}(T_a(X, \mathbb{F}_{q^m}), j) = T_a(Y_j, \mathbb{F}_{q^m})$ are described by the means of Groebner bases of the absolute ideal of X (cf.Corollary 13). Corollary 14 provides such a "twisted embedding" $\overline{\mathbb{F}_q}^k \xrightarrow{\simeq} X \subset \overline{\mathbb{F}_q}^n$, for which the parity check matrices of $\mathrm{Err}(T_a(X, \mathbb{F}_{q^m}), j)$ are obtained from the ones for $T_a(X, \mathbb{F}_{q^m})$ by erasing t rows and t columns. The $\mathbb{F}_{q^m}$-linear decoding maps $\mathrm{Dec} : \mathrm{Err}(T_a(X, \mathbb{F}_{q^m}), j) \rightarrow T_a(X, \mathbb{F}_{q^m})$ arise naturally from the coding theory set up as the composition of the puncturing Π_j at j and its inverse $\Pi_j^{-1} : \Pi_j(T_a(X, \mathbb{F}_{q^m})) \rightarrow T_a(X, \mathbb{F}_{q^m})$. The special choice of the equations of X from Corollary 14 provides a uniform description of Dec at "almost all the points" of X, given by matrices of rational functions of $x_1, \ldots, x_n$ with coefficients from $\mathbb{F}_q$. The last subsection 5.3 describes the duals of the tangent codes $T_a(X, \mathbb{F}_{q^m})$ to X as the gradient codes $\mathrm{Grad}_a I(X, \mathbb{F}_{q^m})$ of the ideals of X over $\mathbb{F}_{q^m}$. In the special case of an existence of a polynomial $h \in I(X, \overline{\mathbb{F}_q}) \setminus \{0\}$ in at most d variables, Proposition 16 establishes the Zariski density of the locus $X_{\mathrm{grad}}^{(\leq d+1)} \subseteq X$ of the gradient codes of minimum distance $\leq d+1$.

A forthcoming article is going to relate some standard operations on tangent codes with appropriate operations of the associated affine varieties. It is going to discuss the construction of morphisms of affine varieties, whose differentials are Hamming isometries of the corresponding tangent codes.

Acknowledgements: The authors are extremely grateful to the referee of the journal "Finite Fields and their Applications", who generously shared his/her insight on the problem through specific remarks and suggestions. The research is partially supported by Contract 015/2014 and Contract 144/2015 with the Scientific Foundation of Kliment Ohridski University of Sofia.

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

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

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 $U \cap W \neq \emptyset$ 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 Xover 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 functional field of X over F. The points $a \in X$ correspond to the maximal ideals $I(a, \overline{\mathbb{F}_q}) \lhd \overline{\mathbb{F}_q}[x_1, \ldots, x_n]$, containing $I(X, \overline{\mathbb{F}_q})$. For any F-rational point

$a \in X(F) := X \cap F^n$ the localization

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

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 $D_a : \mathcal{O}_a(X,F) \rightarrow F$ at $a \in X(F)$ is an F-linear map, subject to Leibnitz-Newton rule $D_a(\psi_1\psi_2) = D_a(\psi_1)\psi_2(a) + \psi_1(a)D_a(\psi_2)$ for $\forall \psi_1, \psi_2 \in \mathcal{O}_a(X,F)$. The F-linear space

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

of the F-linear derivations $D_a : \mathcal{O}_a(X,F) \rightarrow F$ 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 $D_a : \mathcal{O}_a(X,F) \rightarrow F$ at $a \in X(F)$ restricts to an F-linear derivation $D_a : F[X] \rightarrow F$ at a. According to

$$D_a(\varphi_1) = D_a\left(\frac{\varphi_1}{\varphi_2}\right)\varphi_2(a) + \frac{\varphi_1(a)}{\varphi_2(a)} D_a(\varphi_2) \quad \text{for} \quad \forall \varphi_1, \varphi_2 \in F[X] \quad \text{with} \quad \varphi_2(a) \neq 0,$$

any F-linear derivation $D_a : F[X] \rightarrow F$ at $a \in X(F)$ has unique extension to an F-linear derivation $D_a : \mathcal{O}_a(X,F) \rightarrow F$ 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 $D_a : F[X] \rightarrow F$ of the affine ring $F[X]$ of X at $a \in X(F)$ lifts to an F-linear derivation $D_a : F[x_1, \ldots, x_n] \rightarrow F$ 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

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

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

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

over F. That enables to identify the Zariski tangent space

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

to $\overline{\mathbb{F}_q}^n$ at a with the space of the F-linear functionals on $F[x_1 - a_1, \ldots, x_n - a_n]^{(1)}$. Note that $x_1 - a_1, \ldots, x_n - a_n$ is a basis of $F[x_1 - a_1, \ldots, x_n - a_n]^{(1)}$ over F and denote by $\left(\frac{\partial}{\partial x_1}\right)_a, \ldots, \left(\frac{\partial}{\partial x_n}\right)_a$ 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 $F[x_1 - a_1, \ldots, x_n - a_n]^{(1)}$ 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

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

for any generating set $f_1, \ldots, f_m$ of $I(X, F) = \langle f_1, \ldots, f_m \rangle_F$. If

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

is the Jacobian matrix of $f_1, \ldots, f_m$ and $F = \mathbb{F}_{q^s}$ is a finite field then $T_a(X, \mathbb{F}_{q^s}) \subset \mathbb{F}_{q^s}^n$ is the $\mathbb{F}_{q^s}$-linear code with parity check matrix $\frac{\partial f}{\partial x}(a) \in M_{m \times n}(\mathbb{F}_{q^s})$.

Let $X/\mathbb{F}_q \subset \overline{\mathbb{F}_q}^n$ be an irreducible affine variety, defined over $\mathbb{F}_q$ and $a = (a_1, \ldots, a_n) \in X$. The minimal extension $\mathbb{F}_{q^{\delta(a)}} := \mathbb{F}_q(a_1, \ldots, a_n)$ 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 $\delta(a_1), \ldots, \delta(a_n)$. 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

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

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 equal 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 $X = X_1 \cup \ldots \cup X_s$ be a reducible affine variety and $a \in X_{i_1} \cap \ldots \cap X_{i_r}$ with $1 \leq i_1 < \ldots < i_r \leq s$ 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 $T_a(X_{i_1}, \mathbb{F}_{q^{\delta(a)}}) \cup \ldots \cup T_a(X_{i_r}, \mathbb{F}_{q^{\delta(a)}})$ is not an $\mathbb{F}_{q^{\delta(a)}}$-linear subspace of $\mathbb{F}^n_{q^{\delta(a)}}$. That is why we define the Zariski tangent space $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ to a reducible variety $X \subset \overline{\mathbb{F}_q}^n$ at a point $a \in X$ as 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 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 a systematic study of the Zariski tangent spaces to an affine variety see [13], [1], [10], [12] or [6].

3 Immediate properties of tangent codes construction

3.1 Typical minimum distance of a tangent code

For an arbitrary subset $\gamma \in \binom{1,\ldots,n}{d}$ of $\{1, \ldots, n\}$ of cardinality d, the erasing

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

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

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

The minimum distance of a linear code $C \subset \mathbb{F}_q^n$ is related to the kernels of the puncturings of C. Note that the puncturing

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

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

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

of the puncturing

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

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 $\Pi_\gamma : X \to \Pi_\gamma(X)$.

In order to formulate precisely, let us recall that a finite morphism $\varphi : X \to \varphi(X)$ 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 $\varphi : X \to \varphi(X)$ is etale at some point $a \in X$, if the differential $(d\varphi)_a : T_a(X, \mathbb{F}_{q^{\delta(a)}}) \to T_{\varphi(a)}(\varphi(X), \mathbb{F}_{q^{\delta(a)}})$ of φ at a is an $\mathbb{F}_{q^{\delta(a)}}$-linear embedding. Let us denote by $\mathrm{Etale}(\varphi)$ the set of the points $a \in X$, at which the morphism $\varphi : X \to \varphi(X)$ is etale.

Lemma 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* $\Pi_\gamma : X \to \Pi_\gamma(X) \subseteq \overline{\mathbb{F}_q}^{n-d}$ *is its puncturing at* $\gamma \in \binom{1,\ldots,n}{d}$.

(i) The etale locus

$$\mathrm{Etale}(\Pi_\gamma) = X \setminus V\left(\det \frac{\partial f_\delta}{\partial x_\gamma} \ \Big| \ \delta \in \binom{1, \ldots, m}{d}\right) \qquad (1)$$

is a Zariski open subset of X.

(ii) If the set $\mathrm{Etale}(\Pi_\gamma) \cap \Pi_\gamma^{-1}(\Pi_\gamma(X)^{\mathrm{smooth}}) \neq \emptyset$ *is non-empty then the puncturing* $\Pi_\gamma : X \to \Pi_\gamma(X)$ *is a finite morphism,* $\mathrm{Etale}(\Pi_\gamma) \cap \Pi_\gamma^{-1}(\Pi_\gamma(X)^{\mathrm{smooth}}) \subseteq X^{\mathrm{smooth}}$ *and the differentials*

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

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

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

Proof. (i) The kernel of the differential $(d\Pi_\gamma)_a : T_a(X, \mathbb{F}_{q^{\delta(a)}}) \to T_{\Pi_\gamma(a)}(\Pi_\gamma(X), \mathbb{F}_{q^{\delta(a)}})$ consists of the tangent vectors $v(a) \in T_a(X, \mathbb{F}_{q^{\delta(a)}})$ with support $\mathrm{Supp}(v(a)) \subseteq \gamma$. Thus, $\ker(d\Pi_\gamma) \neq \{0^n\}$ exactly when $\mathrm{rk}\frac{\partial f}{\partial x_\gamma}(a) < d$. That justifies

$$X \setminus \mathrm{Etale}(\Pi_\gamma) = X \cap V\left(\det \frac{\partial f_\delta}{\partial x_\gamma} \ \Big| \ \delta \in \binom{1, \ldots, m}{d}\right),$$

whereas (1).

(ii) Let us observe that $\dim T_a(X, \mathbb{F}_{q^{\delta(a)}}) \geq \dim X = k$ at all the points $a \in X$. If $a \in \mathrm{Etale}(\Pi_\gamma) \cap \Pi_\gamma^{-1}(\Pi_\gamma(X)^{\mathrm{smooth}})$ then $(d\Pi_\gamma)_a : T_a(X, \mathbb{F}_{q^{\delta(a)}}) \to T_{\Pi_\gamma(a)}(\Pi_\gamma(X), \mathbb{F}_{q^{\delta(a)}})$ 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

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

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

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

is surjective, $a \in X^{\text{smooth}}$ is a smooth point and $\Pi_\gamma : X \to \Pi_\gamma(X)$ is a finite morphism.

(iii) Without loss of generality, assume that $\gamma = \{1, \ldots, d\}$, $\neg\gamma := \{1, \ldots, n\} \setminus \gamma = \{d+1, \ldots, n\}$ and note that the puncturing $\Pi_\gamma : X \to \Pi_\gamma(X)$ 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 $f_1, \ldots, f_d \in I(X, \overline{\mathbb{F}_q})$, 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

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

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

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

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 $\deg \Pi_\gamma = [\overline{\mathbb{F}_q}(X) : \overline{\mathbb{F}_q}(\Pi_\gamma(X))]$ of Π_γ, one concludes that the intersection $\text{Etale}(\Pi_\gamma) \cap \Pi_\gamma^{-1}(\Pi_\gamma(X)^{\text{smooth}}) \neq \emptyset$ is non-empty in the case of $\text{GCD}(\deg \Pi_\gamma, p) = 1$.

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

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

and $\prod\limits_{s=1}^{d} \frac{\partial f_s}{\partial x_s} \in I(X, \overline{\mathbb{F}_q})$. The absolute ideal $I(X, \overline{\mathbb{F}_q}) \triangleleft \overline{\mathbb{F}_q}[x_1, \ldots, x_n]$ of the irreducible affine variety X is prime, so that $\frac{\partial f_s}{\partial x_s} \in I(X, \overline{\mathbb{F}_q})$ for some $1 \leq s \leq d$. 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 1 (ii) establishes a sort of a generalization of the Implicit Function Theorem, according to which any puncturing $\Pi_\gamma : X \rightarrow \Pi_\gamma(X)$ with an injective differential at some point $a \in \Pi_\gamma^{-1}(\Pi_\gamma(X))^{\rm smooth}$ 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

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

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

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 $\Pi_\gamma : X \rightarrow \Pi_\gamma(X)$ at $|\gamma| = d$ variables, we show that all the tangent codes to X are of minimum distance $\leq d$. When all the puncturings $\Pi_\gamma : X \rightarrow \Pi_\gamma(X)$ 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" the points of X.

