Tangent Codes
Azniv Kasparian, Evgeniya Velikova *

Abstract

We interpret the finite Zariski tangent spaces $T_a(X, F_q^m)$ to an affine variety $X \subset F_q^n$ as linear codes. If the degree of $X$ is relatively prime to the characteristic $p = \text{char} F_q$, we show that the minimum distance of $T_a(X, F_q^m)$ stabilizes while varying $a \in X(F_q^m) := X \cap F_q^m$ and $m \in \mathbb{N}$. The article provides a pseudo-code for obtaining the generic minimum distance of a tangent code and points, at which it is attained. On the other hand, any family of linear codes of fixed length, fixed dimension and arbitrary minimum distance is interpolated by the $F_q$-Zariski tangent bundle of an affine variety $X \subset F_q^n$ with explicit equations, whose degree is divisible by $p = \text{char} F_q$.

A basic problem in the theory of error correcting codes is the construction of linear codes with a priori given length, dimension and minimum distance. That is helpful for the presence of a unique decoding under appropriate upper bound on the number of the perturbed symbols. Except the construction of individual linear codes, one can investigate the stabilization or destabilization of the minimum distance within a family of linear codes of fixed length and dimension. Explicit families enable "to deform" a given linear code into one with the desired minimum distance or to produce a bunch of linear codes with one and a same parameters. In a similar vein, one looks for families of Hamming isometries of linear codes. In order to produce linear codes with given parameters or to construct their Hamming isometries, one makes use of structures, arising from other branches of mathematics.

In the early 80's, Goppa introduced the classical algebraic geometric codes. They consist of values of global holomorphic sections of line bundles over curves. Various geometric properties of the corresponding line bundles estimate the dimension and the minimum distance. Under the presence of extra assumptions, one is able to predict the exact values of these parameters.

The present work introduces another application of algebraic geometry to the coding theory. It interprets the finite Zariski tangent spaces to an affine variety $X$ as linear codes. If the degree of $X$ is relatively prime to the characteristic $p$ of the definition field of $X$, the generic minimum distance $d$ of a finite Zariski tangent space to $X$ is characterized by a global geometric property of $X$. We provide an effective procedure in a form of a pseudo-code, obtaining $d$ and points $a \in X$, at which $d$ is attained. On the other hand, an explicit construction of an affine variety $X$, whose

*This research is partially supported by Contract 101 / 19.04.2013 and Contract 015 / 9.04.2014 with the Scientific Foundation of the University of Sofia
degree is divisible by \( p \), illustrates the possibility for incorporating codes of arbitrary minimum distance within a single Zariski tangent bundle.

Here is a synopsis of the paper. The first section characterizes the generic minimum distance of a tangent code \( T_a(X, \mathbb{F}_q^m) \) to an affine variety \( X \subset \mathbb{P}_q^d \), defined over \( \mathbb{F}_q \), whose degree is relatively prime to \( p = \text{char} \mathbb{F}_q \). More precisely, subsection 1.1 recalls the notion of a Zariski tangent space to an affine variety. The next subsection 1.2 translates the minimum distance \( d \) of a linear code in terms of its punctures at \( d-1 \) or \( d \) coordinates. This description becomes handy for the characterization of the generic minimum distance of a tangent code \( T_a(X, \mathbb{F}_q^m) \) to \( X \), as far as the puncturings of \( T_a(X, \mathbb{F}_q^m) \) coincide with the differentials of the associated puncturings of \( X \) at \( a \in X \).

The same subsection 1.2 introduces the genericity index \( d-1 \) of an irreducible affine variety \( X \subset \mathbb{P}_q^d \) as the maximal non-negative integer, for which any \( n-d+1 \) coordinate functions \( x_{j_1} + I(X, \mathbb{F}_q), \ldots, x_{j_{n-d+1}} + I(X, \mathbb{F}_q) \in \mathbb{F}_q(X) \) contain a transcendence basis of the function field \( \mathbb{F}_q(X) \) of \( X \) over the algebraic closure \( \overline{\mathbb{F}}_q \) of the definition field \( \mathbb{F}_q \) of \( X \). Let \( X/\mathbb{F}_q \subset \mathbb{P}_q^d \) be an irreducible, \( (d-1) \)-generic affine variety, defined over \( \mathbb{F}_q \), whose degree is not divisible by \( p = \text{char} \mathbb{F}_q \). Subsection 1.3 establishes that the generic minimum distance to a complement of a hypersurface in \( X \) are of minimum distance \( d \). This involves an analogue of the Implicit Function Theorem, deriving a lower bound on the generic minimum distance of \( X \) from a lower bound on the generic minimum distance of a tangent code. A sort of an inverse statement of the Implicit Function Theorem provides a lower bound on the generic minimum distance of a finite Zariski tangent space to \( X \), which follows from a lower bound on the genericity index of \( X \). The second section is devoted to an algorithm for obtaining the generic minimum distance of a tangent code and points, at which it is attained. Its first subsection recalls the Hilbert polynomial of an affine variety and an algorithm for its computing. It sketches one of the well known explicit procedures for decomposition of an affine variety into a union of irreducible components. Subsection 2.2 proposes an easy way for computing the genericity index \( d-1 \) of an irreducible affine variety \( X \subset \mathbb{P}_q^d \), out of the set of all the coordinate transcendence bases of the function field \( \mathbb{F}_q(X) \) of \( X \) over \( \overline{\mathbb{F}}_q \). The third subsection provides an algorithm for obtaining the discriminant locus of all the puncturings of \( X \) at \( d-1 \) coordinates and explicit points from its complement. Subsection 2.4 synthesizes the algorithms from the previous three subsections in a pseudo-code. The third section illustrates the stabilization, respectively, the destabilization of the minimum distance within a Zariski tangent bundle to an affine variety \( X \subset \mathbb{P}_q^d \), whose degree is not divisible, respectively, is divisible by the characteristic \( p = \text{char} \mathbb{F}_q \). This is done in the corresponding subsections by explicit constructions of the desired affine varieties \( X \) by their defining equations. The last, fourth section relates the linear Hamming isometries of the tangent codes \( T_a(X, \mathbb{F}_q^m) \) to an affine variety \( X \subset \mathbb{P}_q^d \) with the differentials of appropriate morphisms of \( X \). Subsection 4.1 provides a pattern for construction of a morphism \( \psi : \mathbb{P}_q^d \rightarrow \mathbb{P}_q^d \), whose differentials restrict to linear Hamming isometries \( (d\psi)_a : T_a(X, \mathbb{F}_q^m) \rightarrow T_{\psi(a)}(\psi(X), \mathbb{F}_q^m) \) on the generic Zariski tangent spaces to the affine varieties \( X \subset \mathbb{P}_q^d \), which are not contained in an explicitly given hypersurface \( V(\psi_n) \subset \mathbb{P}_q^d \), depending on \( \psi \). Subsection 4.2 realizes arbitrary families of linear Hamming isometries \( \mathbb{P}_q^d \rightarrow \mathbb{P}_q^d \) by differentials of appropriate explicit morphisms \( \mathbb{P}_q^d \rightarrow \mathbb{P}_q^d \). It observes also that the Frobenius automorphism \( \Phi_q \) of
an affine variety \(X \subset \mathbb{F}_q^n\), defined over \(\mathbb{F}_q\) induces non-linear Hamming isometries between the finite Zariski tangent spaces to \(X\).

1 The genericity index and the generic minimum distance of a tangent code

1.1 Preliminaries on the Zariski tangent spaces to an affine variety

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

\[X = V(f_1, \ldots, f_l) = \{a \in \mathbb{F}_q^n \mid f_1(a) = \ldots = f_l(a) = 0\}\]

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

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

of \(X\) is generated by polynomials \(g_1, \ldots, g_m \in \mathbb{F}_q[x_1, \ldots, x_n]\) with coefficients from \(\mathbb{F}_q\). The affine subvarieties of \(\mathbb{F}_q^n\) form a family of closed subsets. The corresponding topology is referred to as the Zariski topology on \(\mathbb{F}_q^m\). An affine variety \(X \subset \mathbb{F}_q^n\) is irreducible if any decomposition \(X = Z_1 \cup Z_2\) of \(X\) into a union of Zariski closed subsets \(Z_1 \subset X\) has \(X = Z_1\) or \(X = Z_2\). If \(X/\mathbb{F}_q \subset \mathbb{F}_q^n\) is an irreducible affine variety, defined over \(\mathbb{F}_q\), then for any constant field \(\mathbb{F}_q \subset F \subset \mathbb{F}_q\) the function field \(F(X)\) of \(X\) over \(F\) is defined as the fraction field of the affine coordinate ring \(F[X] := F[x_1, \ldots, x_n]/I(X, F)\) of \(X\) over \(F\). The local ring \(\mathcal{O}_a(X, F)\) of an \(F\)-rational point \(a \in X(F) := X \cap F^n\) in \(X\) over \(F\) consists of the quotients \(\frac{a}{F}\) of \(\varphi_1, \varphi_2 \in F[X]\) with \(\varphi_2(a) \neq 0\). An \(F\)-linear derivation \(D_a : \mathcal{O}_a(X, F) \to F\) at \(a \in X(F)\) is an \(F\)-linear map, subject to Leibnitz-Newton rule

\[D_a(\varphi_1 \varphi_2) = D_a(\varphi_1)\varphi_2(a) + \varphi_1(a)D_a(\varphi_2)\]

for derivation of a product of \(\varphi_1, \varphi_2 \in \mathcal{O}_a(X, F)\) at \(a\). The \(F\)-linear space \(T_a(X, F) = \text{Der}_a(\mathcal{O}_a(X, F), F)\) of the \(F\)-linear derivations \(D_a : \mathcal{O}_a(X, F) \to F\) at \(a \in X(F)\) is called the Zariski tangent space to \(X\) at \(a\). The derivation rule of a product of rational functions supplies the derivation rule

\[D_a\left(\frac{\varphi_1}{\varphi_2}\right) = \frac{D_a(\varphi_1)\varphi_2(a) - \varphi_1(a)D_a(\varphi_2)}{\varphi_2(a)^2}\]

of a quotient of \(\varphi_1, \varphi_2 \in F[X]\) \(\varphi_2 \neq 0\). Therefore any at derivations \(D_a : F[X] \to F\) at \(a \in X(F)\) has uniquely determined extension to a derivation \(D_a : \mathcal{O}_a(X, F) \to F\) at \(a\) and there is an \(F\)-linear isomorphism \(T_a(X, F) \simeq \text{Der}_a(F[X], F)\). Further, any derivation \(D_a : F[X] \to F\) lifts to a derivation \(D_a : F[x_1, \ldots, x_n] \to F\), vanishing on the ideal \(I(X, F)\) of \(X\) over \(F\). If \(f_1, \ldots, f_m \in F[x_1, \ldots, x_n]\) is a generating set of \(I(X, F) \subset I(a, F)\), then \(D_a\left(\sum_{i=1}^{m} f_i g_i\right) = \sum_{i=1}^{m} D_a(f_i)g_i(a)\) reveals that

\[T_a(X, F) \simeq \{D_a \in \text{Der}_a(F[x_1, \ldots, x_n], F) \mid D_a(f_1) = \ldots = D_a(f_m) = 0\}.\]
Let us view the polynomials \( F[x_1, \ldots, x_n] = F[x_1 - a_1, \ldots, x_n - a_n] \) as a graded ring
\[
F[x_1, \ldots, x_n] = \bigoplus_{i=0}^{\infty} F[x_1 - a_1, \ldots, x_n - a_n]^{(i)},
\]
where \( F[x_1 - a_1, \ldots, x_n - a_n]^{(i)} \) is the \( F \)-linear space of the homogeneous polynomials of \( x_1 - a_1, \ldots, x_n - a_n \) of degree \( i \). Note that an arbitrary \( F \)-linear derivation \( D_a : F[x_1, \ldots, x_n] \to F \) at \( a \in F^n \) vanishes on \( F[x_1 - a_1, \ldots, x_n - a_n]^{(0)} = F \), according to \( D_a(1) = D_a(1,1) = D_a(1,1) + 1.D_a(1) = 2D_a(1) \). Due to \( D_a|_{F[x_1-a_1,\ldots,x_n-a_n]^{(i)}} = 0 \) for all \( i \geq 2 \), the derivation \( D_a \) is determined uniquely by its \( F \)-linear restriction\[
D_a : F[x_1 - a_1, \ldots, x_n - a_n]^{(1)} = \text{Span}_F(x_1 - a_1, \ldots, x_n - a_n) \to F
\]
on the \( n \)-dimensional space \( F[x_1 - a_1, \ldots, x_n - a_n]^{(1)} \) of the homogeneous linear polynomials. That enables to view the Zariski tangent space
\[
T_a(F_q^n, F) \cong \text{Der}_a(F[x_1, \ldots, x_n], F)
\]
to the \( n \)-dimensional affine space \( F_q^n \) as a subspace of the \( F \)-linear functionals \( \text{Hom}_F(F[x_1 - a_1, \ldots, x_n - a_n]^{(1)}, F) \) on \( F[x_1 - a_1, \ldots, x_n - a_n]^{(1)} \). Since any \( F \)-linear map \( \mathcal{L} : F[x_1 - a_1, \ldots, x_n - a_n]^{(1)} \to F \) extends to an \( F \)-linear derivation \( F[x_1, \ldots, x_n] \to F \) at \( a \), one has an \( F \)-linear isomorphism
\[
\text{Der}_a(F[x_1, \ldots, x_n], F) \cong \text{Hom}_F(F[x_1 - a_1, \ldots, x_n - a_n]^{(1)}, F).
\]
Let us denote by \( \left( \frac{\partial}{\partial x_j} \right)_a \), \( 1 \leq j \leq n \) the uniquely determined \( F \)-linear derivations
\[
\left( \frac{\partial}{\partial x_j} \right)_a : F[x_1, \ldots, x_n] = F[x_1 - a_1, \ldots, x_n - a_n] \to F
\]
at \( a \), which restrict to the dual basis of \( x_j - a_j \), \( 1 \leq j \leq n \) on \( F[x_1 - a_1, \ldots, x_n - a_n]^{(1)} \). These are defined by the equalities
\[
\left( \frac{\partial}{\partial x_j} \right)_a (x_i - a_i) = \delta_{ij} = \begin{cases} 1 & \text{for } 1 \leq i = j \leq n, \\ 0 & \text{for } 1 \leq i \neq j \leq n. \end{cases}
\]
As a result, the Zariski tangent space to \( X \) at \( a \in X(F) \) over \( F \) can be described as
\[
T_a(X,F) = \left\{ v = \sum_{j=1}^{n} v_j \left( \frac{\partial}{\partial x_j} \right)_a \mid \sum_{j=1}^{n} v_j \frac{\partial f_i}{\partial x_j}(a) = 0, \quad \forall 1 \leq i \leq m \right\}
\]
for any generating set \( f_1, \ldots, f_m \) of \( I(X,F) \). Let us denote by
\[
\frac{\partial (f_1, \ldots, f_m)}{\partial (x_1, \ldots, x_n)} = \begin{pmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_m}{\partial x_1} & \cdots & \frac{\partial f_m}{\partial x_n} \end{pmatrix}
\]
the Jacobian matrix of \( f_1, \ldots, f_m \) with respect to \( x_1, \ldots, x_n \) and note that \( T_a(X,F) \) is the right null-space \( RN \frac{\partial (f_1, \ldots, f_m)}{\partial (x_1, \ldots, x_n)}(a) \) of \( \frac{\partial (f_1, \ldots, f_m)}{\partial (x_1, \ldots, x_n)}(a) \) in \( F^n \), i.e., the solution set of the homogeneous linear system with matrix \( \frac{\partial (f_1, \ldots, f_m)}{\partial (x_1, \ldots, x_n)}(a) \in \text{Mat}_{m \times n}(F) \). In terms of the coding theory, any Zariski tangent space \( T_a(X,F) \subset F^n \) over a finite field \( F \) is the linear code of length \( n \) with parity check matrix \( \frac{\partial (f_1, \ldots, f_m)}{\partial (x_1, \ldots, x_n)}(a) \).
1.2 Puncturing of linear codes and affine varieties