Proposition 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

$$X^{(\geq d+1)} = \cap_{\gamma \in \binom{1,\ldots,n}{d}} {\rm Etale}(\Pi_\gamma) =$$

$$X \setminus V \left(\prod_{i \in \binom{1,\ldots,n}{d}} \det \frac{\partial f_{\varphi(i)}}{\partial x_i} \ \Big| \ \forall \varphi : \binom{1,\ldots,n}{d} \rightarrow \binom{1,\ldots,m}{d} \right)$$

is a Zariski open subset of X.

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

(iii) If for any $\gamma \in \binom{1,\ldots,n}{d}$ the puncturing $\Pi_\gamma : X \rightarrow \Pi_\gamma(X)$ is finite and separable then the subset $X^{(\geq d+1)} \subseteq X$ is Zariski dense. In particular, if for any $\gamma \in \binom{1,\ldots,n}{d}$ the puncturing $\Pi_\gamma : X \rightarrow \Pi_\gamma(X)$ is a finite morphism with ${\rm GCD}(\deg \Pi_\gamma, {\rm char}\mathbb{F}_q) = 1$ for $\deg \Pi_\gamma := [\overline{\mathbb{F}_q}(X) : \overline{\mathbb{F}_q}(\Pi_\gamma(X))]$ 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 ${\rm Supp}(v) \subseteq \gamma$ for some $\gamma \in \binom{1,\ldots,n}{d}$. That amounts to

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

and holds exactly when $a \in {\rm Etale}(\Pi_\gamma)$ for $\forall \gamma \in \binom{1,\ldots,n}{d}$.

Let $I(X, \overline{\mathbb{F}_q}) = \langle f_1, \ldots, f_m \rangle \lhd \overline{\mathbb{F}_q}[x_1, \ldots, x_n]$ for some $f_1, \ldots, f_m \in \mathbb{F}_q[x_1, \ldots, x_n]$. 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, $\mathrm{rk} \frac{\partial f}{\partial x_i}(a) = \mathrm{rk} \frac{\partial(f_1, \ldots, f_m)}{\partial(x_{i_1}, \ldots, x_{i_d})}(a) = d$ for all $i \in \binom{1, \ldots, n}{d}$. By $k = \dim X \geq n - m$ there follows $m \geq n - k \geq d$ and $\mathrm{rk} \frac{\partial f}{\partial x_i}(a) = d$ is equivalent to $\det \frac{\partial f_\gamma}{\partial x_i}(a) \neq 0$ for some $\gamma \in \binom{1, \ldots, m}{d}$. Thus,

$$\begin{aligned} X^{(\geq d+1)} = \cap_{i \in \binom{1, \ldots, n}{d}} \left[\cup_{\gamma \in \binom{1, \ldots, m}{d}} \left(X \setminus V \left(\det \frac{\partial f_\gamma}{\partial x_i} \right) \right) \right] = \\ \cap_{i \in \binom{1, \ldots, n}{d}} \left[X \setminus V \left(\det \frac{\partial f_\gamma}{\partial x_i} \ \Big| \ \gamma \in \binom{1, \ldots, m}{d} \right) \right] = \\ X \setminus \cup_{i \in \binom{1, \ldots, n}{d}} V \left(\det \frac{\partial f_\gamma}{\partial x_i} \ \Big| \ \gamma \in \binom{1, \ldots, m}{d} \right) = \\ X \setminus V \left(\prod_{i \in \binom{1, \ldots, n}{d}} \det \frac{\partial f_{\varphi(i)}}{\partial x_i} \ \Big| \ \varphi : \binom{1, \ldots, n}{d} \to \binom{1, \ldots, m}{d} \right), \end{aligned} \tag{2}$$

where $\varphi : \binom{1, \ldots, n}{d} \to \binom{1, \ldots, m}{d}$ vary over all the maps of the collection of the subsets of $\{1, \ldots, n\}$ of cardinality d in the family of the subsets of $\{1, \ldots, m\}$ of cardinality d. The last equality in (2) follows from $\cup_{i \in \binom{1, \ldots, n}{d}} V(S_i) = V \left(\prod_{i \in \binom{1, \ldots, n}{d}} S_i \right)$ for

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

(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

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

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

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

The morphism $\Pi_\gamma : X \to \Pi_\gamma(X)$ is not finite, so that $\dim \Pi_\gamma(X) < \dim X = k$. That leads to a contradiction and implies that $\ker(d\Pi_\gamma)_a \neq 0$ for $\forall a \in \Pi_\gamma^{-1}(\Pi_\gamma(X)^{\mathrm{smooth}})$. As a result, $\Pi_\gamma^{-1}(\Pi_\gamma(X)^{\mathrm{smooth}}) \subseteq X^{(\leq d)}$. According to (i), $X^{(\leq d)}$ 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

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

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

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

□

The proof of Proposition 2 (iii) 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 the puncturing $\Pi_\gamma : X \to \Pi_\gamma(X)$ is not etale 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 $X/\mathbb{F}_q \subset \overline{\mathbb{F}_q}^n$ of $\overline{\mathbb{F}_q}^k$, whose tangent codes $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ at a generic point $a \in X$ reproduce the length n, the dimension k and the minimum distance d of C.

Corollary 3. *Let C be an $\mathbb{F}_q$-linear $[n,k,d]$-code and $\sigma \in \binom{1,\dots,n}{d}$ be a 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, $X = X^{(\leq d)}$ and $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ are $[n,k,d]$-codes at all the points a of the Zariski open, Zariski dense subset $\emptyset \neq X^{(d)} = X^{(\geq d)}$ of X.

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. For any $s \in \sigma \cup \tau$ and $1 \leq i \leq n-k$ let $f_{i,s}(x_s) := H_{i,s}x_s$. In the case of $s \in \{1,\dots,n\} \setminus (\sigma\cup\tau)$ and $1 \leq i \leq n-k$ take

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

for arbitrary $r \in \mathbb{N} \setminus \{1\}$, $b_{i,s,r} \in \mathbb{F}_q$. Consider the polynomials

$$f_i(x_1,\dots,x_n) := \sum_{s=1}^n f_{i,s}(x_s) = \sum_{s=1}^n H_{i,s}x_s + \sum_{s\in\{1,\dots,n\}\setminus(\sigma\cup\tau)} \sum_{r\geq 2} b_{i,s,r}x_s^r \quad \text{for } \forall 1 \leq i \leq n-k$$

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 $\sum\limits_{s\in\sigma'\cup\tau} H_{i,s}x_s = g_i(x_\rho)$ for some $g_i(x_\rho) \in \mathbb{F}_q[x_\rho]$ and any $1 \leq i \leq n-k$. Viewing $x_{\sigma'\cup\tau}$ as a column, formed by the variables, labeled by $\sigma'\cup\tau \in \binom{1,\dots,n}{n-k}$, one can write the equations of X in the form

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

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

$$x_{\sigma'\cup\tau} = (H_{\sigma'\cup\tau})^{-1} \left(\begin{array}{c} g_1(x_\rho) \\ \dots \\ g_{n-k}(x_\rho) \end{array} \right).$$

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

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

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 $d(T_a(X, \mathbb{F}_{q^{\delta(a)}})) \leq d$ at $\forall a \in X$. In other words, $X = X^{(\leq d)}$. 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, $0^n \in X^{(d)} = X^{(\geq d)}$ is non-empty and the finite Zariski tangent space $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ to X at a generic point a 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 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 us choose a family $\mathcal{H} \to S$ 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 $L^\beta_{\mathbb{F}_q}(t)|_{\mathbb{F}_q\setminus\{\beta\}} = 0$. Straightforwardly,

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

Let us denote by

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

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

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

for $1 \leq i \leq n-k$. 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 $\overline{\mathbb{F}_q}^n$, as far as any $a = (a_1,\dots,a_n) \in \mathbb{F}_q^n$ has components $a_j = a_j^q$ and $f_i(a_1,\dots,a_n) = 0$ for $\forall 1 \leq i \leq n-k$. The partial derivatives of f_i are $\frac{\partial f_i}{\partial x_j} = \sum_{b \in \Phi_p(S)} \mathcal{H}(\Phi_p^{-1}(b))_{ij} L^{b_1}_{\mathbb{F}_q}(x_1^p) \dots L^{b_n}_{\mathbb{F}_q}(x_n^p)$ 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 $f_1,\dots,f_{n-k} \in I(X,\overline{\mathbb{F}_q}) = r(\langle f_1,\dots,f_{n-k}\rangle)$, 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 $n+1-k-d \geq 0$. One of the problems in coding theory is to obtain a linear code C' of genus $g' = g-1 \geq 0$ from the given linear code C of genus $g \geq 1$. 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 appropriate 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 5. *Let C be an $\mathbb{F}_q$-linear code of genus $g = n+1-k-d > 0$ with a parity check matrix $H = (H_1 \dots H_n) \in M_{(n-k)\times n}(\mathbb{F}_q)$. Then the image $\Pi_n(C) \subset \mathbb{F}_q^{n-1}$ of the puncturing $\Pi_n : C \to \Pi_n(C)$ is an $\mathbb{F}_q$-linear $[n-1,k,d]$-code if and only if*

$$H_n \not\in \cup_{\lambda \in \binom{1,\dots,n-1}{d-1}} \mathrm{Span}_{\mathbb{F}_q}(H_\lambda).$$

Proof. Straightforwardly, $H_n \not\in \cup_{\lambda \in \binom{1,\dots,n-1}{d-1}} \mathrm{Span}_{\mathbb{F}_q}(H_\lambda)$ if and only if C has no word $c \in C$ of weight d with $n \in \mathrm{Supp}(c)$. This holds exactly when $\Pi_n(C)$ is of minimum distance d.

The dimension $\dim_{\mathbb{F}_q} \Pi_n(C) = \dim_{\mathbb{F}_q} C = k$, as far as $\ker \Pi_n \cap C = \{(0^{n-1}, c_n) \in C\} = \{0^n\}$ whenever $H_n \neq 0^n$.

□

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

Proposition 6. *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 non-empty, Zariski open, Zariski dense subset $S \subseteq X$, such that $0^n \in X$, $T_{0^n}(X, \mathbb{F}_{q^m}) = C \otimes_{\mathbb{F}_q} \mathbb{F}_{q^m}$, the puncturing $\Pi_n : X \to \Pi_n(X)$ 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 $1 \leq j \leq n$. After an appropriate permutation of the columns of H', one can assume 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

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

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

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

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

$$f_i(x_1,\dots,x_k,x_{k+i},x_n) - \frac{c_i}{c_{n-k}} f_{n-k}(x_1,\dots,x_k,x_n) =$$

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

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

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

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 $f_{n-k}(x_1,\dots,x_k,x_n) = 0$ is equivalent to $x_k = \psi_k(x_1,\dots,x_{k-1},x_n)$ for

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

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

$$x_k - \psi_k(x_1,\dots,x_{k-1},x_n) = 0,$$

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

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

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

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 $\overline{\mathbb{F}_q}(\Pi_n(X)) = \overline{\mathbb{F}_q}(x_1 + I(X,\overline{\mathbb{F}_q}),\dots,x_{n-1} + I(X,\overline{\mathbb{F}_q}))$.

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

$$\frac{\partial f}{\partial x}(x_1,\dots,x_n) = (H'_1 \dots H'_{n-1}H_n(x_n)) = \frac{\partial f}{\partial x}(x_n) \tag{3}$$

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

$$\frac{\partial f}{\partial x_\beta}(x_n) = \begin{pmatrix} 1 & 0 & \dots & 0 & c_1x_n^p \\ 0 & 1 & \dots & 0 & c_2x_n^p \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & c_{n-k-1}x_n^p \\ 0 & 0 & \dots & 0 & 1 + c_{n-k}x_n^p \end{pmatrix}$$

with determinant det $\frac{\partial f}{\partial x_\beta}(x_n) = 1 + c_{n-k}x_n^p$. Thus, at any $a \in X \setminus V\left(c_{n-k}x_n^p + 1\right)$, the matrix $\frac{\partial f}{\partial x}(a_n) \in M_{(n-k)\times n}(\mathbb{F}_{q^{\delta(a)}})$ is of rank $\mathrm{rk}\frac{\partial f}{\partial x}(a_n) = n-k$. 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 $\frac{\partial f}{\partial x}(a)$. Since X is smooth, $\dim T_a(X, \mathbb{F}_{q^{\delta(a)}}) = \dim X = k$ at $\forall a \in X$ and $\frac{\partial f}{\partial x}(a)$ is a parity check matrix of $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ if and only if $\mathrm{rk}\frac{\partial f}{\partial x}(a) = n-k$. In particular, $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ has parity check matrix $\frac{\partial f}{\partial x}(a)$ 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 $\frac{\partial f}{\partial x}(0) = H'$ and $T_{0^n}(X, \mathbb{F}_{q^m}) = C \otimes_{\mathbb{F}_q} \mathbb{F}_{q^m}$.