For an arbitrary field \( \mathbb{F}_q \subseteq F \subseteq \mathbb{F}_q^n \) and arbitrary indices \( 1 \leq i_1 < \ldots < i_{d-1} \leq n \), let us denote by

\[
\Pi_i : F^n \rightarrow F^n,
\Pi_i(x_1, \ldots, x_n) = (\ldots, \overline{x_{i_1}}, \ldots, \overline{x_{i_{d-1}}}, \ldots)
\]

the puncturing at \( i = \{i_1, \ldots, i_{d-1}\} \).

We start with a lemma, which characterizes the minimum distance of an \( \mathbb{F}_q \)-linear code \( C \subseteq \mathbb{F}_q^n \) by its puncturings.

**Lemma 1.** An \( \mathbb{F}_q \)-linear code \( C \subseteq \mathbb{F}_q^n \) of length \( n \) and dimension \( \dim_{\mathbb{F}_q} C = k \in \mathbb{N} \) is of minimum distance \( d \leq n + 1 - k \) if and only if for any \( (d-1) \)-tuple of indexes \( i = \{i_1, \ldots, i_{d-1}\} \), the puncturing \( \Pi_i : C \rightarrow \Pi_i(C) \) of \( C \) at \( i \) is an \( \mathbb{F}_q \)-linear embedding and there is a puncturing \( \Pi_j : C \rightarrow \Pi_j(C) \) at \( d \) coordinates \( j = \{j_1, \ldots, j_d\}, \) which is not injective.

**Proof.** By reductio ad absurdum, suppose that \( C \subseteq \mathbb{F}_q^n \) is of minimum distance \( d \) and there is a puncturing \( \Pi_i : C \rightarrow \mathbb{F}_q^{n-d+1} \) at \( i = \{i_1, \ldots, i_{d-1}\} \) with non-trivial kernel \( \ker \Pi_i|_C \neq \{0^n\} \). Then any \( c \in \ker \Pi_i|_C \setminus \{0^n\} \) has support

\[
\text{Supp}(c) := \{1 \leq s \leq n \mid c_s \neq 0\} \subseteq \{i_1, \ldots, i_{d-1}\}
\]

and \( c \) is of weight \( \leq d - 1 \). That contradicts \( d(C) = d \) and justifies the injectiveness of \( \Pi_i : C \rightarrow \mathbb{F}_q^{n-d+1} \) for all \( i = \{i_1, \ldots, i_{d-1}\} \). Further, for any word \( c \in C \) of weight \( d \) the puncturing \( \Pi_j : C \rightarrow \mathbb{F}_q^{n-d} \) at its support \( \text{Supp}(c) = \{j_1, \ldots, j_d\} \) contains \( c \neq 0^n \) in its kernel. Therefore \( \Pi_j|_C \) is not injective.

Conversely, let us assume that for any \( i = \{i_1, \ldots, i_{d-1}\} \subseteq \{1, \ldots, n\} \) the puncturing \( \Pi_i : C \rightarrow \mathbb{F}_q^{n-d+1} \) is injective and there exists a non-injective puncturing \( \Pi_j : C \rightarrow \mathbb{F}_q^{n-d} \) at some \( j = \{j_1, \ldots, j_d\} \subseteq \{1, \ldots, n\} \). If there is a word \( c \in C \) of weight \( 1 \leq s \leq d - 1 \), then for any \( \{i_1, \ldots, i_{d-1}\} \supseteq \{\alpha_1, \ldots, \alpha_s\} = \text{Supp}(c) \) the puncturing \( \Pi_i : C \rightarrow \mathbb{F}_q^{n-d+1} \) contains \( c \in \ker \Pi_i|_C \setminus \{0^n\} \) in its kernel. That contradicts the assumption \( \ker \Pi_i|_C = \{0^n\} \) and shows that the minimum distance of \( C \) is \( d(C) \geq d \). On the other hand, any word \( a \in \ker \Pi_j|_C \setminus \{0^n\} \) has support \( \text{Supp}(a) \subseteq \{j_1, \ldots, j_d\} \). The non-existence of words \( a \) of weight \( wt(a) \leq d - 1 \) specifies that \( \text{Supp}(a) = \{j_1, \ldots, j_d\} \) and \( a \) is of weight \( d \). Thus, \( d(C) = d \).

\[\square\]

In order to characterize the minimum distance of a generic Zariski tangent space \( T_a(X,F) \), \( a \in X(F) \) by a global geometric property of \( X \), let us note that the puncturing \( \Pi_i : T_a(X,F) \rightarrow F^{n-|i|} \) of the Zariski tangent space to \( X \) at \( a \) coincides with the differential of the same puncturing \( \Pi_i : X \rightarrow \Pi_i(X) \) of \( X \). We develop an analogue of the Implicit Function Theorem and its inverse statement, relating a puncturing of an affine variety with its differentials. In order to formulate precisely, let us recall the usual statement of the Implicit Function Theorem. Let \( f = (f_1, \ldots, f_m) : \mathbb{R}^n \rightarrow \mathbb{R}^m \) be an ordered \( m \)-tuple of continuously differentiable functions \( f_i : \mathbb{R}^n \rightarrow \mathbb{R} \) with
det $\frac{\partial (f_1, \ldots, f_m)}{\partial (x_{n-m+1}, \ldots, x_n)}(a) \neq 0$ at some point $a \in \mathbb{R}^n$. Then there exist a Euclidean neighborhood $U' \subseteq \mathbb{R}^{n-m}$ of $a' = (a_1, \ldots, a_{n-m})$, a Euclidean neighborhood $U'' \subseteq \mathbb{R}^m$ of $a'' = (a_{n-m+1}, \ldots, a_n)$ and a continuously differentiable local section $g : U' \to U''$ of the puncturing

$$\Pi'' = \Pi_{\{n-m+1, \ldots, n\}} : f^{-1} f(a) \cap (U' \times U'') = \{(x', g(x')) \mid x' \in U'\} \simeq U' \to U'$$

of the local fibre of $f$ over $f(a)$ at the last $m$ coordinates. Note that the assumption $\det \frac{\partial (f_1, \ldots, f_m)}{\partial (x_{n-m+1}, \ldots, x_n)}(a) \neq 0$ is equivalent to the existence of homogeneous linear functions $x_{n-m+1}(x'), \ldots, x_n(x')$ of $x' = (x_1, \ldots, x_{n-m})$, parameterizing the right null-space

$$RN \frac{\partial (f_1, \ldots, f_m)}{\partial (x_1, \ldots, x_n)}(a) = \{(x', x_{n-m+1}(x'), \ldots, x_n(x')) \mid x' \in \mathbb{R}^{n-m}\} \simeq \mathbb{R}^{n-m}$$

of the Jacobian matrix of $f_1, \ldots, f_m$ at $a$. In the case of polynomials $f_i \in \mathbb{R}[x_1, \ldots, x_n]$, $1 \leq i \leq m$, the fibre $f^{-1} f(a) \subseteq \mathbb{R}^n \subset \mathbb{C}^n$ consists of the $\mathbb{R}$-rational points of the affine variety $X := V(f_1 - f_1(a), \ldots, f_m - f_m(a)) \subset \mathbb{C}^n$. The Zariski tangent space

$$T_a(X, \mathbb{R}) \subseteq RN \frac{\partial (f_1 - f_1(a), \ldots, f_m - f_m(a))}{\partial (x_1, \ldots, x_n)}(a) = RN \frac{\partial (f_1, \ldots, f_m)}{\partial (x_1, \ldots, x_n)}(a),$$

as far as $f_1 - f_1(a), \ldots, f_m - f_m(a) \in I(X, \mathbb{R})$. If we assume that the affine variety $X \subset \mathbb{C}^n$ is irreducible and $\Pi'' = (d\Pi'')_a : T_a(X, \mathbb{R}) \to \mathbb{R}^{n-m}$ is injective, then there exists a Zariski open subset $W \subseteq \mathbb{C}^n$, such that $\Pi' : X \cap W \to \Pi''(X \cap W)$ is a finite morphism. Our Lemma 3 proves this statement in a form, which is convenient for the characterization of the minimum distance of a finite Zariski tangent space to an affine variety. Conversely, if $\Pi' : X \cap W \to \Pi''(X \cap W)$ is a finite morphism then $\Pi''$ is finite and unramified at a generic point $b \in X \cap W$ and its differential $(d\Pi'')(b) = \Pi'' : T_b(X, \mathbb{R}) \to T_{\Pi''(b)}(\Pi''(X), \mathbb{R})$ is injective. In the case of a constant field $F$ of prime characteristic $p = \text{char} F$, one has to assume that the degree of $X \subset \mathbb{F}_p^n$ is relatively prime to $p$, in order to assert that the finite morphism $\Pi' : X \cap W \to \Pi''(X \cap W)$ is unramified at a generic point $b \in X \cap W$.

In order to introduce the genericity index of an affine variety, let us recall that a morphism $f : X \to Y$ of affine varieties is finite if its generic fibres are finite. Equivalently, $f : X \to Y$ is finite if induces a finite extension $f^* : \mathbb{F}_q(f(X)) \hookrightarrow \mathbb{F}_q(X)$ of the corresponding absolute function fields. For an arbitrary irreducible $k$-dimensional affine variety $X \subset \mathbb{F}_q^n$ and any $d \in \mathbb{N}$ with $d - 1 \leq n - k$, we claim the existence of a finite puncturing $\Pi_i : X \to \Pi_i(X)$ at some $i = \{i_1, \ldots, i_{d-1}\}$. More precisely, if $x_{\tau_1} + I(X, \mathbb{F}_q) \ldots x_{\tau_k} + I(X, \mathbb{F}_q) \in \mathbb{F}_q(X)$ is a coordinate transcendence basis of $\mathbb{F}_q(X)$ over $\mathbb{F}_q$ and $\rho = \{\rho_1, \ldots, \rho_{n-k}\} = \{1, \ldots, n\} \setminus \{\tau_1, \ldots, \tau_k\}$, then the puncturing $\Pi_\rho : X \to \Pi_\rho(X)$ is a finite morphism. For any $\{i_1, \ldots, i_{d-1}\} \subseteq \{\rho_1, \ldots, \rho_{n-k}\}$ the puncturing $\Pi_\rho$ factors through the puncturing $\Pi_i : X \to \Pi_i(X)$ at $i = \{i_1, \ldots, i_{d-1}\}$ and the puncturing $\Pi_i^{\rho\setminus i} : \Pi_i(X) \to \Pi_\rho(X)$ at $\rho \setminus i = \{\rho_1, \ldots, \rho_{n-k}\} \setminus \{i_1, \ldots, i_{d-1}\}$.  

6
In other words, there is a commutative diagram

\[
\begin{array}{ccc}
X & \xrightarrow{\Pi_i} & \Pi_i(X) \\
\Pi_\rho \downarrow & \Downarrow & \Pi_\rho(X) \\
\Pi_\rho' & \xrightarrow{\Pi_\rho' \setminus i} & 0
\end{array}
\]

with finite morphism \(\Pi_\rho\). Therefore \(\Pi_i : X \to \Pi_i(X)\) is finite and \(X\) admits a finite puncturing \(\Pi_i : X \to \Pi_i(X)\) at \(d - 1\) coordinates.

**Definition 2.** An affine variety \(X \subset \mathbb{F}^m_q\) is \((d - 1)\)-generic if for any \((d - 1)\)-tuple of indices \(\{i_1, \ldots, i_d\} \subset \{1, \ldots, n\}\) the puncturing \(\Pi_i : X \to \Pi_i(X) \subseteq \mathbb{F}^n_q\) at \(i\) is a finite morphism and there exists a non-finite puncturing \(\Pi_j : X \to \Pi_j(X) \subseteq \mathbb{F}^n_q\) of \(X\) at \(d\) coordinates \(j = \{j_1, \ldots, j_d\}\).

The next lemma can be viewed as an analogue of the Implicit Function Theorem.

**Lemma 3.** Let \(X/\mathbb{F}_q \subset \mathbb{F}^m_q\) be an irreducible affine variety, defined over \(\mathbb{F}_q\) and \(a \in X(\mathbb{F}_q)\) be an \(\mathbb{F}_q\)-rational point of \(X\), at which the \(\mathbb{F}_q\)-Zariski tangent space \(T_a(X, \mathbb{F}_q)\) is of minimum distance \(d(T_a(X, \mathbb{F}_q)) \geq d\). Then the genericity index of \(X\) is \(\geq (d - 1)\).

**Proof.** We claim that \(Z := \text{X}^{\text{sing}} \cup (\cup_{i \mid i = (d - 1)} \Pi^{-1}_i(\Pi(X)^{\text{sing}}))\) is a proper Zariski closed subset of \(X\). First of all, the singular locus \(\text{X}^{\text{sing}}\) is a proper affine subvariety of \(X\). For any \((d - 1)\)-tuple of indices \(\{i_1, \ldots, i_d\}\), \(\Pi_i(\text{X}^{\text{sing}})\) is a proper closed subset of the quasi-affine variety \(\Pi_i(X) \subset \mathbb{F}^n_q\). The continuity of the puncturings \(\Pi_i : X \to \Pi_i(X)\) with respect to the Zariski topology implies that \(\Pi^{-1}_i(\Pi(X)^{\text{sing}})\) are closed subsets of \(X\). There are finitely many \((d - 1)\)-tuples of indices \(\{i_1, \ldots, i_d\}\), so that \(Z\) is a Zariski closed subset of \(X\). Towards \(Z \neq X\), it suffices to note that the assumption \(\Pi^{-1}_i(\Pi(X)^{\text{sing}}) = X\) implies \(\Pi_i(X) = \Pi_i(X)^{\text{sing}}\). As a result, the Zariski closure \(\Pi_i(X) = \Pi_i(X)^{\text{sing}} \subseteq \Pi_i(X)\), which is an absurd. Thus, \(Z \subseteq X\) is a proper Zariski closed subset of \(X\) and \(W_a := X \setminus Z\) is a non-empty Zariski open subset of \(X\).

According to Lemma 1, the assumption \(d(T_a(X, \mathbb{F}_q)) \geq d\) amounts to the injectiveness of the differentials \((d \Pi_i)_a : T_a(X, \mathbb{F}_q) \to T_{\Pi_i(a)}(\Pi_i(X), \mathbb{F}_q)\) for all \(i = \{i_1, \ldots, i_d\} \subset \{1, \ldots, n\}\). Let us fix some generators \(f_1, \ldots, f_m \in I(X, \mathbb{F}_q)\) of \(I(X, \mathbb{F}_q) = \langle f_1, \ldots, f_m \rangle_{\mathbb{F}_q} \subset \mathbb{F}[x_1, \ldots, x_n]\) and recall that \(T_a(X, \mathbb{F}_q)\) is the \(\mathbb{F}_q\)-linear code with parity check matrix \(\partial(f_1, \ldots, f_m)_{(x_1, \ldots, x_n)}(a)\). The \(\mathbb{F}_q\)-linear injectiveness of \((d \Pi_i)_a\) is equivalent to the linear independence of the columns \((\frac{\partial f_1}{\partial x_{i_s}}(a), \ldots, \frac{\partial f_m}{\partial x_{i_s}}(a))^t\), \(1 \leq s \leq d - 1\) of \((\frac{\partial f_1, \ldots, f_m}{\partial x_{i_1}, \ldots, x_{i_d}})(a)\), labeled by \(i\). This, in turn, amounts to the existence of \((d - 1)\)-tuples of indices \(r(i) = \{r(i)_1, \ldots, r(i)_{d-1}\} \subset \{1, \ldots, m\}\), such that the minor

\[
\Delta(r(i), i)_a := \det \left( \frac{\partial (f_{r(i)_1}, \ldots, f_{r(i)_{d-1}})}{\partial (x_{i_1}, \ldots, x_{i_{d-1}})} \right)(a) \neq 0
\]

is non-zero. Let \(W \subset X\) be the Zariski open neighborhood of \(a\), which consists of the points \(b \in X\) with \(\Delta(r(i), i)_b \neq 0\) for all \(i = \{i_1, \ldots, i_{d-1}\} \subset \{1, \ldots, n\}\) and their
associated \((d-1)\)-tuples of indices \(r(i) = \{r(i)_1, \ldots, r(i)_{d-1}\} \subseteq \{1, \ldots, m\}\). By the irreducibility of \(X\), the intersection \(W \cap W_0 \neq \emptyset\) is a non-empty, Zariski open, Zariski dense subset of \(X\). Let us choose some \(b \in W \cap W_0\) and denote by \(\mathbb{F}_{q^m}\) the definition field of \(b\), so that \(b \in (W \cap W_0)(\mathbb{F}_{q^m})\). Then the presence of \(\mathbb{F}_{q^m}\)-linear embeddings

\[
(d\Pi_i)_b : T_b(X, \mathbb{F}_{q^m}) \longrightarrow T_{\Pi_i(b)}(\Pi_i(X), \mathbb{F}_{q^m})
\]

for all \(i = \{i_1, \ldots, i_{d-1}\}\) implies the inequalities

\[
\dim X = \dim_{\mathbb{F}_{q^m}} T_b(X, \mathbb{F}_{q^m}) \leq \dim_{\mathbb{F}_{q^m}} T_{\Pi_i(b)}(\Pi_i(X), \mathbb{F}_{q^m}) = \dim \Pi_i(X) \leq \dim X.
\]

Therefore \(\dim X = \dim \Pi_i(X)\) and \(\Pi : X \to \Pi_i(X)\) are finite morphisms for all \(i = \{i_1, \ldots, i_{d-1}\}\). In other words, the genericity index of \(X\) is \(\geq d - 1\).

Here is an analogue of the reversed statement of the Implicit Function Theorem.

**Lemma 4.** Let \(X/\mathbb{F}_q \subset \mathbb{F}_q^n\) be an irreducible affine variety, defined over \(\mathbb{F}_q\), whose degree \(\deg X\) is not divisible by the characteristic \(p = \text{char} \mathbb{F}_q\) and whose genericity index is \(\geq d - 1\). Then there exist a polynomial \(\Delta \in \mathbb{F}_{q^{m_1}}[x_1, \ldots, x_n]\) and a natural number \(m_1 \in \mathbb{N}\), such that the minimum distance of \(T_n(X, \mathbb{F}_{q^m})\) at any point \(a \in (X \setminus V(\Delta))(\mathbb{F}_{q^m})\) with \(m \in m_1 \mathbb{N}\) is \(d(T_n(X, \mathbb{F}_{q^m})) \geq d\).

**Proof.** For an arbitrary \((d-1)\)-tuple of indices \(i = \{i_1, \ldots, i_{d-1}\}\), let

\[
j = \{j_1, \ldots, j_{n-d+1}\} := \{1, \ldots, n\} \setminus \{i_1, \ldots, i_{d-1}\}
\]

be the complement of \(i\) to \(\{1, \ldots, n\}\). The finite morphism \(\Pi_i : X \to \Pi_i(X)\) induces a finite extension \(\Pi_i^* : \mathbb{F}_{q^m}(\Pi_i(X)) \hookrightarrow \mathbb{F}_q(X)\) of the corresponding (absolute) function fields. For any \(1 \leq s \leq d - 1\) let \(g_{i_s,j}(t) \in \mathbb{F}_q(\Pi_i(X))[t]\) be the minimal polynomial of \(x_{i_s} + I(X, \mathbb{F}_q) \in \mathbb{F}_q(X) \over \mathbb{F}_q(\Pi_i(X))\). The multiplication of \(g_{i_s,j}(t)\) by the least common multiple of the denominators of its coefficients provides a polynomial \(\psi_{i_s,j} \in \mathbb{F}_q[x_{i_s}, x_j] \cap I(X, \mathbb{F}_q)\) of minimal positive degree with respect to \(x_{i_s}\). Let

\[
\Delta := \prod_{i,|i| = d-1} \prod_{s=1}^{d-1} \frac{\partial \psi_{i_s,j}}{\partial x_{i_s}} \in \mathbb{F}_q[x_1, \ldots, x_n].
\]

The polynomial \(\Delta\) has finitely many coefficients and belongs to \(\mathbb{F}_{q^{m_0}}[x_1, \ldots, x_n]\) for some \(m_0 \in \mathbb{N}\). We claim that \(\Delta \not\in I(X, \mathbb{F}_q)\), so that \(X \setminus V(\Delta) \neq \emptyset\) is a non-empty, Zariski open subset of \(X\). The assumption \(\Delta \in I(X, \mathbb{F}_q)\) implies \(\frac{\partial \psi_{i_s,j}}{\partial x_{i_s}} \in I(X, \mathbb{F}_q)\) for some \(i = \{i_1, \ldots, i_{d-1}\}\) and some \(1 \leq s \leq d - 1\), as far as the absolute ideal \(I(X, \mathbb{F}_q) \subseteq \mathbb{F}_{q^m}[x_1, \ldots, x_n]\) of the irreducible affine variety \(X \subset \mathbb{F}_{q^m}\) is prime. We have chosen the polynomial \(\psi_{i,s,j} \in \mathbb{F}_q[x_{i_s}, x_j] \cap I(X, \mathbb{F}_q)\) to be of minimal degree with respect to \(x_{i_s}\), so that its partial \(\frac{\partial \psi_{i,s,j}}{\partial x_{i_s}}\) belongs to \(I(X, \mathbb{F}_q)\) if and only if \(\frac{\partial \psi_{i,s,j}}{\partial x_{i_s}} \equiv 0\) vanishes identically. The last condition happens exactly when the exponents of \(x_{i_s}\) in all the monomials of \(\psi_{i,s,j}\) (with non-zero coefficients) are divisible by the characteristic \(p = \text{char} \mathbb{F}_q\). In particular, the degree \(\deg_{x_{i_s}} \psi_{i,s,j}\) of \(\psi_{i,s,j}\) with respect to \(x_{i_s}\) is to be
is divisible by $p$. By the very definition of $\psi_{i,j}$, the puncturing $\Pi_i : X \rightarrow \Pi_i(X)$ at $i = \{i_1, \ldots, i_{d-1}\}$ is of degree $\deg \Pi_i = \prod_{s=1}^{d-1} \deg_{x_s} \psi_{i,s,j}$, so that $\deg \Pi_i$ turns to be a multiple of $p$. By assumption, $\Pi_i : X \rightarrow \Pi_i(X)$ is a finite morphism, so that $\Pi_i(X)$ is of dimension $\dim \Pi_i(X) = \dim X = k$ and $j = \{j_1, \ldots, j_{n-d+1}\} = \{1, \ldots, n\} \setminus i$ contains a subset $\tau = \{\tau_1, \ldots, \tau_k\}$, labeling a coordinate transcendence basis $x_{\tau_1} + I(X, \mathbb{F}_q), \ldots, x_{\tau_k} + I(X, \mathbb{F}_q) \in \mathbb{F}_q[X]$ of $\mathbb{F}_q(X)$ over $\mathbb{F}_q$. Therefore the complement $\rho = \{\rho_1, \ldots, \rho_{n-k}\} = \{1, \ldots, n\} \setminus \{\tau_1, \ldots, \tau_k\}$ of $\tau$ contains $i$ and the finite dominant puncturing $\Pi_\rho : X \rightarrow \mathbb{F}_q^k$ factors through the puncturing $\Pi_i : X \rightarrow \Pi_i(X)$. In other words, there is a commutative diagram

$$
\begin{array}{ccc}
X & \xrightarrow{\Pi_i} & \Pi_i(X) \\
\Pi_\rho \downarrow & & \downarrow \Pi_\rho \setminus i \\
\Pi_\rho(X) & & \\
\end{array}
$$

of finite surjective morphisms, where $\Pi_\rho \setminus i : \Pi_i(X) \rightarrow \Pi_\rho(X)$ stands for the puncturing at the complement $\rho \setminus i$ of $i$ to $\rho$. Thus, the degree

$$
\deg X = \deg \Pi_\rho \mid X = \deg \Pi_\rho \setminus i \mid \Pi_i(X) \deg \Pi_i \mid X
$$

of $X$ is a multiple of the degree of $\Pi_i \mid X$ and, therefore, $p = \mathbb{F}_q$ divides $\deg X$. That contradicts the assumptions of the lemma and justifies that $X \setminus V(\Delta) \neq \emptyset$ is a non-empty Zariski open subset of the irreducible variety $X$. In particular, $(X \setminus V(\Delta))(\mathbb{F}_q^{m_1}) \neq \emptyset$ for a sufficiently large natural number $m_1$ and $(X \setminus V(\Delta))(\mathbb{F}_q^m) \neq \emptyset$ for all $m \in m_1 \mathbb{N}$.

For an arbitrary $i = \{i_1, \ldots, i_{d-1}\}$, let us note that the finite covering

$$
\Pi_i : X \setminus V(\Delta) \longrightarrow \Pi_i(X \setminus V(\Delta))
$$

is unramified, as far as the branch locus of $\Pi_i \mid X$ is $X \cap V\left(\prod_{s=1}^{d-1} \frac{\partial \psi_{i,s,j}}{\partial x_s}\right)$. Therefore $\Pi_i \mid X \setminus V(\Delta)$ is etale and its differential $(d\Pi_i)_a : T_a(X, \mathbb{F}_q^{m}) \rightarrow T_{\Pi_i(a)}(\Pi_i(X), \mathbb{F}_q^{m})$ is injective at any $a \in (X \setminus V(\Delta))(\mathbb{F}_q^{m})$. By Lemma 1, the minimum distance $d(T_a(X, \mathbb{F}_q^{m}) \geq d$.

Here is the main result of the present section

**Theorem 5.** Let $X/\mathbb{F}_q \subset \overline{\mathbb{F}_q}^n$ be an irreducible, $(d-1)$-generic affine variety, defined over $\mathbb{F}_q$ with GCD($\deg X, \text{char}\mathbb{F}_q$) = 1. Then there exist $\Delta \in \mathbb{F}_q^{m}[x_1, \ldots, x_n] \setminus \{0\}$ and $m_1 \in \mathbb{N}$, such that the Zariski tangent spaces $T_a(X, \mathbb{F}_q^{m})$ to $X$ at all the points $a \in (X \setminus V(\Delta))(\mathbb{F}_q^{m})$ with $m \in m_1 \mathbb{N}$ are of minimum distance $d(T_a(X, \mathbb{F}_q^{m}) = d$.