Let $\Pi_n : \mathcal{C}(a) \to \Pi_n\mathcal{C}(a)$ 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 5,

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

We claim that

$$Y := X \setminus S_o = \{a \in X \,|\, H_n(a_n) \in \cup_{\lambda \in \binom{1,\dots,n-1}{d-1}} \mathrm{Span}_{\overline{\mathbb{F}_q}}(H'_\lambda)\}$$

is a proper Zariski closed subset of X. If so, then $S_o = X \setminus Y$ and

$$U_o := S_o \cap [X \setminus V(c_{n-k}x_n^p + 1)] = X \setminus [Y \cup V(c_{n-k}x_n^p + 1)]$$

are non-empty, Zariski open, Zariski dense subsets of X. By the very definition of U_o, the $\mathbb{F}_{q^{\delta(a)}}$-linear spaces $(d\Pi_n)_a T_a(X, \mathbb{F}_{q^{\delta(a)}})$ are $[n-1, k, d]$-codes at all $a \in U_o$. Towards the study of Y, let

$$Y_\lambda := \{a \in X \,|\, H_n(a_n) \in \mathrm{Span}_{\overline{\mathbb{F}_q}}(H'_\lambda)\} = \{a \in X \,|\, \mathrm{rk}(H'_\lambda H_n(a_n)) < d\}$$

for $\forall \lambda \in \binom{1,\dots,n-1}{d-1}$ and represent $Y = \cup_{\lambda \in \binom{1,\dots,n-1}{d-1}} Y_\lambda$. If

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

is the determinant of the matrix

$$\frac{\partial f_\mu}{\partial x_\lambda}(x_n) = (H'_{\mu,\lambda} H'_{\mu,n}(x_n)) = (H'_{\mu,\lambda} H'_{\mu,n} + x_n^p c_{\mu,n}) \in M_{(n-k)\times(n-k)}(\mathbb{F}_{q^m}[x_n]),$$

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

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

and therefore $Y = \cup_{\lambda \in \binom{1,\dots,n-1}{d-1}} Y_\lambda$ are Zariski closed in X. The assumption

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

for the irreducible affine variety X requires

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

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

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

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

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

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

so that $U_o \subseteq \mathrm{Etale}(\Pi_n)$ is contained in the etale locus of Π_n. Intersecting U_o with the non-empty, Zariski open subset $\Pi_n^{-1}(\Pi_n(X)^{\mathrm{smooth}}) \subseteq X$, one obtains a non-empty, Zariski open, Zariski dense subset $S := U_o \cap \Pi_n^{-1}(\Pi_n(X)^{\mathrm{smooth}}) \subseteq X$, such 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 at $\forall a \in S$, according to Lemma 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 7. *Let C be 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 $\forall (u,v) \in \mathcal{W}$, $u, v \in \overline{\mathbb{F}_q}^{n-k}$.*

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 $\forall \lambda \in \binom{1,\dots,n}{d-1}$ 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, $Z := V(Q) \cup \left(\cup_{\lambda \in \binom{1,\ldots,n}{d-1}} Z_\lambda \times \overline{\mathbb{F}_q}^{n-k} \right)$ 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 $u \not\in \cup_{\lambda \in \binom{1,\ldots,n}{d-1}} Z_\lambda = \cup_{\lambda \in \binom{1,\ldots,n}{d-1}} \mathrm{Span}_{\overline{\mathbb{F}_q}}(H_\lambda)$ and

$$u \not\in \mathcal{H}_v := \{ z \in \overline{\mathbb{F}_q}^{n-k} \mid \langle z, v \rangle = 0 \}$$

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

$$\mathcal{L}_{u,v} : \overline{\mathbb{F}_q}^{n-k} \longrightarrow \mathcal{H}_v,$$

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

which project $\overline{\mathbb{F}_q}^{n-k}$ on $\mathcal{H}_v$, parallel to $\ker \mathcal{L}_{u,v} = \mathrm{Span}_{\overline{\mathbb{F}_q}}(u)$. Let us consider the definition field $\mathbb{F}_{q^{\delta(u,v)}} = \mathbb{F}_q(u_1, \ldots, u_{n-k}, v_1, \ldots, v_{n-k})$ of $(u,v) \in \mathcal{W}$ over $\mathbb{F}_q$ and the matrix $H(u,v) := (\mathcal{L}_{u,v}(H_1) \ldots \mathcal{L}_{u,v}(H_n)) \in M_{(n-k)\times n}(\mathbb{F}_{q^{\delta(u,v)}})$. 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 $\sum\limits_{s=1}^{n} c_s H_s = 0^{n-k}$ 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 $d\mathcal{C}(u,v) \leq d$. If there is a non-zero word $a \in \mathcal{C}(u,v) \setminus \{0^n\}$ with $\mathrm{Supp}(a) \subseteq \lambda = \{\lambda_1, \ldots, \lambda_{d-1}\} \in \binom{1,\ldots,n}{d-1}$ 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 $\sum\limits_{s=1}^{d-1} a_{\lambda_s} H_{\lambda_s} = \lambda_0 u \in \ker \mathcal{L}_{u,v} = \mathrm{Span}_{\overline{\mathbb{F}_q}}(u)$. According to $u \not\in \mathrm{Span}_{\overline{\mathbb{F}_q}}(H_\lambda)$, there follow $\lambda_0 = 0$ and $\mathrm{rk} H_\lambda = \mathrm{rk}(H_{\lambda_1}, \ldots, H_{\lambda_{d-1}}) < d-1$. 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 $\forall (u,v) \in \mathcal{W}$, 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 $\forall 1 \leq s \leq n$, whereas $\mathrm{Span}_{\overline{\mathbb{F}_q}}(\mathcal{L}_{u,v}(H_1), \ldots, \mathcal{L}_{u,v}(H_n)) \subseteq \mathcal{H}_v$ and $\mathrm{rk} H(u,v) \leq \dim_{\overline{\mathbb{F}_q}} \mathcal{H}_v = n-k-1$. On the other hand, $H_s = \mathcal{L}_{u,v}(H_s) + \frac{\langle H_s, v \rangle}{\langle u, v \rangle} u$ for $\forall 1 \leq s \leq n$ imply that

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

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

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

is an absurd, justifying $\mathrm{rk} H(u,v) = n-k-1$ and $\dim \mathcal{C}(u,v) = k+1$ for $\forall (u,v) \in \mathcal{W}$.

□

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 $\geq d+1$, 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 8. *Let C be 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 $\mathcal{C}(a) \subset \mathbb{F}^n_{q^{\delta(a)}}$ 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 $\geq d+1$ at all the points $a \in U$.*

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

$$H_j := H'_j \quad \text{for} \quad 1 \leq j \leq d-1,$$

$$H_j(x_j) := H'_j + x_j c_j \quad \text{for} \quad d \leq j \leq n$$

and to obtain a polynomial matrix

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

Let $\mathbb{F}_{q^m} = \mathbb{F}_q(c_{ij} \,|\, 1 \leq i \leq n-k,\ d \leq j \leq n)$ be the common definition field of all the entries of $c_d, \ldots, c_n$ over $\mathbb{F}_q$. At any point $a \in \overline{\mathbb{F}_q}^n$, we consider the linear code $\mathcal{C}(a)$ over the definition field $\mathbb{F}_{q^{\delta(a)}} = \mathbb{F}_{q^m}(a_1, \ldots, a_n)$ of a over $\mathbb{F}_{q^m}$, which has a parity check matrix $H(a) = H(a_d, \ldots, a_n) \in M_{(n-k)\times n}(\mathbb{F}_{q^{\delta(a)}})$. Our choice of $H(x_d, \ldots, x_n)$ 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 $\geq d+1$ at all $a \in U'$ and $\mathcal{C}(b)$ are of dimension k at all $b \in U''$, in order to have a non-empty, Zariski open, Zariski dense subset $U := U' \cap U'' \subseteq \overline{\mathbb{F}_q}^n$, at which the codes $\mathcal{C}(a)$, $a \in U$ are of length n, dimension k and minimum distance $\geq d+1$.

Regardless of the choice of $c_d, \ldots, c_n \in M_{(n-k)\times 1}(\overline{\mathbb{F}_q})$, let $\gamma := \{1, \ldots, n-k\}$ and note that

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

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 $d \leq j \leq n$, 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 $\forall \beta \in \binom{1,\ldots,j}{d}$ 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 $\geq d+1$ at all $a \in U'$. To this end, let $j = d$, $\lambda := \{1, \ldots, d-1\}$ 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 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 $H_d(x_d) \not\in \mathrm{Span}_{\overline{\mathbb{F}_q}}(H'_\lambda)$ for $\forall x_d \in \overline{\mathbb{F}_q}$, 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 $M_{(n-k)\times 1}(\overline{\mathbb{F}_q})$ 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 $c_d \not\in \mathrm{Span}_{\overline{\mathbb{F}_q}}(H'_\lambda)$. That provides the base of the induction.

Suppose that $d+1 \leq j \leq n$ and $c_d, \dots, c_{j-1} \in M_{(n-k)\times 1}(\overline{\mathbb{F}_q})$ 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 $\forall \beta \in \binom{1,\dots,j-1}{d}$ and $\forall u \in U_{j-1}$. Fix an arbitrary $u \in U_{j-1}$ and choose

$$c_j \in M_{(n-k)\times 1}(\overline{\mathbb{F}_q}) \setminus \left[\cup_{\lambda \in \binom{1,\dots,j-1}{d-1}} \mathrm{Span}_{\overline{\mathbb{F}_q}}(H_\lambda(u)) \right]. \tag{4}$$

The existence of c_j is due to the fact that the finite union $\cup_{\lambda \in \binom{1,\dots,j-1}{d-1}} \mathrm{Span}_{\overline{\mathbb{F}_q}}(H_\lambda(u))$ 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 $\overline{\mathbb{F}_q}$ has non-empty complement. We claim that

$$W_{j-1} := \{ w \in U_{j-1} \,|\, c_j \not\in \cup_{\lambda \in \binom{1,\dots,j-1}{d-1}} \mathrm{Span}_{\overline{\mathbb{F}_q}}(H_\lambda(w)) \}$$

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

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

as far as $\mathrm{rk} H_\beta(u) = d$ for $\forall \beta \in \binom{1,\dots,j-1}{d}$, $\forall u \in U_{j-1}$ implies $\mathrm{rk} H_\lambda(t) = d-1$ for $\forall \lambda \in \binom{1,\dots,j-1}{d-1}$, $\forall t \in U_{j-1}$. Now,

$$\begin{aligned} U_{j-1} \setminus W_{j-1} = \cup_{\lambda \in \binom{1,\dots,j-1}{d-1}} \left\{ t \in U_{j-1} \,\middle|\, \det(H_{\mu,\lambda}(t) c_{\mu,j}) = 0, \ \ \forall \mu \in \binom{1,\dots,n-k}{d} \right\} = \\ \cup_{\lambda \in \binom{1,\dots,j-1}{d-1}} \left[U_{j-1} \cap V \left(\det(H_{\mu,\lambda} c_{\mu,j}) \,\middle|\, \forall \mu \in \binom{1,\dots,n-k}{d} \right) \right] = \\ U_{j-1} \cap V \left(\prod_{\lambda \in \binom{1,\dots,j-1}{d-1}} \det(H_{\mu(\lambda),\lambda} c_{\mu(\lambda),j}) \,\middle|\, \forall \mu : \binom{1,\dots,j-1}{d-1} \to \binom{1,\dots,n-k}{d} \right) \end{aligned}$$

is a Zariski closed subset of U_{j-1}, so that

$$\begin{aligned} W_{j-1} = \\ U_{j-1} \setminus V \left(\prod_{\lambda \in \binom{1,\dots,j-1}{d-1}} \det(H_{\mu(\lambda),\lambda} c_{\mu(\lambda),j}) \,\middle|\, \forall \mu : \binom{1,\dots,j-1}{d-1} \to \binom{1,\dots,n-k}{d} \right) \end{aligned}$$

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) of c_j, $W_{j-1} \neq \emptyset$ is non-empty and, therefore, Zariski dense in $\overline{\mathbb{F}_q}^{j-1}$. Note that

$$U_j := \left\{ (w, w_j) \in W_{j-1} \times \overline{\mathbb{F}_q} \,|\, \mathrm{rk} H_\beta(w, w_j) = d \quad \text{for} \quad \forall \beta \in \binom{1, \dots, j}{d} \right\} =$$
$$\left\{ (w, w_j) \in W_{j-1} \times \overline{\mathbb{F}_q} \,|\, \mathrm{rk}(H_\lambda(w) H_j(w_j)) = d \quad \text{for} \quad \forall \lambda \in \binom{1, \dots, j-1}{d-1} \right\}$$

has complement

$$(W_{j-1} \times \overline{\mathbb{F}_q}) \setminus U_j = \cup_{\lambda \in \binom{1,\dots,j-1}{d-1}} \left\{ (w, w_j) \in W_{j-1} \times \overline{\mathbb{F}_q} \,|\, \mathrm{rk}(H_\lambda(w) H_j(w_j)) < d \right\} =$$
$$\cup_{\lambda \in \binom{1,\dots,j-1}{d-1}} \left\{ (w, w_j) \in W_{j-1} \times \overline{\mathbb{F}_q} \,|\, h_{\mu,\lambda}(w, w_j) = 0 \quad \text{for} \quad \forall \mu \in \binom{1, \dots, n-k}{d} \right\},$$

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

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

then

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

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 $U_j = \emptyset$ 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 $\forall \lambda \in \binom{1,\dots,j-1}{d-1}$, $\forall \mu : \binom{1,\dots,j-1}{d-1} \to \binom{1,\dots,n-k}{d}$. That, in turn, is equivalent to $\det(H_{\mu,\lambda}(x_d, \dots, x_{j-1}) c_{\mu j}) = 0$ for $\forall \mu \in \binom{1,\dots,n-k}{d}$, $\forall \lambda \in \binom{1,\dots,j-1}{d-1}$ and specializes to $\det(H_{\mu,\lambda}(u) c_{\mu j}) = 0$ at the point $u \in U_{j-1}$, used in the choice (4) of c_j. As a result, $\mathrm{rk}(H_\lambda(u) c_j) < d$ for $\forall \lambda \in \binom{1,\dots,j-1}{d-1}$. The inductive hypothesis $\mathrm{rk} H_\beta(u) = d$ for $\forall \beta \in \binom{1,\dots,j-1}{d}$ requires $\mathrm{rk} H_\lambda(u) = d - 1$ for $\forall \lambda \in \binom{1,\dots,j-1}{d-1}$ and $\mathrm{rk}(H_\lambda(u) c_j) < d$ is equivalent to $c_j \in \mathrm{Span}_{\overline{\mathbb{F}_q}}(H_\lambda(u))$ for $\forall \lambda \in \binom{1,\dots,j-1}{d-1}$. That contradicts the choice (4) of c_j and shows that $U_j \neq \emptyset$ is Zariski dense in $\overline{\mathbb{F}_q}^j$.