**Proof.** According to Lemma 4, for a $(d-1)$-generic irreducible variety $X/\mathbb{F}_q \subset \overline{\mathbb{F}_q}^n$ with GCD($\deg X, \text{char}\mathbb{F}_q$) = 1 there exist $\Delta \in \mathbb{F}_q^{m}[x_1, \ldots, x_n]$ and $m_1 \in \mathbb{N}$, such that $d(T_a(X, \mathbb{F}_q^{m}) \geq d$ for all $a \in (X \setminus V(\Delta))(\mathbb{F}_q^{m})$ and all $m \in m_1 \mathbb{N}$. The assumption
$d(T_a(X, \mathbb{F}_q^n)) \geq d + 1$ for some $a \in (X \setminus V(\Delta))(\mathbb{F}_q^n)$ requires $X$ to be of genericity index $\geq d$ by Lemma 3. The contradiction justifies $d(T_a(X, \mathbb{F}_q^n)) = d$ for $\forall a \in (X \setminus V(\Delta))(\mathbb{F}_q^n)$, $\forall m \in m_1 \mathbb{N}$.

2 Algorithm for obtaining the generic minimum distance of a tangent code and the points, at which it is attained

2.1 The decomposition into irreducible components, the degree and the dimension

The input of our algorithm consists of an irreducible $(d-1)$-generic affine variety $X/\mathbb{F}_q \subset \overline{\mathbb{F}}_q^n$ of $GCD(\deg X, \text{char} \mathbb{F}_q) = 1$, given by a generating set $f_1, \ldots, f_m \in \mathbb{F}_q[x_1, \ldots, x_n]$ of its absolute ideal $I(X, \mathbb{F}_q) = \langle f_1, \ldots, f_m \rangle_{\mathbb{F}_q} \triangleleft \mathbb{F}_q[x_1, \ldots, x_n]$. Such a description of an irreducible affine variety can be obtained by starting with arbitrary polynomials $g_1, \ldots, g_r \in \mathbb{F}_q[x_1, \ldots, x_n]$ and computing the primary decomposition of the ideal $\langle g_1, \ldots, g_r \rangle_{\mathbb{F}_q} \triangleleft \mathbb{F}_q[x_1, \ldots, x_n]$, generated by them. For an explanation and comparison of algorithms, executing primary decomposition of a polynomial ideal, one can confer the article [2] of Decker, Greuel and Pfister. Let $\langle g_1, \ldots, g_r \rangle_{\mathbb{F}_q} = Q_1 \cap \ldots \cap Q_t$ be the decomposition into primary ideals with different prime radicals $P_i = \sqrt{Q_i}$, which do not contain $P_j = \sqrt{Q_j}$ for some $j \neq i$ are called minimal. If $P_1, \ldots, P_t$ for some $s \leq t$ are the minimal radicals of the considered primary decomposition then the affine variety $Y = V(g_1, \ldots, g_r) = V(P_1) \cup \ldots \cup V(P_s) \subset \overline{\mathbb{F}}_q^n$ decomposes into irreducible components $V(P_i)$ with explicitly given generators $g_1, \ldots, g_r, g_{i,1}, \ldots, g_{i,s_i} \in \mathbb{F}_q[x_1, \ldots, x_n]$ of $P_i \triangleleft \overline{\mathbb{F}}_q[x_1, \ldots, x_n]$.

There exist effective algorithms for computing the dimension $k$ and the degree $D$ of an affine variety $X = V(f_1, \ldots, f_m)/\mathbb{F}_q \subset \overline{\mathbb{F}}_q^n$. More precisely, if $I = \langle f_1, \ldots, f_m \rangle_{\mathbb{F}_q}$ is the ideal, generated by the equations of $X$, then the Hilbert function

$$HF_X(s) = HF_I(s) := \dim_{\mathbb{F}_q} (\mathbb{F}_q[x_1, \ldots, x_n]/I)^{\leq s}/I^{\leq s}$$

of $X$ is defined as the Hilbert function of the ideal $I$, i.e., as the dimension of the quotient space of the polynomials of total degree $\leq s$ with respect to the subspace $I^{\leq s}$ of the polynomials from $I$ of degree $\leq s$. Hilbert has shown that for a sufficiently large $s \in \mathbb{N}$, the Hilbert function $HF_X(s)$ is a polynomial of $s$ with leading terms

$$\frac{D}{k!} s^k,$$

where $k = \dim X$ and $D = \deg X$. That is why, it suffices to compute the Hilbert polynomial $HF_I(s)$, in order to obtain $k = \dim X = \deg HF_I(s)$ and $D = \deg X = [\deg HF_X(s)])/\text{LC}(HF_X(s))$. In order to outline an algorithm for computing $HF_I(s)$, let us recall that a monomial order $\succ$ of $\mathbb{F}_q[x_1, \ldots, x_n]$ is graded if $x^a \succ x^\beta$ for all the monomials of total degree $|\alpha| > |\beta|$ and $\succ$ restricts to a lexicographic order on the monomials of equal total degree. The ideal $\langle LT(I) \rangle$ of the leading terms of $I$ is
generated by the leading terms $LT(f)$ of all the entries $f \in I$ with respect to the fixed monomial order. According to Proposition 4 from Chapter 9, §3 [1], the Hilbert polynomials $HF_I(s) = HF_{\{LT(I)\}}(s)$ coincide. If $G$ is a Groebner basis of $I$ with respect to the considered monomial order, then the finite set $LT(G)$ generates $\{LT(I)\}$. For an arbitrary monomial ideal $J = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle \triangleleft F[x_1, \ldots, x_n]$, let $MC(J)^{\leq s}$ be the set of the monomials of degree $\leq s$ from the complement of $J$. Then the Hilbert polynomial $HF_J(s) = |MC(J)^{\leq s}|$. By Theorem 3 from Chapter 9, §2 [1], the monomial complement $MC(J) = \bigcup_{i=1}^{t} M(x_{A_i}^{\alpha(i)} F[x_{B_i}])$ consists of the monomials $M(x_{A_i}^{\alpha(i)} F[x_{B_i}])$ from $x_{A_i}^{\alpha(i)} F[x_{B_i}]$ for some decompositions $\{1, \ldots, n\} = A_i \cup B_i$ with $A_i \cap B_i = \emptyset$ and some $\alpha(i) \in (\mathbb{Z}_{\geq 0})^{\lvert A_i \rvert}$. Bearing in mind that the intersections $x_{A_i}^{\alpha(i)} F[x_{B_i}] \cap x_{A_j}^{\alpha(j)} F[x_{B_j}] = x_{A_i}^{\alpha(i)} F[x_{B_i}]$ are of the same form for $B := B_i \cap B_j$, $A := \{1, \ldots, n\} \setminus B$ and an appropriate $\alpha \in (\mathbb{Z}_{\geq 0})^{A_i}$, one computes explicitly $|MC(\{LT(I)\})^{\leq s}| = HF(\{LT(I)\})(s) = HF_I(s) = HF_{X}(s)$ and obtains $k = \dim X$, $D = \deg X$.

### 2.2 The coordinate transcendence bases and the genericity index

Let $X/F_q \subset \overline{F_q}$ be an irreducible $k$-dimensional affine variety, defined over $F_q$ and $F_q \subset F \subset \overline{F_q}$ be a finite extension of $F_q$. For an arbitrary polynomial $g \in \overline{F_q}[x_1, \ldots, x_n]$ there is a finite extension $F_1 \supseteq F$, containing all the coefficients of $g(x_1, \ldots, x_n)$. The finite product

$$g_0(x_1, \ldots, x_n) := \prod_{\sigma \in \text{Gal}(F_1/F)} \sigma g(x_1, \ldots, x_n)$$

is from $F[x_1, \ldots, x_n]$, as far as the action of the absolute Galois group $Gal(\overline{F} = \overline{F_q}/F)$, on $\sigma g(x_1, \ldots, x_n) \in F_1[x_1, \ldots, x_n]$ reduces to the action of $Gal(F_1/F)$ and stabilizes $g_0(x_1, \ldots, x_n)$. That is why, $x_{\tau_1} + I(X, F_q), \ldots, x_{\tau_k} + I(X, F_q) \in F_q[X] = F_q[x_1, \ldots, x_n]/I(X, F_q)$ is a coordinate transcendence basis of $F_q(X)$ over $F_q$ exactly when $x_{\tau_1} + I(X, F), \ldots, x_{\tau_k} + I(X, F) \in F[X]$ constitute a coordinate transcendence basis of $F(X)$ over $F$. A monomial $x^\tau := x_{\tau_1} \ldots x_{\tau_k}$ of degree $\deg x^\tau = k = \dim X$ is said to be associated with a coordinate transcendence basis of $X$ if for any constant field $F$, containing the definition field $F_q$ of $X$, the elements $x_{\tau_1} + I(X, F), \ldots, x_{\tau_k} + I(X, F) \in F[X] \subset F(X)$ form a transcendence basis of $F(X)$ over $F$.

The next lemma provides a combinatorial algorithm for computing the genericity index of an affine variety.

**Lemma 6.** Let $X/F_q \subset \overline{F_q}$ be an irreducible affine variety, whose degree $\deg X$ is not divisible by $p = \text{char} F_q$ and $x^{\tau(1)}, \ldots, x^{\tau(s)}$ be the monomials, associated with all the coordinate transcendence bases of $X$. If

$$\mathcal{M} := \{J \subseteq \{1, \ldots, n\} \mid J \cap \{\tau(i)_1, \ldots, \tau(i)_k\} \neq \emptyset \text{ for } \forall 1 \leq i \leq s\}$$

and $d := \min_{J \in \mathcal{M}} |J|$ then $\dim V(x^{\tau(1)}, \ldots, x^{\tau(s)}) = n - d$ and $X$ is $(d-1)$-generic.

**Proof.** The equality

$$\dim V(x^{\tau(1)}, \ldots, x^{\tau(s)}) = n - \min_{J \in \mathcal{M}} |J|$$

11
is a well known property of the common zero sets of monomials (e.g., cf. Proposition 3 from Chapter 9, §1 of Cox, Little and O’Shea’s [1]). In order to check that $X$ is $(d-1)$-generic for $d := \min_{j \in M} |J|$, let us note that for any subset $i = \{i_1, \ldots, i_{d-1}\} \subset \{1, \ldots, n\}$ of cardinality $|i| = d - 1$ there exists an index $1 \leq j \leq s$ with

$$I \cap \{\tau(j)_1, \ldots, \tau(j)_k\} = \emptyset.$$ 

The coordinate transcendence basis $x_{\tau(j)_1}, \ldots, x_{\tau(j)_k}$ of $X$ is associated with the finite puncturing $\Pi_\rho : X \to \Pi_\rho(X)$ at $\rho = \{1, \ldots, n\} \setminus \{\tau(j)_1, \ldots, \tau(j)_k\}$. The inclusion $i \subseteq \{1, \ldots, n\} \setminus \{\tau(j)_1, \ldots, \tau(j)_k\} = \{\rho_1, \ldots, \rho_{n-k}\}$ implies that the finite puncturing $\Pi_\rho : X \to \Pi_\rho(X)$ factors through the puncturing $\Pi_i : X \to \Pi_i(X)$ at $i = \{i_1, \ldots, i_{d-1}\}$. Thus, $\Pi_i : X \to \Pi_i(X)$ is a finite morphism for any subset $i \subset \{1, \ldots, n\}$ of cardinality $|i| = d - 1$ and the genericity index of $X$ is $\geq d - 1$.

Let us assume that all the puncturings of $X$ at $d = \min_{j \in M} |J|$ coordinates are finite morphisms of $X$ and choose $J_\alpha \in M$ with $|J_\alpha| = d$. Since $\Pi_{J_\alpha} : X \to \Pi_{J_\alpha}(X)$ is a finite morphism, the complement $\alpha := \{1, \ldots, n\} \setminus J_\alpha$ contains the label set $\tau(i) = \{\tau(i)_1, \ldots, \tau(i)_k\}$ of a coordinate transcendence basis $x_{\tau(i)_1}, \ldots, x_{\tau(i)_k}$ of $X$. As a result, $J_\alpha \subseteq \{1, \ldots, n\} \setminus \{\tau(i)_1, \ldots, \tau(i)_k\}$ contradicts $J_\alpha \cap \{\tau(i)_1, \ldots, \tau(i)_k\} \neq \emptyset$ and justifies that $X$ is $(d-1)$-generic. 

\[\square\]

2.3 The discriminant locus of the $(d-1)$-puncturings

Here is an effective procedure for obtaining the polynomials

$$\psi_{i_s,j} \in \overline{F}_q[x_{i_s}, x_j] \setminus \overline{F}_q[x_j]$$

and, therefore, the polynomial

$$\Delta := \prod_{i, |i| = d - 1} \prod_{s=1}^{d-1} \frac{\partial \psi_{i_s,j}}{\partial x_{i_s}}$$

from Theorem 5. For any $i = \{i_1, \ldots, i_{d-1}\}$ with complement $j = \{j_1, \ldots, j_{n-d+1}\} = \{1, \ldots, n\} \setminus \{i_1, \ldots, i_{d-1}\}$ and any $1 \leq s \leq d - 1$, let us consider the lexicographic order of the monomials of $x_1, \ldots, x_n$ with $x_{i_s} > x_{i_s} > x_j$. Suppose that

$$I(X, \overline{F}_q) = (f_1, \ldots, f_m)_{\overline{F}_q} \cap \overline{F}_q[x_1, \ldots, x_n]$$

is generated by $f_1, \ldots, f_m \in \overline{F}_q[x_1, \ldots, x_n]$ and compute a Groebner basis $G_{i_s,j} = \{g_1, \ldots, g_l\}$ of $I := (f_1, \ldots, f_m)_{\overline{F}_q} \cap \overline{F}_q[x_1, \ldots, x_n]$ with respect to this lexicographic order. We claim that the intersection

$$G_{i_s,j}'' := G_{i_s,j} \cap \overline{F}_q[x_{i_s}, x_j] \setminus \overline{F}_q[x_j]$$

consists of a unique polynomial $\psi_{i_s,j} \in I(X, \overline{F}_q) \cap (\overline{F}_q[x_{i_s}, x_j] \setminus \overline{F}_q[x_j])$, which is of minimal degree with respect to $x_{i_s}$ and works for the purpose. Indeed, by the Elimination Theorem 2 from Chapter 3, § 1 of Cox, Little and O’Shea’s [1],

$$G_{i_s,j}' := G_{i_s,j} \cap \overline{F}_q[x_{i_s}, x_{j_1}, \ldots, x_{j_{n-d+1}}]$$