□

5 Simultaneous decoding of tangent codes with fixed error support. Gradient codes.

5.1 The decoding morphism of the bundle of the received words in the bundle of the tangent codes

An important problem in the theory of error correcting codes is the decoding with fixed error support $j \in \binom{1,\ldots,n}{t}$. The hard part of the aforementioned procedure is the description of the space of the received words with error support j. The present section discusses a simultaneous decoding of tangent codes with fixed error support j. In general, the proposed algorithm requires the construction of a Groebner basis and has exponential growth. However, for certain classes of twisted embeddings $\overline{\mathbb{F}_q}^k \simeq X/\mathbb{F}_q \subset \overline{\mathbb{F}_q}^n$, the parity check matrices of the spaces $\mathrm{Err}(T_a(X, \mathbb{F}_{q^{\delta(a)}}), j)$ of the received words with $T_a(X, \mathbb{F}_{q^{\delta(a)}})$-error support j are obtained from the parity check matrices of $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ by erasing t rows and t columns (cf.Corollary 14).

Definition 9. *Let C be an $\mathbb{F}_q$-linear $[n,k,d]$-code and $j \in \binom{1,\ldots,n}{t}$ for some $1 \leq t \leq d-1$. We say that C has unique decoding with error support j if for any $w \in \mathbb{F}_q^n$ there exists at most one $e \in \mathbb{F}_q^n$ with support* $\mathrm{Supp}(e) \subseteq j$ *and $w - e \in C$.*

Recall that a code C has unique decoding with error weight t if for any $w \in \mathbb{F}_q^n$ there exists at most one word $e \in \mathbb{F}_q^n$ of weight $\mathrm{wt}(e) \leq t$ with $w - e \in C$. For any $a = (a_1, \ldots, a_n) \in \mathbb{F}_q^n$ and $j \in \binom{1,\ldots,n}{t}$ let us denote by $a^{(j)} := (a_{j_1}, \ldots, a_{j_t}) \in \mathbb{F}_q^t$, respectively, by $a^{(\neg j)} \in \mathbb{F}_q^{n-t}$ the collection of the components of a, labeled by j, respectively, by $\neg j = \{1, \ldots, n\} \setminus j$ and express $a = (a^{(j)}, a^{(\neg j)})$. If $H \in M_{m \times n}(\mathbb{F}_q)$ is a parity check matrix of C and $i \subseteq \{1, \ldots, m\}$, $j \subseteq \{1, \ldots, n\}$ then put $H(i,j) \in M_{|i| \times |j|}(\mathbb{F}_q)$ for the matrix, formed by the entries $H_{\alpha,\beta}$ of H with $\alpha \in i$ and $\beta \in j$. Let

$$\mathrm{Err}(C, j) := \{w \in \mathbb{F}_q^n \,|\, \exists e \in \mathbb{F}_q^n, \ \ \mathrm{Supp}(e) \subseteq j, \ \ w - e \in C\}$$

be the set of the received words, whose C-error is supported by $j \in \binom{1,\ldots,n}{t}$. The next lemma comprises some trivial observations from coding theory, which are used for decoding tangent codes with fixed error support $j \in \binom{1,\ldots,n}{t}$. It can be useful when the probability for the occurrence of a specific error support $j \in \binom{1,\ldots,n}{t}$ is considerably larger than the one for any other $i \in \binom{1,\ldots,n}{t} \setminus \{j\}$.

Lemma 10. *If C is an $\mathbb{F}_q$-linear $[n,k,d]$-code with parity check matrix $H \in M_{m \times n}(\mathbb{F}_q)$ then for any $j \in \binom{1,\ldots,n}{t}$ with $t \leq d-1$ there exists $i \in \binom{1,\ldots,m}{t}$ with $\det H(i,j) \neq 0$. Denoting*

$$M(i,j) := -H(i,j)^{-1} H(i, \neg j) \in M_{t \times (n-t)}(\mathbb{F}_q),$$

$$N(i,j) := H(\neg i, j) M(i,j) + H(\neg i, \neg j) \in M_{(m-t) \times (n-t)}(\mathbb{F}_q),$$

one expresses

$$C = \{(M(i,j)c^{(\neg j)}, c^{(\neg j)}) \in \mathbb{F}_q^t \times \mathbb{F}_q^{n-t} \,|\, N(i,j)c^{(\neg j)} = 0\}, \tag{5}$$

$$\mathrm{Err}(C, j) = \{(w^{(j)}, w^{(\neg j)}) \in \mathbb{F}_q^t \times \mathbb{F}_q^{n-t} \,|\, N(i,j)w^{(\neg j)} = 0\} \tag{6}$$

and obtains an $\mathbb{F}_q$-linear decoding map

$$\mathrm{Dec}^{(j)} : \mathrm{Err}(C,j) \longrightarrow C,$$

$$\mathrm{Dec}^{(j)}(w) = \mathrm{Dec}^{(j)}(w^{(j)}, w^{(\neg j)}) = (M(i,j)w^{(\neg j)}, w^{(\neg j)})$$

with $\mathrm{Supp}(w - \mathrm{Dec}^{(j)}(w)) \subseteq j$ *for* $\forall w \in \mathrm{Err}(C,j)$.

For any $j \in \binom{1,\dots,n}{t}$ *the code* C *has unique decoding with error support* j.

If $q > 2$ *then* C *has unique decoding with error weight* t *if and only if* $d \geq 2t+1$.

Proof. The columns $H_j \in M_{m\times t}(\mathbb{F}_q)$ of H, labeled by $j \in \binom{1,\dots,n}{t}$ with $t < d$ are of $\mathrm{rk}(H_j) = t$, so that there exists $i \in \binom{1,\dots,m}{t}$ with $\det H(i,j) \neq 0$. The left multiplication of

$$H \begin{pmatrix} c^{(j)} \\ c^{(\neg j)} \end{pmatrix} = \begin{pmatrix} H(i,j) & H(i,\neg j) \\ H(\neg i,j) & H(\neg i,\neg j) \end{pmatrix} \begin{pmatrix} c^{(j)} \\ c^{(\neg j)} \end{pmatrix} = 0_{m\times 1}$$

by the matrix

$$\begin{pmatrix} H(i,j)^{-1} & 0_{t\times(m-t)} \\ -H(\neg i,j)H(i,j)^{-1} & I_{m-t} \end{pmatrix} \in M_{m\times m}(\mathbb{F}_q)$$

provides (5) and $\Pi_j(C) = \{c^{(\neg j)} \in \mathbb{F}_q^{n-t} \mid N(i,j)c^{(\neg j)} = 0\}$. Moreover, the puncturing $\Pi_j : C \to \Pi_j(C)$ is an $\mathbb{F}_q$-linear isomorphism with inverse

$$\Pi_j^{-1}|_{\Pi_j(C)} : \Pi_j(C) \longrightarrow C,$$

$$\Pi_j^{-1}(c^{(\neg j)}) = (M(i,j)c^{(\neg j)}, c^{(\neg j)}) \quad \text{for} \quad \forall c^{(\neg j)} \in \Pi_j(C).$$

Straightforward verification establishes that the space

$$\mathrm{Err}(C,j) = \{(w^{(j)}, c^{(\neg j)}) \in \mathbb{F}_q^t \times \mathbb{F}_q^{n-t} \mid N(i,j)c^{(\neg j)} = 0\} = \Pi_j^{-1}(\Pi_j(C))$$

of the received words, whose C-error is supported by j coincides with the complete preimage of $\Pi_j(C)$ in $\mathbb{F}_q^n$ under Π_j. The composition

$$\mathrm{Dec}^{(j)} = \Pi_j^{-1}|_{\Pi_j(C)}\Pi_j : \mathrm{Err}(C,j) \longrightarrow C,$$

$$\mathrm{Dec}^{(j)}(w^{(j)}, w^{(\neg j)}) = \Pi_j^{-1}(w^{(\neg j)}) = (M(i,j)w^{(\neg j)}, w^{(\neg j)})$$

is a correctly defined $\mathbb{F}_q$-linear decoding map.

In order to show that C has unique decoding with error support $j \in \binom{1,\dots,n}{t}$, suppose that there exists $w \in \mathbb{F}_q^n$ with $w = c + e = \widetilde{c} + \widetilde{e}$ for some $c, \widetilde{c} \in C$ and $e, \widetilde{e} \in \mathbb{F}_q^n$ with $\mathrm{Supp}(e) \subseteq j$, $\mathrm{Supp}(\widetilde{e}) \subseteq j$. Then the word $\widetilde{e} - e = c - \widetilde{c} \in C$ has support $\mathrm{Supp}(c - \widetilde{c}) = \mathrm{Supp}(\widetilde{e} - e) \subseteq j$ of cardinality $|j| = t < d$, which requires $c = \widetilde{c}$ and shows that the decoding with error support j is unique for all $j \in \binom{1,\dots,n}{t}$ with $t \leq d-1$.

It is well known that if $d \geq 2t+1$ then C has unique decoding with error weight t. In order to show that for $t+1 \leq d \leq 2t$ the decoding of C with error weight t is not unique, let us fix a word $c \in C$ with $\mathrm{Supp}(c) = i = \{i_1, \dots, i_d\} \in \binom{1,\dots,n}{d}$ and note that $d - t \leq t < d$. Then the choice of

$$e_{i_s} := c_{i_s}, \quad \widetilde{e_{i_s}} := 0 \quad \text{for} \quad \forall 1 \leq s \leq d-t,$$

$$\widetilde{e_{i_s}} \in \mathbb{F}_q^* \setminus \{-c_{i_s}\}, \quad e_{i_s} := \widetilde{e_{i_s}} + c_{i_s} \quad \text{for} \quad d-t+1 \leq s \leq t,$$

$$e_{i_s} := 0, \quad \widetilde{e_{i_s}} := -c_{i_s} \quad \text{for} \quad t+1 \leq s \leq d \quad \text{and}$$

$$e_r = \widetilde{e_r} := 0 \quad \text{for} \quad r \not\in i$$

supplies a received word $e = \widetilde{e} + c$ with $\mathrm{Supp}(e) = \{i_1, \ldots, i_t\}$, $\mathrm{Supp}(\widetilde{e}) = \{i_{d-t+1}, \ldots, i_d\} \in \binom{1,\ldots,n}{t}$, which is decoded by 0^n and $c \neq 0^n$ with error weight t.

□

Note that the decoding map $\mathrm{Dec}^{(j)} : \mathrm{Err}(C, j) \rightarrow C$ has $\mathbb{F}_q$-linear extension $\mathrm{Dec}^{(j)} : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$, but its values over $\mathbb{F}_q^n \setminus \mathrm{Err}(C, j)$ are not supposed to belong to C.

Definition 11. *Let $X/\mathbb{F}_q \subset \overline{\mathbb{F}_q}^n$ be an irreducible affine variety, defined over $\mathbb{F}_q$.*

(i) The fibration

$$\pi : T^C X := \coprod_{a \in X} T_a(X, \mathbb{F}_{q^{\delta(a)}}) \longrightarrow X$$

with $\pi^{-1}(a) = T_a(X, \mathbb{F}_{q^{\delta(a)}})$ for $\forall a \in X$ is called the bundle of the tangent codes to X.