12
is a Groebner basis of the ideal $I(i_{s,j}) := I \cap \mathbb{F}_q[x_{i_{s}}, x_{j}] \subset \mathbb{F}_q[x_{i_{s}}, x_{j}]$ with respect to the lexicographic order with $x_{i_{s}} > x_{j}$. Applying Lemma 4 from [2], one concludes that $G'_{i_{s,j}} := G'_{i_{s}} \setminus \mathbb{F}_q[x_{j}]$ is a Groebner basis of the extension 

$$I(i_{s,j})' := I(i_{s}, j) \mathbb{F}_q(x_{j})[x_{i_{s}}]$$

of $I(i_{s,j})$ to the polynomial ring $\mathbb{F}_q(x_{j})[x_{i_{s}}]$ of one variable $x_{i_{s}}$ with coefficients from the field $\mathbb{F}_q(x_{j})$ of the rational functions of $x_{j} = \{x_{j_{1}}, \ldots, x_{j_{d+1}}\}$ with $\mathbb{F}_q$-coefficients. The monomial order of $\mathbb{F}_q(x_{j})[x_{i_{s}}]$ is the usual one with $x_{i_{s}}^{\alpha} > x_{j}^{\beta}$ for $\alpha > \beta$, $\alpha, \beta \in \mathbb{Z}_{\geq 0}$. Any ideal of $\mathbb{F}_q(x_{j})[x_{i_{s}}]$ is principal, so that $I'(i_{s}, j)$ has a unique generator $\psi_{i_{s},j} \in \mathbb{F}_q[x_{i_{s}}, x_{j}] \cap \mathbb{F}_q(x_{j})[x_{i_{s}}]$ and $\langle G'\rangle = \langle \psi_{i_{s},j} \rangle$. In order to justify that $\psi_{i_{s},j} \in I(X, \mathbb{F}_q) \cap (\mathbb{F}_q[x_{i_{s}}, x_{j}] \setminus \mathbb{F}_q[x_{j}])$ is of minimal degree $a_{o} \in \mathbb{N}$ with respect to $x_{i_{s}}$, let us assume that $\varphi_{i_{s},j} \in I(X, \mathbb{F}_q) \cap (\mathbb{F}_q[x_{i_{s}}, x_{j}] \setminus \mathbb{F}_q[x_{j}])$ is of minimal degree $b_{o} \in \mathbb{N}$ with respect to $x_{i_{s}}$. Then $b_{o} \leq a_{o}$. On the other hand, $\varphi_{i_{s},j} \in I(i_{s}, j) := I(X, \mathbb{F}_q) \cap \mathbb{F}_q[x_{i_{s}}, x_{j}]$, whereas $\varphi_{i_{s},j} \in I'(i_{s}, j) := I(i_{s}, j) \mathbb{F}_q(x_{j})[x_{i_{s}}]$.

Therefore the leading term $LT(\varphi_{i_{s},j}) = x_{i_{s}}^{a_{o}}x_{j}^{b_{o}}$, $b \in (\mathbb{Z}_{\geq 0})^{n-d+1}$ of $\varphi_{i_{s},j} \in \mathbb{F}_q[x_{i_{s}}, x_{j}]$ with respect to the lexicographic order with $x_{i_{s}} > x_{j}$ is divisible by the leading term $LT(\psi_{i_{s},j}) = x_{i_{s}}^{a}x_{j}^{b}$, $a \in (\mathbb{Z}_{\geq 0})^{n-d+1}$ of $\psi_{i_{s},j}$, since $G'_{i_{s},j} = \{\psi_{i_{s},j}\}$ is a Groebner basis of $I'(i_{s}, j)$. That implies $a_{o} \leq b_{o}$, whereas $a_{o} = b_{o}$ and the polynomial $\psi_{i_{s},j} \in I(X, \mathbb{F}_q) \cap (\mathbb{F}_q[x_{i_{s}}, x_{j}] \setminus \mathbb{F}_q[x_{j}])$ is of minimal degree with respect to $x_{i_{s}}$.

One way for obtaining $m \in \mathbb{N}$ with $(X \setminus V(\Delta))(\mathbb{F}_{q^{m}}) \neq \emptyset$ for all $m \in m_{1}\mathbb{N}$ is by using Fried, Haran and Jarden’s article [3]. They show that if $k := \dim X$, $D := \deg X$, $\delta := \deg \Delta$, then the number $N_{m} := |(X \setminus V(\Delta))(\mathbb{F}_{q^{m}})|$ of the $\mathbb{F}_{q^{m}}$-rational points of $X \setminus V(\Delta)$ satisfies

$$|N_{m} - q^{mk}| \leq (D - 1)(D - 2)q^{m(k - \frac{1}{2})} + C(n, k, D, \delta)q^{m(k - 1)}$$

(1)

for an appropriate constant $C(n, k, D, \delta)$, depending on $n, k, D, \delta$. More precisely, let

$$C_{o}(n, k, D) := 2^{k-1}[D(D - 1)^{2} + 1] + k \left[ 1 + (D - 1)(D - 2) + 2^{m+k-3}2^{m}m^{2}\delta^{2} \right]$$

with $m := \left(\frac{n+D}{n}\right)^{k}$ be Litz’s constant from [5], which works out for the Lang-Weil’s bound

$$|N'_{m} - q^{mk}| \leq (D - 1)(D - 2)q^{m(k - \frac{1}{2})} + C_{o}(n, k, D)q^{m(k - 1)}$$

on the number $N'_{m} := |Y(\mathbb{F}_{q^{m}})|$ of the $\mathbb{F}_{q^{m}}$-rational points of a smooth irreducible projective variety $Y/\mathbb{F}_{q} \subset \mathbb{P}^{n}(\mathbb{F}_{q})$ of dim $Y = k$ and deg $Y = D$ (cf. [4] of Lang and Weil). Then Fried-Haran-Jarden’s constant equals

$$C(n, k, D, \delta) := C_{o}(n, k, D) + 2^{k-1}D(\delta + 1).$$

Note that (1) implies the inequality

$$N_{m} \geq q^{mk} - (D - 1)(D - 2)q^{m(k - \frac{1}{2})} - C(n, k, D, \delta)q^{m(k - 1)} =

q^{m(k - 1)} \left[ q^{m} - (D - 1)(D - 2)q^{\frac{m}{2}} - C(n, k, D, \delta) \right].$$

13
In order to obtain $m_1 \in \mathbb{N}$ with $N_m \geq 1$ for $\forall m = m_1 n \in m_1 \mathbb{N}$, it suffices to have
\[
q^{m_1 n} - (D - 1)(D - 2)q^{m_1 n - 1} - C(n, k, D, \delta) > 0
\]
for all $n \in \mathbb{N}$. The roots of the quadratic equation $t^2 - (D - 1)(D - 2)t - C = 0$ with $C := C(n, k, D, \delta)$ are
\[
\frac{(D - 1)(D - 2) \pm \sqrt{(D - 1)^2(D - 2)^2 + 4C}}{2} < C + \sqrt{C^2 + 4C},
\]
due to $C > (D - 1)(D - 2)$. That is why, one can take
\[
q^{m_1 n} \geq C + 1 = \frac{C + \sqrt{C^2 + 4C} + 4}{2} > C + \sqrt{C^2 + 4C}.
\]
Thus, $m_1 \geq 2 \log_q (C + 1)$ provides $N_m = N_{m_1 n} \geq 1$ for all $n \in \mathbb{N}$.

We propose an algorithm for obtaining points $a \in X \setminus V(\Delta)$ by consecutive puncturings of the coordinates. Let $f_1, \ldots, f_m, h_1, \ldots, h_l \in \mathbb{F}_q[x_1, \ldots, x_n]$ be such polynomials that $X = V(f_1, \ldots, f_m) \subseteq \mathbb{F}_q[x_1, \ldots, x_n]$ is an irreducible affine variety with absolute ideal $I(X, \mathbb{F}_q) = (f_1, \ldots, f_m)_{\mathbb{F}_q}$ and $W_n := V(f_1, \ldots, f_m) \setminus V(h_1, \ldots, h_l) \neq \emptyset$ is a non-empty Zariski open subset of $X$. In the case of $n = 1$, such $X$ is a point. In general, there exists $1 \leq i \leq n$, such that the puncturing $\Pi_i : X \to \Pi_i(X)$ at $x_i$ is a finite morphism. Denote $x' := \{x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n\}$ and fix a lexicographic order with $x_i > x'$. Obtain a Groebner basis $G' = \{g_1, \ldots, g_s\}$ of $I = (f_1, \ldots, f_m)_{\mathbb{F}_q} = I(X, \mathbb{F}_q)$ and extend to a Groebner basis $G''$ of $J = (f_1, \ldots, f_m, h_1, \ldots, h_l)_{\mathbb{F}_q}$. Let $LC_x(G') = \{LC_x(g_1), \ldots, LC_x(g_s)\} \subseteq \mathbb{F}_q[x']$ be the set of the leading coefficients of the entries of $G'$, viewed as polynomials of $x_i$ with coefficients from $\mathbb{F}_q[x']$. The Extension Theorem 3 from Chapter 3, §1 [1] asserts that for an arbitrary point
\[
a' \in V_{n-1}(G' \cap \mathbb{F}_q[x']) \setminus V_{n-1}(LC_x(G')) \subseteq \mathbb{F}_q^{n-1}
\]
the polynomial system of equations $g(x_i, a') = 0, \forall g \in G' \setminus \mathbb{F}_q[x']$ has a solution $a_i \in \mathbb{F}_q$ and for any solution $a_i$ of this system the point $a = (a_i, a')$ belongs to $X$.

We claim that
\[
W_{n-1} := V_{n-1}(G' \cap \mathbb{F}_q[x']) \setminus \{V_{n-1}(G'' \cap \mathbb{F}_q[x']) \cup V_{n-1}(LC_x(G'))\} \subseteq \mathbb{F}_q^{n-1}
\]
is a non-empty quasi-affine subvariety of $\mathbb{F}_q^{n-1}$, and for any point $a' \in W_{n-1}$ the solution $a_i \in \mathbb{F}_q$ of $g(a_i, a') = 0, \forall g \in G' \setminus \mathbb{F}_q[x']$ provides a point $a = (a_i, a') \in W_n := X \setminus V(J)$. Indeed, since $G'$ generates $I$, the point $a \in X = V(I)$. The assumption $a \in V(J)$ implies that $a' = \Pi_i(a) \in \Pi_i V(J)$. By the Closure Theorem 3 from Chapter 3, §2 [1], the Zariski closure of $\Pi_i V(J)$ in $\Pi_i V(J) = V_{n-1}(G'' \cap \mathbb{F}_q[x'])$, so that $a' \in V_{n-1}(G'' \cap \mathbb{F}_q[x'])$, contrary to its choice. That justifies $a \in V(I) \setminus V(J)$. Note that $X = V(I) \subseteq \mathbb{F}_q$ is an irreducible affine variety. Therefore, its image $\Pi_i(X) \subseteq \mathbb{F}_q^{n-1}$ under the puncturing $\Pi_i$ is irreducible, as well as the closure
\[
\Pi_i(X) = V_{n-1}(G' \cap \mathbb{F}_q[x']) = \overline{W_{n-1}}.
\]
That justifies the irreducibility of $W_{n-1}$. As a result, if
\[ W'_{n-1} := V_{n-1}(G' \cap \mathbb{F}_q[x']) \setminus V_{n-1}(G'' \cap \mathbb{F}_q[x']) , \]
\[ W''_{n-1} := V_{n-1}(G' \cap \mathbb{F}_q[x']) \setminus V_{n-1}(LC_{x_i}(G')) , \]
then it suffices to check that $W'_{n-1} \neq \emptyset$ and $W''_{n-1} \neq \emptyset$, in order to assert that $W_{n-1} = W'_{n-1} \cap W''_{n-1} \neq \emptyset$. The assumption $W_{n-1} = \emptyset$ implies the inclusion $V_{n-1}(G' \cap \mathbb{F}_q[x']) \subseteq V_{n-1}(G'' \cap \mathbb{F}_q[x'])$. Making use of $G' \subseteq G''$, one concludes that $G' \cap \mathbb{F}_q[x'] \subseteq G'' \cap \mathbb{F}_q[x']$, whereas $V_{n-1}(G'' \cap \mathbb{F}_q[x']) \subseteq V_{n-1}(G' \cap \mathbb{F}_q[x'])$. Thus,
\[ \Pi_i(X) = V_{n-1}(G' \cap \mathbb{F}_q[x']) = V_{n-1}(G'' \cap \mathbb{F}_q[x']) = \Pi_i(V(J)) . \]
As far as $\Pi_i : W_n \rightarrow \Pi_i(W_n)$ is a finite morphism and the Zariski closure $\overline{W_n} = X$, one has $\dim X = \dim V(I) = \dim \Pi_i(V(I)) = \Pi_i(V(J)) \leq \dim V(J)$. On the other hand, $W_n := X \setminus V(J) \neq \emptyset$ implies that $\dim V(J) < \dim V(I) = \dim X$, which is absurd, justifying $W'_{n-1} \neq \emptyset$. In a similar vein, note that the assumption $W''_{n-1} = \emptyset$ requires
\[ \Pi_i(X) = V_{n-1}(G' \cap \mathbb{F}_q[x']) \subset V_{n-1}(LC_{x_i}(G')) , \]
whereas $LC_{x_i}(G') \subseteq I(\Pi_i(X), \mathbb{F}_q) = I(\Pi_i(X), \mathbb{F}_q)$. The choice of a finite morphism $\Pi_i : X \rightarrow \Pi_i(X)$ forces $G' \setminus \mathbb{F}_q[x'] \neq \emptyset$. By Lemma 4 from [2], $G' \setminus \mathbb{F}_q[x']$ is a Groebner basis of the extension $I^\sigma := \mathbb{F}_q(x')[x_i] \triangleleft \mathbb{F}_q(x')[x_i]$ with respect to the induced lexicographic order of $x'$. Note that $\mathbb{F}_q(x')[x_i]$ is a principal ideal domain and choose a generator $g$ of $I^\sigma = (G' \setminus \mathbb{F}_q[x']) \triangleleft (\mathbb{F}_q(x')[x_i])$. The polynomial $g$ is a multiple of the minimal polynomial $p_i(t) \in \mathbb{F}_q(\Pi_i(X))$ of $x_i + I(X, \mathbb{F}_q) \in \mathbb{F}_q(X)$ over $\mathbb{F}_q(\Pi_i(X))$. Therefore, its leading coefficient $LC_{x_i}(g) \in \mathbb{F}_q[\Pi_i(X)] \setminus \{0\}$ does not belong to the ideal $I(\Pi_i(X), \mathbb{F}_q)$ of $\Pi_i(X)$. The contradiction justifies $W''_{n-1} \neq \emptyset$ and $W_{n-1} \neq \emptyset$. Finally, let
\[ \mathcal{P} := (G'' \cap \mathbb{F}_q[x']) . LC_{x_i}(G') := \{ gh \mid g \in G'' \cap \mathbb{F}_q[x'], \ h \in LC_{x_i}(G') \} \]
be the set of the products of the elements of $G'' \cap \mathbb{F}_q[x']$ with the entries of $LC_{x_i}(G')$. Then $V_{n-1}(G'' \cap \mathbb{F}_q[x']) \cup V_{n-1}(LC_{x_i}(G')) = V_{n-1}(\mathcal{P})$ and
\[ W_{n-1} = V_{n-1}(G' \cap \mathbb{F}_q[x']) \setminus V_{n-1}(\mathcal{P}) . \]

### 2.4 A pseudo-code for obtaining tangent codes of generic minimum distance

The aforementioned algorithms are synthesized by the following pseudo-code.

**Algorithm for obtaining the generic minimum distance $d$ of a tangent code and points $a \in X(\mathbb{F}_q^m)$ with $d(T_a(X, \mathbb{F}_q^m)) = d$**

**Input:** Irreducible $X/\mathbb{F}_q$ of dim $X = k$, $\deg X = D$, $GCD(D, \text{char}\mathbb{F}_q) = 1$ and $f_1, \ldots, f_m \in \mathbb{F}_q[x_1, \ldots, x_n]$ with $I(X, \mathbb{F}_q) = (f_1, \ldots, f_m)_{\mathbb{F}_q}$

**Output:** $d \in \mathbb{N}$, $\Delta \in \mathbb{F}_q^m[x_1, \ldots, x_n]$, $a \in X \setminus V(\Delta)(\mathbb{F}_q^m)$ with $d(T_a(X, \mathbb{F}_q^m)) = d$

**Step 1 - obtaining all the coordinate transcendence bases $\overline{\tau}$ of $X$**

\[ B := \emptyset \]
$S := \{x_\tau \subset x \mid |x_\tau| = k\}$

FOR EACH $x'' \in S$ DO

$x' := x \setminus x''$

$G := \text{Groebner Basis of } I = \langle f_1, \ldots, f_m \rangle_{\mathbb{F}_q} / x' >_{\text{lex}} x''$

IF $G \cap \mathbb{F}_q[x''] = \emptyset$ THEN $B := B \cup \{x''\}$
ELSE DO NOTHING

$S := S \setminus \{x''\}$

Step 2 - obtaining $d \in \mathbb{N}$, such that $X$ is $(d - 1)$-generic

$M := \{J \subset \{1, \ldots, n\} \mid J \cap x_\tau \neq \emptyset \text{ for } \forall x_\tau \in B\}$

d := \min\{|J| \mid J \in M\}$

Step 3 - obtaining $\Delta := \prod_{i,|i|=d-1} \prod_{s=1}^{d-1} \frac{\partial \psi_{is,i}}{\partial x_{is}}$

$R := \{i \subset \{1, \ldots, n\} \mid |i| = d - 1\}$

FOR EACH $i \in R$ DO $j := \{1, \ldots, n\} \setminus i$

FOR EACH $1 \leq s \leq d - 1$ DO

$G_{i,s,j} := \text{Groebner Basis } I / x_i_{\setminus i_s} >_{\text{lex}} x_{i_s} >_{\text{lex}} x_j$

$\psi_{i,s,j} := G_{i,s,j} \cap (\mathbb{F}_q[x_{i_s}, x_j] \setminus \mathbb{F}_q[x_j])$

Step 4 - obtaining $a \in W_n := X \setminus V(\Delta)$

$S_n := \{x_1, \ldots, x_n\}$

$I_n := I(x, \mathbb{F}_q) = \langle f_1, \ldots, f_m \rangle$

$J_n := \langle f_1, \ldots, f_m, \Delta \rangle$

$Q_n := f_1, \ldots, f_m$

$P_n := f_1, \ldots, f_m, \Delta$

$W_n := V(Q_n) \setminus V(P_n)$

$N := n$

$M := \max(\dim X, 1)$

WHILE $N > M$ DO

CHOOSE $x_\tau \in B \cap S_N$

CHOOSE $i_\tau \in \{1, \ldots, n\} \setminus \{\tau_1, \ldots, \tau_k\}$

$T_N := S_N \setminus \{x_{i_\tau}\}$

$G'_{n} := \text{Groebner Basis of } I_n / x_{i_\tau} >_{\text{lex}} T_N$

$G''_{n} := \text{Groebner Basis of } J_n / x_{i_\tau} >_{\text{lex}} T_N, G'_{n} \subset G''_{n}$

$I_{N-1} := \langle G'_{n} \cap \mathbb{F}_q[T_N] \rangle$

$J_{N-1} := \langle G''_{n} \cap \mathbb{F}_q[T_N] \rangle$

$Q_{N-1} := G''_{n} \cap \mathbb{F}_q[T_N]$

$P_{N-1} := \langle G''_{n} \cap \mathbb{F}_q[T_N] \rangle \cdot LC_{x_{i_\tau}}(G'_{n})$

$W_{N-1} := V(Q_{N-1}) \setminus V(P_{N-1})$

$N := N - 1$

CHOOSE $a_M \in W_M \subset \mathbb{F}_q^M$

$L := M$

WHILE $L \leq n$ DO

$L := L + 1$

$a_{i_L} := \text{SOLUTION OF } g(x_{i_L}, T_L) = 0 \text{ FOR ALL } g \in I_L \setminus \mathbb{F}_q[T_L]$
3 Stabilization and destabilization of the minimum distance within a tangent bundle

The present section provides a series of $k$-dimensional irreducible affine varieties $X/F_q \subset F_q^n$ with $\text{GCD}(\text{deg} X, \text{char} F_q) = 1$, which have an a priori given $F_q$-linear $[n, k, d]$-code $C \subset F_q^n$ as its Zariski tangent space $T_{0^n}(X, F_q) = C$ at the origin $0^n \in X$ and reproduce the length $n$, the dimension $k$ and the minimum distance $d$ of $C$ by the Zariski tangent spaces $T_a(X, F_q^m)$ at its generic points $a \in X(F_q^m)$, $m \in \mathbb{N}$. On the other hand, for any family $\mathcal{C}$ of $F_q$-linear codes of fixed length $n$, fixed dimension $k$ and arbitrary minimum distance, it constructs a $k$-dimensional affine variety $X/F_q \subset F_q^n$, whose degree $\text{deg} X$ is divisible by the characteristic $\text{char} F_q$ and whose $F_q$-Zariski tangent bundle contains $\mathcal{C}$. These statements illustrate the stabilization (respectively, the destabilization) of the minimum distance within a Zariski tangent bundle to an affine variety $X$, whose degree $\text{deg} X$ is not divisible (respectively, is divisible) by the characteristic $\text{char} F_q$.

3.1 Reproducing the minimum distance of a linear code by a Zariski tangent bundle

**Proposition 7.** Let $C \subset F_q^n$ be an $F_q$-linear code of length $n$, dimension $k$ and minimum distance $d$ over a field $F_q$ of characteristic $p = \text{char} F_q$. Then there exist a $k$-dimensional affine variety $X/F_q \subset F_q^n$ with $\text{GCD}(\text{deg} X, p) = 1$ and a non-empty Zariski open subset $W \subseteq X^\text{smooth}$, such that $0^n \in W$, $T_{0^n}(X, F_q) = C$ and $T_a(X, F_q^m) \subset F_q^n$ are $F_q^m$-linear codes of length $n$, dimension $k$ and minimum distance $d$ for all $m \in \mathbb{N}$ and all the $F_q^m$-rational points $a \in W(F_q^m)$ of $W$.

**Proof.** Let $H \in \text{Mat}_{(n-k) \times n}(F_q)$ be a parity check matrix of the $k$-dimensional linear code $C \subset F_q^n$. Then $H$ is of rank $\text{rk}(H) = n - k$ and there exist linearly independent columns $H_{i_1}, \ldots, H_{i_{n-k}} \in \text{Mat}_{(n-k) \times 1}(F_q)$ of $H$. Choose a permutation $\sigma \in \text{Sym}(n)$ with $\sigma(i_s) = s$ for all $1 \leq s \leq n - k$ and apply it to the coordinate functions $x_1, \ldots, x_n$ on $F_q^n$. That transforms the parity check matrix of $C$ in the form $H = (I_{n-k} H')$, where $I_{n-k}$ stands for the identity matrix of size $n - k$ and $H' \in \text{Mat}_{(n-k) \times k}(F_q)$. Denote by $H_1, \ldots, H_n \in \text{Mat}_{(n-k) \times 1}(F_q)$ the columns of $H$. The code $C$ of minimum distance $d$ contains a word $c \in C$ of weight $d$. If $\text{Supp}(c) = \{j_1, \ldots, j_d\}$ for some $1 \leq j_1 < \ldots < j_d \leq n$ then $\sum_{s=1}^{d} c_{j_s} H_{j_s} = 0_{(n-k) \times 1}$ with $c_{j_s} \in F_q^*$ and

$$H_{j_d} = - \sum_{s=1}^{d-1} c_{j_s} c_{j_d}^{-1} H_{j_s}.$$  

Note that $j_d > n - k$, as far as the first $n - k$ columns of $H$ are $F_q$-linearly independent. For any $1 \leq i \leq n - k$ and $i \leq j \leq n$, $j \neq j_d$, let us denote by $H_{ij}$ the entry of $H$ from the $i$-th row and $j$-th column. Then choose a polynomial

$$f_{i,j}(x_j) := H_{ij} x_j + \sum_{r \geq 2, r \not\equiv 0 \text{ (mod $p$)}} a_{i,j,r} x_j^r \in F_q[x_j]$$
and note that $\frac{\partial f_{ij}}{\partial x_j} |_{x_j=0} = H_{ij}$. Put

$$f_{i,j,a}(x_{ja}) := -\sum_{s=1}^{d-1} c_{js} c_{ja}^{-1} f_{i,j,s}(x_{ja}) \in \mathbb{F}_q[x_{ja}] \quad \text{for } \forall 1 \leq i \leq n - k$$

and observe that

$$\frac{\partial f_{i,j,a}}{\partial x_{ja}} \bigg|_{x_{ja}=0} = -\sum_{s=1}^{d-1} c_{js} c_{ja}^{-1} \frac{\partial f_{i,j,s}}{\partial x_{ja}} \bigg|_{x_{ja}=0} = -\sum_{s=1}^{d-1} c_{js} c_{ja}^{-1} H_{ij,s} = H_{ij,a}.$$ 

The polynomials

$$f_i(x_i, \ldots, x_n) := \sum_{j=i}^{n} f_{i,j}(x_j) \in \mathbb{F}_q[x_i, \ldots, x_n] \quad \text{for } 1 \leq i \leq n - k$$

are claimed to cut a $k$-dimensional affine variety

$$X := V(f_1(x_1, \ldots, x_n), f_2(x_2, \ldots, x_n), \ldots, f_{n-k}(x_{n-k}, \ldots, x_n) \subset \mathbb{F}_q^n,$$

defined over $\mathbb{F}_q$, whose degree is not divisible by $p = \text{char} \mathbb{F}_q$. To this end, by an induction on $0 \leq t \leq n - k - 1$, one observes that

$$X_t := V(f_{n-k-t}(x_{n-k-t}, \ldots, x_n), \ldots, f_{n-k}(x_{n-k}, \ldots, x_n)) \subset \mathbb{F}_q^{k+t+1}$$

is a finite covering of the affine space $\mathbb{F}_q^n$ with coordinate functions $x_{n-k+1}, \ldots, x_n$. For $t = 0$ the hypersurface $X_0 := V(f_{n-k}(x_{n-k}, \ldots, x_n)) \subset \mathbb{F}_q^{k+1}$ with coordinate functions $x_{n-k}, \ldots, x_n$ is $k$-dimensional, as far as the polynomial

$$f_{n-k}(x_{n-k}, \ldots, x_n) = \left[ x_{n-k} + \sum_{r \geq 2, r \not\equiv 0(\text{mod } p)} a_{n-k,n-k,r} x_{n-k}^r \right] + \sum_{j=n-k+1}^{n} f_{n-k,j}(x_j)$$

depends on $x_{n-k}$ and the puncturing $\Pi_{n-k} : X_0 \to \Pi_{n-k}(X_0) \subset \mathbb{F}_q^n$ at $x_{n-k}$ is a finite morphism. If the puncturing $\Pi_{(n-k-t, \ldots, n-k)} : X_t \to \mathbb{F}_q^{k}$ is a finite covering for some $0 \leq t \leq n - k - 2$, then the puncturing $\Pi_{(n-k-t-1)} : X_{t+1} \to X_t$ is a finite covering, as far as the polynomial

$$f_{n-k-t-1}(x_{n-k-t-1}, x_{n-k-t}, \ldots, x_{n-k}) = \left[ x_{n-k-t-1} + \sum_{r \geq 2, r \not\equiv 0(\text{mod } p)} a_{n-k-t-1,n-k-t-1,r} x_{n-k-t-1}^r \right] + \sum_{j=n-k-t}^{n} f_{n-k-t-1,j}(x_j) \in \mathbb{F}_q[x_{n-k-t-1}, \ldots, x_n]$$
depends on $x_{n-k-t-1}$ and the polynomials $f_{n-k-t}(x_{n-k-t}, x_n), \ldots, f_{n-k}(x_{n-k}, x_n)$ do not depend on $x_{n-k-t-1}$. Thus, $X_{n-k-1} := X$ is a finite covering of $\overline{F}_q$ and $X/\overline{F}_q \subset \overline{F}_q^n$ is a $k$-dimensional affine variety, defined over $\mathbb{F}_q$. All monomials of $f_i(x_1, \ldots, x_n)$, $1 \leq i \leq n - k$ (with non-zero coefficients) are of degree, relatively prime to the characteristic $p = \text{char} \overline{F}_q$, so that $p$ does not divide $\deg X$.