(ii) If

$$\mathrm{Err}(T_a(X, \mathbb{F}_{q^{\delta(a)}}), j) := \{w \in \mathbb{F}_{q^{\delta(a)}}^n \,|\, \exists e \in \mathbb{F}_{q^{\delta(a)}}^n, \quad \mathrm{Supp}(e) \subseteq j, \quad w - e \in T_a(X, \mathbb{F}_{q^{\delta(a)}})\}$$

is the $\mathbb{F}_{q^{\delta(a)}}$-linear space of the received words, whose $T_a(X, \mathbb{F}_{q^{\delta(a)}})$-error is supported by $j \in \binom{1,\ldots,n}{t}$ then

$$\pi_E : \mathrm{Err}(T^C X, j) := \coprod_{a \in X} \mathrm{Err}(T_a(X, \mathbb{F}_{q^{\delta(a)}}), j) \longrightarrow X$$

with $\pi_E^{-1}(a) = \mathrm{Err}(T_a(X, \mathbb{F}_{q^{\delta(a)}}), j)$ for $\forall a \in X$ is the bundle of the received words, whose $T^C X$-error is supported by j.

(iii) For an arbitrary subset $S \subseteq X$, a bundle morphism $\Psi : \mathrm{Err}(T^C X, j)|_S \rightarrow T^C X|_S$ of the corresponding restrictions is a map, which closes the commutative diagram

$$\begin{tikzcd}
\mathrm{Err}(T^C X, j)|_S \arrow[r, "\Psi"] \arrow[d, "\pi_E"'] & T^C X|_S \arrow[dl, "\pi"] \\
S &
\end{tikzcd}$$

and has $\mathbb{F}_{q^{\delta(a)}}$-linear restrictions

$$\Psi : \mathrm{Err}(T_a(X, \mathbb{F}_{q^{\delta(a)}}), j) \longrightarrow T_a(X, \mathbb{F}_{q^{\delta}(a)}) \quad \textit{for} \quad \forall a \in S.$$

We use the term bundle of the tangent codes for $T^C X := \coprod_{a \in X} T_a(X, \mathbb{F}_{q^{\delta(a)}})$ since the notion of a tangent bundle of X is coined in the literature for $TX := \coprod_{a \in X} T_a(X, \overline{\mathbb{F}_q})$.

The next proposition observes that the decoding maps of the tangent codes with fixed error support $j \in \binom{1,\ldots,n}{t}$ form a bundle morphism and identifies the bundle $\mathrm{Err}(T^C X, j)$ of the received words with $T^C X$-error supported by j with the bundle of the tangent codes of an appropriate affine variety $Y_j \subseteq \overline{\mathbb{F}_q}^n$. The hard part of the decoding procedure is the description of $\mathrm{Err}(T^C X, j)$. The proof of Proposition 12 makes use of a Groebner basis, in order to justify the coincidence of bundles $T^C Y_j|_{U_j} = \mathrm{Err}(T^C X, j)|_{U_j}$ over a Zariski open, Zariski dense subset $U_j \subseteq X^{\mathrm{smooth}} \cap Y_j^{\mathrm{smooth}}$. Bearing in mind the high complexity of the construction of a Groebner basis, one concludes that the tangent codes set up itself is useless for decoding problems, in general. Applications are possible only over specific affine varieties X, for which the description of Y_j is immediate. Corollary 14 illustrates the possibility for such a choice of equations of X, for which the polynomial parity check matrix of the bundle $T^C Y_j|_{U_j} = \mathrm{Err}(T^C X, j)|_{U_j}$ is obtained from the one for $T^C X|_{U_j}$ by deleting t rows and t columns,

Proposition 12. *Let $X/\mathbb{F}_q \subset \overline{\mathbb{F}_q}^n$ be an irreducible affine variety, defined over $\mathbb{F}_q$ with non-empty subset $X^{(\geq t+1)} = \{a \in X \,|\, d(T_a(X, \mathbb{F}_{q^{\delta(a)}})) \geq t+1\}$ and some generators $f_1, \ldots, f_m \in \mathbb{F}_q[x_1, \ldots, x_n]$ of $I(X, \overline{\mathbb{F}_q}) = \langle f_1 \ldots, f_m \rangle \triangleleft \overline{\mathbb{F}_q}[x_1, \ldots, x_n]$.*

(i) For any $j \in \binom{1,\ldots,n}{t}$ there exist a Zariski open covering $X^{(\geq t+1)} = \cup_{i \in \binom{1,\ldots,m}{t}} X(i,j)$ by $X(i,j) := X^{(\geq t+1)} \setminus V\left(\det \frac{\partial f_i}{\partial x_j}\right)$ and bundle morphisms

$$\mathrm{Dec}^{(i,j)} : \mathrm{Err}(T^C X, j)|_{X(i,j)} \longrightarrow T^C X|_{X(i,j)},$$

$$\mathrm{Dec}^{(i,j)}(w) = \left(- \left(\frac{\partial f_i}{\partial x_j}(\pi_E(w)) \right)^{-1} \frac{\partial f_i}{\partial x_{\neg j}}(\pi_E(w)) w^{(\neg j)}, w^{(\neg j)} \right) \quad \textit{for} \quad \forall i \in \binom{1, \ldots, m}{t},$$

which decode simultaneously the received words with $T^C X$-error supported by j.

(ii) For any $j \in \binom{1,\ldots,n}{t}$ with $\neg j = \{1, \ldots, n\} \setminus j$ let $\Pi_j : \overline{\mathbb{F}_q}^n \to \overline{\mathbb{F}_q}^{n-t}$ be the puncturing at j and $\overline{\Pi_j(X)}$ be the Zariski closure of $\Pi_j(X)$ in $\overline{\mathbb{F}_q}^{n-t}$. Then the cylinder

$$Y_j := \Pi_j^{-1}(\overline{\Pi_j(X)}) \simeq \overline{\mathbb{F}_q}^t \times \overline{\Pi_j(X)}$$

with base $\overline{\Pi_j(X)}$ in $\overline{\mathbb{F}_q}^n$ is an irreducible $(k+t)$-dimensional affine variety, containing X,

$$U_j := X^{(\geq t+1)} \cap \Pi_j^{-1}(\Pi_j(X)^{\mathrm{smooth}}) \subseteq X^{\mathrm{smooth}} \cap Y_j^{\mathrm{smooth}}$$

is a non-empty, Zariski open, Zariski dense subset of X and the bundles

$$T^C Y_j|_{U_j} = T^C \overline{\mathbb{F}_q}^t \times T^C \overline{\Pi_j(X)}|_{U_j} = \mathrm{Err}(T^C X, j)|_{U_j}$$

coincide over U_j. In particular, $\dim_{\mathbb{F}_{q^{\delta(a)}}} \mathrm{Err}(T_a(X, \mathbb{F}_{q^{\delta(a)}}), j) = k + t$ for $\forall a \in U_j$.

Proof. (i) By (2) from the proof of Proposition 2 (i),

$$X^{(\geq t+1)} = \cap_{j \in \binom{1,\ldots,n}{t}} \left[\cup_{i \in \binom{1,\ldots,m}{t}} \left(X \setminus V\left(\det \frac{\partial f_i}{\partial x_j} \right) \right) \right] \subseteq$$
$$\cup_{i \in \binom{1,\ldots,m}{t}} \left(X \setminus V\left(\det \frac{\partial f_i}{\partial x_j} \right) \right) \quad \text{for} \quad \forall j \in \binom{1, \ldots, n}{t}.$$

Therefore

$$X^{(\geq t+1)} \subseteq \cup_{i \in \binom{1,\dots,m}{t}} \left(X^{(\geq t+1)} \setminus V \left(\det \frac{\partial f_i}{\partial x_j} \right) \right) = \cup_{i \in \binom{1,\dots,m}{t}} X(i,j) \subseteq X^{(\geq t+1)}$$

and the Zariski open subset $X^{(\geq t+1)} = \cup_{i \in \binom{1,\dots,m}{t}} X(i,j)$ of X is covered by the Zariski open subsets $X(i,j) \subseteq X$. At any $a \in X(i,j)$ the tangent code $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ has a parity check matrix $\frac{\partial f}{\partial x}(a)$ with $\det \frac{\partial f_i}{\partial x_j}(a) \neq 0$. The application of Lemma 10 yields $\mathbb{F}_{q^{\delta(a)}}$-linear decoding maps

$$\mathrm{Dec}^{(i,j)} : \mathrm{Err}(T_a(X, \mathbb{F}_{q^{\delta(a)}}), j) \longrightarrow T_a(X, \mathbb{F}_{q^{\delta(a)}}),$$

$$\mathrm{Dec}^{(i,j)}(w^{(j)}, w^{(\neg j)}) = \left(- \left(\frac{\partial f_i}{\partial x_j}(a) \right)^{-1} \frac{\partial f_i}{\partial x_{\neg j}}(a) w^{(\neg j)}, w^{(\neg j)} \right)$$

with error support j for $\forall a \in X(i,j)$.

(ii) By its very definition,

$$Y_j := \Pi_j^{-1}(\overline{\Pi_j(X)}) = \{ a = (a^{(j)}, a^{(\neg j)}) \in \overline{\mathbb{F}_q}^n \,|\, \Pi_j(a) = a^{(\neg j)} \in \overline{\Pi_j(X)} \} \simeq \overline{\mathbb{F}_q}^t \times \overline{\Pi_j(X)}$$

is isomorphic to the product of the affine space $\overline{\mathbb{F}_q}^t$ with $\overline{\Pi_j(X)} \subseteq \overline{\mathbb{F}_q}^{n-t}$ and that is why we say that Y_j is the cylinder with base $\overline{\Pi_j(X)}$ in $\overline{\mathbb{F}_q}^n$. Let $I^{(\neg j)} := I(X, \overline{\mathbb{F}_q}) \cap \overline{\mathbb{F}_q}[x_{\neg j}] \triangleleft \overline{\mathbb{F}_q}[x_{\neg j}]$ be the j-th elimination ideal of $I(X, \overline{\mathbb{F}_q})$ and

$$V^{(\neg j)}(I^{(\neg j)}) := \{ a^{(\neg j)} \in \overline{\mathbb{F}_q}^{n-t} \,|\, g(a^{(\neg j)}) = 0 \quad \text{for} \quad \forall g \in I^{(\neg j)} \}$$

be the affine variety of $I^{(\neg j)}$ in $\overline{\mathbb{F}_q}^{n-t}$. The Closure Theorem 3 from Chapter 3, §2 of [3] asserts that $\overline{\Pi_j(X)} = V^{(\neg j)}(I^{(\neg j)})$ and justifies

$$Y_j = V(I^{(\neg j)}) = \{ a = (a^{(j)}, a^{(\neg j)}) \in \overline{\mathbb{F}_q}^n \quad | \quad g(a^{(\neg j)}) = 0 \quad \text{for} \quad \forall g \in I^{(\neg j)} \}. \tag{7}$$

In particular, $I^{(\neg j)} \otimes_{\overline{\mathbb{F}_q}} \overline{\mathbb{F}_q}[x_j] \subseteq I(Y_j, \overline{\mathbb{F}_q}) \triangleleft \overline{\mathbb{F}_q}[x_1, \dots, x_n]$.

By Hilbert's Nullstellensatz, $IV^{(\neg j)}(I^{(\neg j)}) = r(I^{(\neg j)}) \triangleleft \overline{\mathbb{F}_q}[x_{\neg j}]$ for the radical $r(I^{(\neg j)})$ of $I^{(\neg j)}$ in $\overline{\mathbb{F}_q}[x_{\neg j}]$. We claim that $r(I^{(\neg j)}) = I^{(\neg j)}$ and $I^{(\neg j)}$ is a prime ideal of $\overline{\mathbb{F}_q}[x_{\neg j}]$. Indeed, if $f^N \in I^{(\neg j)} := I(X, \overline{\mathbb{F}_q}) \cap \overline{\mathbb{F}_q}[x_{\neg j}]$ for some $f \in \overline{\mathbb{F}_q}[x_{\neg j}]$ and $N \in \mathbb{N}$ then $f^N \in I(X, \overline{\mathbb{F}_q})$. The absolute ideal $I(X, \overline{\mathbb{F}_q}) \triangleleft \overline{\mathbb{F}_q}[x_1, \dots, x_n]$ of the irreducible variety $X \subset \overline{\mathbb{F}_q}^n$ is prime, so that $f \in I(X, \overline{\mathbb{F}_q}) \cap \overline{\mathbb{F}_q}[x_{\neg j}] = I^{(\neg j)}$ and $r(I^{(\neg j)}) = I^{(\neg j)}$ is a radical ideal. If $fg \in I^{(\neg j)} \subseteq I(X, \overline{\mathbb{F}_q})$ for some $f, g \in \overline{\mathbb{F}_q}[x_{\neg j}]$ then $f \in I(X, \overline{\mathbb{F}_q}) \cap \overline{\mathbb{F}_q}[x_{\neg j}] = I^{(\neg j)}$ or $g \in I(X, \overline{\mathbb{F}_q}) \cap \overline{\mathbb{F}_q}[x_{\neg j}] = I^{(\neg j)}$ and $I^{(\neg j)} \triangleleft \overline{\mathbb{F}_q}[x_{\neg j}]$ is a prime ideal. As a result, the variety $\overline{\Pi_j(X)} = V^{(\neg j)}(I^{(\neg j)})$ with absolute ideal $I(\overline{\Pi_j(X)}, \overline{\mathbb{F}_q}) = I^{(\neg j)}$ is irreducible, as well as its product $\overline{\mathbb{F}_q}^t \times \overline{\Pi_j(X)} \simeq Y_j$ with the affine space $\overline{\mathbb{F}_q}^t$.