We claim that the absolute ideal $I(X, \overline{F}_q)$ of $X = V(f_1, \ldots, f_{n-k})$ is generated by the defining equations $f_1, \ldots, f_{n-k} \in \mathbb{F}_q[x_1, \ldots, x_n]$ of $X$. To this end, note that $f_1(x_1, \ldots, x_n), \ldots, f_{n-k}(x_{n-k}, \ldots, x_n)$ is a Groebner basis of $I := (f_1, \ldots, f_{n-k}) \overline{F}_q \subset \overline{F}_q[x_1, \ldots, x_n]$ with respect to the lexicographic order with $x_1 > x_2 > \ldots > x_n$. According to Theorem 3 and Proposition 4 from Chapter 2, § 9 [1], it suffices to observe that the leading monomials $LM(f_i) \in \mathbb{F}_q[x_i]$ of $f_i(x_i, \ldots, x_n)$ with $1 \leq i \leq n$ are pairwise relatively prime. Due to $\{f_1, \ldots, f_{n-k}\} \cap \mathbb{F}_q[x_{n-k+1}, \ldots, x_n] = \emptyset$, the extension

$$I^e := I\overline{F}_q(x_{n-k+1}, \ldots, x_n)[x_1, \ldots, x_{n-k}] \subset \overline{F}_q(x_{n-k+1}, \ldots, x_n)[x_1, \ldots, x_{n-k}]$$

is a proper ideal of $\overline{F}_q(x_{n-k+1}, \ldots, x_n)[x_1, \ldots, x_{n-k}]$. Lemma 4 from [2] implies that $f_1(x_1, \ldots, x_n), \ldots, f_{n-k}(x_{n-k}, \ldots, x_n)$ is a Groebner basis of $I^e$ with respect to the lexicographic order with $x_1 > \ldots > x_{n-k}$. By the very definition of the polynomials $f_i(x, \ldots, x_n) = \sum_{j=1}^n f_{ij}(x_j)$ with $f_{ii}(x_i) \in \overline{F}_q[x_i] \setminus \{0\}$, the leading coefficients $LC(f_i) \in \overline{F}_q(x_{n-k+1}, \ldots, x_n)[x_1, \ldots, x_{n-k}]$ of $f_i$, viewed as polynomials of $x_1, \ldots, x_{n-k}$ belong to $\overline{F}_q$. The Noether quotient

$$(I : 1^\infty) := \{g \in \overline{F}_q[x_1, \ldots, x_n] \mid g^m \in I \text{ for some } m \in \mathbb{N}\} = I.$$ 

Therefore, the radical $\sqrt{I}$ of $I$ is

$$I(X, \overline{F}_q) = \sqrt{I} = (I : 1^\infty) \cap \sqrt{(I, 1)} = I \cap \overline{F}_q[x_1, \ldots, x_n] = I$$

and the polynomials $f_1, \ldots, f_{n-k} \in \mathbb{F}_q[x_1, \ldots, x_n]$ generate $I(X, \overline{F}_q)$.

Now, we are ready to define the non-empty Zariski open subset $W \subset X$ from the statement of the proposition. By the very definition of $f_i(x_1, \ldots, x_n)$, $1 \leq i \leq n - k$, the Jacobian matrix

$$\begin{pmatrix}
\frac{\partial f_1(x_1)}{\partial x_1} & \frac{\partial f_1(x_2)}{\partial x_2} & \cdots & \frac{\partial f_1(x_{n-k})}{\partial x_{n-k}} & \cdots & \frac{\partial f_1(x_n)}{\partial x_n} \\
0 & \frac{\partial f_2(x_1)}{\partial x_1} & \cdots & \frac{\partial f_2(x_{n-k})}{\partial x_{n-k}} & \cdots & \frac{\partial f_2(x_n)}{\partial x_n} \\
\vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & \frac{\partial f_{n-k}(x_1)}{\partial x_1} & \cdots & \frac{\partial f_{n-k}(x_n)}{\partial x_n}
\end{pmatrix}.$$

Due to $I(X, \overline{F}_q) = I = (f_1, \ldots, f_{n-k}) \overline{F}_q[x_1, \ldots, x_n]$, for any $m \in \mathbb{N}$ and $a \in X(\overline{F}_q^m)$ the Zariski tangent space $T_a(X, \mathbb{F}_q^m) \subset \mathbb{F}_q^m$ has a parity check matrix $\frac{\partial (f_1, \ldots, f_{n-k})}{\partial (x_1, \ldots, x_n)}(a)$. According to $f_i(0^n) = 0$ for $1 \leq i \leq n$, the origin $0^n \in X = V(f_1, \ldots, f_{n-k})$ belongs to $X$. Moreover,

$$\frac{\partial (f_1, \ldots, f_{n-k})}{\partial (x_1, \ldots, x_n)}(0^n) = H = (I_{n-k}|H'),$$
so that the Zariski tangent space $T_{0^n}(X, \mathbb{F}_q) = C$. A sufficient condition for $T_a(X, \mathbb{F}_q^m)$ to be of dimension $k$ over $\mathbb{F}_q^m$ is

$$\det \frac{\partial (f_1, \ldots, f_{n-k})}{\partial (x_1, \ldots, x_n)} (a) \neq 0.$$ 

Since $C$ is of minimum distance $d$, for any $i = \{i_1, \ldots, i_{d-1}\} \subset \{1, \ldots, n\}$ the columns $H_{i_1}, \ldots, H_{i_{d-1}} \in \text{Mat}_{(n-k) \times 1}(\mathbb{F}_q)$ of $H$ are $\mathbb{F}_q$-linearly independent. Then there exists a subset $r(i) = \{r(i)_1, \ldots, r(i)_{d-1}\} \subseteq \{1, \ldots, n-k\}$, such that the matrix $H(r(i), i) \in \text{Mat}_{(d-1) \times (d-1)}(\mathbb{F}_q)$, cut by the rows of $H$, labeled by $r(i)$ and the columns of $H$, labeled by $i$ has det $H(r(i), i) \neq 0$. We define $W$ to be the subset of $X$, which consists of the points $a \in X$ with det $\left( \frac{\partial (f_1, \ldots, f_{n-k})}{\partial (x_1, \ldots, x_n)} (a) \right) \neq 0$ and

$$\text{Jac}(r(i), i)(a) := \det \left( \frac{\partial (f_1, \ldots, f_{n-k})}{\partial (x_1, \ldots, x_n)} (r(i)), i(a) = \det \frac{\partial (f_{r(i)}, \ldots, f_{r(i)_{d-1}})}{\partial (x_{r(i)}, \ldots, x_{i_{d-1}})} (a) \neq 0.$$ 

According to $0^n \in W$, the Zariski open subset $W \subseteq X$ is non-empty. Further, $\dim_{\mathbb{F}_q} T_a(X, \mathbb{F}_q^m) = k$ for all $a \in W$ by det $\left( \frac{\partial (f_1, \ldots, f_{n-k})}{\partial (x_1, \ldots, x_n)} (a) \right) \neq 0$. We claim that the minimum distance $d(T_a(X, \mathbb{F}_q^m)) = d$ for all $a \in W$. To this end, note that at any point $b \in \overline{W}$, the $j_{d-i}$th column of $\frac{\partial (f_1, \ldots, f_{n-k})}{\partial (x_1, \ldots, x_n)} (b)$ is the same $\mathbb{F}_q$-linear combination of the columns, labeled by $j_1, \ldots, j_{d-1}$ as the $j_{d-i}$th column of $H$. Thus, the word $c = (0, \ldots, 0, c_{j_1}, 0, \ldots, 0, c_{j_{d-1}}, 0) \in C$ of weight $d$ belongs to all the $\mathbb{F}_q^m$-linear codes with parity check matrix $\frac{\partial (f_1, \ldots, f_{n-k})}{\partial (x_1, \ldots, x_n)} (b)$ for some $b \in \mathbb{F}_q^n$ and, in particular, $c \in T_a(X, \mathbb{F}_q^m)$ for all $a \in X(\mathbb{F}_q^m)$. That justifies the upper bound $d(T_a(X, \mathbb{F}_q^m)) \leq d$ on the minimum distance of a tangent code at $a \in X(\mathbb{F}_q)$. For any $a \in W$ and any $i = \{i_1, \ldots, i_{d-1}\}$ one has $\text{Jac}(r(i), i)(a) \neq 0$, so that each column of $\frac{\partial (f_1, \ldots, f_{n-k})}{\partial (x_1, \ldots, x_{i_{d-1}})}(a) = d - 1$ and the puncturing $\Pi : T_a(X, \mathbb{F}_q^m) \rightarrow \mathbb{F}_q^m$ is injective. As a result, the minimum distance $d(T_a(X, \mathbb{F}_q^m)) > d - 1$, whereas $d(T_a(X, \mathbb{F}_q^m)) = d$ for $\forall a \in W(\mathbb{F}_q^m)$. 

**Remark:** In order to have an irreducible affine variety $X/\mathbb{F}_q \subset \overline{W}$, subject to the properties, stated in Proposition 7, it suffices to choose

$$f_{i,i}(x_i) := H_{ii}x_i = 1 \quad \text{for} \quad \forall 1 \leq i \leq n - k.$$ 

Then for any $1 \leq i \leq n - k$ there exist polynomials $g_i(x_{i+1}, \ldots, x_n)$, such that $f_i(x_i, \ldots, x_n) = x_i - g_i(x_{i+1}, \ldots, x_n)$. As a result, the puncturing $\Pi = \Pi_{(1, \ldots, n-k)} : X \rightarrow \mathbb{F}_q^k$ is invertible by a morphism $\Pi^{-1}$.

### 3.2 Tangent bundle interpolation of a deformation of the minimum distance with fixed length and dimension

The next proposition illustrates the possibility for incorporating codes with various minimal distances within a single Zariski tangent bundle.
Proposition 8. Let $C \rightarrow S$ be a family of $\mathbb{F}_q$-linear codes $C(a) \subset \mathbb{F}_q^n$ of length $n$, dimension $k = \dim_{\mathbb{F}_q} C(a)$ and arbitrary minimum distance, parameterized by a subset $S \subset \mathbb{F}_q^n$. Then there is a $k$-dimensional affine variety $X/\mathbb{F}_q \subset \mathbb{F}_q^n$, whose degree $\deg X$ is divisible by the characteristic $p = \text{char} \mathbb{F}_q$, such that $\mathbb{F}_q^n \subset X \subset X^{\text{smooth}}(\mathbb{F}_q)$ and the Zariski tangent spaces $T_a(X, \mathbb{F}_q) = C(a)$ to $X$ at $a \in S$ over $\mathbb{F}_q$ coincide with the members of the family.

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

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

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

$$L_{\mathbb{F}_q}^0(t) := \prod_{\alpha \in \mathbb{F}_q^n} (t - \alpha) \left\{ \prod_{\alpha \in \mathbb{F}_q^n} (t - \alpha) \right\}^{-1} = (t^q - 1)(-1)^{-1} = -(t^q - 1).$$

Towards an explicit calculation of $L_{\mathbb{F}_q}^\beta(t)$ for $\beta \in \mathbb{F}_q^n$, let us denote by $\sigma_1, \ldots, \sigma_{q-1}$ the elementary symmetric polynomials of the roots of $f(t) := \prod_{\alpha \in \mathbb{F}_q^n} (t - \alpha) = t^q - 1$. Put $\tau_1, \ldots, \tau_{q-2}$ for the elementary symmetric polynomials of the roots of the monic polynomial

$$f_\beta(t) := \prod_{\alpha \in \mathbb{F}_q^n \setminus \{\beta\}} (t - \alpha) = \frac{f(t)}{t - \beta} = \frac{t^q - 1}{t - \beta} = t^q - 2 + \sum_{s=0}^{q-3} (-1)^{q-2-s} \tau_{q-2-s} t^s.$$

Then the relations

$$\tau_1 + \beta = \sigma_1 = 0,$$

$$\tau_s + \beta \tau_{s-1} = \sigma_s = 0 \quad \text{for} \quad 2 \leq s \leq q - 2 \quad \text{and} \quad \beta \tau_{q-2} = \sigma_{q-1} = (-1)^q,$$

reveal that $\tau_s = (-\beta) \tau_{s-1}$ for $1 \leq s \leq q - 2$, $\tau_0 := 1$ form a geometric progression $\{\tau_s\}_{s=1}^{q-2}$ with quotient $(-\beta)$. As a result,

$$\tau_s = (-\beta)^s \quad \text{for} \quad 1 \leq s \leq q - 2$$

and

$$f_\beta(t) = t^q - 2 + \sum_{s=0}^{q-3} \beta^{q-2-s} t^s = t^q - 2 + \sum_{s=0}^{q-3} \beta^{q-2-s} t^s,$$