In order to relate the bundles $T^C Y_j$ and $\mathrm{Err}(T^C X, j)$, note that $\Pi_j : X \to \Pi_j(X)$ are finite morphisms for $\forall j \in \binom{1,\dots,n}{t}$, according to Proposition 2 (ii) and $X^{(\geq t+1)} \neq \emptyset$. Therefore $\dim \overline{\Pi_j(X)} = \dim \Pi_j(X) = \dim X = k$, $\dim Y_j = \dim \overline{\Pi_j(X)} + t = k + t$. Observe that $I^{(\neg j)} := \langle f_1, \dots, f_m \rangle_{\overline{\mathbb{F}_q}} \cap \overline{\mathbb{F}_q}[x_{\neg j}]$ admits a generating set $g_1, \dots, g_l \in \mathbb{F}_q[x_1, \dots, x_n]$ with coefficients from $\mathbb{F}_q$. In order to obtain such $g_1, \dots, g_l$, one can apply Buchberger's algorithm to the generating set $f_1, \dots, f_m \in \mathbb{F}_q[x_1, \dots, x_n]$ of $I(X, \overline{\mathbb{F}_q}) \triangleleft \overline{\mathbb{F}_q}[x_1, \dots, x_n]$ and to construct a Groebner basis $f_1, \dots, f_m, f_{m+1}, \dots, f_s \in \mathbb{F}_q[x_1, \dots, x_n]$ of $I(X, \overline{\mathbb{F}_q})$ with respect to a lexicographic order with $x_j > x_{\neg j}$. By Elimination Theorem 2 from Chapter 3, § 1 of [3], $g := \{f_1, \dots, f_s\} \cap \mathbb{F}_q[x_{\neg j}]$ is a Groebner basis of $I^{(\neg j)} = I(X, \overline{\mathbb{F}_q}) \cap \overline{\mathbb{F}_q}[x_{\neg j}]$ with respect to the induced lexicographic order. In particular, $g = \{g_1, \dots, g_l\} \subset \mathbb{F}_q[x_1, \dots, x_n]$ is a generating set of $I^{(\neg j)} = I(\overline{\Pi_j(X)}, \overline{\mathbb{F}_q}) \triangleleft \overline{\mathbb{F}_q}[x_{\neg j}]$ with coefficients from $\mathbb{F}_q$ and the Zariski tangent spaces $T_b(\overline{\Pi_j(X)}, \mathbb{F}_{q^{\delta(a)}}) \subset \mathbb{F}_{q^{\delta(a)}}^{n-t}$ to $\overline{\Pi_j(X)}$ have parity check matrices $\frac{\partial g}{\partial x_{\neg j}}(b)$. According to $I^{(\neg j)} = \langle g_1, \dots, g_l \rangle \subset I(Y_j, \overline{\mathbb{F}_q})$, the Zariski tangent spaces $T_a(Y_j, \mathbb{F}_{q^{\delta(a)}})$ to Y_j are contained in the $\mathbb{F}_{q^{\delta(a)}}$-linear codes of length n with parity check matrix $\frac{\partial g}{\partial x_{\neg j}}(a^{(\neg j)})$. On the other hand, $\frac{\partial g}{\partial x_{\neg j}}(a^{(\neg j)})$ are parity check matrices of $T_{\Pi_j(a)}(\overline{\Pi_j(X)}, \mathbb{F}_{q^{\delta(a)}}) \subset \mathbb{F}_{q^{\delta(a)}}^{n-t}$ for $\forall \Pi_j(a) \in \overline{\Pi_j(X)}$. Thus, at any $a \in \Pi_j^{-1}(\overline{\Pi_j(X)}^{\text{smooth}})$ one has

$$t + k = \dim Y_j \leq \dim T_a(Y_j, \mathbb{F}_{q^{\delta(a)}}) \leq n - \text{rk}\frac{\partial g}{\partial x_{\neg j}}(a^{(\neg j)}) =$$

$$n - [n - t - \dim T_{\Pi_j(a)}(\overline{\Pi_j(X)}, \mathbb{F}_{q^{\delta(a)}})] = t + \dim \overline{\Pi_j(X)} = t + k,$$

whereas $\Pi_j^{-1}(\overline{\Pi_j(X)}^{\text{smooth}}) \subseteq Y_j^{\text{smooth}}$ and

$$T_a(Y_j, \mathbb{F}_{q^{\delta(a)}}) = \{(w^{(j)}, w^{(\neg j)}) \in \mathbb{F}_{q^{\delta(a)}}^t \times \mathbb{F}_{q^{\delta(a)}}^{n-t} \,\Big|\, \frac{\partial g}{\partial x_{\neg j}}(a^{(\neg j)}) w^{(\neg j)} = 0\} =$$

$$T_{a^{(j)}}(\overline{\mathbb{F}_q}^t, \mathbb{F}_{q^{\delta(a)}}) \times T_{\Pi_j(a)}(\overline{\Pi_j(X)}, \mathbb{F}_{q^{\delta(a)}})$$

at all the points a of the non-empty, Zariski open, Zariski dense subset

$$U_j := X^{(\geq t+1)} \cap \Pi_j^{-1}(\Pi_j(X)^{\text{smooth}}) \subseteq \Pi_j^{-1}(\Pi_j(X)^{\text{smooth}}) \subseteq \Pi_j^{-1}(\overline{\Pi_j(X)}^{\text{smooth}})$$

of X. Any $a \in U_j \subseteq X^{(\geq t+1)}$ is contained in some

$$X(i,j) := X^{(\geq t+1)} \setminus V\left(\det \frac{\partial f_i}{\partial x_j}\right) \subseteq X \setminus V\left(\det \frac{\partial f_\delta}{\partial x_j} \,\Big|\, \delta \in \binom{1, \dots, m}{t}\right) = \text{Etale}(\Pi_j)$$

by (i) and Lemma 1 (i). Therefore $\emptyset \neq U_j \subseteq \text{Etale}(\Pi_j) \cap \Pi_j^{-1}(\Pi_j(X)^{\text{smooth}})$, so that Lemma 1 (ii) applies to provide $U_j \subseteq \text{Etale}(\Pi_j) \cap \Pi_j^{-1}(\Pi_j(X)^{\text{smooth}}) \subseteq X^{\text{smooth}}$ and the invertibility of the $\mathbb{F}_{q^{\delta(a)}}$-linear maps

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

at $\forall a \in U_j$. Note that at an arbitrary point $a \in X(i,j)$ the inverse map is

$$\Pi_j^{-1} : T_{\Pi_j(a)}(\overline{\Pi_j(X)}, \mathbb{F}_{q^{\delta(a)}}) \longrightarrow T_a(X, \mathbb{F}_{q^{\delta(a)}}),$$

$$\Pi_j^{-1}(v^{(\neg j)}) = \left(- \left(\frac{\partial f_i}{\partial x_j}(a) \right)^{-1} \frac{\partial f_i}{\partial x_{\neg j}}(a) v^{(\neg j)}, v^{(\neg j)} \right)$$

for all $v^{(\neg j)} \in T_{\Pi_j(a)}(\overline{\Pi_j(X)}, \mathbb{F}_{q^{\delta(a)}}) = \{v^{(\neg j)} \in \mathbb{F}^{n-t}_{q^{\delta(a)}} \mid \frac{\partial g}{\partial x_{\neg j}}(a^{(\neg j)})v^{(\neg j)} = 0\}$. Thus,

$$H = \begin{pmatrix} \frac{\partial f_i}{\partial x_j}(a) & \frac{\partial f_i}{\partial x_{\neg j}}(a) \\ & \\ 0 & \frac{\partial g}{\partial x_{\neg j}}(a) \end{pmatrix} \in M_{(t+l)\times n}(\mathbb{F}_{q^{\delta(a)}})$$

is a parity check matrix of $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ with $\det H(i,j) = \det \frac{\partial f_i}{\partial x_j}(a) \neq 0$ and the application of Lemma 10 to H yields

$$\mathrm{Err}(T_a(X, \mathbb{F}_{q^{\delta(a)}}), j) =$$

$$\left\{ (w^{(j)}, w^{(\neg j)}) \in \mathbb{F}^t_{q^{\delta(a)}} \times \mathbb{F}^{n-t}_{q^{\delta(a)}} \,\middle|\, \frac{\partial g}{\partial x_{\neg j}}(a^{(\neg j)})w^{(\neg j)} = 0 \right\} = T_a(Y_j, \mathbb{F}_{q^{\delta(a)}})$$

at $\forall a \in X(i,j)$. The decoding maps $\mathrm{Dec}^{(i,j)} = \pi_j^{-1}|_{T_{\Pi_j(a)}(\Pi_j(X), \mathbb{F}_{q^{\delta(a)}})}\Pi_j$ from the proof of 10 take values in $T^C X$ at all the points $a \in X(i,j)$.

□

5.2 The bundle of the received words

As an immediate consequence of the proof of Proposition 12, we obtain the following

Corollary 13. *Let $X \subset \overline{\mathbb{F}_q}^n$ be an irreducible affine variety with $X^{(\geq t+1)} \neq \emptyset$ and*

$$I(X, \overline{\mathbb{F}_q}) = \langle f_1, \ldots, f_m \rangle \lhd \overline{\mathbb{F}_q}[x_1, \ldots, x_n] \quad \text{for some} \quad f_1, \ldots, f_m \in \mathbb{F}_q[x_1, \ldots, x_n].$$

Suppose that $f_1, \ldots, f_m, f_{m+1}, \ldots, f_s \in \mathbb{F}_q[x_1, \ldots, x_n]$ is a Groebner basis of $I(X, \overline{\mathbb{F}_q})$ with respect to a lexicographic order with $x_j > x_{\neg j}$ for some $j \in \binom{1,\ldots,n}{t}$ and put $g = \{g_1, \ldots, g_l\} = \{f_1, \ldots, f_m, f_{m+1}, \ldots, f_s\} \cap \mathbb{F}_q[x_{\neg j}]$. Then for any $a \in X(i,j) = X^{(\geq t+1)} \setminus V\left(\det \frac{\partial f_i}{\partial x_j}\right)$ with $i \in \binom{1,\ldots,s}{t}$ the space of the received words with $T_a(X, \mathbb{F}_{q^{\delta(a)}})$-error supported by j is

$$\mathrm{Err}(T_a(X, \mathbb{F}_{q^{\delta(a)}}), j) = \{(w^{(j)}, w^{(\neg j)}) \in \mathbb{F}^t_{q^{\delta(a)}} \times \mathbb{F}^{n-t}_{q^{\delta(a)}} \mid \frac{\partial g}{\partial x_{\neg j}}(a^{(\neg j)})w^{(\neg j)} = 0\}$$

and the decoding morphism of bundles

$$\mathrm{Dec}^{(i,j)} : \mathrm{Err}(T^C X, j)|_{X(i,j)} \longrightarrow T^C X|_{X(i,j)}$$

restricts to $\mathbb{F}_{q^{\delta(a)}}$-linear maps

$$\mathrm{Dec}^{(i,j)} : \mathrm{Err}(T_a(X, \mathbb{F}_{q^{\delta(a)}}), j) \longrightarrow T_a(X, \mathbb{F}_{q^{\delta(a)}}),$$

$$\mathrm{Dec}^{(i,j)}(w^{(j)}, w^{(\neg j)}) = \left(-\left(\frac{\partial f_i}{\partial x_j}(a) \right)^{-1} \frac{\partial f_i}{\partial x_{\neg j}}(a) w^{(\neg j)}, w^{(\neg j)} \right).$$

The algorithms, constructing Groebner bases of $I(X, \overline{\mathbb{F}_q}) = \langle f_q, \dots, f_m\rangle \triangleleft \overline{\mathbb{F}_q}[x_1, \dots, x_n]$, containing $f_1, \dots, f_m$ are of exponential growth and it is worthless to decode tangent codes by the means of Corollary 13. Instead, one can choose such equations $f_q, \dots, f_m \in \mathbb{F}_q[x_1, \dots, x_n]$ of X, which are a priori known to form a Groebner basis with respect to an appropriate lexicographic order. Here is an example

Corollary 14. *Let $H \in M_{(n-k)\times n}(\mathbb{F}_q)$ be a parity check matrix of an $\mathbb{F}_q$-linear code C of length n, dimension k and minimum distance $\geq t+1$ with*

$$H_{ij} = 0 \quad \textit{for} \quad \forall 1 \leq j < i \leq n-k \quad \textit{and}$$

$$H_{ii} = 1 \quad \textit{for} \quad \forall 1 \leq i \leq n-k.$$

For arbitrary polynomials $h_i(x_{i+1}, \dots, x_n) \in \langle x_{i+1}, \dots, x_n\rangle^2 \cap \mathbb{F}_q[x_{i+1}, \dots, x_n]$ without terms of total degree < 2, consider the polynomials

$$f_i(x_i, x_{i+1}, \dots, x_n) = x_i + \sum_{s=i+1}^{n} H_{is}x_s + h_i(x_{i+1}, \dots, x_n) \quad \textit{for} \quad 1 \leq i \leq n-k.$$

Then:

(i) $X = V(f_1, \dots, f_{n-k})/\mathbb{F}_q \subset \overline{\mathbb{F}_q}^n$ is a smooth irreducible k-dimensional affine variety, isomorphic to $\overline{\mathbb{F}_q}^k$ with $0^n \in X$ and $T_{0^n}(X, \mathbb{F}_q) = C$;

(ii) $f_1, \dots, f_{n-k}$ is a Groebner basis of $\langle f_1, \dots, f_{n-k}\rangle \triangleleft \overline{\mathbb{F}_q}[x_1, \dots, x_n]$ with respect to the lexicographic order with $x_1 > \dots > x_t > x_{t+1} > \dots > x_n$;

(iii) $X^{(\geq t+1)} \neq \emptyset$ is a Zariski open, Zariski dense subset of X;

(iv) at any $a \in X^{(\geq t+1)}$ the space $\mathrm{Err}(T_a(X, \mathbb{F}_{q^{\delta(a)}}), j)$ of the received words with $T_a(X, \mathbb{F}_{q^{\delta(a)}})$-error, supported by $j = \{1, \dots, t\} \in \binom{1,\dots,n}{t}$ consists of the solutions $w \in \mathbb{F}_{q^{\delta(a)}}^n$ of the homogeneous linear system

$$\frac{\partial(f_{t+1}, \dots, f_{n-k})}{\partial(x_{t+1}, \dots, x_n)}(a_{t+1}, \dots, a_n) \begin{pmatrix} w_{t+1} \\ \dots \\ w_n \end{pmatrix} = 0_{(n-k-t)\times 1}; \tag{8}$$

(v) the decoding morphism of bundles $\mathrm{Dec} : \mathrm{Err}(T^C X, j)|_{X^{(\geq t+1)}} \longrightarrow T^C X|_{X^{(\geq t+1)}}$ is given by

$$\mathrm{Dec}(w) = \left(- \left(\frac{\partial f_i}{\partial x_j}(\pi_E(w)) \right)^{-1} \frac{\partial f_i}{\partial x_{\neg j}}(\pi_E(w))w^{(\neg j)}, w^{(\neg j)} \right). \tag{9}$$

with $i = \{1, \dots, t\} \in \binom{1,\dots,n-k}{t}$, $j = \{1, \dots, t\} \in \binom{1,\dots,n}{t}$, $\neg j = \{1, \dots, n\} \backslash j = \{t+1, \dots, n\}$ over the entire Zariski open, Zariski dense subset $X^{(\geq t+1)}$ of X.

Proof. (i) By an induction on the number of the equations $n-k \geq 1$, we prove the existence of polynomials $g_1, \dots, g_{n-k} \in \mathbb{F}_q[x_{n-k+1}, \dots, x_n]$, such that

$$X = V(f_1, \dots, f_{n-k}) = \{(g_1(a''), \dots, g_{n-k}(a''), a'') \,|\, \forall a'' := (a_{n-k+1}, \dots, a_n) \in \overline{\mathbb{F}_q}^k\}. \tag{10}$$

Then the puncturing $\Pi_\delta : \overline{\mathbb{F}_q}^n \to \overline{\mathbb{F}_q}^k$ at $\delta = \{1, \ldots, n-k\} \in \binom{1,\ldots,n}{n-k}$ is an isomorphism of affine varieties with inverse

$$\Pi_\delta^{-1}(a'') = (g_1(a''), \ldots, g_{n-k}(a''), a'') \quad \text{for} \quad \forall a'' = (a_{n-k+1}, \ldots, a_n) \in \overline{\mathbb{F}_q}^k.$$

In particular, X is a smooth irreducible k-dimensional affine variety, defined over $\mathbb{F}_q$. To this end, note that for $n-k=1$ and $g_1(x_2, \ldots, x_n) := -\sum\limits_{s=2}^{n} H_{1s}x_s + h_1(x_2, \ldots, x_n)$ one has $X = V(f_1) = \{(g_1(a''), a'') \,|\, \forall a'' := (a_2, \ldots, a_n) \in \overline{\mathbb{F}_q}^{n-1}\}$. If we assume that

$$V(f_1, \ldots, f_{n-k-1}) = \{(g_1'(a'), \ldots, g_{n-k-1}'(a'), a') \,|\, \forall a' := (a_{n-k}, \ldots, a_n) \in \overline{\mathbb{F}_q}^{k+1}\}$$

for some $g_1', \ldots, g_{n-k-1}' \in \mathbb{F}_q[x_{n-k}, \ldots, x_n]$ then introducing

$$g_{n-k}(x_{n-k+1}, \ldots, x_n) := -\sum_{s=n-k+1}^{n} H_{n-k,s}x_s - h_{n-k}(x_{n-k+1}, \ldots, x_n) \quad \text{and}$$

$$g_i(x_{n-k+1}, \ldots, x_n) := g_i'(g_{n-k}(x_{n-k+1}, \ldots, x_n), x_{n-k+1}, \ldots, x_n) \quad \text{for} \quad \forall 1 \leq i \leq n-k-1,$$

one concludes that

$$V(f_1, \ldots, f_{n-k-1}, f_{n-k}) =$$
$$\{(g_1(a''), \ldots, g_{n-k-1}(a''), g_{n-k}(a''), a'') \,|\, \forall a'' := (a_{n-k+1}, \ldots, a_n) \in \overline{\mathbb{F}_q}^k\}$$

and proves (10).

(ii) The leading terms of f_i with respect to the lexicographic order with $x_1 > \ldots > x_n$ are $\mathrm{LT}(f_i) = x_i$ for $\forall 1 \leq i \leq n-k$. These are pairwise relatively prime monomials, i.e., $\mathrm{LCM}(\mathrm{LT}(f_i), \mathrm{LT}(f_j)) = x_i x_j = \mathrm{LT}(f_i)\mathrm{LT}(f_j)$ for $\forall 1 \leq i < j \leq n-k$. Combining Theorem 3 with Proposition 4 from Chapter 2, § 9, [3], one concludes that $f_1, \ldots, f_{n-k}$ is a Groebner basis of $\langle f_1, \ldots, f_{n-k} \rangle \lhd \overline{\mathbb{F}_a}[x_1, \ldots, x_n]$ with respect to the lexicographic order with $x_1 > \ldots > x_n$.

(iii) By Proposition 2 (i), $X^{(\geq t+1)}$ is a Zariski open subset of X. It suffices to show that $0^n \in X^{(\geq t+1)}$, in order to conclude that $X^{(\geq t+1)} \neq \emptyset$ is non-empty and, therefore, Zariski dense in the irreducible affine variety X. Straightforward verification establishes that $0^n \in X = V(f_1, \ldots, f_{n-k})$ and $\frac{\partial f}{\partial x}(0^n) = \frac{\partial(f_1, \ldots, f_{n-k})}{\partial(x_1, \ldots, x_n)}(0^n) = H \in M_{(n-k)\times n}(\mathbb{F}_q)$. According to $f_1, \ldots, f_{n-k} \in I(X, \overline{\mathbb{F}_q})$, the Zariski tangent space $T_{0^n}(X, \mathbb{F}_q)$ to X at the origin 0^n is contained in the linear code C with parity check matrix H. Since X is smooth and k-dimensional, $\dim_{\mathbb{F}_q} T_{0^n}(X, \mathbb{F}_q) = \dim_{\mathbb{F}_q} C = k$, whereas $T_{0^n}(X, \mathbb{F}_q) = C$. By assumption, C is of minimum distance $\geq t+1$, so that $0^n \in X^{(\geq t+1)}$.

(iv) Note that the Singleton Bound for C reads as $t+1 \leq n+1-k$ and guarantees that $t \leq n-k$. Now, an immediate application of Corollary 13 provides (8).

(v) At an arbitrary point $a \in X$, the Jacobian matrix $\frac{\partial f}{\partial x}(a)$ has an invertible minor

$$\frac{\partial(f_1,\dots,f_t)}{\partial(x_1,\dots,x_t)}(a) = \left(\begin{array}{ccccc} 1 & \frac{\partial h_1}{\partial x_2}(a) + H_{12} & \frac{\partial h_1}{\partial x_3}(a) + H_{13} & \dots & \frac{\partial h_1}{\partial x_t}(a) + H_{1t} \\ 0 & 1 & \frac{\partial h_2}{\partial x_3}(a) + H_{23} & \dots & \frac{\partial h_2}{\partial x_t}(a) + H_{2t} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \end{array} \right)$$

of order t with rows, labeled by $i = \{1,\dots,t\} \in \binom{1,\dots,n-k}{t}$ and columns, labeled by $j = \{1,\dots,t\} \in \binom{1,\dots,n}{t}$. In the notations from Proposition 12 (i), that implies $X^{(\geq t+1)} \subseteq X(i,j) := X^{(\geq t+1)} \setminus V\left(\frac{\partial f_i}{\partial x_j}\right) \subseteq X^{(\geq t+1)}$, whereas $X^{(\geq t+1)} = X(i,j)$. Thus, the decoding bundle morphism is defined over the entire $X^{(\geq t+1)}$ by formula (9).

□

5.3 Gradient codes

Let $X \subset \overline{\mathbb{F}_q}^n$ be an affine variety, whose absolute ideal $I(X, \overline{\mathbb{F}_q}) = \langle f_1,\dots,f_m\rangle_{\overline{\mathbb{F}_q}}$ is generated by $f_1,\dots,f_m \in \mathbb{F}_q[x_1,\dots,x_n]$. Then for any point $a = (a_1,\dots,a_n) \in X$ with definition field $\mathbb{F}_{q^{\delta(a)}} = \mathbb{F}_q(a_1,\dots,a_n)$ over $\mathbb{F}_q$, the ideal

$$I(X, \mathbb{F}_{q^{\delta(a)}}) := \{g \in \mathbb{F}_{q^{\delta(a)}}[x_1,\dots,x_n] \,|\, g(b) = 0, \forall b \in X\}$$

of X over $\mathbb{F}_{q^{\delta(a)}}$ is generated by $f_1,\dots,f_m$. The gradient of $g \in I(X, \mathbb{F}_{q^{\delta(a)}})$ is the ordered n-tuple

$$\mathrm{grad}(g) := \left(\frac{\partial g}{\partial x_1},\dots,\frac{\partial g}{\partial x_n}\right) \in \mathbb{F}_{q^{\delta(a)}}[x_1,\dots,x_n]^n$$

of its partial derivatives. The subset

$$\mathrm{Grad}_a I(X, \mathbb{F}_{q^{\delta(a)}}) := \left\{ \mathrm{grad}_a(g) = \left(\frac{\partial g}{\partial x_1},\dots,\frac{\partial g}{\partial x_n}\right) \in \mathbb{F}^n_{q^{\delta(a)}} \,\middle|\, g \in I(X, \mathbb{F}_{q^{\delta(a)}}) \right\}$$

of $\mathbb{F}^n_{q^{\delta(a)}}$ is an $\mathbb{F}_{q^{\delta(a)}}$-linear code, which we call the gradient code to X at a. The fibration

$$\pi : \mathrm{Grad}^C I(X) := \coprod_{a \in X} \mathrm{Grad}_a I(X, \mathbb{F}_{q^{\delta(a)}}) \longrightarrow X$$

with $\pi^{-1}(a) = \mathrm{Grad}_a I(X, \mathbb{F}_{q^{\delta(a)}})$ for $\forall a \in X$ will be referred to as the bundle of the gradient codes to X.

Lemma 15. *Let $X/\mathbb{F}_q \subset \overline{\mathbb{F}_q}^n$ be an affine variety, defined over $\mathbb{F}_q$. Then the dual*

$$(T^C X)^{\perp} = \mathrm{Grad}^C I(X) \tag{11}$$

of the bundle $T^C X$ of the tangent codes to X is the bundle $\mathrm{Grad}^C I(X)$ of the gradient codes to X.