21
according to $\beta^{q-2} = \beta^{-1}$ for $\forall \beta \in \mathbb{F}_q^*$. Now,

$$L_{\beta q}(t) := \frac{tf_\beta(t)}{\beta f_\beta(\beta)} = \frac{t^{q-1} + \sum_{s=1}^{q-2} \beta^{-s} t^s}{t^{q-1} + \sum_{s=1}^{q-2} 1}\beta^{q-1}$$

$$(q - 1)^{-1} \left[ t^{q-1} + \sum_{s=1}^{q-2} \beta^{-s} t^s \right] = \left[ t^{q-1} + \sum_{s=1}^{q-2} \beta^{-s} t^s \right]$$

for arbitrary $\beta \in \mathbb{F}_q^*$. Let us denote by

$$\Phi_p : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n,$$

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

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

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

for $1 \leq i \leq n - k$. We claim that the affine variety $X := V(f_1, \ldots, f_{n-k}) \subset \mathbb{F}_q^n$ satisfies the required conditions. First of all, $\mathbb{F}_q^n \subset X$, as far as an arbitrary point $a = (a_1, \ldots, a_n) \in \mathbb{F}_q^n$ has components $a_j = a_j^q$ and $f_i(a_1, \ldots, a_n) = 0$ for $\forall 1 \leq i \leq n - k$. By the very definition, $f_i(x_1, \ldots, x_n)$ are of degree $\text{deg} f_i = pn(q - 1) + q$, divisible by the characteristic $p = \text{char} \mathbb{F}_q$, so that the degree $\text{deg} X$ of $X$ is a multiple of $p$. Straightforwardly, the partial derivatives

$$\frac{\partial f_i}{\partial x_j} = \sum_{b \in \Phi_p(S)} \mathcal{H}(\Phi_p^{-1}(b))_{ij} L_{F_q}^{b_1} (x_1^p) \ldots L_{F_q}^{b_n} (x_n^p)$$

and their values at $a \in S$ equal

$$\frac{\partial f_i}{\partial x_j}(a) = \mathcal{H}(\Phi_p^{-1}(b))_{ij} = \mathcal{H}(a)_{ij}.$$

Note that the composition of Lagrange interpolation polynomials with the Frobenius automorphism $\Phi_p$ is designed in such a way that to adjust $\frac{\partial (f_1, \ldots, f_{n-k})}{\partial (x_1, \ldots, x_n)}(a) = \mathcal{H}(a)$ at all the points $a \in S$. At an arbitrary point $a \in S \subset X(\mathbb{F}_q) := X \cap \mathbb{F}_q^n$, the Zariski tangent space $T_a(X, \mathbb{F}_q)$ is contained in the right null-space of the Jacobian matrix $\frac{\partial (f_1, \ldots, f_{n-k})}{\partial (x_1, \ldots, x_n)}(a) = \mathcal{H}(a)$, so that $T_a(X, \mathbb{F}_q) \subseteq \mathcal{C}(a)$. Now

$$k \leq \dim X \leq \dim \mathbb{F}_q T_a(X, \mathbb{F}_q) \leq \dim \mathbb{F}_q \mathcal{C}(a) = k$$

implies that $\mathcal{C}(a) = T_a(X, \mathbb{F}_q)$, $\dim X = k$ and any $a \in S$ is a smooth point of $X$. \hfill \blacksquare
4 Families of Hamming isometries

A map $I : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$ is called a Hamming isometry if it preserves the Hamming distance, i.e., $d(Ix, Iy) = d(x, y)$ for all $x, y \in \mathbb{F}_q^n$, where

$$d(x, y) := |\{1 \leq i \leq n \mid x_i \neq y_i\}|$$

stands for the number of the different components of $x$ and $y$. All Hamming isometries are bijective maps. More precisely, if we assume the existence of differentials of $\psi$, then $0 = d(Ix, Iy) = d(x, y)$ contradicts $x \neq y$.

The present section provides a pattern for a construction of a global morphism $\psi : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$, depending explicitly on $\psi$, such that the differentials of $\psi$ restrict to linear Hamming isometries

$$(d\psi)_a : T_a(X, \mathbb{F}_q^n) \rightarrow T_{\psi(a)}(\psi(X), \mathbb{F}_q^n)$$

on the tangent codes to the affine varieties $X \subseteq \mathbb{F}_q^n$ at generic points $a \in X \setminus V(\psi)$. Further, an arbitrary family $I \rightarrow S$ of $\mathbb{F}_q$-linear Hamming isometries $I(a) : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$, parameterized by a subset $S \subseteq \mathbb{F}_q^n$, is realized by the differentials $(d\varphi)_a = I(a)$ of an appropriate $\mathbb{F}_q$-morphism $\varphi : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$ at $a \in S$.

4.1 Finite morphisms with isometric differentials

**Proposition 9.** For arbitrary polynomials $\psi_1, \ldots, \psi_n \in \mathbb{F}_q[x_1, \ldots, x_n]$ and an arbitrary permutation $\sigma \in \text{Sym}(n)$, let us consider the morphism

$$\psi := (x_{\sigma(1)}\psi_{\sigma(1)}(x_1^p, \ldots, x_n^p), \ldots, x_{\sigma(n)}\psi_{\sigma(n)}(x_1^p, \ldots, x_n^p)) : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$$

and the hypersurface $V(\psi) \subset \mathbb{F}_q^n$ with equation

$$\psi_0(x_1, \ldots, x_n) := \psi_1(x_1^p, \ldots, x_n^p) \cdots \psi_n(x_1^p, \ldots, x_n^p),$$

where $p = \text{char}(\mathbb{F}_q)$ stands for the characteristic of the basic field $\mathbb{F}_q$. Then any irreducible affine variety $X \subset \mathbb{F}_q^n$, which is not entirely contained in the hypersurface $V(\psi)$, has a non-empty Zariski open, Zariski dense subset

$$W := X^\text{smooth} \cap \psi^{-1}(\psi(X)^\text{smooth}) \setminus V(\psi),$$

such that the differentials of $\psi$ restrict to $\mathbb{F}_q^n$-linear Hamming isometries

$$(d\psi)_a : T_a(X, \mathbb{F}_q^n) \rightarrow T_{\psi(a)}(\psi(X), \mathbb{F}_q^n)$$

at all the points $a \in W(\mathbb{F}_q^n)$ of $W$.

**Proof.** It suffices to prove the proposition for the $\mathbb{F}_q$-morphism

$$\varphi := \sigma^{-1}\psi = (\varphi_1 = x_1\psi_1(x_1^p, \ldots, x_n^p), \ldots, \varphi_n = x_n\psi_n(x_1^p, \ldots, x_n^p)) : X \rightarrow \psi(X),$$

where $\varphi$ restricts to an isometry on each component of $X$. Then any finite map $\varphi : X \rightarrow \psi(X)$ is realized by a finite isometry $\varphi : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$. Hence the proposition follows from the construction of the global morphism $\psi$. 

23
as far as the permutation $\sigma^{-1} \in \text{Sym}(n)$ coincides with its differentials at any point $a \in \mathbb{F}_q^n$ and is a linear Hamming isometry. If

$$\Phi_p : \mathbb{F}_q[x_1, \ldots, x_n] \rightarrow \mathbb{F}_q[x_1, \ldots, x_n],$$

$$\Phi_p(f(x_1, \ldots, x_n)) := f(x_1^p, \ldots, x_n^p)$$

then the matrix of

$$(d\varphi)_a : T_a(\mathbb{F}_q^n, \mathbb{F}_q^n) \rightarrow T_{\varphi(a)}(\mathbb{F}_q^n, \mathbb{F}_q^n)$$

with respect to the basis $\left( \frac{\partial}{\partial x_j} \right)_a, 1 \leq i \leq n$ of $T_a(\mathbb{F}_q^n, \mathbb{F}_q^n)$ and the basis $\left( \frac{\partial}{\partial y_j} \right)_{\varphi(a)}, 1 \leq j \leq n$ of $T_{\varphi(a)}(\mathbb{F}_q^n, \mathbb{F}_q^n)$ is the Jacobian matrix

$$\frac{\partial(\varphi_1, \ldots, \varphi_n)}{\partial(x_1, \ldots, x_n)}(a) = \begin{pmatrix}
\Phi_p(\psi_1)(a) & 0 & \ldots & 0 \\
0 & \Phi_p(\psi_2)(a) & \ldots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \ldots & \Phi_p(\psi_n)(a)
\end{pmatrix}$$

of the components of $\varphi$ at $a$. Note that at any point $a \in (X \setminus V(\psi_\alpha))(\mathbb{F}_q^n)$ the differential $(d\varphi)_a : T_a(\mathbb{F}_q^n, \mathbb{F}_q^n) \rightarrow T_{\varphi(a)}(\mathbb{F}_q^n, \mathbb{F}_q^n)$ is an $\mathbb{F}_q^n$-linear Hamming isometry and restricts to an $\mathbb{F}_q^n$-linear Hamming isometry

$$(d\varphi)_a : T_a(X, \mathbb{F}_q^n) \rightarrow (d\varphi)_a T_a(X, \mathbb{F}_q^n) \subseteq T_{\varphi(a)}(\varphi(X), \mathbb{F}_q^n)$$

onto its image. We claim that $W \neq \emptyset$ is a non-empty Zariski open subset. Due to the irreducibility of $X$ it suffices to note that $X^{\text{smooth}} \neq \emptyset$, $X \setminus V(\psi_\alpha) \neq \emptyset$ and to justify that $X \cap \varphi^{-1}(\varphi(X)^{\text{smooth}}) \neq \emptyset$. Indeed, the assumption $X \cap \varphi^{-1}(\varphi(X)^{\text{smooth}}) = \emptyset$ implies that $\varphi(X) = \varphi(X)^{\text{sing}}$, whereas $\varphi(X)^{\text{smooth}} = \emptyset$, which is an absurd.

\[\square\]

### 4.2 Interpolation of linear Hamming isometries by differentials of a morphism

**Proposition 10.** Let $\mathcal{I} \rightarrow S$ be a family of $\mathbb{F}_q$-linear Hamming isometries $\mathcal{I}(a) \in \text{GL}(\mathbb{F}_q, \mathbb{F}_q)$, $\mathcal{I}(a) : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$, parameterized by a subset $S \subseteq \mathbb{F}_q^n$. Then there exists an $\mathbb{F}_q$-morphism $\varphi = (\varphi_1, \ldots, \varphi_n) : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$, whose differentials $(d\varphi)_a = \mathcal{I}(a)$ at $\forall a \in S$ coincide with the given isometries.

**Proof.** Let us consider the polynomials

$$\varphi_i(x_1, \ldots, x_n) := \sum_{b \in \Phi_p(S)} \sum_{j=1}^n \mathcal{I}(\Phi_p^{-1}(b))_{ij} (x_j - x_j^q) L_{\mathbb{F}_q}(x_1^p) \ldots L_{\mathbb{F}_q}(x_n^p)$$

for $1 \leq i \leq n$, where

$$\Phi_p : \mathbb{F}_q \rightarrow \mathbb{F}_q^m,$$

$$\Phi_p(a_1, \ldots, a_n) = (a_1^p, \ldots, a_n^p) \quad \text{for} \quad \forall a = (a_1, \ldots, a_n) \in \mathbb{F}_q$$

24
stands for the Frobenius automorphism of degree \( p = \text{char} \mathbb{F}_q \). Straightforwardly,

\[
\frac{\partial \phi_i}{\partial x_j} = \sum_{b \in \Phi_p(S)} \mathcal{I}(\Phi_p^{-1}(b))_{ij} L_{\mathbb{F}_q}(x^p_1) \ldots L_{\mathbb{F}_q}(x^p_n)
\]

for \( \forall 1 \leq i, j \leq n \), whereas

\[
\frac{\partial \phi_i}{\partial x_j}(a) = \mathcal{I}(a)_{ij} \quad \forall a \in S \subseteq \mathbb{F}_q^n.
\]

Therefore \( \mathcal{I}(a) \in \text{GL}(n, \mathbb{F}_q) \) is the matrix of the differential

\[
(d\phi)_a : T_a(\mathbb{F}_q^n, \mathbb{F}_q) \rightarrow T_{\phi(a)}(\mathbb{F}_q^n, \mathbb{F}_q)
\]

with respect to the basis \( \left( \frac{\partial}{\partial x_j} \right)_a, 1 \leq j \leq n \) of \( T_a(\mathbb{F}_q^n, \mathbb{F}_q) \) and the basis \( \left( \frac{\partial}{\partial y_i} \right)_{\phi(a)}, 1 \leq i \leq n \) of \( T_{\phi(a)}(\mathbb{F}_q^n, \mathbb{F}_q) \).

Finally, note that an arbitrary affine variety \( X/\mathbb{F}_q \subset \mathbb{F}_q^n \) admits a bijective morphism \( \Phi_q : X \rightarrow X \), which is not birational (or an isomorphism), as far as its inverse map \( \Phi_q^{-1} : X \rightarrow X \) is not a morphism. The Frobenius automorphism \( \Phi_q \) restricts to bijective maps \( \Phi_q : X(\mathbb{F}_q^m) \rightarrow X(\mathbb{F}_q^m) \) of the finite sets \( X(\mathbb{F}_q^m) \) of the \( \mathbb{F}_q^m \)-rational points of \( X \) and, in particular, to the identity \( \Phi_q = \text{Id} : X(\mathbb{F}_q) \rightarrow X(\mathbb{F}_q) \) of the \( \mathbb{F}_q \)-rational points. One can view

\[
\Phi_q : T(X, \mathbb{F}_q^m) \rightarrow T(X, \mathbb{F}_q^m)
\]

as a non-linear Hamming isometry of the Zariski tangent bundles \( T(X, \mathbb{F}_q^m) \) for all \( m \in \mathbb{N} \). Note that \( \Phi_q : T_a(X, \mathbb{F}_q^m) \rightarrow T_{\Phi_q(a)}(X, \mathbb{F}_q^m) \) interchanges the fibres over \( a \in X(\mathbb{F}_q^m) \setminus X(\mathbb{F}_q) \) and acts on the fibres \( \Phi_q : T_a(X, \mathbb{F}_q^m) \rightarrow T_a(X, \mathbb{F}_q^m) \) over \( a \in X(\mathbb{F}_q) \).

References

[1] 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.

[2] W. Decker, G.-M. Greuel, G. Pfister, Primary decomposition : algorithms and comparisons, in Algorithmic Algebra an Number Theory (eds. G.-M. Greuel, B.H. Matzat and G. Hiss ), Springer, (1998), 187–220.

[3] M.D. Fried, D. Haran and M. Jarden Effective counting of the points of definable sets over finite fields Israel Journal of Mathematics , 85 (1994), 103–133.

[4] S. Lang and A. Weil Number of points of varieties in finite fields, American Journal of Mathematics, 76 (1954), 819–827.

[5] W. List, Die Anzahl der rationalen Punkte von Varietäten über einem endlichen Körper., Diplomarbeit, Heidelberg, 1975.