Proof. The equality (11) is meant as a coincidence $T_a(X, \mathbb{F}_{q^{\delta(a)}})^{\perp} = \mathrm{Grad}_a I(X, \mathbb{F}_{q^{\delta(a)}})$ of the fibres at all the points $a \in X$. By the very definition, if $f_1, \ldots, f_m \in \mathbb{F}_q[x_1, \ldots, x_n]$ is a generating set of $I(X, \overline{\mathbb{F}_q})$ then $T_a(X, \mathbb{F}_{q^{\delta(a)}})^{\perp}$ is the linear code with a generator matrix

$$\frac{\partial f}{\partial x}(a) = \begin{pmatrix} \mathrm{grad}_a(f_1) \\ \ldots \\ \mathrm{grad}_a(f_m) \end{pmatrix}.$$

Therefore

$$T_a(X, \mathbb{F}_{q^{\delta(a)}})^{\perp} = \left\{ \sum_{j=1}^{m} \lambda_j \mathrm{grad}_a(f_j) = \mathrm{grad}_a\left(\sum_{j=1}^{m} \lambda_j f_j \right) \ \Big| \ \lambda_j \in \mathbb{F}_{q^{\delta(a)}} \right\}$$

is a subspace of $\mathrm{Grad}_a I(X, \mathbb{F}_{q^{\delta(a)}})$, as far as $\sum\limits_{j=1}^{m} \lambda_j f_j \in I(X, \mathbb{F}_{q^{\delta(a)}})$.

Conversely, any $g \in I(X, \mathbb{F}_{q^{\delta(a)}}) = \langle f_1, \ldots, f_m \rangle \triangleleft \mathbb{F}_{q^{\delta(a)}}[x_1, \ldots, x_n]$ is of the form $g = \sum\limits_{j=1}^{m} g_j f_j$ for some $g_j \in \mathbb{F}_{q^{\delta(a)}}[x_1, \ldots, x_n]$. Its gradient $\mathrm{grad}(g) = \sum\limits_{j=1}^{m} f_j \mathrm{grad}(g_j) + g_j \mathrm{grad}(f_j)$ has value

$$\mathrm{grad}_a(g) = \sum_{j=1}^{m} g_j(a) \mathrm{grad}_a(f_j) \in \mathrm{Span}_{\mathbb{F}_{q^{\delta(a)}}}(\mathrm{grad}_a(f_j) \,|\, 1 \leq j \leq m) = T_a(X, \mathbb{F}_{q^{\delta(a)}})^{\perp}$$

at $a \in X$, as far as $\forall f_j \in I(X, \mathbb{F}_{q^{\delta(a)}}) \subseteq I(a, \mathbb{F}_{q^{\delta(a)}})$. That suffices for the inclusion $\mathrm{Grad}_a I(X, \mathbb{F}_{q^{\delta(a)}}) \subseteq T_a(X, \mathbb{F}_{q^{\delta(a)}})^{\perp}$ and $T_a(X, \mathbb{F}_{q^{\delta(a)}})^{\perp} = \mathrm{Grad}_a I(X, \mathbb{F}_{q^{\delta(a)}})$.

□

The union $\coprod\limits_{a \in X} \mathrm{Grad} I(X, \mathbb{F}_{q^{\delta(a)}})$ of the subspaces

$$\mathrm{Grad} I(X, \mathbb{F}_{q^{\delta(a)}}) = \{\mathrm{grad}(g) \,|\, g \in I(X, \mathbb{F}_{q^{\delta(a)}})\} \subseteq \mathbb{F}_{q^{\delta(a)}}[x_1, \ldots, x_n]^n$$

can be viewed as a sheaf of sections

$$\mathrm{grad}(g) : X(\mathbb{F}_{q^{\delta(a)}}) \longrightarrow \mathrm{Grad}^C I(X)|_{X(\mathbb{F}_{q^{\delta(a)}})},$$

$$b \mapsto \mathrm{grad}_b(g).$$

In such a way, the gradient codes appear to be of a similar nature with the algebro-geometric Goppa codes, which consist of the values of the global sections of line bundles over curves $Y/\mathbb{F}_q \subset \mathbb{P}^N(\overline{\mathbb{F}_q})$, at ordered n-tuples of $\mathbb{F}_q$-rational points of Y. For a systematic study of the algebro-geometric Goppa codes see [16], [14], [9] or [7].

For an arbitrary integer $1 \leq s \leq n$, let us consider the loci

$$X^{(\geq s)}_{\mathrm{grad}} := \{a \in X \ \mid \ d(\mathrm{grad}_a I(X, \mathbb{F}_{q^{\delta(a)}})) \geq s\},$$

$$X^{(\leq s)}_{\mathrm{grad}} := \{a \in X \ \mid \ d(\mathrm{grad}_a I(X, \mathbb{F}_{q^{\delta(a)}})) \leq s\},$$

at which the gradient codes to X are of minimum distance $\geq s$, respectively, $\leq s$. The next proposition shows that the presence of a non-zero polynomial $h \in I(X, \overline{\mathbb{F}_q})$ in at most d variables is sufficient for the presence of an upper bound d on the minimum distance of a gradient code to a generic point of X.

Proposition 16. *Let $X/\mathbb{F}_q \subset \overline{\mathbb{F}_q}^n$ be an irreducible affine variety, defined over $\mathbb{F}_q$. If there exists a non-zero polynomial $h \in I(X, \overline{\mathbb{F}_q}) \cap \overline{\mathbb{F}_q}[x_\beta]$ of $|\beta| = d$ variables and $\Pi_{\neg\beta} : X \to \overline{\mathbb{F}_q}^d$ is the puncturing at the complement $\neg\beta$ of β then*

$$X^{(\geq d+1)}_{\rm grad} \subseteq \Pi^{-1}_{\neg\beta}(\Pi_{\neg\beta}(X)^{\rm sing}) \subsetneqq X,$$

so that $X^{(\leq d)}_{\rm grad}$ is Zariski dense in X.

Proof. Let $f_1, \dots, f_m \in \mathbb{F}_q[x_1, \dots, x_n]$ be a generating set of $I(X, \overline{\mathbb{F}_q}) \triangleleft \overline{\mathbb{F}_q}[x_1, \dots, x_n]$, $G_{\neg\beta,\beta} \subset \mathbb{F}_q[x_1, \dots, x_n]$ be a Groebner basis of $\langle f_1, \dots, f_m \rangle_{\mathbb{F}_q} \triangleleft \mathbb{F}_q[x_1, \dots, x_n]$ with respect to a lexicographic order with $x_{\neg\beta} > x_\beta$ and $G_\beta := G_{\neg\beta,\beta} \cap \mathbb{F}_q[x_\beta] = \{g_1, \dots, g_l\}$. By the Elimination Theorem 2 from Chapter 3, §1 of [3], G_β is a Groebner basis of the elimination ideal $I^{(\beta)} := I(X, \overline{\mathbb{F}_q}) \cap \overline{\mathbb{F}_q}[x_\beta]$. The presence of a non-zero polynomial $h \in I^{(\beta)}$ implies that the set $G_\beta \neq \emptyset$ is non-empty. The proof of Proposition 12 (ii) has established that the absolute ideal $I(\overline{\Pi_{\neg\beta}(X)}, \overline{\mathbb{F}_q}) = I^{(\beta)} = \langle G_\beta \rangle_{\overline{\mathbb{F}_q}}$ of the Zariski closure $\overline{\Pi_{\neg\beta}(X)}$ of $\Pi_{\neg\beta}(X)$ in $\overline{\mathbb{F}_q}^d$ coincides with $I^{(\beta)} = \langle G_\beta \rangle_{\overline{\mathbb{F}_q}}$. Therefore $\overline{\Pi_{\neg\beta}(X)} \subsetneqq \overline{\mathbb{F}_q}^d$ is an irreducible affine variety of dimension $\dim \Pi_{\neg\beta}(X) < d$.

For any $g_i \in G_\beta \subset I(\Pi_{\neg\beta}(X), \overline{\mathbb{F}_q}) \subseteq I(X, \overline{\mathbb{F}_q})$ and $a \in X$ note that $\mathrm{grad}_a(g_i) \in \overline{\mathbb{F}_q}^n$ is a word of weight $\leq d$, as far as $g_i \in \mathbb{F}_q[x_\beta]$ depends on at most $|\beta| = d$ variables. In particular, for $a \in X^{(\geq d+1)}_{\rm grad}$ there follows $\mathrm{grad}_{\Pi_{\neg\beta}(a)}(g_i) = \mathrm{grad}_a(g_i)(a) = 0_{1\times n}$. Thus,

$$\frac{\partial(g_1, \dots, g_l)}{\partial x_\beta}(\Pi_{\neg\beta}(a)) = \left(\begin{array}{c} \mathrm{grad}_{\Pi_{\neg\beta}(a)}(g_1) \\ \dots \\ \mathrm{grad}_{\Pi_{\neg\beta}(a)}(g_l) \end{array} \right) = 0_{l\times n} \quad \text{at} \quad \forall a \in X^{(\geq d+1)}_{\rm grad}$$

and $X^{(\geq d+1)}_{\rm grad}$ is contained in the affine variety

$$Z := V\left(\frac{\partial g_i}{\partial x_j} \;\Bigg|\; 1 \leq i \leq l, \;\; 1 \leq j \leq n \right) \subseteq \overline{\mathbb{F}_q}^n.$$

We claim that

$$Z \subseteq \Pi^{-1}_{\neg\beta}(\Pi_{\neg\beta}(X)^{\rm sing}). \tag{12}$$

Indeed, if $a \in Z$ then $\frac{\partial G_\beta}{\partial x_\beta}(\Pi_{\neg\beta}(a)) = 0_{l\times n}$ and $T_{\Pi_{\neg\beta}(a)}(\Pi_{\neg\beta}(X), \mathbb{F}_{q^{\delta(a)}}) = \mathbb{F}^d_{q^{\delta(a)}}$. According to $\dim \Pi_{\neg\beta}(X) < d$ there follows $\Pi_{\neg\beta}(a) \in \Pi_{\neg\beta}(X)^{\rm sing}$, which is equivalent to (12). Thus, $X^{(\geq d+1)}_{\rm grad} \subseteq \Pi^{-1}_{\neg\beta}(\Pi_{\neg\beta}(X)^{\rm sing})$ for the proper affine subvariety $\Pi^{-1}_{\neg\beta}(\Pi_{\neg\beta}(X)^{\rm sing}) \subsetneqq X$. Now

$$\Pi^{-1}_{\neg\beta}(\Pi_{\neg\beta}(X)^{\rm smooth}) = X \setminus \Pi^{-1}_{\neg\beta}(\Pi_{\neg\beta}(X)^{\rm sing}) \subseteq X \setminus X^{(\geq d+1)}_{\rm grad} = X^{(\leq d+1)}_{\rm grad}$$

for the non-empty, Zariski open subset $\Pi^{-1}_{\neg\beta}(\Pi_{\neg\beta}(X)^{\rm smooth})$ of X, so that $X^{(\leq d+1)}_{\rm grad}$ is Zariski dense in X.

□

References

[1] M. C. Beltrametti, E. Carletti, D. Gallarati, 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] D. Cox, J. Little, D. O'Shea, *Ideals, Varieties, and Algorithms - An Introduction to Computational Algebraic Geometry and Commutative Algebra*, Undergraduate Texts in Mathematics, Springer, 1997.

[4] S. Dodunekov and I. Landgev, Near MDS-codes, *Journal of Geometry*, **54** (1995), 30–43.

[5] I. Duursma, Weight distribution of geometric Goppa codes, *Transections of the American Mathematical Society*, **351** (1999), 3609–3639.

[6] J. Harris, *Algebraic Geometry - A First Course,* Graduate Texts in Mathematics, Springer, 1992.

[7] W. C. Huffman, V. Pless, *Fundamentals of Error Correcting Codes*, Cambridge University Press, 2003.

[8] A. Kasparian, I. Marinov, Duursma's reduced polynomial, arXiv:1505.01993v1[cs.IT] 8 May 2015

[9] H. Niederreiter and Ch. Xing, *Algebraic geometry in Coding Theory and Cryptography*, Princeton University Press, 2009.

[10] K. O'Grady, *A First Course in Algebraic Geometry,* 2012.

[11] R. Pellikaan On the efficient decoding of algebraic-geometric codes, *Eurocode 92* (P. Camion, P. Charpin and S. Harari eds.) Udine, CISM Courses and Lectures **339**, Springer, Wien, 1993, 231–253.

[12] M. Reid, *Undergraduate Algebraic Geometry,* London Mathematical Society Student Texts, 1989.

[13] I. R. Shafarevich, *Basic Algebraic Geometry,* v.1, 2, Moscow, 1988.

[14] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer, 1993.

[15] M. A. Tsfasman, S. G. Vlădut, T. Zink, Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound, *Math. Nachr.* **109** (1982), 21–28.

[16] M. Tsfasman, S. Vlădut, D. Nogin, *Algebraic Geometry Codes: Basic Notions,* Providence, RI: American Mathematical Society, 2007.